



Cambium Networks™









User Guide

PTP 850C/PTP 850E

System Release 13.1



Accuracy

While reasonable efforts have been made to assure the accuracy of this document, Cambium Networks assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. Cambium reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Cambium does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others. It is possible that this publication may contain references to, or information about Cambium products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Cambium intends to announce such Cambium products, programming, or services in your country.

Copyrights

This document, Cambium products, and 3rd Party software products described in this document may include or describe copyrighted Cambium and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Cambium, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Cambium, its licensors, or the 3rd Party software supplied material contained in the Cambium products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Cambium. Furthermore, the purchase of Cambium products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Cambium or other 3rd Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Cambium.

License Agreements

The software described in this document is the property of Cambium and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

High Risk Materials

Cambium and its supplier(s) specifically disclaim any express or implied warranty of fitness for any high risk activities or uses of its products including, but not limited to, the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, life support, or weapons systems (“High Risk Use”). Any High Risk is unauthorized, is made at your own risk and you shall be responsible for any and all losses, damage or claims arising out of any High Risk Use.

© 2025 Cambium Networks Limited. All Rights Reserved.

Contents

About This User Guide 43
1.1.1 What You Should Know 43
1.1.2 Target Audience 43
1.1.3 Related Documents 43
1.1.4 Contacting Cambium Networks 44
1.1.5 Purpose 46
1.1.6 Cross references 46
1.1.7 Feedback 46
1.2 Problems and warranty 47
1.2.1 Reporting problems 47
1.2.2 Repair and service 47
1.2.3 Hardware warranty 47
1.3 Security advice 48
1.4 Warnings, cautions, and notes 48
1.4.1 Warnings 48
1.4.2 Cautions 48
1.4.3 Notes 48
1.5 Caring for the environment 49
1.5.1 In EU countries 49
1.5.2 In non-EU countries 49
2. Introduction 50
2.1.1 PTP 850C Overview 50
2.1.2 PTP 850S Overview 51
2.1.3 PTP 850E Overview 51
2.2 System Overview 52
2.2.1 Configuration Tips 52
2.2.2 PTP 850E Overview 53
2.2.3 PoE Injector Overview 53
2.2.4 The Web-Based Element Management System 54
2.3 Reference Guide to Web EMS Menu Structure 76
3. Getting Started 86
3.1 Antenna Alignment Mode (PTP 850E) 86
Antenna Alignment Mode Overview 86
Antenna Alignment Mode Operation 88
3.2 Assigning IP Addresses in the Network 89
3.3 Establishing a Connection 89
3.4 PC Setup 89
3.5 Logging on 90
Logging in Without Knowing the IP Address 91
3.6 Changing Your Password 92

3.7 Applying a Pre-Defined Configuration File 93
3.8 Performing Quick Platform Setup 96
3.9 Enabling Dynamic IPv6 Addresses Via DHCPv6 98
3.10 Configuring In-Band Management 102
3.11 Changing the Management IP Address 103
3.12 Enabling Dynamic IPv6 Addresses Via DHCPv6 105
3.13 Configuring DSCP/TC for Management 106
3.14 Configuring the Activation Key 107
3.14.1 Activation Key Overview 108
3.14.2 Viewing the Activation Key Status Parameters 108
3.14.3 Entering the Activation Key 110
3.14.4 To activate demo mode: 110
3.14.5 Activation Key Reclaim 110
3.14.6 Displaying a List of Activation-Key-Enabled Features 111
3.15 Setting the Time and Date (Optional) 120
3.16 Enabling the Interfaces (Interface Manager) 128
PTP 850E Management Interface 131
3.17 Configuring the Radio (MRMC) Script(s) 133
3.17.1 Radio Profiles 137
3.18 Running the Frequency Scanner (PTP 850E) 140
3.19 Configuring the Radio Parameters 144
3.20 Creating Service(s) for Traffic 148
3.21 Configuring CPRI 148
3.22 Operating in FIPS Mode 157
3.22.1 Initial Configuration of FIPS-Compliant Unit Redundancy Configuration 159
3.22.2 Replacing a Unit in a FIPS-Compliant Unit Redundancy Configuration 159
3.23 Encrypting the Protection Link 159

4. Configuration Guide 161

4.1 System Configurations 161

5. Configuring an PTP 850 Unit Using Basic Mode 162
5.1.1 Device View 163
5.1.2 Unit Summary 163
5.1.3 Quick Configuration 164
5.1.4 Platform 164

6. Configuring a Link Using the Quick Configuration Wizard 186
6.1.1 Configuring a 1+0 Link Using the Quick Configuration Wizard 187
6.1.2 Configuring a 2+0 Multi-Carrier ABC Link Using the Quick Configuration Wizard 193
6.1.3 Configuring a Layer 1 Link Bonding Link Using the Quick Configuration Wizard – Main Unit 200
6.1.4 Configuring a Multiband (Enhanced Multi-Carrier ABC) Link Using the Quick Configuration Wizard 213

6.1.5 Configuring a Multiband Link with Layer 1 Link Bonding Using the Quick Configuration Wizard – Main Unit....219
6.1.6 Configuring a Paired (Attached) Unit in a Layer 1 Link Bonding Group....228

7. Configuring Links, Link Groups, and Unit Redundancy....237
7.1.1 Multi-Carrier ABC Overview....237

7.2 Layer 1 Link Bonding....242
7.2.1 Layer 1 Link Bonding Overview....242
7.2.2 Layer 1 Link Bonding and Line Redundancy....244
7.2.3 Requirements and Limitations for Enhanced Link Bonding Mode....247
7.2.4 Link Bonding L1 Capacity Calculator....248
7.2.5 Configuring Layer 1 Link Bonding....250
7.2.6 Enabling Link Bonding Throughput Enhancement....266
7.2.7 Editing a Link Bonding Group or its Members....270
7.2.8 Displaying Statistics for a Link Bonding Group....272
7.2.9 Deleting a Link Bonding Group....274
7.2.10 L1 and L2 Header Compensation Values....276
7.2.11 Configuring Synchronization in a Link Bonding Node....388
7.2.12 Procedure for Upgrading an Existing Link Bonding Group from Standard Mode to Enhanced Mode....391
7.2.13 Procedure for Configuring Third-Party Devices for Operation in Link Bonding Configurations 393

7.3 Configuring 4+0 Layer 1 Link Bonding....400
7.3.1 4+0 Layer 1 Link Bonding Overview....400
7.3.2 Configuring 4+0 Layer 1 Link Bonding....402
7.3.3 Configuring Line Redundancy with Multiband and Link Bonding....410
7.3.4 Enabling Link Bonding Throughput Enhancement for 4+0 Layer 1 Link Bonding....415
7.3.5 Editing a Link Bonding Group or its Members....417
7.3.6 Displaying Statistics for a Link Bonding Group....417
7.3.7 Deleting a Link Bonding Group....418

7.4 Configuring Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP....418
7.4.1 Overview of Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP....419
7.4.2 Configuring a Layer 1 Link Bonding Node with PTP 850C and PTP 820C or PTP 820C-HP 421
7.4.3 Enabling Link Bonding Throughput Enhancement for Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP....430
7.4.4 Editing a Link Bonding Group or its Members....431
7.4.5 Displaying Statistics for a Link Bonding Group....431
7.4.6 Deleting a Link Bonding Group....432

7.5 Configuring Multiband....433
7.5.1 Multiband Overview....433
7.5.2 Multiband Operation....433
7.5.3 Multiband Configuration....437
7.5.4 Editing a Multiband Group or its Members....442
7.5.5 Multiband Management....443
7.5.6 Configuring Synchronization in a Multiband Node....446
7.5.7 Multiband with Layer 1 Link Bonding – Hardware Configuration....451
7.5.8 Multiband with Layer 1 Link Bonding and Line Redundancy....452
7.5.9 Configuring Multiband with Layer 1 Link Bonding....454
7.5.10 Configuring Synchronization in a Multiband Node with Layer 1 Link Bonding....462
7.5.11 Enabling Link Bonding Throughput Enhancement for Multiband with Layer 1 Link Bonding 464
7.5.12 Editing a Multiband Link Bonding Group or its Members....465

7.5.13 Displaying Statistics for a Multiband Link Bonding Group 465
7.5.14 Deleting a Multiband Link Bonding Group 466

7.6 Configuring XPIC 466
7.6.1 XPIC Overview 466
7.6.2 Configuring Layer 1 Link Bonding (Optional – PTP 850E Only) 471
7.6.3 Configuring the Radio Carriers 484
7.6.4 Deleting an AMCC (XPIC) Group 487
7.6.5 Performing Antenna Alignment for XPIC 492
7.6.6 XPIC Status and Troubleshooting 494

7.7 Configuring Line Redundancy for Link Bonding Configurations 495
7.7.1 Line Redundancy with Link Bonding – Force-Switch and Lockout 497

7.8 Configuring Unit Redundancy 499
7.8.1 Unit Redundancy Overview 500
7.8.2 Configuring Ethernet Interface Protection 502
7.8.3 Configuring Unit Redundancy 504
7.8.4 Configuring Revertive Protection 507
7.8.5 Viewing the Configuration of the Standby unit 507
7.8.6 Editing Standby Unit Settings 508
7.8.7 Viewing Link and Protection Status and Activity 509
7.8.8 Manually Switching to the Standby Unit 509
7.8.9 Disabling Automatic Switchover to the Standby Unit 510
7.8.10 Disabling Unit Redundancy 510

Configuring Link Aggregation (LAG) and LACP 510

8. Unit Management 526

8.1 Defining the IP Protocol Version for Initiating Communications 526

8.2 Configuring the Remote Unit's IP Address 527
8.2.1 Changing the Subnet of the Remote IP Address 528

8.3 Configuring SNMP 529

8.4 Configuring Trap Managers 532

8.5 Installing and Configuring an FTP or SFTP Server 534

8.6 Configuring the Internal Ports for FTP or SFTP 537

8.7 Upgrading the Software 538
8.7.1 Viewing Current Software Versions 538
8.7.2 Software Upgrade Overview 539
8.7.3 Downloading and Installing Software 540
8.7.4 Downloading Software Via HTTP or HTTPS 540
8.7.5 Downloading Software Via FTP or SFTP 542
8.7.7 Installing Software 545
8.7.8 Configuring a Timed Installation 547

8.8 Backing Up and Restoring Configurations 548
8.8.1 Configuration Management Overview 548
8.8.2 Viewing Current Backup Files 548
8.8.3 Setting the Configuration Management Parameters 550
8.8.4 Exporting a Configuration File 553
8.8.5 Importing a Configuration File 555

8.8.6 Deleting a Configuration File....556
8.8.7 Backing Up the Current Configuration....556
8.8.8 Restoring a Saved Configuration....556
8.8.9 Editing CLI Scripts....557
8.9 Setting the Unit to the Factory Default Configuration....558
8.10 Performing a Unit Reset....559
8.11 Configuring NTP....562
8.12 Displaying Unit Inventory....566
8.13 Displaying SFP DDM and Inventory Information....567
8.13.1 SFP DDM Alarms....567
8.13.2 Displaying Information about an SFP transceiver....568
8.13.3 Displaying PMs about an SFP transceiver and Configuring SFP RX Signal Power Thresholds....570
8.14 Defining a Login Banner....572
9. Radio Configuration....574
9.1 Viewing the Radio Status and Settings....575
9.2 Configuring the Remote Radio Parameters....580
9.3 Configuring ATPC and ATPC Override Timer....581
9.4 Configuring Header De-Duplication and Frame Cut-Through....583
9.5 Configuring AES-256 Payload Encryption....587
9.6 Configuring and Viewing Radio PMs and Statistics....590
9.6.1 Configuring BER Thresholds and Displaying Current BER....591
9.6.2 Displaying MRMC Status....592
9.6.3 Displaying MRMC PMs and Configuring ACM Profile Thresholds....595
9.6.4 Displaying and Clearing Defective Block Counters....597
9.6.5 Displaying Signal Level PMs and Configuring Signal Level PM Thresholds....598
9.6.6 Displaying Modem BER (Aggregate) PMs....600
9.6.7 Displaying MSE PMs and Configuring MSE PM Thresholds....602
9.6.8 Displaying XPI PMs and Configuring XPI PM Thresholds....604
9.6.9 Displaying Traffic PMs....605
9.6.10 Displaying Frame Error Rate PMs....610
9.6.11 Displaying Ethernet Interface Counters....612
10. Ethernet Services and Interfaces....614
10.1 Configuring Ethernet Service(s)....615
10.1.1 Ethernet Services Overview....615
10.1.2 General Guidelines for Provisioning Ethernet Services....616
10.1.3 The Ethernet Services Page....616
10.1.4 Adding an Ethernet Service....617
10.1.5 Editing a Service....619
10.1.6 Deleting a Service....619
10.1.7 Enabling, Disabling, or Deleting Multiple Services....620
10.1.8 Viewing Service Details....620
10.1.9 Configuring Service Points....620
10.2 Setting the MRU Size and the S-VLAN Ethertype....635

10.2.1 S-VLAN Ethertype 0x8100 (CISCO Mode) 636
10.3 Configuring Ethernet Interfaces 636
10.4 Configuring Automatic State Propagation and Link Loss Forwarding 643
10.5 Viewing Ethernet PMs and Statistics 646
10.5.1 RMON Statistics 646
10.5.2 Egress CoS Statistics 648
10.5.3 Port TX Statistics 650
10.5.4 Port RX Statistics 653
11. Quality of Service (QoS) 657
11.1 QoS Overview 657
11.2 Configuring Classification 659
11.2.1 Classification Overview 660
11.2.2 Configuring Ingress Path Classification on a Logical Interface 661
11.2.3 Modifying the C-VLAN 802.1Q UP and CFI Bit Classification Table 665
11.2.4 Modifying the S-VLAN 802.1 UP and DEI Bit Classification Table 667
11.2.5 Modifying the DSCP Classification Table 668
11.2.6 Modifying the MPLS EXP Bit Classification Table 671
11.3 Configuring Policers (Rate Metering) 675
11.3.1 Policer (Rate Metering) Overview 675
11.3.2 Configuring Policer Profiles 675
11.3.3 Assigning Policers to Interfaces 678
11.3.4 Configuring the Ingress and Egress Byte Compensation 684
11.4 Configuring Marking 686
11.4.1 Marking Overview 686
11.4.2 Enabling Marking 686
11.4.3 Modifying the 802.1Q Marking Table 686
11.4.4 Modifying the 802.1AD Marking Table 688
11.5 Configuring WRED 689
11.5.1 WRED Overview 689
11.5.2 Configuring WRED Profiles 689
11.5.3 Assigning WRED Profiles to Queues 692
11.6 Configuring Egress Shaping 693
11.6.1 Egress Shaping Overview 693
11.6.2 Configuring Queue Shaper Profiles 693
11.6.3 Assigning a Queue Shaper Profile to a Queue 698
11.7 Configuring Scheduling 700
11.7.1 Scheduling Overview 700
11.7.2 Configuring Priority Profiles 700
11.7.3 Configuring WFQ Profiles 704
11.7.4 Assigning a Queue Priority Profile to an Interface 707
11.7.5 Assigning a Queue WFQ Profile to an Interface 707
11.7.6 Assigning a Service Bundle WFQ Profile to a Service Bundle 709
11.7.7 Enabling Hierarchical QoS (H-QoS) 710
11.7.8 H-QoS Overview 710
11.7.9 Configuring H-QoS 710

11.8 Configuring and Displaying Queue-Level PMs 711

12. Ethernet Protocols 716

12.1 Configuring G.8032 716

12.2 Configuring MSTP 729

12.3 Configuring Ethernet Bandwidth Notification (ETH-BN) 748
12.3.1 ETH-BN Overview 748
12.3.2 Adding an ETH-BN entity 748
12.3.3 Editing an ETH-BN Entity 751
12.3.4 Deleting an ETH-BN Entity 751
12.3.5 Viewing the Statistics for an ETH-BN Entity 751

12.4 Configuring LLDP 752
12.4.1 LLDP Overview 752

13. Synchronization 770

13.1 Configuring the Sync Source 770
13.1.1 Viewing the Sync Source Status 771
13.1.2 Adding a Sync Source 772
13.1.3 Editing a Sync Source 773
13.1.4 Deleting a Sync Source 773

13.2 Configuring the Outgoing Clock and SSM Messages 773

13.3 Configuring 1588 Transparent Clock 775

13.4 Configuring 1588 Boundary Clock 779
13.4.1 Enabling Boundary Clock 779
13.4.2 Displaying and Setting the Boundary Clock Default Parameters 782
13.4.3 Displaying the Boundary Clock Advanced Parameters 783
13.4.4 Displaying the Boundary Clock Port Parameters 785
13.4.5 Displaying the Boundary Clock Port Statistics 786
13.4.6 Disabling 1588 PTP 787

14. Access Management and Security 789

14.1 Quick Security Configuration 789
14.1.1 Quick Security Configuration – General Parameters Page 790
14.1.2 Quick Security Configuration – Protocols Page 790
14.1.3 Quick Security Configuration – Access Control Page 791
14.1.4 Quick Security Configuration – RSA Key & Certificate Page 792

14.2 Configuring the General Access Control Parameters 793

14.3 Configuring the Password Security Parameters 795

14.4 Configuring the Session Timeout 796

14.5 Configuring Users 797
14.5.1 User Configuration Overview 797
14.5.2 Configuring User Profiles 798
14.5.3 Adding User Accounts 801
14.5.4 Editing and Blocking Users 803

14.6 Configuring RADIUS 804

14.6.1 RADIUS Overview....804
14.6.2 Activating RADIUS Authentication....805
14.6.3 Configuring the RADIUS Server Attributes....805
14.6.4 Configuring a RADIUS Server....806
14.7 Configuring TACACS+....825
14.7.1 TACACS+ Overview....825
14.7.2 Activating TACACS+ Authentication and Authorization....826
14.7.3 Configuring the TACACS+ Server Attributes....827
14.7.4 Configuring a TACACS+ Server....829
14.8 Viewing Remote Access User Connectivity and Permissions....831
14.9 Configuring X.509 CSR Certificates....833
14.9.1 Generating a Certificate Signing Request (CSR) File....833
14.9.2 Downloading a Certificate....836
14.10 Enabling HTTPS....837
14.11 Downloading and Installing an RSA Key....838
14.12 Blocking Telnet Access....842
14.13 Configuring Access Control Lists....842
14.14 Uploading the Security Log....845
14.15 Uploading the Configuration Log....848
14.16 Configuring the Import/Export Security Settings....851
14.17 Configuring SSO Web Login with Microsoft Entra ID....852
15. Alarm Management and Troubleshooting....856
15.1 Viewing Current Alarms....856
15.2 Viewing Alarm Statistics....858
15.3 Viewing and Saving the Event Log....859
15.4 Editing Alarm Text and Severity | Disabling Alarms and Event....860
15.4.1 Displaying Alarm Information....860
15.4.2 Viewing the Probable Cause and Corrective Actions for an Alarm Type....862
15.4.3 Editing an Alarm Type and Disabling Alarms and Events....862
15.4.4 Enabling the Auto Negotiation Speed Alarm....864
15.4.5 Setting Alarms to their Default Values....864
15.5 Configuring Voltage Alarm Thresholds and Displaying Voltage PMs....864
15.6 Uploading Unit Info....867
15.6.1 Uploading a Unit Info File Via HTTP or HTTPS....867
15.6.2 Uploading a Unit Info File Via FTP or SFTP....869
15.7 Configuring Syslog....871
15.7.1 Syslog Overview....871
15.7.2 Syslog Configuration....873
15.8 Performing Diagnostics....874
15.8.1 Performing Radio Loopback....875
15.8.2 Performing Ethernet Loopback....876

15.8.3 Configuring Service OAM (SOAM) Fault Management (FM) 877

16. Web EMS Utilities 896

16.1 Restarting the HTTP Server 896

16.2 Calculating an ifIndex 896

16.3 Displaying, Searching, and Saving a list of MIB Entities 897

17. Getting Started (CLI) 899

17.1 General (CLI) 899

17.2 Establishing a Connection (CLI) 900
17.2.1 PC Setup (CLI) 900

17.3 Logging On (CLI) 900

17.4 General CLI Commands 901
17.4.1 Changing Your Password (CLI) 902

17.5 Configuring In-Band Management (CLI) 902

17.6 Changing the Management IP Address (CLI) 903

17.7 Configuring the Activation Key (CLI) 905
17.7.1 Activation Key Overview (CLI) 906
17.7.2 Viewing the Activation Key Status Parameters (CLI) 906
17.7.3 Entering the Activation Key (CLI) 906
17.7.4 Activating a Demo Activation Key (CLI) 907
17.7.5 Activation Key Reclaim (CLI) 907
17.7.6 Displaying a List of Activation-Key-Enabled Features (CLI) 907

17.8 Setting the Time and Date (Optional) (CLI) 907
17.8.1 Setting the Daylight Savings Time (CLI) 909

17.9 Enabling the Interfaces (Interface Manager) 924
17.9.1 PTP 850E Management Interface (CLI) 926

17.10 Configuring the Radio (MRMC) Script(s) (CLI) 927
17.10.1 Displaying Available MRMC Scripts (CLI) 927
17.10.2 Assigning an MRMC Script to a Radio Carrier (CLI) 929

17.11 Configuring the Radio Parameters (CLI) 939
17.11.1 Entering Radio View (CLI) 940
17.11.2 Changing the Default Carrier (PTP 850C only) 940
17.11.3 Muting and Unmuting a Radio (CLI) 940
17.11.4 Configuring the Transmit (TX) Frequency (CLI) 941
17.11.5 Configuring the Transmit (TX) Level (CLI) 941
17.11.6 Enabling ACM with Adaptive Transmit Power (CLI) 941
17.11.7 Enabling Adjacent Channel Mode (CLI) 942

17.12 Configuring the RSL Threshold Alarm (CLI) 942

17.13 Creating Service (s) for Traffic (CLI) 943

17.14 Configuring CPRI (CLI) 943
17.14.1 Requirements for FIPS Compliance (CLI) 946

18. Configuration Guide (CLI) 950

18.1 System Configurations (CLI) 950

18.2 Configuring Multi-Carrier ABC (CLI) 951
18.2.1 Multi-Carrier ABC Overview (CLI) 951
18.2.2 Configuring a Multi-Carrier ABC Group (CLI) 951
18.2.3 Configuring 4+0 Layer 1 Link Bonding (CLI) 952
18.2.4 Configuring 4+0 Layer 1 Link Bonding (CLI) 953
18.2.5 Configuring Synchronization in a 4+0 Layer 1 Link Bonding Node (CLI) 955
18.2.6 Editing a Link Bonding Group or its Members (CLI) 959
18.2.7 Displaying Statistics for a Link Bonding Group (CLI) 961
18.2.8 Deleting a Link Bonding Group (CLI) 962
18.2.9 Configuring Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP (CLI) 962
18.2.10 (CLI) Configuring a Layer 1 Link Bonding Node with PTP 850C and PTP 820C or PTP 820C-HP 963
18.2.11 Configuring Synchronization in a Layer 1 Link Bonding Node with PTP 850C and PTP 820C or PTP 820C-HP (CLI) 965
18.2.12 Enabling Link Bonding Throughput Enhancement for Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP 967
18.2.13 Editing a Link Bonding Group or its Members (CLI) 968
18.2.14 Displaying Statistics for a Link Bonding Group (CLI) 969
18.2.15 Deleting a Link Bonding Group (CLI) 970

18.3 Configuring Multiband (CLI) 972
18.3.1 Multiband Overview (CLI) 975
18.3.2 Multiband Configuration (CLI) 975
18.3.3 Multiband Management (CLI) 977

18.4 Configuring Multiband with Layer 1 Link Bonding (CLI) 979
18.4.1 Configuring Multiband with Layer 1 Link Bonding (CLI) 981
18.4.2 Configuring Line Redundancy with Multiband and Link Bonding (CLI) 988
18.4.3 Enabling Link Bonding Throughput Enhancement for Multiband with Layer 1 Link Bonding (CLI) 991
18.4.4 Editing a Multiband Link Bonding Group or its Members (CLI) 993
18.4.5 Displaying Group Statistics for a Multiband Link Bonding Group (CLI) 994
18.4.6 Deleting a Multiband Link Bonding Group (CLI) 995

18.5 Configuring XPIC (CLI) 995
18.5.1 Configuring Layer 1 Link Bonding (Optional – PTP 850E Only) (CLI) 996
18.5.2 Configuring the Radio Carriers for XPIC (CLI) 1003
18.5.3 Configuring the Radio Carriers for XPIC an PTP 850C (CLI) 1003
18.5.4 Configuring the Radio Carriers for XPIC on an PTP 850E (CLI) 1004
18.5.5 Deleting an AMCC (XPIC) Group 1005
18.5.6 Displaying XPIC Status (CLI) 1006

18.6 Configuring Line Redundancy for Link Bonding Configurations (CLI) 1007
18.6.1 Line Redundancy with Link Bonding – Force-Switch and Lockout (CLI) 1012

18.7 Configuring Unit Redundancy (CLI) 1012
18.7.1 Configuring Ethernet Interface Protection (CLI) 1013
18.7.2 Configuring Unit Redundancy (CLI) 1014
18.7.3 Configuring Revertive Protection (CLI) 1016
18.7.4 Viewing the Configuration of the Standby Unit (CLI) 1016
18.7.5 Editing Standby Unit Settings (CLI) 1016

18.7.6 Viewing Link and Protection Status and Activity (CLI) 1017
18.7.7 Manually Switching to the Standby Unit (CLI) 1018
18.7.8 Disabling Automatic Switchover to the Standby Unit (CLI) 1018
18.7.9 Disabling Unit Redundancy (CLI) 1018

18.8 Configuring Link Aggregation (LAG) and LACP (Optional) (CLI) 1018
18.8.1 Configuring a LAG Group (CLI) 1019
18.8.2 Configuring LACP (CLI) 1019
18.8.3 Configuring Multi-Homing (CLI) 1019
18.8.4 Viewing LAG Details (CLI) 1020
18.8.5 Editing and Deleting a LAG Group (CLI) 1020
18.8.6 Enabling and Disabling the LAG Group Shutdown in Case of Degradation Event Option (CLI) 1023
18.8.7 Configuring Enhanced LAG Distribution (CLI) 1023
18.8.8 Displaying LACP Parameters and Statistics (CLI) 1024

19. Unit Management (CLI) 1030

19.1 Defining the IP Protocol Version for Initiating Communications (CLI) 1030

19.2 Configuring the Remote Unit's IP Address (CLI) 1030
19.2.1 Configuring the Remote Radio's IP Address in IPv4 format (CLI) 1031
19.2.2 Configuring the Remote Radio's IP Address in IPv6 format (CLI) 1031

19.3 Configuring SNMP (CLI) 1033
19.3.1 Configuring Basic SNMP Settings (CLI) 1033
19.3.2 Configuring SNMPv3 (CLI) 1034
19.3.3 Displaying the SNMP Settings (CLI) 1035
19.3.4 Configuring Trap Managers (CLI) 1036

19.4 Configuring the Internal Ports for FTP or SFTP (CLI) 1038

19.5 Upgrading the Software (CLI) 1038
19.5.1 Software Upgrade Overview (CLI) 1039
19.5.2 Viewing Current Software Versions (CLI) 1039
19.5.3 Configuring a Software Download (CLI) 1039
19.5.4 Downloading a Software Package (CLI) 1041
19.5.5 Installing and Upgrading Software (CLI) 1043

19.6 Backing Up and Restoring Configurations (CLI) 1043
19.6.1 Configuration Management Overview (CLI) 1044
19.6.2 Setting the Configuration Management Parameters (CLI) 1044
19.6.3 Backing up and Exporting a Configuration File (CLI) 1046
19.6.4 Importing and Restoring a Configuration File (CLI) 1047
19.6.5 Editing CLI Scripts (CLI) 1047

19.7 Setting the Unit to the Factory Default Configuration (CLI) 1048

19.8 Performing a Unit Reset (CLI) 1048

19.9 Resetting the Remote Unit (CLI) 1049

19.10 Configuring Unit Parameters (CLI) 1049

19.11 Configuring NTP (CLI) 1051

19.12 Displaying Unit Inventory (CLI) 1054

19.13 Displaying SFP DDM and Inventory Information (CLI) 1055
19.13.1 Displaying Static Information about an SFP Transceiver (CLI) 1056

19.13.2 Displaying Dynamic (DDM) Information about an SFP Transceiver (CLI) 1058
19.13.3 Displaying DDM PMs about an SFP Transceiver (CLI)....1059
19.13.4 Configuring SFP Tccransceiver Voltage Thresholds (CLI)....1061

20. Radio Configuration (CLI)....1062

20.1 Viewing the Radio Status and Settings (CLI)....1064

20.2 Viewing and Configuring the Remote Radio Parameters (CLI)....1065
20.2.1 Displaying Communication Status with the Remote Radio (CLI)....1066
20.2.2 Displaying Remote Radio's Location (CLI) 1066
20.2.3 Muting and Unmuting the Remote Radio (CLI)....1066
20.2.4 Displaying the Remote Radio's RX Level (CLI)....1068
20.2.5 Configuring the Remote Radio's TX Level (CLI)....1068
20.2.6 Configuring Remote ATPC (CLI)....1068
20.2.7 Displaying the Remote Unit's Most Severe Alarm (CLI)....1069

20.3 Configuring ATPC and ATPC Override Timer (CLI)....1069

20.4 Configuring Header De-Duplication (CLI)....1072
20.4.1 Displaying Header De-Duplication Information (CLI)....1074

20.5 Configuring Frame Cut-Through (CLI)....1074

20.6 Configuring AES-256 Payload Encryption (CLI)....1075

20.7 Configuring and Viewing Radio PMs and Statistics (CLI)....1078
20.7.1 Displaying General Modem Status and Defective Block PMs (CLI)....1079
20.7.2 Displaying Excessive BER (Aggregate) PMs (CLI)....1079
20.7.3 Displaying BER Level and Configuring BER Parameters (CLI)....1081
20.7.4 Configuring RSL Thresholds (CLI)....1082
20.7.5 Configuring TSL Thresholds (CLI)....1082
20.7.6 Displaying RSL and TSL Levels (CLI)....1083
20.7.7 Configuring the Signal Level Threshold (CLI)....1084
20.7.8 Configuring the MSE Thresholds and Displaying the MSE PMs (CLI)....1085
20.7.9 Displaying Traffic PMs (CLI)....1094

21. Ethernet Services and Interfaces (CLI)....1103

21.1 Configuring Ethernet Services (CLI)....1103
21.1.1 Ethernet Services Overview (CLI)....1103
21.1.2 General Guidelines for Provisioning Ethernet Services (CLI)....1104
21.1.3 Defining Services (CLI)....1104
21.1.4 Configuring Service Points (CLI)....1110
21.1.5 Defining the MAC Address Forwarding Table for a Service (CLI)....1130

21.2 Setting the MRU Size and the S-VLAN Ethertype (CLI)....1138
21.2.1 Configuring the S-VLAN Ethertype (CLI)....1139
21.2.2 Configuring the C-VLAN Ethertype (CLI)....1139
21.2.3 Configuring the MRU (CLI)....1140

21.3 Configuring Ethernet Interfaces (CLI)....1140
21.3.1 Entering Interface View (CLI)....1141
21.3.2 Displaying the Operational State of the Interfaces in the Unit (CLI)....1142
21.3.3 Viewing Interface Attributes (CLI)....1142
21.3.4 Configuring the QSFP Interface on an PTP 850E (CLI)....1143
21.3.5 Configuring an Interface's Media Type (CLI)....1144

21.3.6 Configuring an Interface's Speed and Duplex State (CLI) 1144
21.3.7 Configuring an Interface's Auto Negotiation State (CLI) 1145
21.3.8 Configuring an Interface's IFG (CLI) 1146
21.3.9 Configuring an Interface's Preamble (CLI) 1146
21.3.10 Adding a Description for the Interface (CLI) 1146

21.4 Configuring Automatic State Propagation and Link Loss Forwarding (CLI) 1147

21.5 Configuring Receipt of CSF PDUs (CLI) 1160

21.6 Viewing Ethernet PMs and Statistics (CLI) 1160
21.6.1 Displaying RMON Statistics (CLI) 1161
21.6.2 Configuring Ethernet Port PMs and PM Thresholds (CLI) 1162
21.6.3 Displaying Ethernet Port PMs (CLI) 1162
21.6.4 Clearing Ethernet Port PMs (CLI) 1166
21.6.5 Displaying Link Bonding PMs (CLI) 1167

22. Quality of Service (QoS) (CLI) 1172

22.1 Configuring Classification (CLI) 1172
22.1.1 Classification Overview (CLI) 1172
22.1.2 Configuring Ingress Path Classification on a Logical Interface (CLI) 1173
22.1.3 Configuring VLAN Classification and Override (CLI) 1173
22.1.4 Configuring DSCP Classification (CLI) 1175
22.1.5 Configuring MPLS Classification (CLI) 1177
22.1.6 Configuring 802.1p Classification (CLI) 1179
22.1.7 Configuring a Default CoS (CLI) 1191
22.1.8 Configuring Ingress Path Classification on a Service Point (CLI) 1192
22.1.9 Configuring Ingress Path Classification on a Service (CLI) 1192

22.2 Configuring Policers (Rate Metering) (CLI) 1192
22.2.1 Overview of Rate Metering (Policing) (CLI) 1192
22.2.2 Configuring Rate Meter (Policer) Profiles (CLI) 1193
22.2.3 Displaying Rate Meter Profiles (CLI) 1195
22.2.4 Deleting a Rate Meter Profile (CLI) 1195
22.2.5 Attaching a Rate Meter (Policer) to an Interface (CLI) 1196
22.2.6 Attaching a Rate Meter (Policer) to a Service Point and CoS (CLI) 1210
22.2.7 Configuring the Line Compensation Value for a Rate Meter (Policer) (CLI) 1212
22.2.8 Displaying Rate Meter Statistics for an Interface (CLI) 1212

22.3 Configuring Marking (CLI) 1214
22.3.1 Marking Overview (CLI) 1214
22.3.2 Configuring Marking Mode on a Service Point (CLI) 1215
22.3.3 Marking Table for C-VLAN UP Bits (CLI) 1216
22.3.4 Marking Table for S-VLAN UP Bits (CLI) 1218

22.4 Configuring WRED (CLI) 1219
22.4.1 WRED Overview (CLI) 1219
22.4.2 Configuring WRED Profiles (CLI) 1220
22.4.3 Assigning a WRED Profile to a Queue (CLI) 1222

22.5 Configuring Shapers (CLI) 1222
22.5.1 Configuring Queue Shapers for PTP 850C and PTP 850E (CLI) 1223
22.5.2 Configuring Egress Line Compensation for Shaping for PTP 850C and PTP 850E (CLI) 1230
22.5.3 Configuring Service Bundle Shapers for PTP 850C (CLI) 1231
22.5.4 Configuring Shapers for PTP 850S (CLI) 1247

22.6 Configuring Scheduling (CLI) 1254
22.6.1 Overview of Egress Scheduling (CLI) 1254
22.6.2 Configuring Queue Priority (CLI) 1255
22.6.3 Configuring Interface Priority Profiles (CLI) 1256
22.6.4 Attaching a Priority Profile to an Interface (CLI) 1258
22.6.5 Configuring Weighted Fair Queuing (WFQ) (CLI) 1259

22.7 Displaying Ingress Statistics (CLI) 1265
22.7.1 Displaying Ingress Statistics per Interface (CLI) 1265
22.7.2 Displaying Ingress Statistics per Service Point (CLI) 1265

22.8 Displaying Egress PMs and Statistics (CLI) 1266
22.8.1 Displaying Queue-Level Statistics (CLI) 1267
22.8.2 Configuring and Displaying Queue-Level PMs (CLI) 1268
22.8.3 Displaying Service Bundle-Level Statistics (CLI) 1270

23. Ethernet Protocols (CLI) 1273

23.1 Configuring G.8032 (CLI) 1273

23.2 Configuring MSTP (CLI) 1288

23.3 Configuring Ethernet Bandwidth Notification (ETH-BN) (CLI) 1307

23.4 Configuring LLDP (CLI) 1311

24. Synchronization (CLI) 1323

24.1 Changing the ETSI/ANSI Mode (CLI) 1323

24.2 Configuring the Sync Source (CLI) 1323
24.2.1 Configuring an Ethernet Interface as a Synchronization Source (CLI) 1325
24.2.2 Configuring a Radio Interface as a Synchronization Source (CLI) 1328

24.3 Configuring the Outgoing Clock (CLI) 1331

24.4 Changing the Default Quality (CLI) 1332

24.5 Configuring the Revertive Timer (CLI) 1333

24.6 Configuring SSM Messages (CLI) 1334

24.7 Displaying Synchronization Status and Parameters (CLI) 1335

24.8 Configuring 1588 Transparent Clock (CLI) 1336

24.9 Configuring 1588 Boundary Clock (CLI) 1338

25. Access Management and Security (CLI) 1355

25.1 Blocking Telnet Access (CLI) 1355

25.2 Configuring the General Access Control Parameters (CLI) 1355
25.2.1 Configuring the Inactivity Timeout Period (CLI) 1356
25.2.2 Configuring Blocking Upon Login Failure (CLI) 1356
25.2.3 Configuring Blocking of Unused Accounts (CLI) 1357

25.3 Configuring the Password Security Parameters (CLI) 1358
25.3.1 Configuring Password Aging (CLI) 1358
25.3.2 Configuring Password Strength Enforcement (CLI) 1359
25.3.3 Forcing Password Change Upon First Login (CLI) 1360

25.3.4 Displaying the System Password Settings (CLI) 1361
25.4 Configuring Users (CLI) 1361
25.4.1 User Configuration Overview (CLI) 1361
25.4.2 Configuring User Profiles (CLI) 1362
25.4.3 Configuring User Accounts (CLI) 1364
25.5 Configuring RADIUS (CLI) 1365
25.6 Displaying Remote Access Users 1367
25.7 Configuring X.509 CSR Certificates (CLI) 1368
25.7.1 Generating a Certificate Signing Request (CSR) File (CLI) 1369
25.7.2 Downloading a Certificate (CLI) 1371
25.7.3 Enabling HTTPS (CLI) 1372
25.8 Configuring HTTPS Cipher Hardening (CLI) 1373
25.9 Downloading and Installing an RSA Key (CLI) 1373
25.10 Blocking Telnet Access (CLI) 1377
25.11 Configuring Access Control Lists (CLI) 1377
25.12 Uploading the Security Log (CLI) 1379
25.13 Uploading the Configuration Log (CLI) 1381
25.14 Enabling NETCONF (CLI) 1383
25.15 Terminating all Active Sessions (CLI) 1383

26. Alarm Management and Troubleshooting (CLI) 1385

26.1 Viewing Current Alarms (CLI) 1385
26.2 Viewing the Event Log (CLI) 1385
26.3 Editing Alarm Text and Severity (CLI) 1386
26.3.1 Displaying Alarm Information (CLI) 1386
26.3.2 Editing an Alarm Type (CLI) 1386
26.3.3 Setting Alarms to their Default Values (CLI) 1387
26.4 Configuring a Timeout for Trap Generation (CLI) 1387
26.5 Disabling Alarms and Events (CLI) 1388
26.6 Configuring Voltage Alarm Thresholds and Displaying Voltage PMs (CLI) 1389
26.7 Uploading Unit Info (CLI) 1390
26.8 Activating the Radio Logger (CLI) 1393
26.9 Configuring Port Mirroring (CLI) 1394
26.10 Configuring Syslog (CLI) 1394
26.10.1 Syslog Configuration (CLI) 1394
26.11 Performing Diagnostics (CLI) 1396
26.11.1 Performing Radio Loopback (CLI) 1396
26.11.2 Performing Ethernet Loopback (CLI) 1397
26.11.3 Configuring Service OAM (SOAM) Fault Management (FM) (CLI) 1398
26.11.4 SOAM Overview (CLI) 1398

26.11.5 Configuring MDs (CLI) 1399
26.11.6 Configuring MA/MEGs (CLI) 1400
26.11.7 Configuring MEPs (CLI) 1403

26.12 Working in CW Mode (Single or Dual Tone) (CLI) 1413

27. Maintenance 1415

Troubleshooting Tips 1416

27.2 Temperature Ranges 1418
27.2.1 Troubleshooting Tips 1418

27.3 PTP 850C Interface Pin-outs and LEDS 1419

27.4 PTP 850E Connector Pin-outs 1425
27.4.1 P2 (Eth 1) – MGT/PoE GbE Electrical Interface (RJ-45) 1426
27.4.2 P3 (Eth 2) GbE Optical Interface (SFP) 1426
27.4.3 P4 (Eth 3, Eth 4, Eth 5, Eth 6) 40 GbE Optical Interface (QSFP) 1426
27.4.4 P5 (Eth 7) 10G Optical Interface (SFP+) 1427
27.4.5 Protection/XPIC Port 1427
27.4.6 RSL Interface 1427

27.5 PTP 850E LEDs 1427
27.5.1 P2 MGT/PoE GbE Electrical Interface (RJ-45) LEDs 1427
27.5.2 P4/Eth3-6 40G Optical Interface (QSFP) LEDs 1428
27.5.3 P5/Eth7 1/10G Optical Interface (SFP+) LEDs 1428
27.5.4 Status LED 1428
27.5.5 Protection LED 1428
27.5.6 PTP 850S Interface Pin-outs 1428

27.6 PoE Injector Pin-outs and LEDs – Standard PoE 1434

27.7 PoE Injector Pin-outs and LEDs – Standard PoE 1435
27.7.1 PoE Injector Pin-outs and LEDs – Standard PoE 1435
27.7.2 PoE Injector LEDs – Standard PoE 1436

27.8 PoE Injector Pin-outs and LEDs – Passive PoE 1437
27.8.1 PoE Injector Pin-outs and LEDs – Passive PoE 1437
27.8.2 PoE Injector LEDs – Passive PoE 1438

28. Alarms List 1439
28.1.1 Glossary 1553

List of Figures

Figure 1 Main Web EMS Page PTP 850C 55
Figure 2 Main Web EMS Page – PTP 850S 56
Figure 3 Main Web EMS Page – PTP 850E 56
Figure 4 Displaying a Representation of the Front Panel 57
Figure 5 *Main Web EMS Page with Representation of Front Panel – PTP 850S* 57
Figure 6 Main Web EMS Page with Representation of Front Panel – PTP 850E 58
Figure 7 Main Web EMS Page with Representation of Front Panel 58
Figure 8: Interface Manager Page Showing All Interfaces (PTP 850E) 59
Figure 9: Interface Manager Page Showing Interfaces with Admin Status Up (PTP 850E) 59
Figure 10: Main Web EMS Page with Active and Standby Tabs 62
Figure 11: Merged (All) Tab – Interface Manager Page 63
Figure 12: Merged (All) Tab – Radio Parameters Page 63
Figure 13: Merged (All) Tab – Current Alarms Page 63
Figure 14: Merged (All) Tab – Event Log Page 64
Figure 15: Related Pages Drop-Down List 64
Figure 16: Page Refresh Options 64
Figure 17: Automatic Refresh Interval Drop-Down List 65
Figure 18: Export to CSV Button 65
Figure 19: Help Button 65
Figure 20: Interactive User Guide – Example of Context-Related Page 66
Figure 21: Interactive User Guide – Preview 66
Figure 22 Unit Summary Page- PTP 850C 67
Figure 23 Unit Summary Page – PTP 850S 67
Figure 24 Unit Summary Page – PTP 850E 68
Figure 25 Unit Summary Page – Customizing Columns 68
Figure 26: Link Summary Page (PTP 850C) 69
Figure 27: Link Summary Page (PTP 850E) 69
Figure 28: Link Summary Page – Radio Parameters (PTP 850C) 71
Figure 29: Link Summary Page – Radio Parameters (PTP 850E) 72
Figure 30 Security summary page 73
Figure 31 Security Summary Page – Customizing Columns 75
Figure 32: Antenna Alignment Page 88
Figure 33 Internet Protocol Properties Window 90
Figure 34 Login Page 90
Figure 35 Change User Password Page 92

Figure 36 Quick Configuration – From File Page 95
Figure 37 Quick Configuration – From File Page – Configuration File Loaded 95
Figure 38 Quick Configuration – Platform Setup Page 96
Figure 39 Quick Configuration– Platform Setup Summary Page 101
Figure 40 Local Networking Configuration Page – In-Band Management 103
Figure 41 Local Networking Configuration Page 104
Figure 42: Local Networking Configuration Page (IPv6 Automatic Mode) 106
Figure 43 Activation Key Configuration Page 109
Figure 44 Activation Key Overview Page 111
Figure 45 Time Services Page 121
Figure 46 Interface Manager Page-PTP 850C 129
Figure 47 Interface Manager Page-PTP 850E 129
Figure 48 Interface Manager Page-PTP 850S 129
Figure 49 Interface Manager – Edit Page 130
Figure 50 Multiple Selection Operation Section (Interface Manager Page) 130
Figure 51: Traffic over Management Page 133
Figure 52 MRMC Symmetrical Scripts Page-PTP 850C 134
Figure 53 MRMC Symmetrical Scripts Page-PTP 850S 134
Figure 54 MRMC Symmetrical Scripts Page-PTP 850E 135
Figure 55 **MRMC Symmetrical Scripts Page – Configuration** 135
Figure 56 Frequency Scanner Page – Continuous Mode 141
Figure 57 Frequency Scanner Page – Single Mode 142
Figure 58 Frequency Scanner Results – Graph Format (Continuous Mode) 144
Figure 59 Frequency Scanner Results – Graph Format (Single Mode) 144
Figure 60: Radio Parameters Page 146
Figure 61: Interface Manager Page – Enabling the CPRI Port 152
Figure 62: Sync Source Page 153
Figure 63: Sync Source – Add Page (CPRI – BBU) 153
Figure 64: Sync Source – Add Page (CPRI – RRH) 153
Figure 65: Ethernet Services Page 154
Figure 66: Ethernet Services - Add page (CPRI) 154
Figure 67: Ethernet Services Page – CPRI Service 155
Figure 68: Ethernet Service Points Page (Empty) 156
Figure 69: Ethernet Service Points - Add Page (CPRI Service Point on CPRI Port) 156
Figure 70: Ethernet Service Points Page (Populated for CPRI Service) 157
Figure 71: Security General Configuration Page 158
Figure 72 1+0 Quick Configuration Wizard – Ethernet Selection (PTP 850C) 187

Figure 73 1+0 Quick Configuration Wizard – Ethernet Selection (PTP 850C) 188
Figure 74 1+0 Quick Configuration Wizard – Ethernet Selection (PTP 850E) 188
Figure 75 1+0 Quick Configuration Wizard – Page 2 189
Figure 76 1+0 Quick Configuration Wizard – Page 3 189
Figure 77 1+0 Quick Configuration Wizard – Page 4 190
Figure 78 1+0 Quick Configuration Wizard – Page 5 190
Figure 79 1+0 Quick Configuration Wizard – Page 6 191
Figure 80 1+0 Quick Configuration Wizard – Page 5 (In Band Management = Yes) 192
Figure 81 1+0 Quick Configuration Wizard – Page 7 (Summary Page) 192
Figure 82: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Ethernet Selection 193
Figure 83: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio #1 Selection Page 194
Figure 84: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio #2 Selection Page 194
Figure 85: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio XPIC Configuration Page 195
Figure 86: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio Parameters Configuration Page . 195
Figure 87: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio Parameters Configuration Page (XPIC) 196
Figure 88: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio MRMC Script Configuration Page 196
Figure 89: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio MRMC Script Configuration Page – XPIC 197
Figure 90: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Management Configuration Page 198
Figure 91: 2 + 0 Multi Carrier ABC Quick Configuration Wizard –Summary Page 199
Figure 92: Multiband Link Bonding Quick Configuration Wizard – Ethernet Selection Page (PTP 850E) 201
Figure 93: Link Bonding Quick Configuration Wizard – Ethernet Selection Page PTP 850C 202
Figure 94: Link Bonding Quick Configuration Wizard – Number of Members Page PTP 850C 203
Figure 95: Link Bonding Quick Configuration Wizard – Member #1 Page (4+0 with PTP 850C – Single-Cable Configuration) 204
Figure 96: Link Bonding Quick Configuration Wizard – Member #1 Page (4+0 with PTP 850C – Two-Cable Configuration) 204
Figure 97: Link Bonding Quick Configuration Wizard – Member #1 Page (PTP 850C with PTP 820C or PTP 820C-HP – Single-Cable Configuration) 205
Figure 98: Link Bonding Quick Configuration Wizard – Member #1 Page (PTP 850C with PTP 820C or PTP 820C-HP – Two-Cable Configuration) 205
Figure 99: Link Bonding Quick Configuration Wizard – Member #2 Page 206
Figure 100: Link Bonding Quick Configuration Wizard – XPIC Page 207
Figure 101: Link Bonding Quick Configuration Wizard – Radio MRMC Script Configuration Page (XPIC Selected) 208
Figure 102: Link Bonding Quick Configuration Wizard – Radio MRMC Script Configuration Page (XPIC not Selected) 208
Figure 103: Link Bonding Quick Configuration Wizard – Radio Parameters Configuration Page (XPIC Selected) 209

Figure 104: Link Bonding Quick Configuration Wizard – Radio Parameters Configuration Page (XPIC not Selected) 210
Figure 105: Link Bonding Quick Configuration Wizard – Management Configuration Page 211
Figure 106: Quick Configuration Wizard – Summary Page (4+0 with PTP 850C) 212
Figure 107 Multiband Quick Configuration Wizard – Page 1 213
Figure 108 Multiband Quick Configuration Wizard – Page 2 214
Figure 109 Multiband Quick Configuration Wizard – Page 3 214
Figure 110 Multiband Quick Configuration Wizard – Page 4 215
Figure 111 Multiband Quick Configuration Wizard – Page 5 216
Figure 112 Multiband Quick Configuration Wizard – Page 6 217
Figure 113 Multiband Quick Configuration Wizard – Summary Page 218
Figure 114: Multiband Link Bonding Quick Configuration Wizard – Ethernet Selection Page 220
Figure 115: Multiband Link Bonding Quick Configuration Wizard – Number of Members Page 221
Figure 116: Multiband Link Bonding Quick Configuration Wizard – Member #1 Page 222
Figure 117: Multiband Link Bonding Quick Configuration Wizard – Member #1 Page (Single-Cable Configuration) 222
Figure 118: Multiband Link Bonding Quick Configuration Wizard – Member #1 Page (Two-Cable Configuration) 223
Figure 119: Multiband Link Bonding Quick Configuration Wizard – Member #2 Page 224
Figure 120: Multiband Link Bonding Quick Configuration Wizard – Radio MRMC Script Configuration Page 225
Figure 121: Multiband Link Bonding Quick Configuration Wizard – Radio Parameters Configuration Page 225
Figure 122: Multiband Link Bonding Quick Configuration Wizard – Management Configuration Page 226
Figure 123: Multiband Quick Configuration Wizard – Summary Page 227
Figure 124: Link Bonding Attached Unit Quick Configuration Wizard – Ethernet Selection Page (PTP 850E) 228
Figure 125: Link Bonding Attached Unit Quick Configuration Wizard – Ethernet Selection Page (PTP 850C) 229
Figure 126: Link Bonding Attached Unit Quick Configuration Wizard – Radio/Multi Carrier ABC Interface Page (PTP 850E) 229
Figure 127: Link Bonding Attached Unit Quick Configuration Wizard – Radio/Multi Carrier ABC Interface Page (PTP 850C) 230
Figure 128: Link Bonding Attached Unit Quick Configuration Wizard – XPIC Page 230
Figure 129: Link Bonding Attached Unit Quick Configuration Wizard – Radio MRMC Script Configuration Page (PTP 850E) 231
Figure 130: Link Bonding Attached Unit Quick Configuration Wizard – Radio MRMC Script Configuration Page (PTP 850C) 231
Figure 131: Link Bonding Attached Unit Quick Configuration Wizard – Radio Parameters Configuration Page (PTP 850E) 232
Figure 132: Link Bonding Attached Unit Quick Configuration Wizard – Radio Parameters Configuration Page (PTP 850C) 232

Figure 133: Link Bonding Attached Unit Quick Configuration Wizard – Additional Parameters Page (Enhanced Link Bonding Mode) 233
Figure 134: Link Bonding Attached Unit Quick Configuration Wizard – Additional Parameters Page (Standard Link Bonding Mode) 233
Figure 135: Multiband Link Bonding Quick Configuration Wizard – Management Configuration Page 235
Figure 136: Multiband Quick Configuration Wizard – Summary Page 236
Figure 137: 4+0 PTP 850C with Layer 1 Link Bonding and Line Redundancy 244
Figure 138: Multiband with Layer 1 Link Bonding and Line Redundancy – Multiband Antenna 245
Figure 139: Multiband with Layer 1 Link Bonding and Line Redundancy – Separate Antennas 245
Figure 140: Layer 1 Link Bonding with Line and External Management Redundancy 247
Figure 141: Link Bonding Page (Multiband) 248
Figure 142: Link Bonding Edit Members Page (Multiband) 249
Figure 143: Link Bonding Edit Page 249
Figure 144: Link Bonding Page (Empty) 252
Figure 145: Link Bonding Group Wizard – Page 1 252
Figure 146: Link Bonding Group Wizard – Member #1 Page (PTP 850C) 253
Figure 147: Link Bonding Group Wizard – Member #1 Page (PTP 850E) 253
Figure 148: Link Bonding Group Wizard – Member #2 Page (PTP 850C) 254
Figure 149: Link Bonding Group Wizard – Member #2 Page (PTP 850E) 254
Figure 150: Link Bonding Group Wizard – Selection Summary Page (PTP 850C) 255
Figure 151: Link Bonding Group Wizard – Selection Summary Page (PTP 850E) 255
Figure 152: Link Bonding Page (Populated) (PTP 850C) 255
Figure 153: Link Bonding Groups – Edit Members Page (PTP 850C as main unit) 257
Figure 154: Link Bonding Groups – Edit Members Page (PTP 850E as main unit) 257
Figure 155: Link Bonding – Members Bandwidth Control Page (Single-Cable Configuration with PTP 850C as main unit and attached unit) 259
Figure 156: Link Bonding – Members Bandwidth Control Page (Two-Cable Configuration with PTP 850C as main unit and attached unit) 259
Figure 157: Link Bonding – Members Bandwidth Control Page (Single-Cable Configuration with PTP 850E as main unit) 259
Figure 158: Link Bonding – Members Bandwidth Control Page (Two-Cable Configuration with PTP 850E as main unit) 259
Figure 159: Bandwidth Notification Page (Empty) 260
Figure 160: Bandwidth Notification – Add Page (PTP 850C) 260
Figure 161: Bandwidth Notification – Add Page (PTP 850E) 261
Figure 162: Bandwidth Notification Page (Populated with Radio BNM) 261
Figure 163: Radio Ethernet Interface Configuration Page (PTP 850C) 267
Figure 164: Link Bonding Groups – Edit Page 270
Figure 165: Link Bonding Groups – Member Statistics Page (PTP 850C as main unit) 272

Figure 166: Link Bonding Groups – Member Statistics Page (PTP 850E as main unit) 272
Figure 167: Link Bonding Groups – Member Statistics Page 274
Figure 168: SOAM MD Page – MD for Link Bonding 394
Figure 169: SOAM MA/MEG Page – MEG for Link Bonding 395
Figure 170: SOAM MEP Page – MEP for Link Bonding 397
Figure 171: Link Bonding – Members CCM LOC Page 398
Figure 172: Layer 1 Link Bonding Operation – 4+0 PTP 850C 401
Figure 173: Link Bonding Page (Empty) 402
Figure 174: Link Bonding Group Wizard – Page 1 403
Figure 175: Link Bonding Group Wizard – Member #1 Page 403
Figure 176: Link Bonding Group Wizard – Member #2 Page 404
Figure 177: Link Bonding Group Wizard – Selection Summary Page 404
Figure 178: Link Bonding Page (Populated) 404
Figure 179: Link Bonding – Members Bandwidth Control Page (Single-Cable Configuration) 406
Figure 180: Link Bonding – Members Bandwidth Control Page (Two-Cable Configuration) 406
Figure 181: Link Bonding Groups – Edit Members Page 406
Figure 182: Bandwidth Notification Page (Empty) 407
Figure 183: Bandwidth Notification – Add Page 407
Figure 184: Bandwidth Notification Page (Populated with Radio BNM) 408
Figure 185: Line Redundancy Page (Main Unit) 410
Figure 186: Line Redundancy Page (Paired Unit) 411
Figure 187: Radio Ethernet Interface Configuration Page (PTP 850C) 416
Figure 188: Link Bonding Groups – Edit Page 417
Figure 189: Link Bonding Groups – Member Statistics Page 418
Figure 190: Link Bonding Groups – Member Statistics Page 418
Figure 191: Layer 1 Link Bonding Operation – PTP 850C and PTP 820C (ESS) 420
Figure 192: Layer 1 Link Bonding Operation – PTP 850C and PTP 820C (ESX) 420
Figure 193: Layer 1 Link Bonding Operation – PTP 850C and PTP 820C-HP 421
Figure 194: Link Bonding Page (Empty) 422
Figure 195: Link Bonding Group Wizard – Page 1 422
Figure 196: Link Bonding Group Wizard – Member #1 Page 423
Figure 197: Link Bonding Group Wizard – Member #2 Page 424
Figure 198: Link Bonding Group Wizard – Selection Summary Page 424
Figure 199: Link Bonding Page (Populated) 425
Figure 200: Link Bonding – Members Bandwidth Control Page (Single-Cable Configuration) 426
Figure 201: Link Bonding – Members Bandwidth Control Page (Two-Cable Configuration) 426
Figure 202: Link Bonding Groups – Edit Members Page (PTP 850C with PTP 820C) 426

Figure 203: Bandwidth Notification Page (Empty) 427
Figure 204: Bandwidth Notification – Add Page 428
Figure 205: Bandwidth Notification Page (Populated with Radio BNM) 428
Figure 206: Link Bonding Groups – Edit Page 431
Figure 207: Link Bonding Groups – Member Statistics Page 432
Figure 208: Link Bonding Groups – Member Statistics Page 432
Figure 209: Multiband Operation – PTP 850E and PTP 820C (Single Cable for Traffic, Management, and Synchronization) 435
Figure 210: Multiband Operation – PTP 850E and PTP 820C 436
Figure 211: Multiband Operation – PTP 850E and Third-Party Unit 437
Figure 212: Multi Carrier ABC Groups Page (Empty) 438
Figure 213: Create ABC Group Wizard – Page 1 438
Figure 214: Create ABC Group Wizard – Page 2 439
Figure 215: Create ABC Group Wizard – Page 3 439
Figure 216: Create ABC Group Wizard – Selection Summary 441
Figure 217: Multi Carrier ABC Groups Page (Populated with Multiband Group) 441
Figure 218: Multi Carrier ABC Groups – Edit Group Page 442
Figure 219: Multi Carrier ABC Groups – Edit Members Page 442
Figure 220: Multi Carrier ABC Groups – Add/Remove Members Page 443
Figure 221: Multiband Configuration with Direct Inband Management to the Attached Unit via a Separate Optical Cable 444
Figure 222: Multiband Configuration with Direct Inband Management to the Paired Unit 445
Figure 223: Multiband Configuration with Out-of-Band Management to Both Units 446
Figure 224 Multiband Configuration with SyncE – Single Cable for SyncE 448
Figure 225 Multiband Configuration with SyncE – Separate Cable for SyncE 448
Figure 226: Multiband with Layer 1 Link Bonding – Multiband Antenna 451
Figure 227: Multiband with Layer 1 Link Bonding – Separate Antenna 451
Figure 228: Multiband with Layer 1 Link Bonding and Line Redundancy – Multiband Antenna 453
Figure 229: Multiband with Layer 1 Link Bonding and Line Redundancy – Separate Antennas 453
Figure 230: Link Bonding Page (Empty) 455
Figure 231: Link Bonding Group Wizard – Page 1 455
Figure 232: Link Bonding Group Wizard – Radio Member 456
Figure 233: Link Bonding Group Wizard – Ethernet Member 456
Figure 234: Link Bonding Group Wizard – Selection Summary Page 457
Figure 235: Link Bonding Page (Populated) 457
Figure 236: Link Bonding Groups – Edit Members Page 457
Figure 237: Link Bonding – Members Bandwidth Control Page 460
Figure 238: Bandwidth Notification Page (Empty) 460

Figure 239: Bandwidth Notification – Add Page....461
Figure 240: Bandwidth Notification Page (Populated with Radio BNM)....461
Figure 241: Radio Ethernet Interface Configuration Page (PTP 850E)....464
Figure 242: Link Bonding Groups – Edit Page....465
Figure 243: Link Bonding Groups – Member Statistics Page....465
Figure 244: Link Bonding Groups – Member Statistics Page....466
Figure 245: 2+0 XPIC Configuration - Direct Mount (with Link Bonding)....468
Figure 246: 2+0 XPIC Configuration – Integrated Antenna (with Link Bonding)....469
Figure 247 2+0 XPIC Configuration – Direct Mount....470
Figure 248 2+0 XPIC Configuration – Integrated Antenna....470
Figure 249: Link Bonding Page (Empty)....472
Figure 250: Link Bonding Group Wizard....472
Figure 251: Link Bonding Group Wizard....472
Figure 252: Link Bonding Group Wizard....473
Figure 253: Link Bonding Group Wizard – Selection Summary Page....473
Figure 254: Link Bonding Page (Populated)....474
Figure 255: Link Bonding Groups – Edit Members Page....474
Figure 256: Link Bonding – Members Bandwidth Control Page....477
Figure 257: Bandwidth Notification Page (Empty)....477
Figure 258: Bandwidth Notification – Add Page....478
Figure 259: Bandwidth Notification Page (Populated with Radio BNM)....478
Figure 260: Link Bonding Groups – Edit Page....483
Figure 261: Link Bonding Groups – Member Statistics Page....483
Figure 262: Link Bonding Groups – Member Statistics Page....484
Figure 263 Advanced Multi Carrier Configuration Page....485
Figure 264 AMCC Group – Select Group Parameters Page....485
Figure 265 AMCC Group – Select Member Parameters Page....486
Figure 266 AMCC Group – Select MRMC Parameters Page....486
Figure 267 AMCC Group – Selection Summary Page....487
Figure 268 Advanced Multi Carrier Configuration Page (Populated)....488
Figure 269 AMCC Group – Edit Page....488
Figure 270 Advanced Multi Carrier Configuration Page (Populated) – PTP 850C....494
Figure 271 Advanced Multi Carrier Configuration Page (Populated) – PTP 850E....494
Figure 272: Line Redundancy Page (Main Unit)....495
Figure 273: Line Redundancy Page (Attached Unit)....496
Figure 274: Line Redundancy Page (Attached Unit)....498
Figure 275: Line Redundancy Page – Management View Mode....499

Figure 276: Management Splitter Connection 501
Figure 277: Logical Interfaces – Edit Page 504
Figure 278: Management Interface Configuration Page 505
Figure 279: Unit Redundancy Page 505
Figure 280: Unit Redundancy Page when Redundancy Enabled 506
Figure 281: Standby Tab of Radio Parameters Page 508
Figure 282: Unit Redundancy Page 509
Figure 283 Create LAG Group – Page 1 513
Figure 284 Create LAG Group – Final Page 513
Figure 285 Link Aggregation - Edit Page 514
Figure 286: Link Aggregation – Add/Remove Members Page 514
Figure 287 LAG Distribution Function (DF) Page 517
Figure 288 LACP Aggregation Page 519
Figure 289 LACP Port Status Page 520
Figure 290 *LACP Port Status – View Page* 521
Figure 291 LACP Port Statistics Page 523
Figure 292 LACP Port Debug Page 524
Figure 293 Local Networking Configuration Page 527
Figure 294 Remote Networking Configuration Page 527
Figure 295 SNMP Parameters Page 529
Figure 296 V3 Users Page 530
Figure 297 V3 Users - Add Page 531
Figure 298 Trap Managers Page 532
Figure 299 Trap Managers - Edit Page 533
Figure 300 FileZilla Server User Configuration 536
Figure 301 FileZilla Server Shared Folder Setup 537
Figure 302 FTP Port Page 538
Figure 303 Versions Page 538
Figure 304 Download & Install Page – HTTP/ HTTPS Download – No File Selected 541
Figure 305 Download & Install page – HTTP/ HTTPS Download – File Selected 541
Figure 306 Download & Install Page - FTP 542
Figure 307 FTP Parameters Page 543
Figure 308 Install parameters Page 547
Figure 309 Install parameters page- Software Management Timer 547
Figure 310 Backup Files Page 549
Figure 311 Configuration Management Page 550
Figure 312 FTP Parameters Page 550

Figure 313 Configuration Management Page – HTTP/HTTPS 553
Figure 314: Chassis Configuration Page – PTP 850C 558
Figure 315: Chassis Configuration Page – PTP 850E 558
Figure 316 Unit Parameters Page 560
Figure 317 NTP Configuration Page 563
Figure 318: NTP Configuration Edit Page (Disabled) 563
Figure 319: NTP Configuration Edit Page (Enabled) 565
Figure 320 Inventory Page 566
Figure 321 SFP Transceiver Inventory and DDM Page 568
Figure 322 SFP PM Report Page 571
Figure 323: SFP RX Power Thresholds Configuration – Edit Page (PTP 850C) 571
Figure 324 Login Banner Page 573
Figure 325 Radio Parameters Page 575
Figure 326 Radio Parameters Page – PTP 850C 576
Figure 327 Radio Parameters Page – PTP 850S 577
Figure 328 Radio Parameters Page – PTP 850E 578
Figure 329 Remote Radio Parameters Page (PTP 850E) 580
Figure 330 ATPC Page 582
Figure 331 Radio Ethernet Interface Configuration Page 584
Figure 332 Radio Ethernet Interface Counters Page 586
Figure 333 Payload Encryption Page 589
Figure 334 Radio Payload Encryption Page with Master Key Displayed 590
Figure 335 Radio BER Thresholds Page 592
Figure 336 MRMC Status Page 593
Figure 337 MRMC PM Report Page 595
Figure 338 Counters Page 597
Figure 339 Signal Level PM Report Page 598
Figure 340 Signal Level Thresholds Configuration - Edit Page 599
Figure 341 Aggregate PM Report Page 600
Figure 342 MSE PM Report Page 602
Figure 343 Modem MSE Thresholds Configuration – Edit Page 603
Figure 344 XPI PM Report Page 604
Figure 345 XPI Thresholds Configuration – Edit Page 605
Figure 346 Capacity PM Report Page 606
Figure 347 Ethernet Radio Capacity and Throughput Threshold Page 607
Figure 348 Utilization PM Report Page 608
Figure 349 Ethernet Radio Utilization Threshold Page 609

Figure 350 Frame Error PM Report Page 610
Figure 351 Radio Ethernet Interface Counters Page 612
Figure 352 Ethernet Services Page 616
Figure 353 Ethernet Services - Add page 618
Figure 354 Multiple Selection Operation Section (Ethernet Services) 620
Figure 355 Ethernet Service Points Page 622
Figure 356 Ethernet Service Points Page – Ingress Attributes 626
Figure 357 Ethernet Service Points Page – Egress Attributes 627
Figure 358 Ethernet Service Points - Add Page 631
Figure 359 Attached VLAN List Page 633
Figure 360 Attached VLAN List - Add Page 633
Figure 361 Ethernet General Configuration Page 635
Figure 362: QSFP Module Configuration Page 638
Figure 363: Physical Interfaces Page – PTP 850C 639
Figure 364: Physical Interfaces Page – PTP 850E 639
Figure 365 Physical Interfaces - Edit Page 640
Figure 366 Automatic State Propagation Page 644
Figure 367 Automatic State Propagation - Add Page 644
Figure 368 RMON Page PTP 850C 646
Figure 369 RMON Page PTP 850E 647
Figure 370 RMON Page – Hiding and Displaying Columns 647
Figure 371 Egress Cos Statistics Page 649
Figure 372 Egress CoS Statistics – Edit Page 650
Figure 373 Ethernet Port TX PM Report Page 650
Figure 374 Ethernet PM Port Admin Page 652
Figure 375 Ethernet Port Tx Threshold Page 653
Figure 376: Ethernet Port RX PM Report Page 654
Figure 377 Ethernet PM Port Admin Page 655
Figure 378 Ethernet Port Rx Threshold Page 655
Figure 379 QoS Block Diagram 657
Figure 380: Standard QoS and H-QoS Comparison 659
Figure 381 Logical Interfaces Page-PTP 850C 662
Figure 382 Logical Interfaces - Edit Page 664
Figure 383 802.1Q Classification Page 666
Figure 384 802.1Q Classification - Edit Page 666
Figure 385 802.1AD Classification Page 667
Figure 386 802.1Q Classification - Edit Page 667

Figure 387 DSCP Classification Page 668
Figure 388 DSCP Classification - Edit Page 670
Figure 389 MPLS Classification Page 671
Figure 390 MPLS Classification - Edit Page 672
Figure 391 MAC DA Classification – Add Page 674
Figure 392 MAC DA Classification – Edit Page 674
Figure 393 Policer Profile Page 676
Figure 394 Policer Profile - Add Page 676
Figure 395 Logical Interfaces – Policers Page – Unicast Policer (Default) 678
Figure 396 Logical Interfaces – Policers Page – Multicast Policer 680
Figure 397: Logical Interfaces – Policers Page – Multicast Policer 681
Figure 398: Logical Interfaces – Policers Page – Unknown Multicast Policer 682
Figure 399 Logical Interfaces – Policers Page – Broadcast Policer 682
Figure 400 Logical Interfaces – Policers Page – Ethertype Policer 684
Figure 401 802.1Q Marking Page 687
Figure 402 802.1Q Marking - Edit Page 687
Figure 403 802.1AD Marking Page 688
Figure 404 802.1AD Marking - Edit Page 688
Figure 405 WRED Profile Page 690
Figure 406 WRED Profile - Add Page 690
Figure 407 Logical Interfaces – WRED Page 692
Figure 408: Logical Interfaces – WRED - Edit Page 692
Figure 409 Queue Shaper Profile Page 693
Figure 410 Queue Shaper Profile – Add Page 694
Figure 411 Service Bundle Shaper Profile Page 697
Figure 412 Logical Interfaces – Shaper – Egress Queue Shaper 698
Figure 413 Logical Interfaces – Egress Queue Shaper Configuration – Add Page 699
Figure 414 Scheduler Priority Profile Page 701
Figure 415 Scheduler Priority Profile – Add Page 701
Figure 416 Scheduler WFQ Profile Page 705
Figure 417 Scheduler WFQ Profile – Add Page 705
Figure 418 Logical Interfaces – Scheduler – Egress Port Scheduling Priority 707
Figure 419 Logical Interfaces – Scheduler – Egress Port Scheduling Queue WFQ 707
Figure 420: Logical Interfaces – Scheduler – Egress Port Scheduling Service Bundle WFQ 709
Figure 421: Logical Interfaces Page – Edit (QoS Mode) 711
Figure 422 Egress CoS PM Configuration Page 713
Figure 423 Egress CoS PM Configuration – Add Page 714

Figure 424 Egress CoS PM Page....715
Figure 425 Bandwidth Notification Page....749
Figure 426 Bandwidth Notification – Add Page....749
Figure 427 Bandwidth Notification - Statistics Page (ETH-BN)....751
Figure 428 LLDP Remote System Management Page....753
Figure 429 LLDP Configuration Parameters Page....755
Figure 430 LLDP Port Configuration Page....756
Figure 431 LLDP Port Configuration - Edit Page....757
Figure 432 LLDP Destination Address Table Page....758
Figure 433 LLDP Management TLV Configuration Page....759
Figure 434 LLDP Remote System Management Page....760
Figure 435 LLDP Local System Parameters Page....761
Figure 436 LLDP Local System Port Page....763
Figure 437 LLDP Local System Management Page....764
Figure 438 LLDP Local System Management – View Page....764
Figure 439 LLDP Statistic Page....765
Figure 440 LLDP Port TX Statistics Page....767
Figure 441 LLDP Port RX Statistics Page....768
Figure 442 Sync Source Page....771
Figure 443 Sync Source – Add Page....772
Figure 444 Outgoing Clock Page....775
Figure 445 Outgoing Clock – Edit Page....775
Figure 446 1588 Transparent Clock – Edit Page....778
Figure 447 1588 Boundary Clock – Port Parameters Page....780
Figure 448 1588 Boundary Clock – Port Parameters – Edit Page....780
Figure 449 1588 Boundary Clock – Clock Default Parameters Page....782
Figure 450 Boundary Clock Default Parameters....783
Figure 451 1588 Boundary Clock – Clock Advanced Parameters Page....784
Figure 452 1588 Boundary Clock – Port Statistics Page....786
Figure 453 Quick Configuration Security General Parameters Page....790
Figure 454 Quick Configuration Security Protocols Page....791
Figure 455 Quick Configuration Security Access Control Page....792
Figure 456 Quick Configuration Security RSA Key & Certificate Page....793
Figure 457 Access Control General Configuration Page....793
Figure 458 Access Control User Accounts - Edit Page....794
Figure 459 Access Control Password Management Page....795
Figure 460 Protocols Control Page....796

Figure 461 Access Control User Profiles Page 798
Figure 462 Access Control User Profiles - Add Page 800
Figure 463: Access Control User Accounts Page 801
Figure 464: Access Control User Accounts - Add Page 802
Figure 465: Access Control User Accounts - Edit Page 803
Figure 466: Access Control User Accounts - Edit Page (User Blocked) 804
Figure 467 Remote Access Control Configuration Page (RADIUS) 805
Figure 468 Radius Configuration – Edit Page 806
Figure 469 Server Manager – Creating User Groups 808
Figure 470 Server Manager – Creating Users 809
Figure 471 Server Manager – User Password Settings 810
Figure 472 Server Manager – Creating a RADIUS Client 811
Figure 473 Create Network Policy – Specify Name and Connection Type 812
Figure 474 Create Network Policy – Select Condition 813
Figure 475 Create Network Policy – User Group added to Policy's Conditions 813
Figure 476 Create Network Policy – Specifying Access Permission 814
Figure 477 Create Network Policy – Configuring Authentication Methods 815
Figure 478 Create Network Policy – Insecure Authentication Method Query 815
Figure 479 Create Network Policy – Configuring Constraints 816
Figure 480 Create Network Policy – Configuring Settings 817
Figure 481 Create Network Policy – Adding Vendor Specific Attributes 818
Figure 482 Create Network Policy – Selecting to Add Attribute Information 818
Figure 483 Create Network Policy – Specifying the Vendor 819
Figure 484 Create Network Policy – Configuring Vendor-Specific Attribute Information 820
Figure 485 Create Network Policy – Stopping/Starting NPS Services 821
Figure 486: Remote Access Control Configuration Page (TACACS+) 827
Figure 487: TACACS+ Configuration – Edit Page 828
Figure 488 Remote Access Users Page 832
Figure 489 Remote Access Users Table - View 832
Figure 490 Security Certificate Request Page 834
Figure 491 FTP Parameters Page (Security Certificate Request) 835
Figure 492 Security Certification Download and Install Page 836
Figure 493 FTP Parameters Page (Security Certification Download & Install) 836
Figure 494 RSA Key Download & Install Page (HTTP Selected) 839
Figure 495 RSA Key Download & Install Page (FTP Selected) 840
Figure 496 FTP Parameters Page 840
Figure 497 Protocols Control Page 842

Figure 498: Access Control List Configuration Page 843
Figure 499: Access Control List Configuration for IPv4 - Add 844
Figure 500: Access Control List Configuration for IPv6 - Add 844
Figure 501: Access Control List Configuration Page – Failsafe Timer 845
Figure 502 Security Log Upload Page 845
Figure 503 FTP Parameters Page (Security Log Upload) 847
Figure 504 Configuration Log Upload Page 848
Figure 505 Configuration Log Upload Page 850
Figure 506 Security General Configuration Page 852
Figure 507: SSO Login Page 853
Figure 508: SSO Logout Page 854
Figure 509: SSO Page 854
Figure 510 Current Alarms Page 856
Figure 511 Current Alarms - View Page 857
Figure 512 Alarm Statistics Page 858
Figure 513 Event Log 859
Figure 514 Alarm Configuration Page 860
Figure 515 Alarm Configuration Page – Expanded 862
Figure 516 Alarm Configuration - Edit Page 862
Figure 517: Alarm Configuration – Edit Page 864
Figure 518 Voltage Alarm Configuration Page 865
Figure 519 Voltage Alarm Configuration – Edit Page 866
Figure 520 Voltage PM Report Page 866
Figure 521: Unit Info Page – HTTP/HTTPS Upload 868
Figure 522: Unit Info Page – FTP/SFTP Upload 869
Figure 523: FTP Parameters Page 870
Figure 524: Remote SysLog Server Configuration Page 873
Figure 525: Remote SysLog Server Configuration Page – Edit 874
Figure 526 Radio Loopbacks Page 875
Figure 527 Logical Interfaces – Loopback Page 876
Figure 528 SOAM MD Page 878
Figure 529 SOAM MD Page 878
Figure 530 SOAM MA/MEG Page 879
Figure 531 SOAM MA/MEG – Add Page 881
Figure 532 MEP List Page 884
Figure 533 Add MEP Page 884
Figure 534 SOAM MEP Page 885

Figure 535 Add SOAM MEP Wizard – Page 1 885
Figure 536 Add SOAM MEP Wizard – Page 2 886
Figure 537 Add SOAM MEP Wizard –Summary Page 886
Figure 538 SOAM MEP - Edit Page 888
Figure 539 SOAM MEP DB Table 890
Figure 540 MEP Last Invalid CCMS Page 891
Figure 541 SOAM MEP Loopback Page 893
Figure 542 Restart HTTP Page 896
Figure 543 ifIndex Calculator Page 896
Figure 544 MIB Reference Table Page 897
Figure 545: Radio Ethernet Interface Configuration Page (PTP 850C) 959
Figure 546 1588 Boundary Clock – Current Configuration Sample Display (CLI) 1345
Figure 547 1588 Boundary Clock – Default Parameters Sample Display (CLI) 1346
Figure 548 1588 Boundary Clock – Advanced (General) Parameters Sample Display (CLI) 1347
Figure 549 1588 Boundary Clock – Time Parameters Sample Display (CLI) 1347
Figure 550 1588 Boundary Clock Port Parameters (CLI) 1349
Figure 551 1588 Boundary Clock Statistics (CLI) 1352
Figure 552 PTP 850E Interfaces 1425
Figure 553: RSL Pins 1427
Figure 554: PoE Injector Connectors 1435

List of Tables

Table 1 Web EMS Menu Hierarchy – Platform Menu 76
Table 2 Web EMS Menu Hierarchy – Faults Menu 79
Table 3 Web EMS Menu Hierarchy – Radio Menu 79
Table 4 Web EMS Menu Hierarchy – Ethernet Menu 80
Table 5 Web EMS Menu Hierarchy – Sync Menu 84
Table 6 Web EMS Menu Hierarchy – Quick Configuration Menu 84
Table 7 Web EMS Menu Hierarchy – Utilities Menu 85
Table 8 Activation Key Status Parameters 109
Table 9 Activation Key-Enabled-Features Table Parameters 111
Table 10 Activation Key-Enabled-Features Description 113
Table 11 Time Services Parameters 121
Table 12 MRMC Symmetrical Scripts Page Parameters 136
Table 13 Available Radio Profiles – PTP 850E (62.5 MHz and 125 MHz) 139
Table 14 Available Radio Profiles – PTP 850E (250 MHz to 2000 MHz – XPIC) 139
Table 15 System Configurations 161
Table 16: Cable for External Management Redundancy 246
Table 17: L1 Header Compensation for Ethernet Interface Connected to PTP 850E or PTP 850EX 366
Table 18: L1Header Compensation for Ethernet Interface Connected to PTP 820C/PTP 820C-HP 367
Table 19: L1Header Compensation for Ethernet Interface Connected to Third-Party Devices 381
Table 20: L2 Header Compensation for Link Bonding Group Members 383
Table 21: Link Bonding Line Redundancy Status Parameters 413
Table 22: L1 Header Compensation for Radio Interface (PTP 850E-PTP 850C Multiband Configuration) 458
Table 23: L1 Header Compensation for Radio Interface (PTP 850E XPIC Configuration) 474
Table 24: Management Cables for Unit Redundancy 501
Table 25 LACP Aggregation Status Parameters 519
Table 26 LACP Port Status Parameters 521
Table 27 LACP Port Statistics 523
Table 28 LACP Port Debug Statistics 524
Table 29 SNMP V3 Authentication Parameters 531
Table 30 Trap Manager Parameters 533
Table 31 Software Versions Page Columns 539
Table 32 Download & Install Status Parameters 546
Table 33 Backup Files Page Columns 549
Table 34 Unit Parameters 561
Table 35 NTP Status Parameters 565

Table 36 SFP Inventory Parameters 569
Table 37 SFP Digital Diagnostic Monitoring (DDM) Parameters 570
Table 38 DDM PMs 572
Table 39 Radio Status Parameters 579
Table 40 Remote Radio Parameters 581
Table 41 Radio Ethernet Interface Counters Fields 586
Table 42 MRMC Status Parameters 594
Table 43 MRMC PMs 596
Table 44 Signal Level PMs 598
Table 45 Signal Level Thresholds 600
Table 46 Modem BER (Aggregate) PMs 601
Table 47 Modem MSE PMs 602
Table 48 XPI PMs 604
Table 49 Capacity/Throughput PMs 607
Table 50 Utilization PMs 609
Table 51 Frame Error Rate PMs 610
Table 52 Ethernet Interface Counter Fields 612
Table 53 Ethernet Services Page Parameters 617
Table 54 General Service Point Attributes 622
Table 55 Attached Interface Types 624
Table 56 Service Point Ingress Attributes 626
Table 57 Service Point Egress Attributes 627
Table 58 VLAN Classification Parameters 634
Table 59 Ethernet Interface Speed and Auto-Negotiation Options – PTP 850C 641
Table 60 Ethernet Interface Speed and Auto-Negotiation Options – PTP 850S 641
Table 61 Physical Interface Status Parameters 643
Table 62 Ethernet TX Port PMs 651
Table 63 Ethernet RX Port PMs 654
Table 64 Logical Interfaces Page-PTP 850S 662
Table 65 Logical Interfaces Page-PTP 850E 662
Table 66 Logical Interface Classification Parameters 664
Table 67 Policer Profile Parameters 677
Table 68 Queue Shaper Profile Parameters 694
Table 69 WFQ Profile Example 704
Table 70 ETH-BN Status Parameters 750
Table 71 ETH-BN Entity Statistics Parameters 752
Table 72 LLDP Remote System Management Parameters 754

Table 73 LLDP Read-Only Configuration Parameters....755
Table 74 LLDP Port Configuration Status Parameters....757
Table 75 LLDP Management TLV Parameters....759
Table 76 LLDP Remote System Management Parameters....760
Table 77 LLDP Local System Parameters....761
Table 78 LLDP Local System Port Parameters....763
Table 79 LLDP Local System Management Parameters....765
Table 80 LLDP Statistics....766
Table 81 LLDP Port TX Statistics....767
Table 82 LLDP Port RX Statistics....768
Table 83 Sync Source Parameters....771
Table 84 Boundary Clock Advanced Parameters....784
Table 85 Boundary Clock Port Parameters....785
Table 86 Boundary Clock Port Statistics....786
Table 87 RSA File Download & Install Status Parameters....841
Table 88 Alarm Information....858
Table 89 Event Log Information....859
Table 90 Alarm Configuration Page Parameters....861
Table 91 Voltage PMs....867
Table 92: Syslog Severity Values....872
Table 93 SOAM MA/MEG Configuration Parameters....881
Table 94 SOAM MA/MEG Status Parameters....883
Table 95 SOAM MEP Parameters....887
Table 96 SOAM MEP DB Table Parameters....890
Table 97 IP Address (IPv4) CLI Parameters....903
Table 98 IP Address (IPv6) CLI Parameters....905
Table 99 Local Time Configuration CLI Parameters....908
Table 100: Daylight Savings Time CLI Parameters....910
Table 101 Interface Configuration CLI Parameters....925
Table 102 MRMC Script CLI Parameters....928
Table 103: MRMC Script Assignation to Radio Carrier CLI Parameters....930
Table 104 System Configurations (CLI)....950
Table 105: LAG Group CLI Parameters....1020
Table 106: LACP Aggregation Status Parameters (CLI)....1025
Table 107: LACP Port Status Parameters (CLI)....1026
Table 108: LACP Port Statistics (CLI)....1028
Table 109 Remote Unit IP Address (IPv4) CLI Parameters....1031

Table 110 Remote Unit IP Address (IPv6) CLI Parameters 1032
Table 111 Basic SNMP CLI Parameters 1033
Table 112 SNMPv3 CLI Parameters 1034
Table 113 Trap Managers CLI Parameters 1036
Table 114 Software Download CLI Parameters 1040
Table 115 Configuration Management CLI Parameters 1045
Table 116 Configuration Backup and Restore CLI Parameters 1046
Table 117 Configuration Import and Restore CLI Parameters 1047
Table 118 Unit Parameters CLI Parameters 1050
Table 119: NTP CLI Parameters 1052
Table 120 SFP Inventory Parameters (CLI) 1056
Table 121 SFP Digital Diagnostic Monitoring (DDM) Parameters (CLI) 1058
Table 122 Remote Radio Mute/Unmute CLI Parameters 1066
Table 123 Remote Radio TX Level CLI Parameters 1068
Table 124 Remote Radio ATPC CLI Parameters 1068
Table 125 Radio ATPC CLI Parameters 1071
Table 126 Header De-Duplication CLI Parameters 1072
Table 127 Aggregate PMs (CLI) 1080
Table 128 Excessive BER CLI Parameters 1082
Table 129 RSL Thresholds CLI Parameters 1082
Table 130 TSL Thresholds CLI Parameters 1083
Table 131 RSL and TSL PMs (CLI) 1084
Table 132 Signal Level Threshold CLI Parameters 1085
Table 133 MSE CLI Parameters 1085
Table 134 MSE PMs (CLI) 1087
Table 135: Capacity/Throughput PMs (CLI) 1096
Table 136: Throughput PMs (CLI) 1098
Table 137: Utilization PMs (CLI) 1101
Table 138 Adding Ethernet Service CLI Parameters 1104
Table 139 Entering Ethernet Service View CLI Parameters 1106
Table 140 Displaying Ethernet Service Details CLI Parameters 1107
Table 141 Ethernet Service Operational State CLI Parameters 1107
Table 142 Ethernet Service CoS Mode CLI Parameters 1108
Table 143 Ethernet Service EVC CLI Parameters 1109
Table 144 Deleting Ethernet Service CLI Parameters 1109
Table 145 Service Points per Service Type 1111
Table 146 Service Point Types per Interface 1111

Table 147 Legal Service Point – Interface Type Combinations per Interface – SAP and SNP 1112
Table 148 Legal Service Point – Interface Type Combinations per Interface – Pipe and MNG 1113
Table 149 Add Service Point CLI Parameters 1116
Table 150 Enable/Disable Broadcast Frames CLI Parameters 1120
Table 151 Service Point CoS Preservation CLI Parameters 1121
Table 152 Service Point Enable/Disable Flooding CLI Parameters 1122
Table 153 C-VLAN CoS Preservation Mode CLI Parameters 1124
Table 154 C-VLAN Preservation CLI Parameters 1124
Table 155 S-VLAN CoS Preservation CLI Parameters 1126
Table 156 Service Bundle CLI Parameters 1127
Table 157 VLAN Bundle to Service Point CLI Parameters 1128
Table 158 Display Service Point Attributes CLI Parameters 1128
Table 159 Delete Service Point Attributes CLI Parameters 1130
Table 160 MAC Address Forwarding Table Maximum Size CLI Parameters 1133
Table 161 MAC Address Forwarding Table Aging Time CLI Parameters 1133
Table 162 Adding Static Address to MAC Address Forwarding Table CLI Parameters 1134
Table 163 Enabling MAC Address Learning CLI Parameters 1138
Table 164 Configure S-VLAN Ethertype CLI Parameters 1139
Table 165 Configure MRU CLI Parameters 1140
Table 166 Entering Interface View CLI Parameters 1141
Table 167 Interface Media Type CLI Parameters 1144
Table 168 Interface Speed and Duplex State CLI Parameters 1144
Table 169 Interface Auto Negotiation State CLI Parameters 1145
Table 170 Interface IFG CLI Parameters 1146
Table 171 Interface Preamble CLI Parameters 1146
Table 172 Interface Description CLI Parameters 1147
Table 173: Automatic State Propagation to an Ethernet Port CLI Parameters 1150
Table 174 RMON Statistics CLI Parameters 1161
Table 175 Port PM Thresholds CLI Parameters 1162
Table 176 Ethernet Port PMs 1164
Table 177: Link Bonding PMs (CLI) 1169
Table 178 VLAN Classification and Override CLI Parameters 1173
Table 179 DSCP Classification Table Default Values 1176
Table 180 Modify DSCP Classification Table CLI Parameters 1177
Table 181 Trust Mode for MPLS CLI Parameters 1178
Table 182 MPLS EXP Bit Classification Table Default Values 1178
Table 183 MPLS EXP Bit Classification Table Modification CLI Parameters 1179

Table 184: 802.1p Trust Mode CLI Parameters 1179
Table 185: C-VLAN 802.1 UP and CFI Bit Classification Table Default Values 1181
Table 186: C-VLAN 802.1 UP and CFI Bit Classification Table CLI Parameters 1182
Table 187: S-VLAN 802.1 UP and DEI Bit Classification Table Default Values 1185
Table 188: S-VLAN 802.1 UP and DEI Bit Classification Table CLI Parameters 1187
Table 189 Default CoS CLI Parameters 1191
Table 190 Rate Meter Profile CLI Parameters 1194
Table 191 Assigning Rate Meter for Unicast Traffic CLI Parameters 1197
Table 192: Assigning Rate Meter for Unknown Unicast Traffic CLI Parameters 1198
Table 193 Assigning Rate Meter for Multicast Traffic CLI Parameters 1203
Table 194: Assigning Rate Meter for Multicast Traffic CLI Parameters 1204
Table 195 Assigning Rate Meter for Broadcast Traffic CLI Parameters 1209
Table 196 Assigning Rate Meter per Ethertype CLI Parameters 1210
Table 197 Assigning Line Compensation Value for Rate Meter CLI Parameters 1212
Table 198 Marking Mode on Service Point CLI Parameters 1215
Table 199 Marking Table for C-VLAN UP Bits 1216
Table 200 802.1q CoS and Color to UP and CFI Bit Mapping Table CLI Parameters 1217
Table 201 802.1ad UP Marking Table (S-VLAN) 1218
Table 202 802.1ad UP Marking Table (S-VLAN) CLI Parameters 1219
Table 203 WRED Profile CLI Parameters 1220
Table 204 Assigning WRED Profile to Queue CLI Parameters 1222
Table 205: Queue Shaper Profiles CLI Parameters 1224
Table 206 Attaching Shaper Profile to Queue CLI Parameters 1229
Table 207 Egress Line Compensation for Shaping CLI Parameters 1230
Table 208 Interface Priority Profile Example 1255
Table 209 Interface Priority Profile CLI Parameters 1256
Table 210 Interface Priority Sample Profile Parameters 1257
Table 211 Attaching Priority Profile to Interface CLI Parameters 1258
Table 212 WFQ Profile Example 1259
Table 213 WFQ Profile CLI Parameters 1262
Table 214 WFQ Sample Profile Parameters 1263
Table 215 Attaching WFQ Profile to Interface CLI Parameters 1264
Table 216 Egress Queue Level PMs CLI Parameters 1267
Table 217 Egress Service Bundle Level PMs CLI Parameters 1271
Table 218 ETH-BN Entity CLI Parameters 1309
Table 219 Sync Source Ethernet CLI Parameters 1326
Table 220 Sync Source Radio CLI Parameters 1328

Table 221 Outgoing Clock CLI Parameters 1332
Table 222: Synchronization Revertive Timer CLI Parameters 1333
Table 223 Boundary Clock Configuration CLI Parameters 1340
Table 224 Boundary Clock Default Settings – CLI Parameters 1346
Table 225 Boundary Clock Default Parameters 1346
Table 226 Boundary Clock Advanced Parameters (CLI) 1348
Table 227 Boundary Clock Port Parameters (CLI) 1349
Table 228 Boundary Clock Configuration CLI Parameters 1350
Table 229 Boundary Clock Port Statistics (CLI) 1352
Table 230 Inactivity Timeout Period CLI Parameters 1356
Table 231 Blocking Upon Login Failure CLI Parameters 1356
Table 232 Blocking Unused Accounts CLI Parameters 1357
Table 233 Password Aging CLI Parameters 1358
Table 234 Password Strength Enforcement CLI Parameters 1360
Table 235 Force Password Change on First Time Login CLI Parameters 1360
Table 236 User Profile CLI Parameters 1362
Table 237 User Profile Access Protocols CLI Parameters 1363
Table 238 User Accounts CLI Parameters 1365
Table 239 Activate RADIUS CLI Parameters 1366
Table 240 Configure RADIUS Server CLI Parameters 1366
Table 241 CSR Generation and Upload CLI Parameters 1369
Table 242 Certificate Download and Install CLI Parameters 1371
Table 243 RSA Key Download and Install CLI Parameters 1375
Table 244 Security Log CLI Parameters 1380
Table 245 Configuration Log CLI Parameters 1382
Table 246 Editing Alarm Text and Severity CLI Parameters 1386
Table 247 Restoring Alarms to Default CLI Parameters 1387
Table 248 Uploading Unit Info CLI Parameters 1391
Table 249 Radio Loopback CLI Parameters 1396
Table 250 Ethernet Loopback CLI Parameters 1397
Table 251 Maintenance Domain CLI Parameters 1399
Table 252 SOAM MEG CLI Configuration Parameters 1401
Table 253 MEP CLI Configuration Parameters 1405
Table 254 MEP and Remote MEP Status Parameters (CLI) 1407
Table 255 Loopback CLI Parameters 1412
Table 256 CW Mode CLI Parameters 1414
Table 257: PTP 850E MGT Interface - RJ-45/ Pinouts 1426

Table 258: PoE Injector PoE Port - RJ-45 Pinouts 1435
Table 259: PoE Injector RJ-45 Data Port Supporting 10/100/1000Base-T 1436

About This User Guide

This document explains how to configure and operate PTP 850 devices. This document applies to System release 13.0. For a full description of feature limitations per release, refer to the Release Notes for the System release you are using.

1.1.1 What You Should Know

Some features described in this manual may not be available in the current release. Please consult the Release Notes for the functionality supported in the specific release you are using.

1.1.2 Target Audience

This manual is intended for use by individuals responsible for configuration and administration of an PTP 850 system or network.

1.1.3 Related Documents

- PTP 850C Technical Description
- PTP 850E Technical Description
- PTP 850S Technical Description
- PTP 850C Installation Guide
- PTP 850E Installation Guide
- PTP 850S Installation Guide
- PTP 850 MIB Reference

This guide contains the following Chapters:

2Introduction

3Getting Started

4Configuration Guide

8Unit Management

9Radio Configuration

10Ethernet Services and Interfaces

11Quality of Service (QoS)

13Synchronization

14Access Management and Security

15Alarm Management and Troubleshooting

16 Web EMS Utilities

17Getting Started (CLI)

19Unit Management (CLI)

20Radio Configuration (CLI)s

21Ethernet Services and Interfaces (CLI)

22Quality of Service (QoS) (CLI)

24Synchronization (CLI)

25Access Management and Security (CLI)

26Alarm Management and Troubleshooting (CLI)

27Maintenance

28Alarms List

1.1.4 Contacting Cambium Networks

Support website:	https://support.cambiumnetworks.com
Main website:	http://www.cambiumnetworks.com
Sales enquiries:	solutions@cambiumnetworks.com
Support enquiries:	https://support.cambiumnetworks.com
Repair enquiries	https://support.cambiumnetworks.com
Telephone number list:	http://www.cambiumnetworks.com/support/contact-support

Support website:	https://support.cambiumnetworks.com
Address:	Cambium Networks Limited, Unit B2, Linhay Business Park, Eastern Road Ashburton, United Kingdom, TQ13 7UP

1.1.5 Purpose

Cambium Networks Point-To-Point (PTP) documents are intended to instruct and assist personnel in the operation, installation and maintenance of the Cambium Networks PTP equipment and ancillary devices. It is recommended that all personnel engaged in such activities be properly trained.

Cambium Networks disclaims all liability whatsoever, implied or express, for any risk of damage, loss or reduction in system performance arising directly or indirectly out of the failure of the customer, or anyone acting on the customer's behalf, to abide by the instructions, system parameters, or recommendations made in this document.

1.1.6 Cross references

References to external publications are shown in italics. Other cross references, emphasized in blue text in electronic versions, are active links to the references.

This document is divided into numbered chapters that are divided into sections. Sections are not numbered, but are individually named at the top of each page, and are listed in the table of contents.

1.1.7 Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents. Send feedback to support@cambiumnetworks.com.

1.2 Problems and warranty

1.2.1 Reporting problems

If any problems are encountered when installing or operating this equipment, follow this procedure to investigate and report:

1. Search this document and the software release notes of supported releases.
2. Visit the support website.
3. Ask for assistance from the Cambium Networks product supplier.
4. Gather information from affected units, such as any available diagnostic downloads.
5. Escalate the problem by emailing or telephoning support.

1.2.2 Repair and service

If unit failure is suspected, obtain details of the Return Material Authorization (RMA) process from the support website.

1.2.3 Hardware warranty

Cambium Networks's standard hardware warranty is for one (1) year from date of shipment from Cambium Networks or a Cambium distributor. Cambium Networks warrants that hardware will conform to the relevant published specifications and will be free from material defects in material and workmanship under normal use and service. Cambium shall within this time, at its own option, either repair or replace the defective product within thirty (30) days of receipt of the defective product. Repaired or replaced product will be subject to the original warranty period but not less than thirty (30) days.

To register PTP products or activate warranties, visit the support website. For warranty assistance, contact the reseller or distributor.



Caution

Using non-Cambium parts for repair could damage the equipment or void warranty. Contact Cambium for service and repair instructions.

Portions of Cambium equipment may be damaged from exposure to electrostatic discharge. Use precautions to prevent damage.

1.3 Security advice

Cambium Networks systems and equipment provide security parameters that can be configured by the operator based on their particular operating environment. Cambium recommends setting and using these parameters following industry recognized security practices. Security aspects to be considered are protecting the confidentiality, integrity, and availability of information and assets. Assets include the ability to communicate, information about the nature of the communications, and information about the parties involved.

In certain instances Cambium makes specific recommendations regarding security practices, however the implementation of these recommendations and final responsibility for the security of the system lies with the operator of the system.

1.4 Warnings, cautions, and notes

The following describes how warnings and cautions are used in this document and in all documents of the Cambium Networks document set.

1.4.1 Warnings

Warnings precede instructions that contain potentially hazardous situations. Warnings are used to alert the reader to possible hazards that could cause loss of life or physical injury. A warning has the following format:

Warning

Warning text and consequence for not following the instructions in the warning.

1.4.2 Cautions

Cautions precede instructions and are used when there is a possibility of damage to systems, software, or individual items of equipment within a system. However, this damage presents no danger to personnel. A caution has the following format:



Caution

Caution text and consequence for not following the instructions in the caution.

1.4.3 Notes

A note means that there is a possibility of an undesirable situation or provides additional information to help the reader understand a topic or concept. A note has the following format:

Note

Note text.

1.5 Caring for the environment

The following information describes national or regional requirements for the disposal of Cambium Networks supplied equipment and for the approved disposal of surplus packaging.

1.5.1 In EU countries

The following information is provided to enable regulatory compliance with the European Union (EU) directives identified and any amendments made to these directives when using Cambium equipment in EU countries.



1.5.1.1 Disposal of Cambium equipment

European Union (EU) Directive 2002/96/EC Waste Electrical and Electronic Equipment (WEEE)

Do not dispose of Cambium equipment in landfill sites. For disposal instructions, refer to http://www.cambiumnetworks.com/support

1.5.1.2 Disposal of surplus packaging

Do not dispose of surplus packaging in landfill sites. In the EU, it is the individual recipient's responsibility to ensure that packaging materials are collected and recycled according to the requirements of EU environmental law.

1.5.2 In non-EU countries

In non-EU countries, dispose of Cambium equipment and all surplus packaging in accordance with national and regional regulations.

2. Introduction

This section includes:

- PTP 850C Overview
- PTP 850S Overview
- PTP 850E Overview
- PoE Injector Overview
- Configuration Tips
- The Web-Based Element Management System
- Reference Guide to Web EMS Menu Structure

This user guide provides instructions for configuring and operating the following products:

- PTP 850C
- PTP 850S
- PTP 850E

Each of these products can be used with a Cambium Networks-approved PoE Injector.

Wherever applicable, the manual notes the specific distinctions between these products. The manual also notes when specific features are only applicable to certain products and not others.

2.1.1 PTP 850C Overview

PTP 850C is a MultiCore microwave radio suitable for all deployment scenarios. PTP 850 provides cutting-edge capabilities that enable operators to base entire networks, from small cells to massive aggregation sites, on this single product.

Cambium Networks's PTP 850C sets a new standard for microwave transmission, offering

16 Gbps switching capacity, channel spacing of up to 224 MHz1, and a wide range of modulations, from BPSK to 4096 QAM with ACM. These and other advanced capabilities are combined in PTP 850C with the full range of Cambium Networks's MultiCore technologies to produce an all-outdoor product that can be used throughout the microwave network, from small cells to massive aggregation sites.

The ability to use PTP 850C throughout the network offers the possibility of simplifying network deployment and maintenance by reducing complexity, costs, and time-to-revenue.

PTP 850C is easily and quickly deployable compared with fiber, enabling operators to achieve faster time to new revenue streams, lower total cost of ownership, and long-term peace of mind.

PTP 850C can deliver multi-Gbps capacity on a single frequency channel, setting a new standard for efficient spectrum use. PTP 850C's unique MultiCore radio architecture is based on an advanced parallel radio processing engine, built

---

1 224 MHz is planned for future release. With 224 MHz channels, PTP 850C will support up to 2 Gbps per carrier, for up to 8 Gbps in 4+0 Dualband configurations.

around Cambium Networks's in-house chipsets. The result is superior radio performance with reduced power consumption and form-factor.

Additionally, PTP 850C's MultiCore architecture enables operators to start with a single core with the option of enabling the second core remotely when network capacity requirements increase.

PTP 850C can be deployed as a stand-alone all-outdoor radio. In future releases, it will also be possible to use PTP 850C as an upgrade path to achieve the highest possible capacity of any existing link by utilizing Cambium Networks unique Layer 1 Carrier Bonding technique for Dualband configurations.[2]

2.1.2 PTP 850S Overview

PTP 850S features high capacity, while combining all the benefits of disaggregated wireless backhaul. A compact, cost-optimized universal radio, Cambium Networks PTP 850S considerably simplifies installation time and efforts on site to further accelerate the deployment of wireless broadband networks in rural and suburban areas.

PTP 850S operates over channels of 14 to 224 MHz3, with modulations of BPSK to 4096 QAM, enabling it to provide capacity of up to 2 Gbps over a single carrier.

The PTP 850S can be deployed as a stand-alone all-outdoor radio. In future System relase versions, it will also be possible to use PTP 850S as an upgrade path to achieve the highest possible capacity of any existing link by utilizing Cambium Networks unique Dualband Layer 1 Carrier Bonding. Cambium Networks unique Dualband engine enables the combination of any two microwave channels over the air, and significantly enhances the link's performance by optimizing traffic distribution between the two carriers. Retaining the same network configuration and cabling while upgrading existing links presents additional benefits to mobile operators and enables them to lower total cost of ownership.4

For a full description of the PTP 850S, including supported features and specifications, refer to the Technical Description for PTP 850S.

2.1.3 PTP 850E Overview

PTP 850E is a versatile high-capacity backhaul Ethernet system which operates in the E-band (71-76 GHz, 81-86 GHz). Its light weight and small footprint make it versatile for many different applications. Thanks to its small footprint, low power consumption, and simple installation, PTP 850E can be installed in many different types of remote outdoor locations.

PTP 850E operates over 62.5, 125, 250, 500, 750, 1000, 1250, 1500, 1750, and 2000

MHz channels to deliver up to 20 Gbps of Ethernet throughput in several system configurations.

2 With 224 MHz channels, PTP 850C will support up to 2 Gbps per carrier.

3 Dualband will provide configurations of up to 4+0, using two channels, with total capacity of up to 4 Gbps over 112 MHz channels or 8 MHz over 224 channels.

4 Dualband configurations are planned for future release.

2.2 System Overview

2.2.1 Configuration Tips

This section describes common issues and how to avoid them.

Ethernet Port configuration

The Ethernet ports of a PTP 850E are not enabled by default in a new unit. You must manually enable the Ethernet port or ports in order for the unit to process Ethernet traffic. See Enabling the Interfaces (Interface Manager)

For RJ-45 ports, it is recommended to enable Auto-Negotiation for both the local port and its peer in order to obtain optimal performance.

For SFP ports, it is recommended to disable Auto-Negotiation.

For instructions, see Configuring Ethernet Interfaces.

SyncE Interface Configuration

When configuring a Sync source or outgoing clock on an Ethernet interface, the Media Type of the interface must be RJ-45 or SFP, not Auto-Type. See Synchronization.

In-Band Management

In order to use in-band management with an external switch, it must be supported on the external switch.

When configuring in-band management, be sure to tag the management traffic to avoid overflow of the CPU.

If you are using 1588 Transparent Clock, make sure the Transparent Clock settings are symmetrical; that is, make sure Transparent Clock is either enabled or disabled on both sides of the link. To avoid loss of management, make sure to configure Transparent Clock on the remote side of the link first, then on the local side.

It is strongly recommended to assign the management service (1025) a CoS of 7 to ensure that management packets receive high priority and are not discarded in instances of network congestion.

For instructions on configuring in-band management on the PTP 850E, see Configuring in-Band Management.

Software Upgrade

When upgrading software via HTTP, make sure the software package is *not* unzipped. For instructions, see Upgrading the Software.

Configuration Management and Backup Restoration

Configuration files can only be copied to the same PTP 850 hardware type with the same part number as the unit from which they were originally saved. For example, a PTP 850E configuration file can only be restored to a PTP 850E with the same part number as the unit from which it was saved.

2.2.2 PTP 850E Overview

PTP 850E is a versatile high capacity backhaul Ethernet system which operates in the E-band (71-76 GHz, 81-86 GHz). Its light weight and small footprint make it versatile for many different applications. Thanks to its small footprint, low power consumption, and simple installation, PTP 850E can be installed in many different types of remote outdoor locations.

PTP 850E operates over 62.5, 125, 250, 500, 1000 and 2000 MHz channels to deliver up to 20 Gbps of Ethernet throughput in several system configurations.

For a full description of the PTP 850E, including supported features and specifications, refer to the *Technical Description for PTP 850E*.

2.2.3 PoE Injector Overview

The PoE injector box is designed to offer a single cable solution for connecting both data and the DC power supply to the PTP 850E. To do so, the PoE injector combines 48VDC input and GbE signals via a standard CAT5E cable using a proprietary design.

The PoE injector can be ordered with a DC feed protection and with +24VDC support, as well as EMC surge protection for both indoor and outdoor installation options. It can be mounted on poles, walls, or inside racks.



Note

An AC-power PoE Injector option is also available. Contact your Cambium representative for details.

Two models of the PoE Injector are available:

N000082L022A PTP 820 PoE Injector all outdoor, redundant DC input, +24VDC support

N000082L164A PTP 820C INDOOR AC POE INJECTOR, 90W

For power redundancy, a passive PoE injector is required. The following passive PoE Injector model is available for power redundancy:

AC_POE_STD_PWR_INDOOR – Includes one DC power port with a power input range of 90VAC to 264VAC.

2.2.4 The Web-Based Element Management System

This section includes:

- Introduction to the Web EMS
- Web EMS Page Layout
- Front Panel Representation
- Quick Password and Logout Icon
- Hiding Interfaces that are Admin Down
- Active, Standby, and Merged (All) Tabs
- Related Pages Drop-Down List
- Page Refresh and Refresh Interval
- Export to CSV Option
- Interactive User Guide
- Advanced Mode and Basic Mode
- Unit Summary Page
- Radio Summary Page
- The Security Summary Page

2.2.4.1 Introduction to the Web EMS

The Element Management System (Web EMS) is an HTTP web-based element manager that enables the operator to perform configuration operations and obtain statistical and performance information related to the system, including:

Configuration Management – Enables you to view and define configuration data.

Fault Monitoring – Enables you to view active alarms.

Performance Monitoring – Enables you to view and clear performance monitoring values and counters.

Diagnostics and Maintenance – Enables you to define and perform loop back tests and software updates.

Security Configuration – Enables you to configure security features.

User Management – Enables you to define users and user groups.

The Web EMS opens to a page that summarizes the key unit parameters. The next page, when scrolling down the Web EMS main menu, summarizes the key radio parameters. See The Unit Summary Page and **Error! Reference source not found.**.

A Web-Based EMS connection to the unit can be opened using a Web browser (Internet Explorer, Mozilla Firefox, or Google Chrome). The Web-Based EMS uses a graphical interface.

The Web-Based EMS shows the actual unit configuration and provides easy access to any interface. A wide range of configuration, testing, and system monitoring tasks can be performed through the Web EMS.

Note

The alarms and system configuration details shown in this manual do not necessarily represent actual parameters and values on a fully operating PTP 850E system. Some of the pages and tasks described in this Manual may not be available to all users, based on the actual system configuration, activation key, and other details.

2.2.4.2 Web EMS Page Layout

Each Web EMS page includes the following sections:

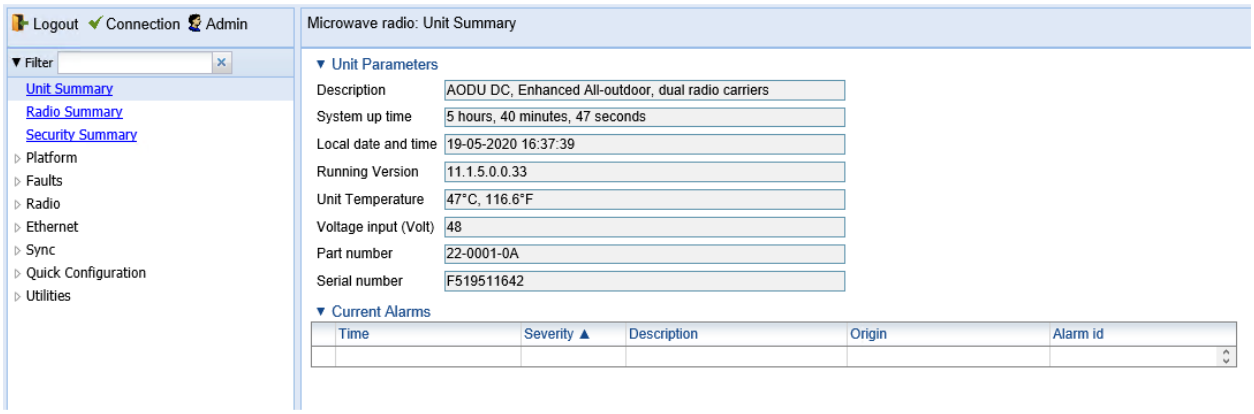
The left section of the page displays the Web EMS menu tree:

Click to display the sub-options under a menu item.

Click to hide the sub-options under a menu item.

The main section of the page provides the page's basic functionality.

Figure 1 Main Web EMS Page PTP 850C



Optionally, you can display a representation of the PTP 850 front panel by clicking either the arrow in the center or the arrow at the right of the bottom toolbar.

Figure 2 Main Web EMS Page – PTP 850S

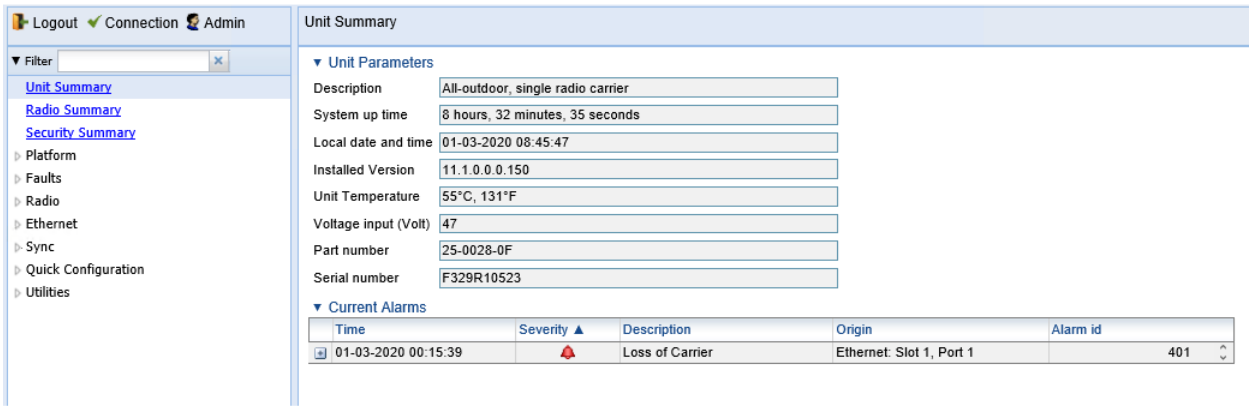
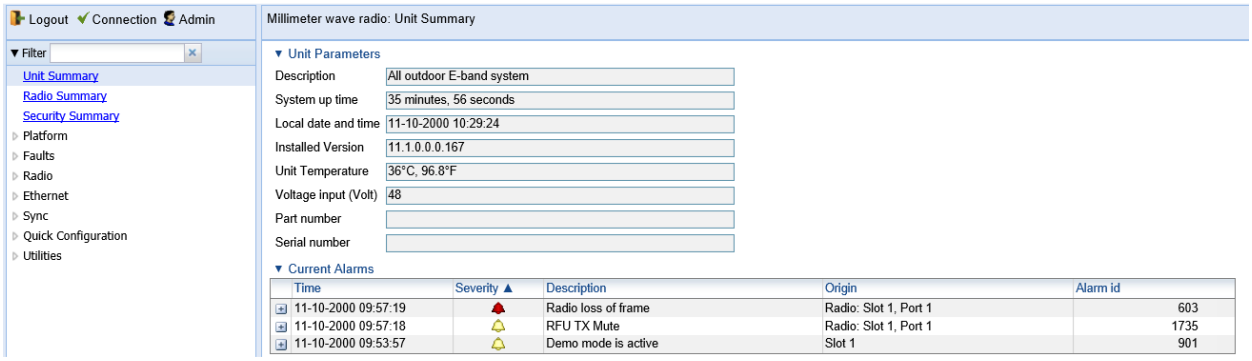


Figure 3 Main Web EMS Page – PTP 850E



2.2.4.3 Front Panel Representation

Optionally, you can display a representation of the PTP 850 front panel by clicking either the arrow in the center or the arrow at the right of the bottom toolbar.

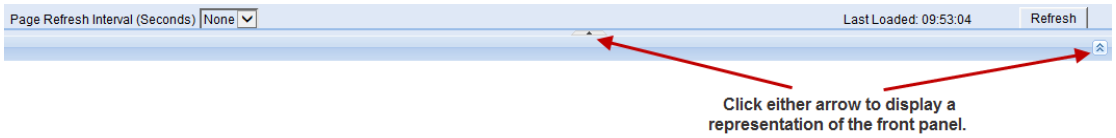


Figure 4 Displaying a Representation of the Front Panel

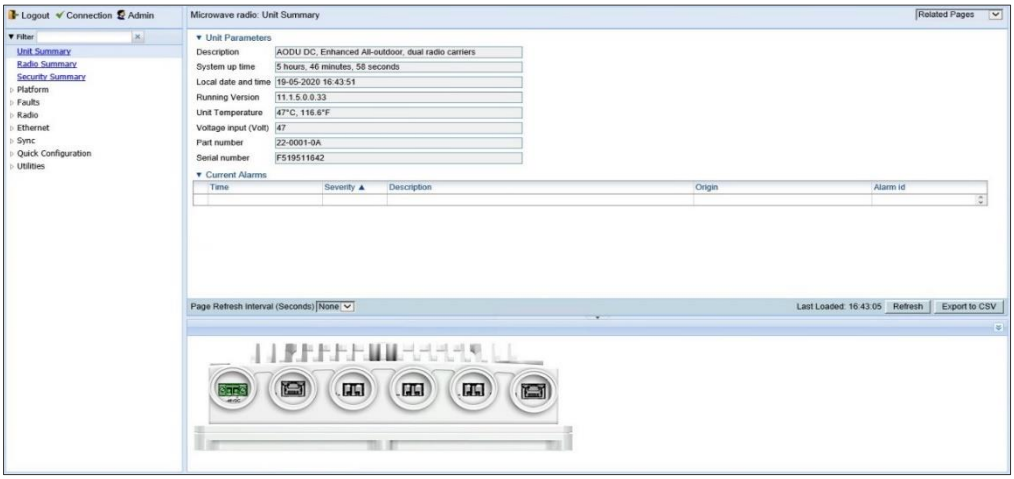


Figure 5 *Main Web EMS Page with Representation of Front Panel – PTP 850S*

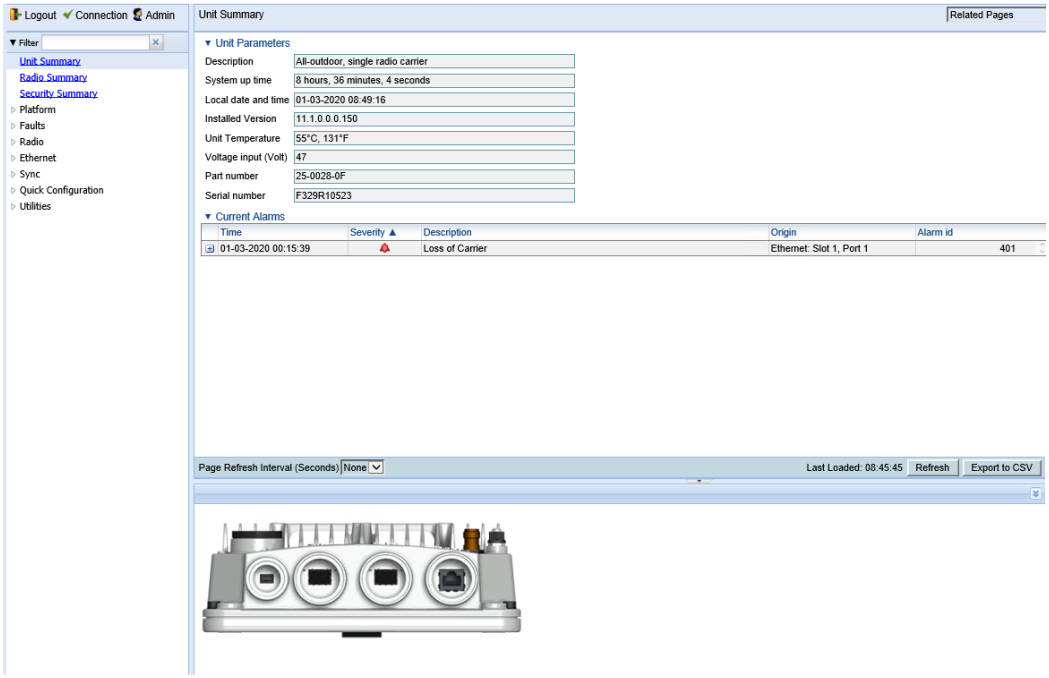


Figure 6 Main Web EMS Page with Representation of Front Panel – PTP 850E

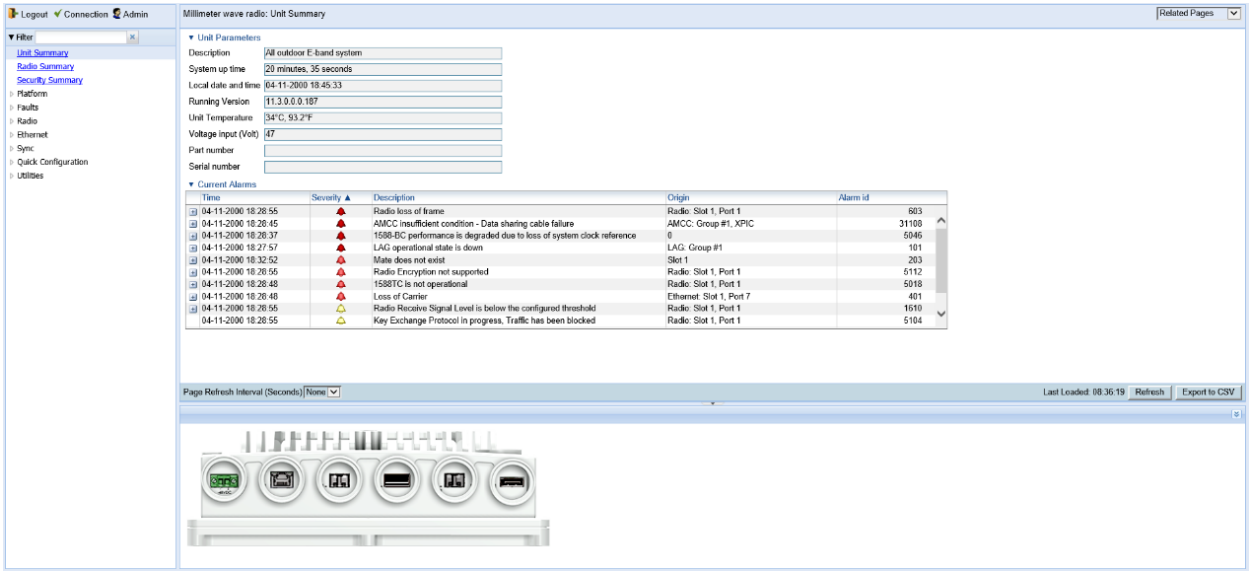
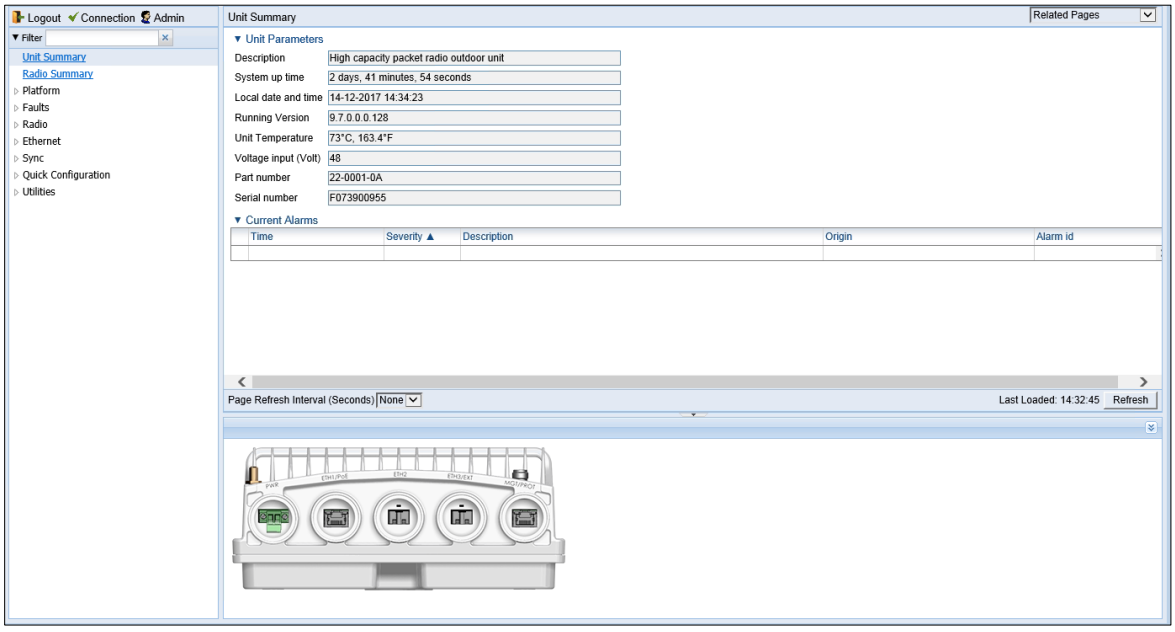
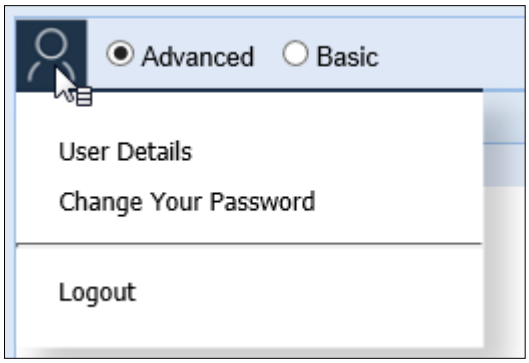


Figure 7 Main Web EMS Page with Representation of Front Panel



2.2.4.4 Quick Password and Logout Icon

To display your user details, change your password, or logout, click the icon on the upper left of any Web EMS screen and select the relevant option.



2.2.4.5 Hiding Interfaces that are Admin Down

In pages that display interfaces, you can choose to display only those interfaces with an Admin status of **Up**. Simply select **Show only interfaces with Admin status 'Up'** at the upper left of the table to hide all interfaces with Admin status **Down**. For example, for the Interface Manager page, Figure 8 shows all interfaces and Figure ***9*** displays only interfaces with Admin status **Up** after **Show only interfaces with Admin status 'Up'** has been selected.

Figure 8: Interface Manager Page Showing All Interfaces (PTP 850E)

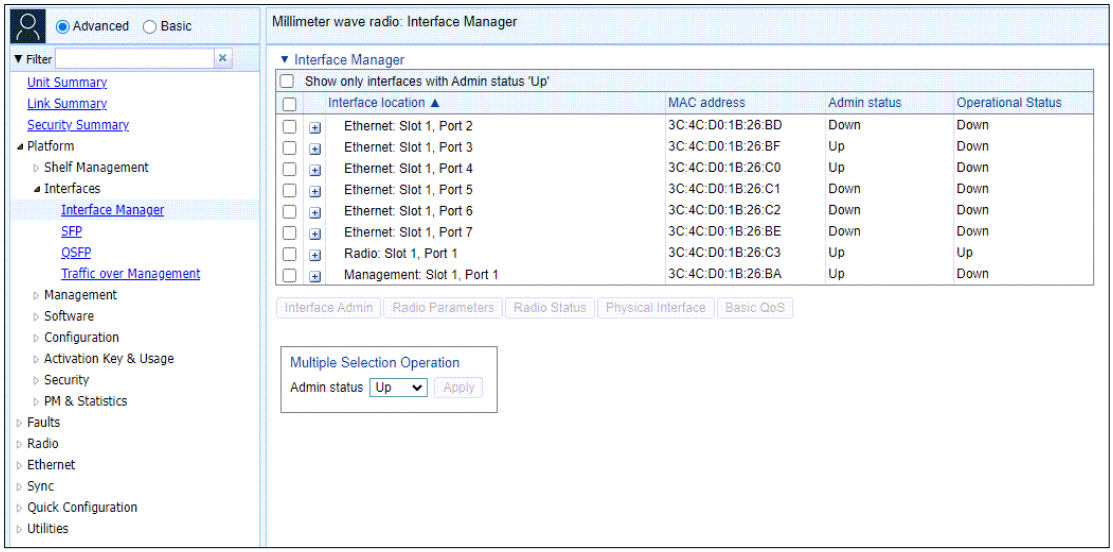
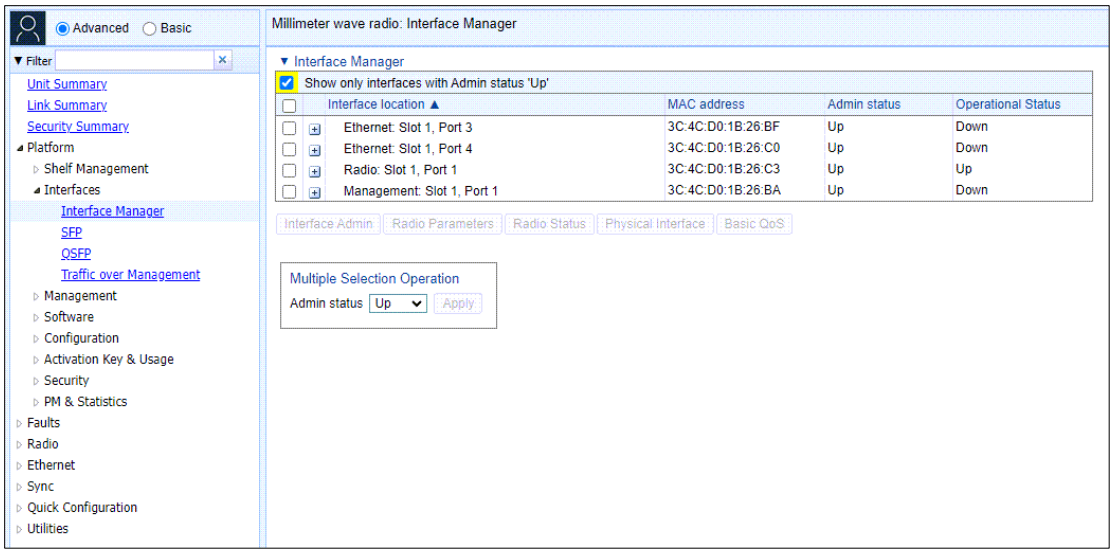


Figure 9: *Interface Manager Page Showing Interfaces with Admin Status Up (PTP 850E)*



2.2.4.6 Active, Standby, and Merged (All) Tabs

When Unit Redundancy is enabled, two tabs appear on the top of the main section. These tabs are labeled *Active* and *Standby* and enable you to configure the Active and Standby units separately if necessary. The title above the main section indicates whether you are working with the Active or Standby unit. For details on configuring Unit Redundancy, see **You can configure** lockout and forced switchover in the bottom of the Line Redundancy page.

To force the line redundancy for traffic to remain in its current state (lockout), click **Lockout** in the **Traffic Interfaces State** section on the lower left of the page. Lockout can be used to override Revertive mode and keep the configuration in switchover mode, should this be necessary.

To clear a Lockout, click **Clear Lockout**, which appears in place of the **Lockout** button when Lockout state has been activated.

The current lockout state is displayed in the **Lockout State** field.

To force a traffic switchover regardless of whether a failure state exists, click **Force Switch** in the **Traffic Interfaces State** section on the lower left of the page.

To prevent Revertive mode from operating to return the configuration to normal configuration, click **Lockout** after implementing the forced switchover.

Note: The Revertive timer only applies to traffic. Line redundancy for external management does not have a revertive timer.

To force line redundancy for external management to remain in its current state (lockout), click **Lockout** in the **Management Interfaces State** section on the lower right of the page. The lockout remains in effect for the time configured in the **Management Lockout Duration** field.

When management lockout is active, the **Lockout State** field displays the time remaining for the lockout. To end the lockout state, click **Clear Lockout**.

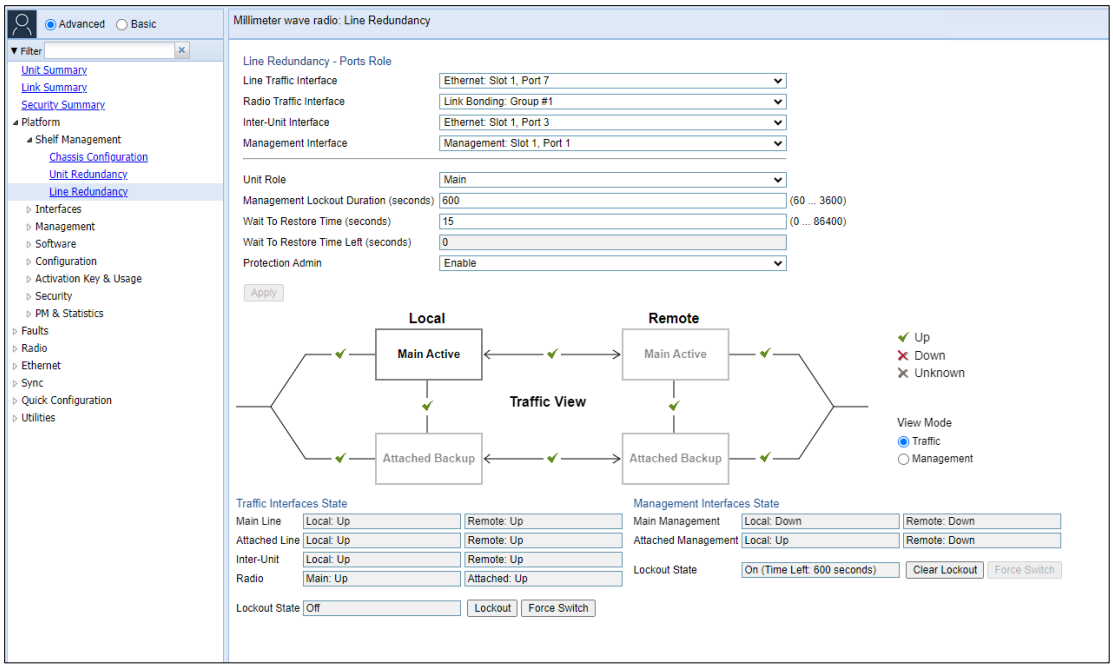


Figure 274: Line Redundancy Page (Attached Unit)

To force an external management switchover regardless of whether a failure state exists, click **Force Switch** in the **Management Interfaces State** section on the lower right of the page.

Line Redundancy with Multiband and Link Bonding –Status ParametersThe Line Redundancy page displays the status of line redundancy for both traffic and external management, in both graphic format and through status fields that display the state of the interfaces.

Status indications for traffic are available for the following interfaces:

- Main Line – The active interface attached to the external switch.
- Attached Line – The inactive (backup) interface attached to the external switch.
- Inter-Unit – The connection between the main and attached units.
- Radio The radio link.

Possible operational statuses are:

- Down – The interface is down.
- Unknown – Communication with the interface is unavailable.
- Invalid – Line redundancy is disabled on at least one of the devices. This indication is only available on the graphical display.
- Up – The specified interface is up.

Note: For management interfaces, **Down** can mean the interface is either down or in standby mode. To avoid loops, the system only allows one management interface to be active at the same time.

To display the status of external management redundancy, select **Management** in the View Mode section to the right of the graphical display.

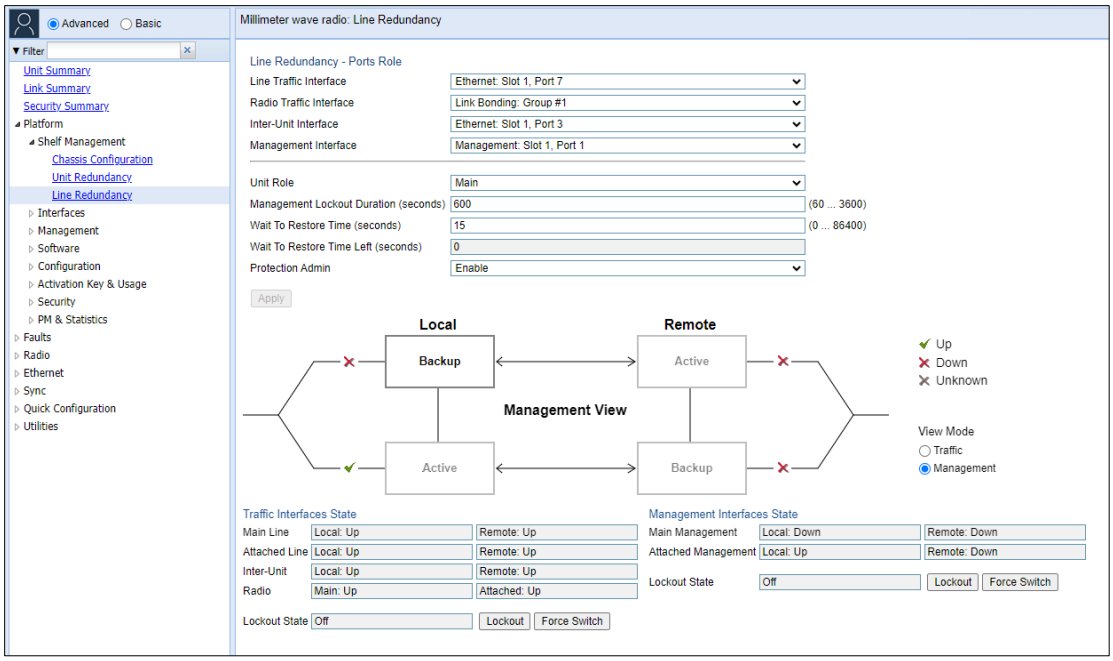


Figure 275: Line Redundancy Page – Management View Mode

Configuring Unit Redundancy.

Note: Unit Redundancy is only available PTP 850E.

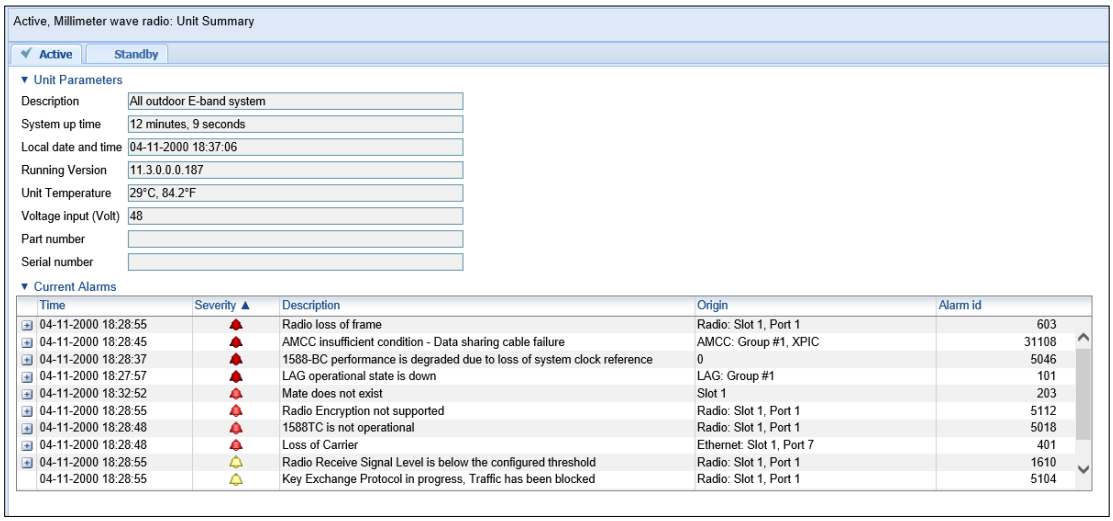


Figure 10: *Main Web EMS Page with Active and Standby Tabs*

Certain Web EMS pages include an additional, merged tab labelled **All**. The **All** tab includes rows for both the Active and the Standby unit, so that you can work with both units from a single page. In merged pages, an additional column labelled **Device Role** appears to indicate whether the row is from the Active or the Standby unit.

The **All** tab appears in the following Web EMS pages.

- Interface Manager
- Radio Parameters

- Current Alarms
- Event Log

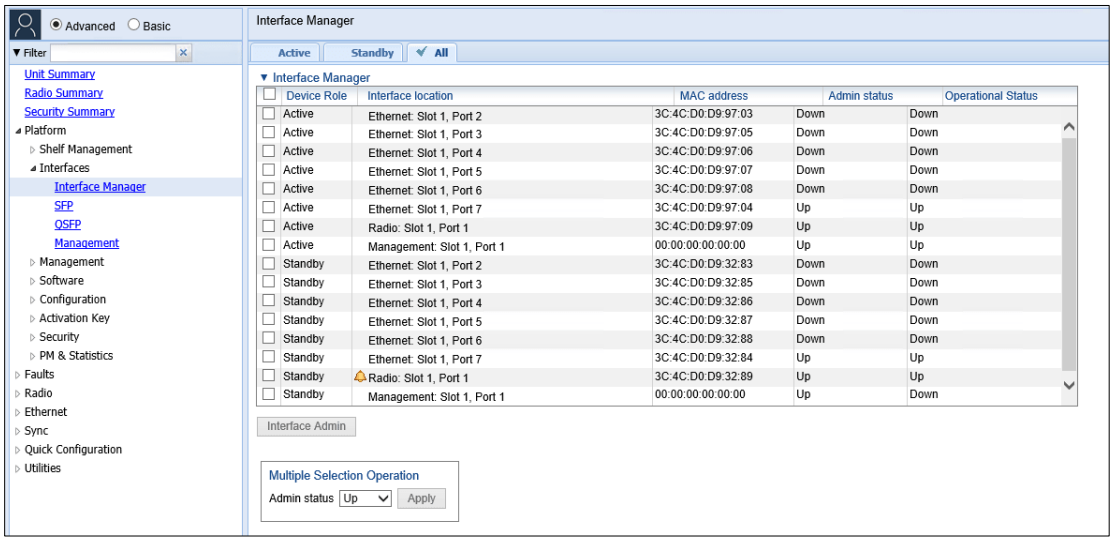


Figure 11: Merged (All) Tab – Interface Manager Page

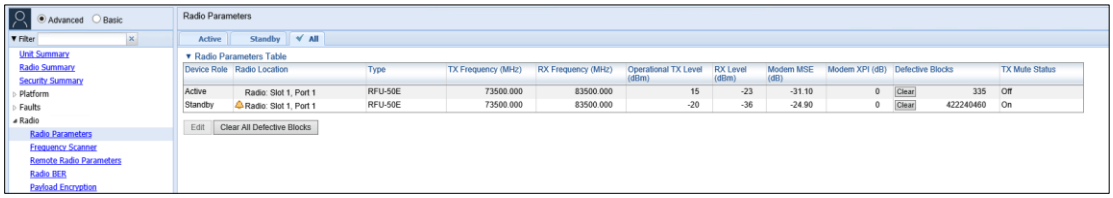


Figure 12: Merged (All) Tab – Radio Parameters Page

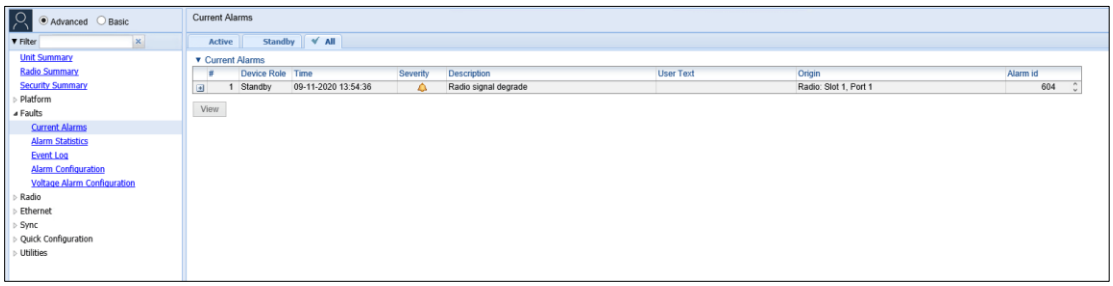


Figure 13: Merged (All) Tab – Current Alarms Page

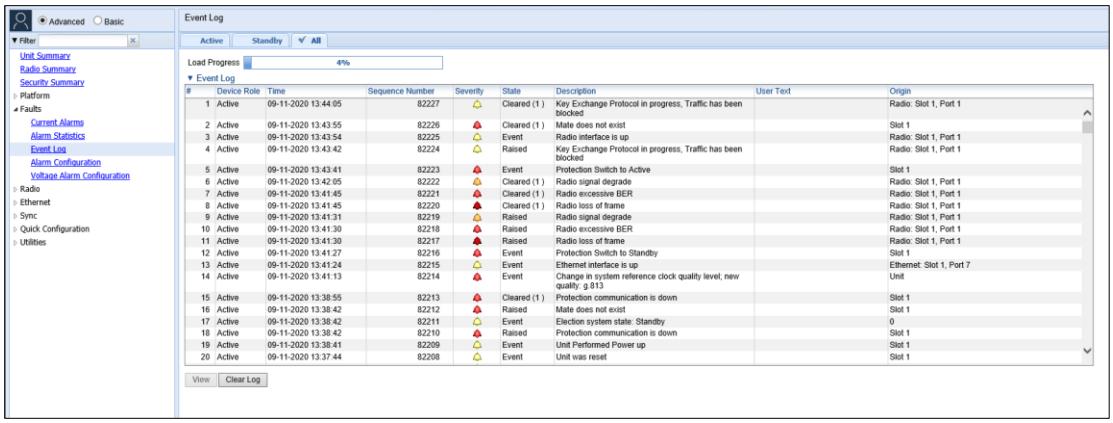


Figure 14: Merged (All) Tab – Event Log Page

2.2.4.7 Related Pages Drop-Down List

Certain pages include a **Related Pages** drop-down list on the upper right of the main section of the page. You can navigate to a page related to the current page by selecting the page from this list.

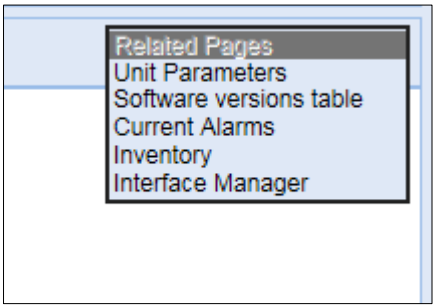


Figure 15: Related Pages Drop-Down List

2.2.4.8 Page Refresh and Refresh Interval

To refresh the current page in the Web EMS, click **Refresh** on the lower right of the page.

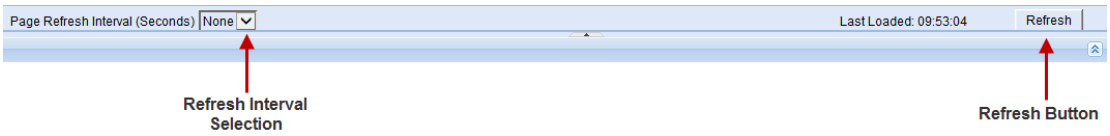


Figure 16: Page Refresh Options

You can also set the page to refresh automatically at selected intervals. Click the arrow next to **Page Refresh Interval (Seconds)** on the lower left of the page and select the automatic refresh interval (in seconds).

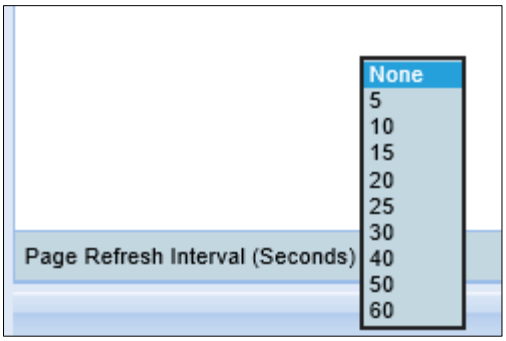


Figure 17: Automatic Refresh Interval Drop-Down List

2.2.4.9 Export to CSV Option

Certain pages include an **Export to CSV** button on the lower right of the main section of the page. Click **Export to CSV** to save the data on the page to a .csv file.

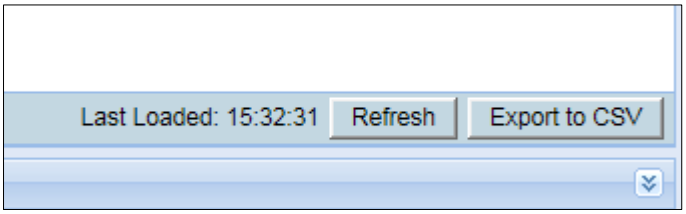


Figure 18: Export to CSV Button

2.2.4.10 Interactive User Guide

From the Web EMS, you can open an Interactive User Guide for the product you are using. The Interactive User Guide is based on this User Guide but utilizes AI to determine the Web EMS page you are using and to perform AI-assisted searches.

Note: This feature is not available for PTP 850E.

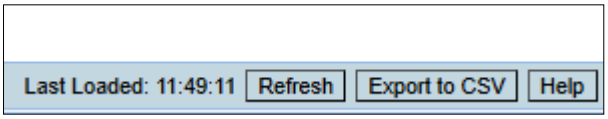


Figure 19: Help Button

The Interactive User Guide opens to a place related to the Web EMS page that is currently open, as in the example shown in Figure 20.

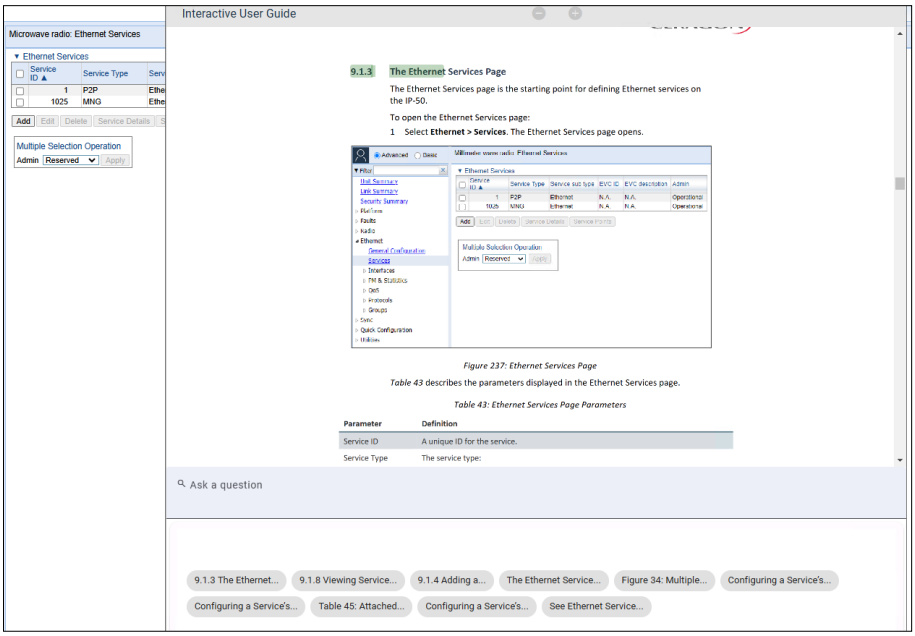


Figure 20: Interactive User Guide – Example of Context-Related Page

At the bottom of the Interactive User Guide is a list of topics that may be relevant to the current Web EMS page. In the *Ask a question* field above the topics, you can ask a question in free text to help the AI refine the list of topics displayed.

Click a topic to display the full text of that topic in the Interactive User Guide. Before you click, you can hover the mouse over a topic to display a preview of the topic, as shown in the example in Figure 21.

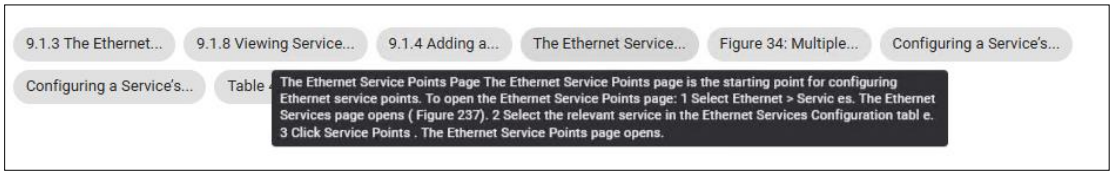


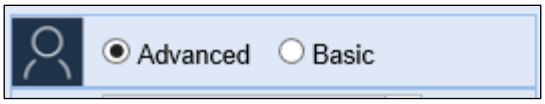
Figure 21: Interactive User Guide – Preview

Note: The first time you open the Interactive User Guide per device and per browser, it may take up to 30 seconds to open. It opens more quickly subsequent times, unless you delete cookies or use an incognito window.

2.2.4.11 Advanced Mode and Basic Mode

The Web EMS includes the following menu tree options:

- Advanced – Includes all available options, including both basic link and configuration and advanced configuration such as QoS and Ethernet protocols.
- Basic – Provides a basic set of menu options that cover most or all of the configurations necessary to set up and maintain an PTP 850 unit, including link configuration wizards for most link types. The purpose of Basic mode is to provide the average user with a menu tree that is simple to navigate yet includes most or all options that most users need.



You can toggle between Advanced or Basic mode by clicking **Advanced** and **Basic** in the upper left corner or any page in the Web EMS. The default mode is **Advanced** mode.

This manual includes a separate chapter to guide you through PTP 850 configuration using Basic mode, with cross-references to more detailed explanations of PTP 850 features found elsewhere in the manual. Except in the Basic mode chapter, references to the Web EMS menu structure and screens refer to Advanced mode except when otherwise noted.

2.2.4.12 The Unit Summary Page

The Unit Summary page is the first page that appears when you log into the Web EMS. It gathers the unit parameters, current alarms and unit inventory information on a single page for quick viewing.

Figure 22 Unit Summary Page- PTP 850C

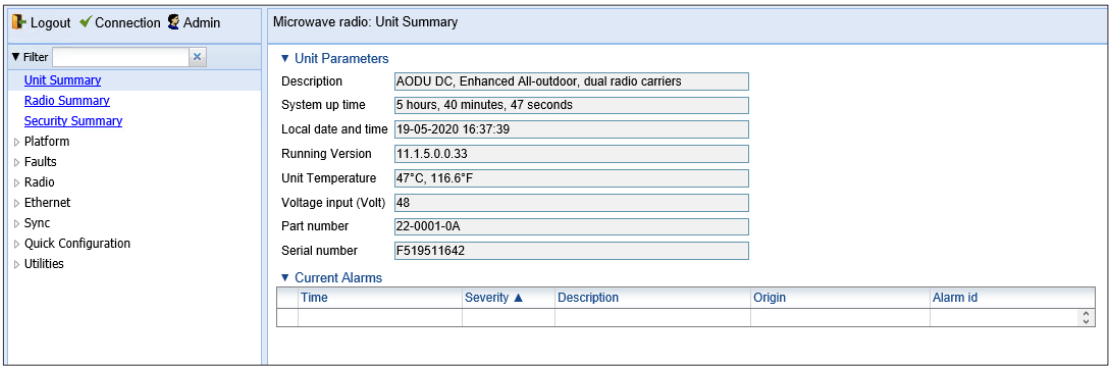


Figure 23 Unit Summary Page – PTP 850S

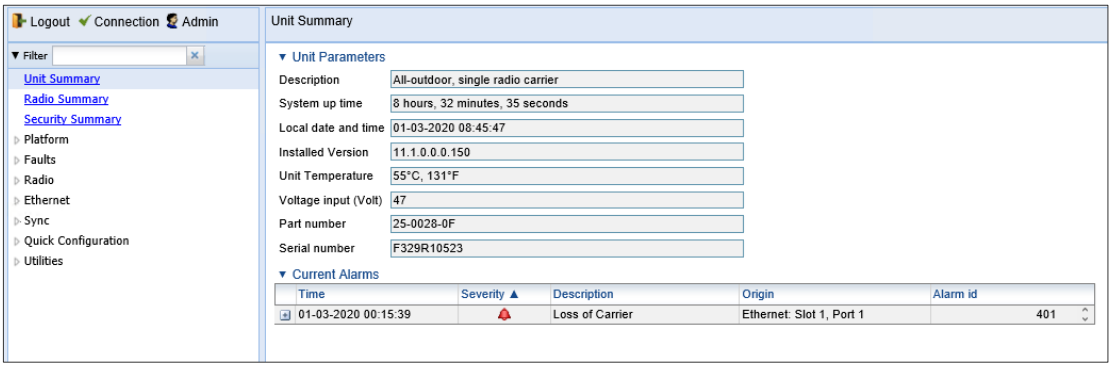
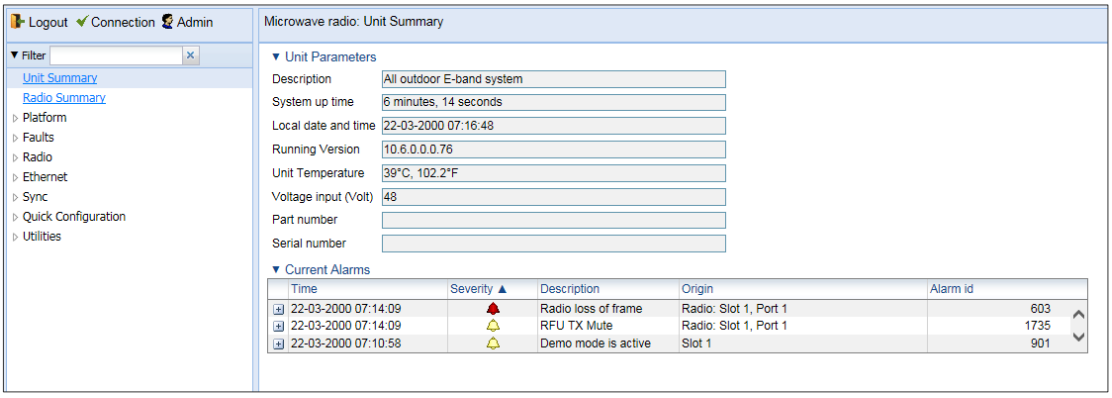


Figure 24 Unit Summary Page – PTP 850E



The Unit Summary page includes:

Unit Parameters – Basic unit parameters such as the current software version, unit temperature, and voltage input level. For additional information, see Configuring Unit Parameters.

Current Alarms – All alarms currently raised on the unit. For additional information, see Viewing Current Alarms.

The Unit Summary page can be customized to include only specific columns and tables. This enables you to hide information you do not need in order to focus on the information that is most relevant.

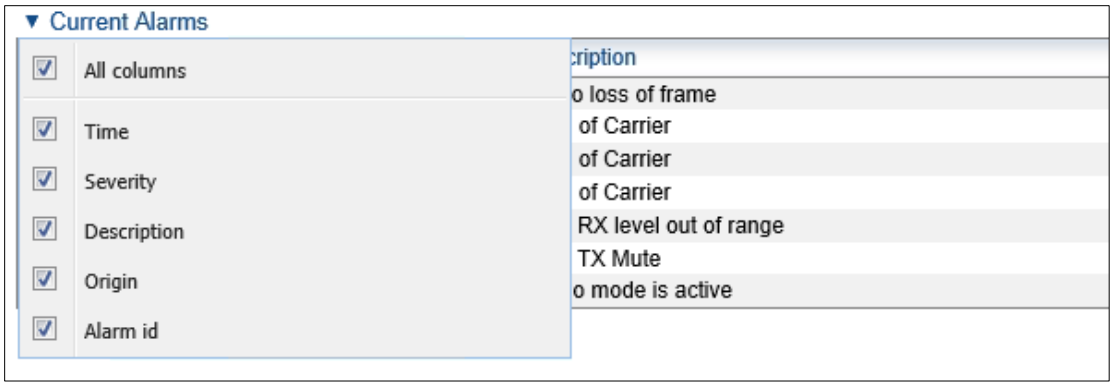
To hide a specific section of the Unit Summary page, click the section title. To display a section that has been hidden, click the section title again.

To customize which columns appear in a section, click ▼ next to the section title. A list of columns is displayed. Select only the columns you want to display and click ▼ again.

Note

When one or more columns are hidden, the ▼ icon turns white (▽).

Figure 25 Unit Summary Page – Customizing Columns



2.2.4.13 The Link Summary Page

The Link Summary page displays the link status and parameters in graphical format, and enables users to display and configure radio parameters for the local and remote devices.

To display the Link Summary page, select **Link Summary** from the Web EMS main menu.

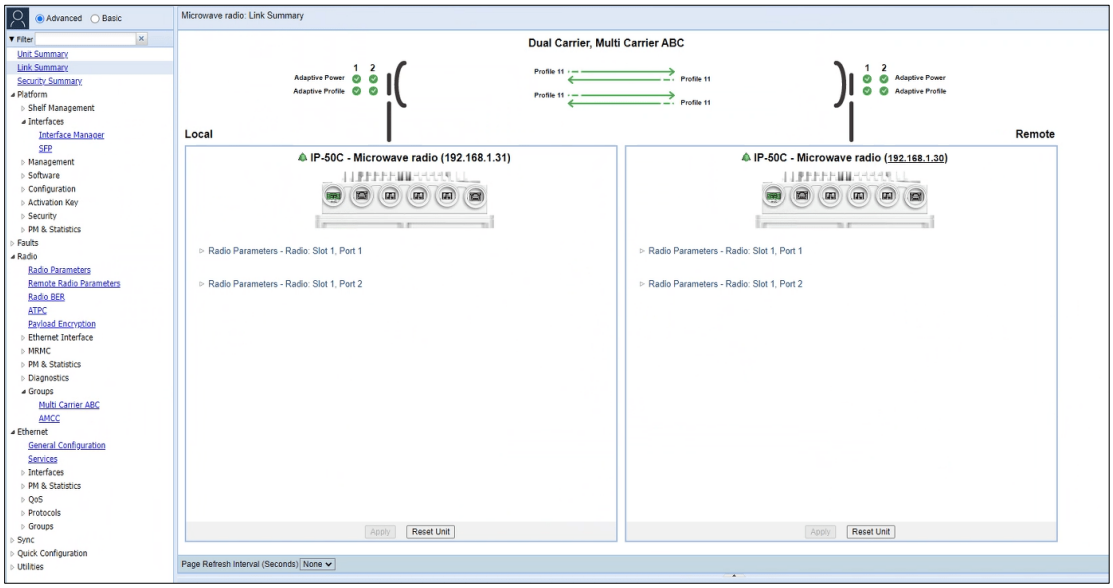


Figure 26: Link Summary Page (PTP 850C)

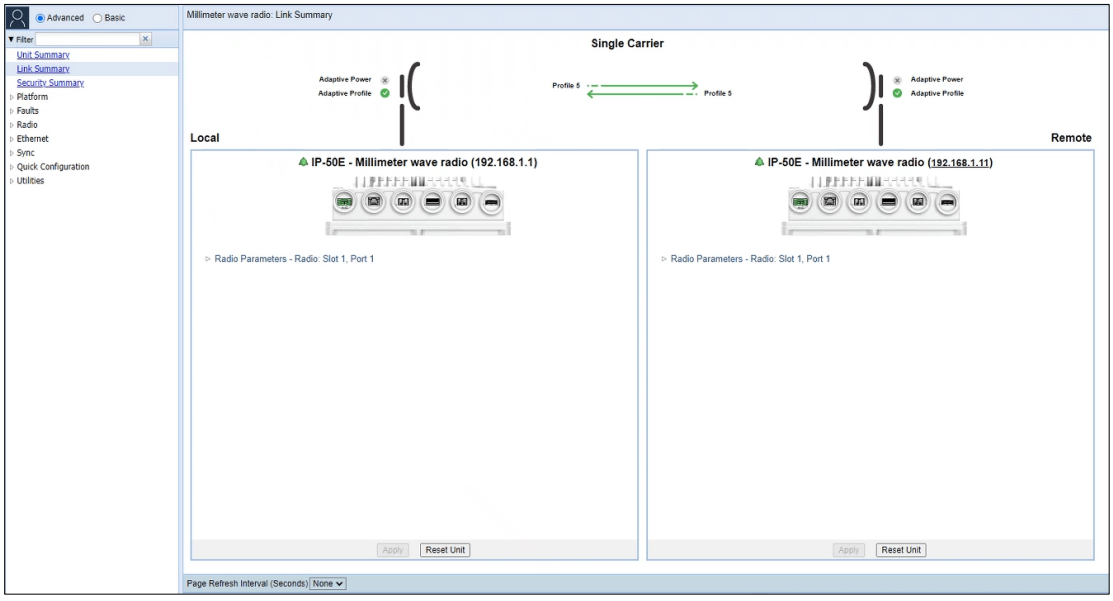


Figure 27: Link Summary Page (PTP 850E)

The Link Summary page includes the following information:

- **Type of Link** – The Link Summary page indicates at the top what kind of link is operating. Among the possible links types are Single Carrier, Multi-Carrier ABC, Multiband, East/West, and more.
- **State of Link** – The color of the arrows indicates whether the link is Up or Down, as follows:
  -  - Link is Up (green).
  - - Link is Down because the radio is not transmitting (mute) (grey).
  -  - Link is Down because the radio is not receiving (red).
- **Radio Payload Encryption** – When AES-256 Payload Encryption is enabled, the arrows that represent the link indicate that AES-256 payload encryption is enabled and its validation state:
  -  – AES-256 Payload Encryption is enabled and valid.
  -  – AES-256 Payload Encryption is enabled but not valid.

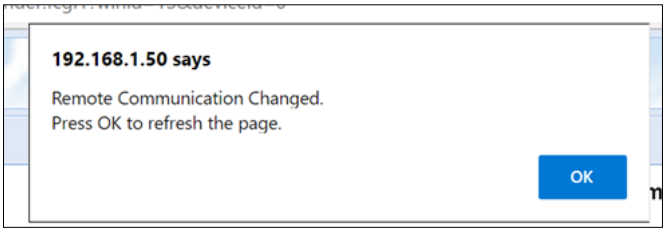
  For additional information, see Error! Reference source not found..
- **ACM Profile –** The Link Summary page displays the current operating ACM profile for each link direction and (for PTP 850C) for each radio. See Error! Reference source not found..
- **Adaptive Power –** Indicates for each side of the link and each radio whether Adaptive TX Power is enabled (✓) or disabled (×). See Error! Reference source not found..
- **Adaptive Profile –** Indicates for each side of the link and each radio whether the radio script is configured to Adaptive ACM mode (✓) or Fixed ACM mode (×). See Error! Reference source not found..
- **Alarm Status –** The icon to the left of the device type indicates whether there are any alarms on the local and remote devices. If there are no alarms, the icon is green (🔔). If there are alarms, the icon is red (🔔). For more information, scroll over the icon to display a tooltip:
  - For the local device, the tooltip displays the description, severity, and source of each active alarm.
  - For the remote device, the tooltip displays the severity of the active alarm with the highest level of severity.
- **IP Address –** The IP address of the local (left) and remote (right) devices is displayed above the graphical representation of the device.
- **XPIC –** For XPIC configurations, the Link Summary page displays the polarization of each link by the letter V (vertical) or H (Horizontal) next to the antenna icon:





Note: The XPIC indication is not available for PTP 850C.

If the status of the link changes while the Link Summary page is open, you are prompted to refresh the page.



In addition to displaying the link's status, the Link Summary page enables you to display and configure the main radio parameters for both the local and the remote radios. To display the radio parameters, click **Radio Parameters**. For links with two radio carriers, click **Radio Parameters** for the radio interface you want to display or configure.

The parameters available in the Link Summary page include:

- **MRMC script parameters** – See Error! Reference source not found..
- **TX and RX Frequency** – See Error! Reference source not found..
- **Admin and Operational Status** (Local only) – See Viewing the Radio Status and Settings.
- **RX Level and Adaptive TX Power** – See Error! Reference source not found. and Viewing the Radio Status and Settings.
- **ATPC** – See Error! Reference source not found..
- **TX Mute** – See Error! Reference source not found..
- **TX Level** – See Error! Reference source not found..

Note: For the remote unit, the only parameters that can be changed are the **Reference RX Level**, **ATPC Admin**, and **TX Mute**. The other parameters are read-only.

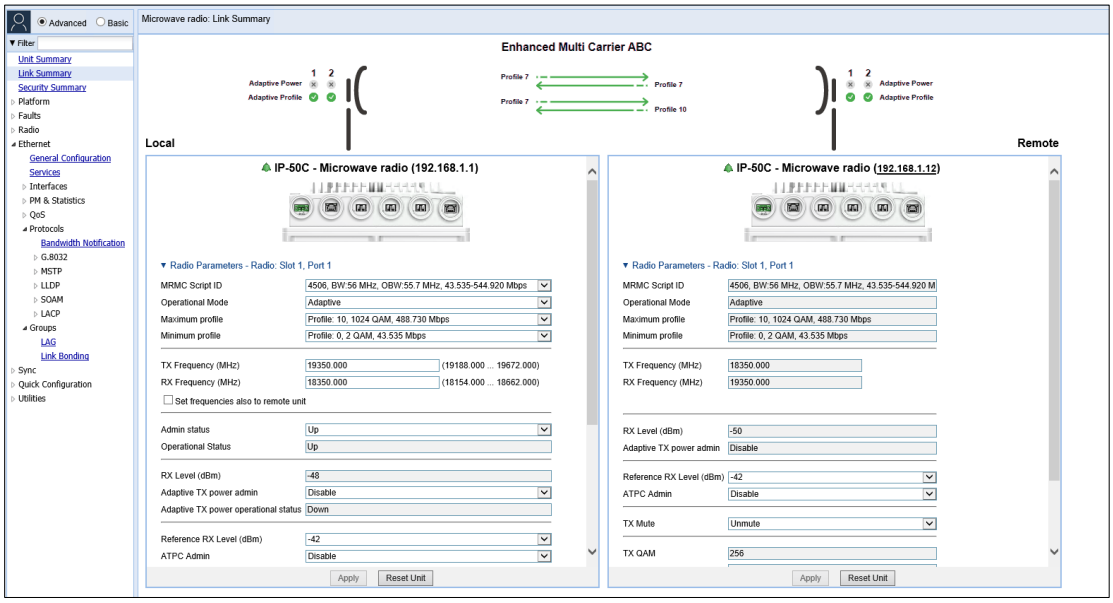


Figure 28: Link Summary Page – Radio Parameters (PTP 850C)

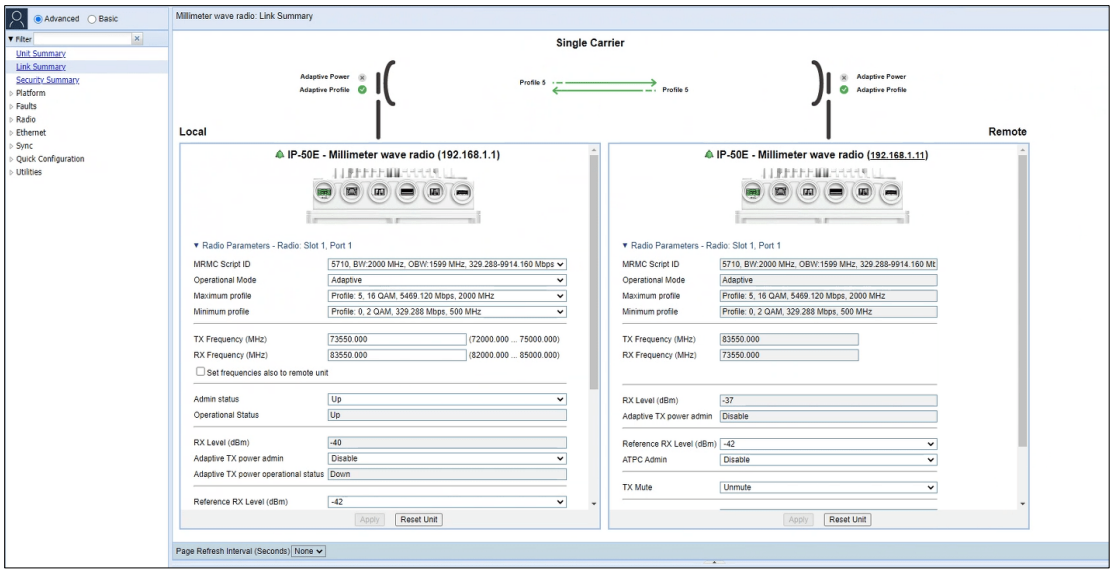
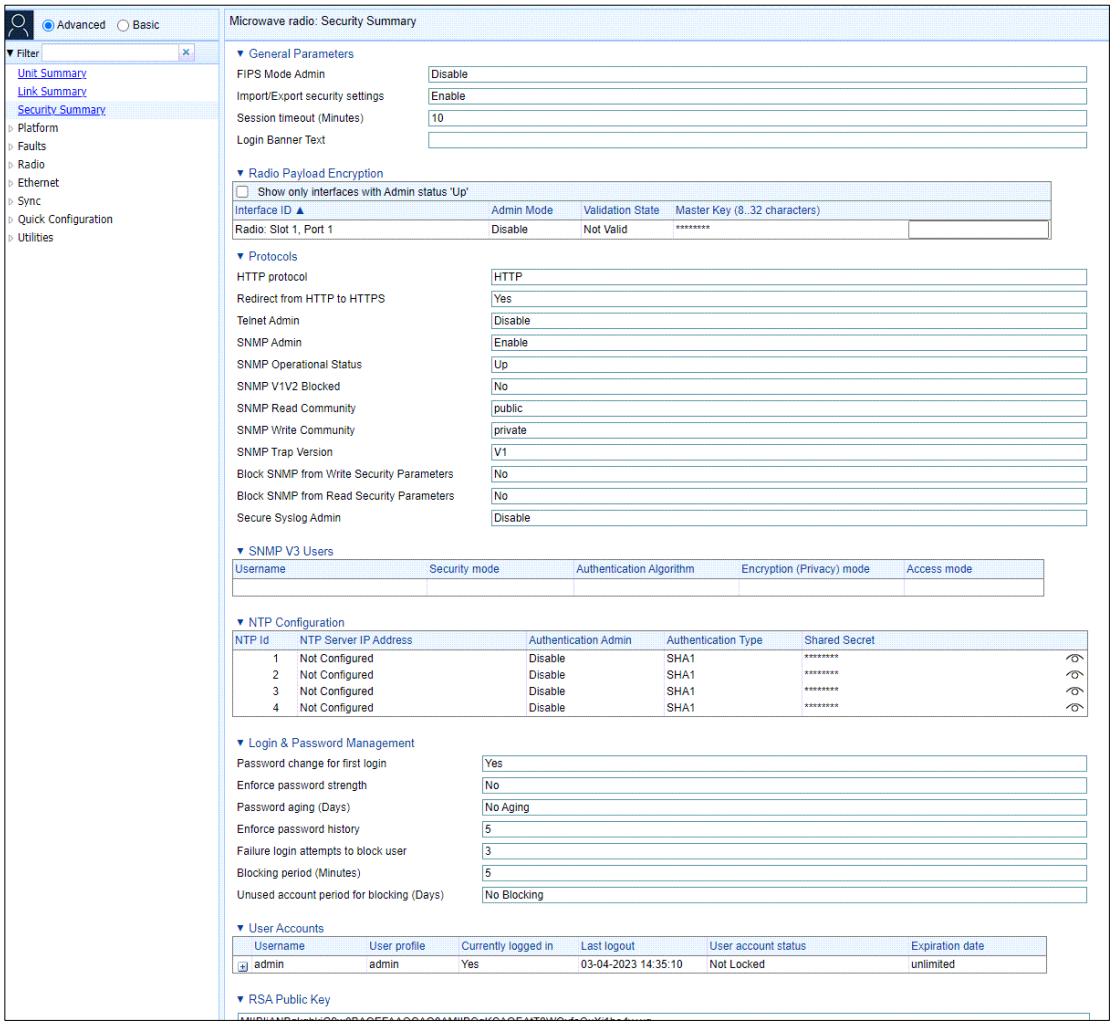


Figure 29: Link Summary Page – Radio Parameters (PTP 850E)

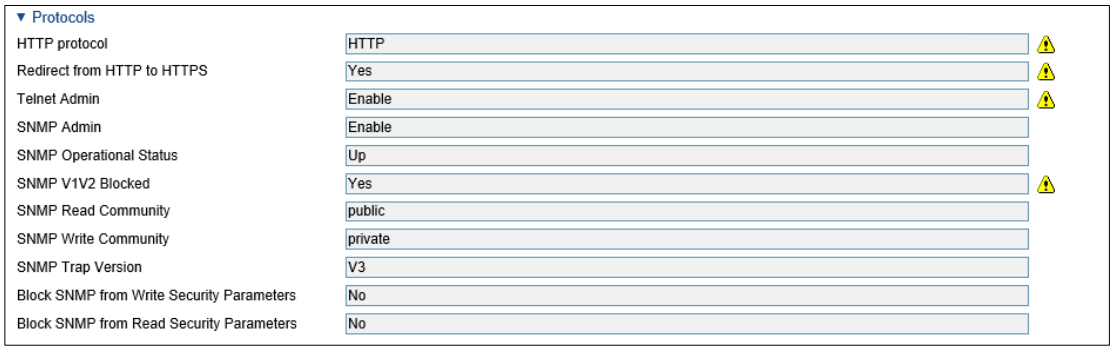
2.2.4.14 The Security Summary Page

The Security Summary page gathers a number of important security-related parameters on a single page for quick viewing. To display the Security Summary page, select **Security Summary** from the Web EMS main menu.

Figure 30 Security summary page



If FIPS mode is enabled, a yellow Warning icon may appear next to certain items. These items indicate fields for which the current security settings are not appropriate for FIPS mode. Hover over an item to display a tooltip explaining the warning.



The Security Summary page includes:

General Parameters – Includes the following fields:

- **FIPS Mode Admin** – Not relevant for PTP 850E.
- **Import/Export security settings** – See Configuring the Import/Export Security Settings.
- **Session Timeout (Minutes)** – See Configuring the Session Timeout.
- **Login Banner Text** – See Defining a Login Banner.

Protocols – Displays information about the current configuration of the following protocols used for communicating with the device:

- **`HTTP** – See *Configuring X.509 CSR Certificates*.
- **Telnet** – See *Blocking Telnet Access*.
- **SNMP** – See *Configuring SNMP*.

SNMP V3 Users – Displays a list of SNMP V3 users configured on the device. For additional information, see Configuring SNMP.

Login & Password Management – Displays login and password security parameters configured on the device. See Configuring the General Access Control Parameters and Configuring the Password Security Parameters.

User Accounts – Displays a list of users configured for the device and their parameters. See Configuring Users.

RSA Key – Displays the public RSA key currently configured on the device. See Downloading and Installing an RSA Key.

The Security Summary page can be customized to include only specific columns and tables. This enables you to hide information you do not need in order to focus on the information that is most relevant.

To hide a specific section of the Radio Summary page, click the section title. To display a section that has been hidden, click the section title again.

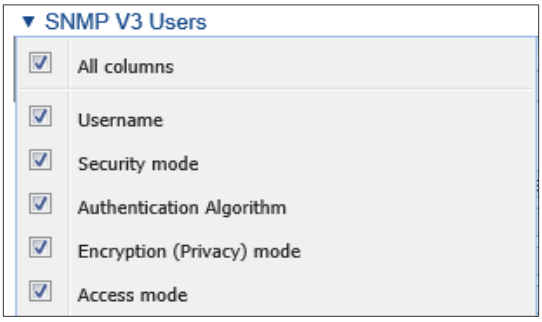
To customize which columns appear in a section, click next to the section title. A list of columns is displayed. Select only the columns you want to display and click again.



Note

When one or more columns are hidden, the icon turns white ( ).

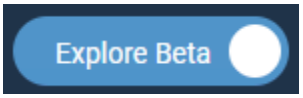
Figure 31 Security Summary Page – Customizing Columns



2.2.4.15 Future Web EMS Preview (Beta)

This Release version includes a preview of the future Web EMS, which will significantly enhance the user experience for customers. Users can access the preview (beta) version of the future Web EMS by toggling the **Explore Beta** button in the upper right of the Web EMS. This option is available in all Web EMS pages.

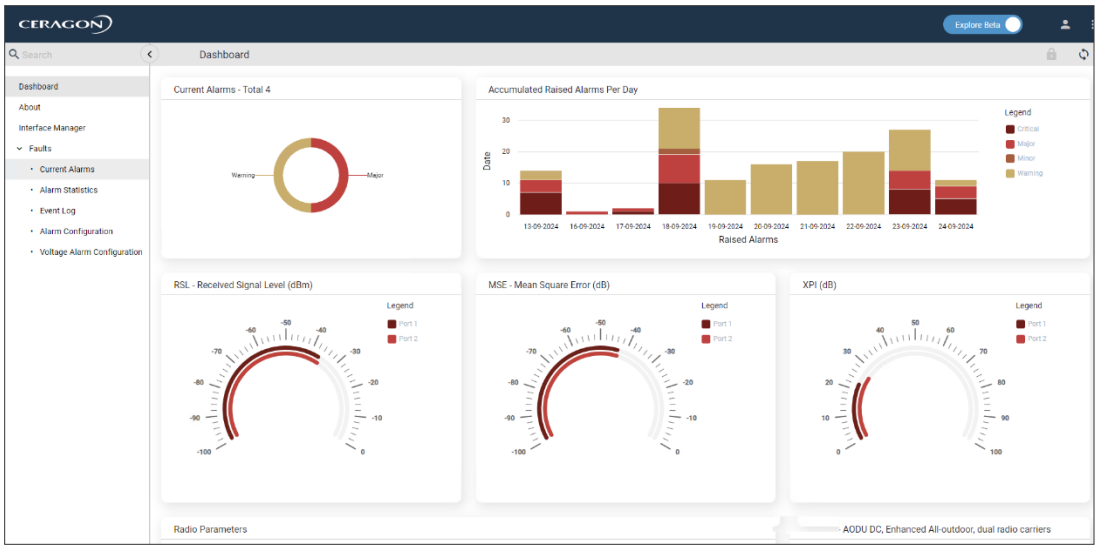
The **Explore Beta** field appears in gray when the user is using the current Web EMS. When the user is using the future Web EMS, the **Explore Beta** field appears in blue:



The following pages are available using the future Web EMS format:

- **Dashboard** – A new opening page that displays important information about alarms, RSL levels, MSE levels, and XPI levels at a glance. This provides the user with the ability to instantly assess the link status.
- **Interface Manager** – An enhanced version of the current Interface Manager page.
- **Faults** – Includes all Web EMS pages related to fault management, such as Current Alarms, Event Log, Alarm Configuration, and more.

The following figure provides an example of the Dashboard:



Any time the user wants to return to the current Web EMS, the user toggles the **Explore Beta** button in the upper right of the Web EMS.

Every time the user changes from the current Web EMS to the future Web EMS beta version, the user must log in again.

Cambium welcomes feedback on its future Web EMS design, which will be expanded in future versions and eventually adopted as the full Web EMS. To provide feedback and inquire about future availability, please contact your representative.

2.3 Reference Guide to Web EMS Menu Structure

The following table shows the Web EMS menu hierarchy, with links to the sections in this document that provide instructions for the relevant menu item.

Note

Some menu items are only available if the relevant activation key or feature is enabled.

Table 1 Web EMS Menu Hierarchy – Platform Menu

Sub-Menus	For Further Information
Shelf Management > Chassis Configuration	Performing a Hard (Cold) Reset Setting the Unit to the Factory Default Configuration
Shelf Management > Unit Redundancy	Configuring 1+1 HSB Unit Protection
Shelf Management > Line Redundancy	Configuring Line Redundancy with Multiband and Line Bonding
Interfaces > Interface Manager	Enabling the Interfaces (Interface Manager)

Sub-Menus	For Further Information
Interfaces > SFP	**Error! Reference source not found.**
Interfaces > Traffic over Management	PTP 850E Management Interface
Management > Unit Parameters	Configuring Unit Parameters
Management > NTP Configuration	Configuring NTP
Management > Time Services	Setting the Time and Date (Optional)
Management > Inventory	Displaying Unit Inventory
Management > Unit Info	
Management > Remote SysLog	Configuring Syslog
Management > Login Banner	Defining a Login Banner
Management > Networking > Local	Configuring In-Band Management Changing the Management IP Address Defining the IP Protocol Version for Initiating Communications
Management > Networking > Remote	Configuring the Remote Unit's IP Address
Management > SNMP > SNMP Parameters	Configuring SNMP
Management > SNMP > Trap Managers	Configuring Trap Managers
Management > SNMP > V3 Users	Configuring SNMP
Software > Versions	Viewing Current Software Versions
Software > Download & Install	Downloading and Installing Software Configuring a Timed Installation
Configuration > Timer Parameters	Planned for future release.
Configuration > Backup Files	Viewing Current Backup Files

Sub-Menus	For Further Information
Configuration > Configuration Management	Backing Up and Restoring Configurations
Activation Key > Activation Key Configuration	
Activation Key > Activation Key Overview	Displaying a List of Activation-Key-Enabled Features
Security > General > Configuration	Planned for future release.
Security > General > Security Log Upload	Uploading the Security Log
Security > General > Configuration Log Upload	The File transfer progress field displays the progress of any current security log upload operation. Uploading the Configuration Log
Security > User Access Control > Remote Access Control > SSO	Configuring SSO Web Login with Microsoft Entra ID
Security > X.509 Certificate > CSR	Configuring X.509 CSR Certificates
Security > X.509 Certificate > Download & Install	Configuring X.509 CSR Certificates
Security > Access Control > General	Configuring the General Access Control Parameters
Security > Access Control > User Profiles	Configuring User Profiles
Security > Access Control > User Accounts	Adding User Accounts
Security > Access Control > Password Management	Configuring the Password Security Parameters
Security > Access Control > Change Password	Changing Your Password
Security > Access Control > Radius > Radius Configuration	Planned for future release.

Sub-Menus	For Further Information
Security > Access Control > Radius > Radius Users	Planned for future release.
Security > Protocols Control	Configuring the Session Timeout Blocking Telnet Access
PM & Statistics > SFP	Planned for future release.
PM & Statistics > Voltage	Configuring Voltage Alarm Thresholds and Displaying Voltage PMs

Table 2 Web EMS Menu Hierarchy – Faults Menu

Sub-Menus	For Further Information
Current alarms	Viewing Current Alarms
Alarm Statistics	Viewing Alarm Statistics
Event Log	
Alarm Configuration	
Voltage Alarm Configuration	Configuring Voltage Alarm Thresholds

Table 3 Web EMS Menu Hierarchy – Radio Menu

Sub-Menus	For Further Information
Radio Parameters	
Frequency Scanner	Running the Frequency Scanner
Remote Radio Parameters	
Radio BER Thresholds	
Ethernet Interface > Counters	
MRMC > Symmetrical Scripts > ETSI	
MRMC > Symmetrical Scripts > FCC	
MRMC > MRMC Status	
PM & Statistics > Counters	Displaying and Clearing Defective Block Counters

Sub-Menus	For Further Information
PM & Statistics > Signal Level	Displaying Signal Level PMs
PM & Statistics > Aggregate	
PM & Statistics > MSE	Displaying MSE PMs
PM & Statistics > MRMC	Displaying MRMC PMs
PM & Statistics > Traffic > Capacity/Throughput	
PM & Statistics > Traffic > Utilization	
Diagnostics > Loopback	Performing Radio Loopback
Groups > Multi Carrier ABC	Configuring Multiband

Table 4 Web EMS Menu Hierarchy – Ethernet Menu

Sub-Menus	For Further Information
General Configuration	Setting the MRU Size and the S-VLAN Ethertype
Services	Configuring Ethernet Service(s)
Interfaces > Physical Interfaces	Configuring Ethernet Interfaces
Interfaces > Logical Interfaces	Configuring Ingress Path Classification on a Logical Interface Assigning Policers to Interfaces Configuring the Ingress and Egress Byte Compensation Assigning WRED Profiles to Queues Assigning a Queue Shaper Profile to a Queue Assigning a Queue Priority Profile to an Interface Assigning a Queue WFQ Profile to an Interface Performing Ethernet Loopback

Sub-Menus	For Further Information
Interfaces > ASP & LLF	Configuring Automatic State Propagation and Link Loss Forwarding
PM & Statistics > RMON	RMON Statistics
PM & Statistics > Port TX	Port TX Statistics
PM & Statistics > Port RX	Port RX Statistics
PM & Statistics > Egress CoS Statistics	Egress CoS *Statistics*
PM & Statistics > Egress CoS PM > Configuration	Configuring and Displaying Queue-Level PMs
PM & Statistics > Egress CoS PM > Egress CoS PM	Configuring and Displaying Queue-Level PMs
PM & Statistics > Link Bonding > Utilization	Link Bonding PMs
PM & Statistics > Link Bonding > Throughput	Link Bonding PMs
QoS > Classification > 802.1Q	Modifying the C-VLAN 802.1Q UP and CFI Bit Classification Table
QoS > Classification > 802.1AD	Modifying the S-VLAN 802.1 UP and DEI Bit Classification Table
QoS > Classification > DSCP	Modifying the DSCP Classification Table
QoS > Classification > MPLS	Modifying the MPLS EXP Bit Classification Table
QoS > Policer > Policer Profile	Configuring Policer Profiles
QoS > Marking > 802.1Q	Modifying the 802.1Q Marking Table

Sub-Menus	For Further Information
QoS > Marking > 802.1AD	Modifying the 802.1AD Marking Table
QoS > WRED > WRED Profile	Configuring WRED
QoS > Shaper > Queue Profiles	Configuring Queue Shaper Profiles
QoS > Scheduler > Priority Profiles	Configuring Priority Profiles
QoS > Scheduler > WFQ Profiles	Configuring WFQ Profiles
Protocols > Bandwidth Notification	Planned for future release.
Protocols > LLDP > Remote Management	Planned for future release.
Protocols > LLDP > Advanced > Configuration > Parameters	Planned for future release.
Protocols > LLDP > Advanced > Configuration > Port Configuration	Planned for future release.
Protocols > LLDP > Advanced > Configuration > Destination Address	Planned for future release.
Protocols > LLDP > Advanced > Configuration > Management TLV	Planned for future release.
Protocols > LLDP > Advanced > Remote System > Management	Planned for future release.

Sub-Menus	For Further Information
Protocols > LLDP > Advanced > Remote System > Remote Table	Planned for future release.
Protocols > LLDP > Advanced > Local System > Parameters	Planned for future release.
Protocols > LLDP > Advanced > Local System > Port	Planned for future release.
Protocols > LLDP > Advanced > Local System > Management	Planned for future release.
Protocols > LLDP > Advanced > Statistic > General	Planned for future release.
Protocols > LLDP > Advanced > Statistic > Port TX	Planned for future release.
Protocols > LLDP > Advanced > Statistic > Port RX	Planned for future release.
Protocols > SOAM > MD	Configuring Service OAM (SOAM) Fault Management (FM)
Protocols > SOAM > MA/MEG	Configuring Service OAM (SOAM) Fault Management (FM)
Protocols > SOAM > MEP	Configuring Service OAM (SOAM) Fault Management (FM)
Protocols > LACP > Aggregation	Planned for future release.
Protocols > LACP > Port > Status	Planned for future release.
Protocols > LACP > Port > Statistics	Planned for future release.

Sub-Menus	For Further Information
Protocols > LACP > Port > Debug	Planned for future release.
Interfaces > Groups > LAG	Planned for future release.

Table 5 Web EMS Menu Hierarchy – Sync Menu

Sub-Menus	For Further Information
SyncE Regenerator	Planned for future release.
Sync Source	Configuring the Sync Source
Outgoing Clock	Configuring the Outgoing Clock and SSM Messages
1588 > General Configuration	
1588 > Transparent Clock	
1588 > Boundary Clock > Clock Parameters > Default	Planned for future release.
1588 > Boundary Clock > Clock Parameters > Advanced	Planned for future release.
1588 > Boundary Clock > Port Parameters	Planned for future release.
1588 > Boundary Clock > Port Statistics	Planned for future release.

Table 6 Web EMS Menu Hierarchy – Quick Configuration Menu

Sub-Menus	For Further Information
From Release Plan	Planned for future release.
Platform Setup	Performing Quick Platform Setup
Security > General Parameters	Quick Security Configuration – General Parameters Page
Security > Protocols	Quick Security Configuration – Protocols Page
Security > Access Control	Quick Security Configuration – Access Control Page

Sub-Menus	For Further Information
Security > RSA Key & Certificate	Quick Security Configuration – RSA Key & Certificate Page
PIPE > Single Carrier > 1 + 0	Configuring a 1+0 Link Using the Quick Configuration Wizard
PIPE > Link Bonding > Configure as Main (Multiband) PTP 850E	Configuring a Layer 1 Link Bonding Link Using the Quick Configuration Wizard
PIPE > Link Bonding > Configure as Main (N+0)3 PTP 850C	Configuring a Layer 1 Link Bonding Link Using the Quick Configuration Wizard
PIPE > Link Bonding > Configure as Attached	Configuring a Layer 1 Link Bonding Link Using the Quick Configuration Wizard

Table 7 Web EMS Menu Hierarchy – Utilities Menu

Sub-Menus	For Further Information
Restart HTTP	Restarting the HTTP Server
ifIndex Calculator	Calculating an ifIndex
MIB Reference Guide	Displaying, Searching, and Saving a list of MIB Entities

3. Getting Started

This chapter lists and describes the steps that you must perform to establish basic connectivity with the PTP 850 unit and the basic radio parameters necessary to establish a link. Some of the procedures in this chapter are only necessary for certain hardware configurations or link types, as described below.

This section includes:

- Antenna Alignment Mode (PTP 850E)
- Assigning IP Addresses in the Network
- Establishing a Connection
- Logging on
- Changing Your Password
- Applying a Pre-Defined Configuration File
- Performing Quick Platform Setup
- Configuring In-Band Management
- Changing the Management IP Address
- Enabling Dynamic IPv6 Addresses Via DHCPv6
- Configuring DSCP/TC for Management
- Configuring the Activation Key
- Setting the Time and Date (Optional)
- Enabling the Interfaces (Interface Manager)
- Configuring the Radio (MRMC) Script(s)
- Running the Frequency Scanner
- Configuring the Radio Parameters
- **Error! Reference source not found.**
- Creating Service(s) for Traffic
- Configuring CPRI
- Operating in FIPS Mode
- Encrypting the Protection Link

3.1 Antenna Alignment Mode (PTP 850E)

Antenna Alignment Mode Overview

FromSystem Release 13.0, PTP 850E has two operational modes:

- Alignment Mode – Used exclusively for antenna alignment.

- Operational Mode – Used for normal operation.

These modes are mutually exclusive. In Alignment Mode, the only Web EMS page you should use is the Antenna Alignment page. Using any other Web EMS page when in Alignment Mode can cause the system to become unstable.

When a new PTP 850E device is powered up for the first time running System Release 13.0 or higher, it is automatically activated in Alignment Mode.

In Alignment Mode, the transmitter is unmuted by default, as opposed to normal operating mode, and reception is possible at much lower RX levels as described below.

This enables operators to perform alignment on a new PTP 850E device without the need to perform any management or initial configuration whatsoever.

If an PTP 850E device running a System Release version older than 13.0 is upgraded to System Release 13.0 or higher, it comes up in normal operating mode after the upgrade.

If an PTP 850E device running System Release 13.0 or higher is reset to its default settings, the default operating mode when the device comes back up is as follows:

If Alignment Mode was never disabled since the new device was first powered up, the device comes back up in Alignment Mode.

If Alignment Mode was disabled even once, the device comes up in normal operating mode even if the device was in Alignment Mode when it was reset to its default settings.

In any case, you can enable and disable Alignment Mode from the Antenna Alignment page of the Web EMS as described below.

The purpose of Alignment Mode is to facilitate antenna alignment and installation. Alignment Mode enables reception at much lower Rx levels. It also leads to better detection of the antenna's initial position for purposes of alignment.

As a result, installers can align the antenna faster and more accurately. This saves installation costs by shortening the average time of installation.

When alignment has been completed, you can exit Alignment Mode and configure the device for ordinary usage. Alternatively, if the device will not go into operation right away, it should be powered down so that it will not continue to transmit in Alignment Mode.



Note

It is recommended that you verify the link's RSL levels in normal operational mode rather than in Alignment Mode once antenna alignment has been completed.

Alignment Mode is completely detached from ordinary operating mode. This means that configurations you make in the Antenna Alignment page have no application to the ordinary configuration of the device. If you attempt to change the radio parameters outside of the Antenna Alignment page while the device is in Alignment Mode, unexpected functionality may occur.

By default, the Receiver is set to the minimum receiving bandwidth. The default frequencies are set automatically according to whether the device hardware is High or Low, with the following default frequencies:

- High unit:
    - TX Frequency: 83,500 MHz

- RX Frequency: 73,500 MHz

- Low Unit:
  - TX Frequency: 73,500 MHz
  - RX Frequency: 83,500 MHz

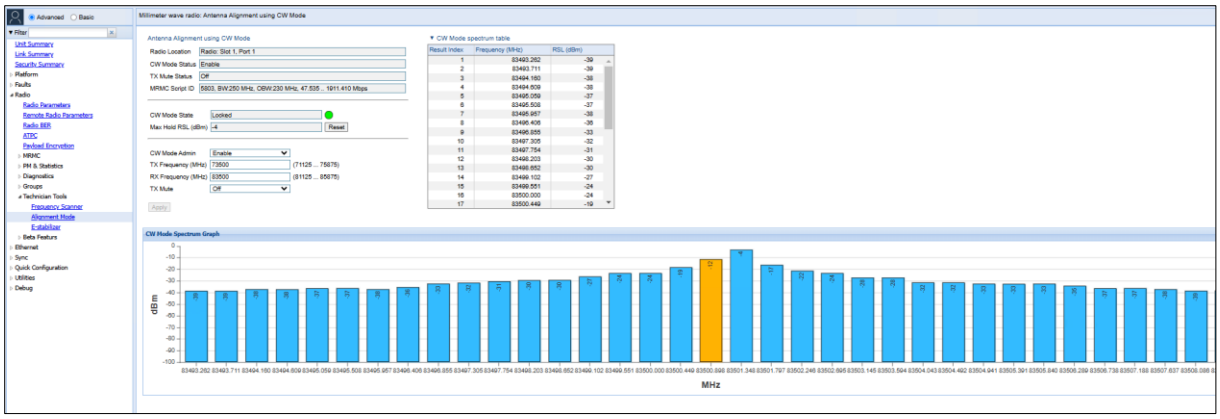
Disabling Alignment Mode causes a unit reset.

Antenna Alignment Mode Operation

To configure the Alignment Mode settings and change from Alignment Mode to regular operating mode (and back to Alignment Mode):

1. Select **Radio > Technician Tools > Antenna Alignment**. The Antenna Alignment page opens.

   Figure 32: Antenna Alignment Page



1 In the **CW Mode Admin** field, select **Disable** to disable Alignment Mode and return to regular operation or **Enable** to enable Alignment Mode. Disabling Alignment Mode causes unit reset.
2 The **TX Frequency (MHz.)** and **RX Frequency (MHz.)** fields enable you to change the default frequency settings.
3 The **TX Mute** field enables you to mute or unmute the transmitter. By default, the transmitter is unmuted in Alignment Mode.
4 The **CW Mode State** field displays the status of the link:
   - **Locked** – The link with the remote unit is up.
   - **Standby** – There is currently no link. This could be because the remote unit is offline or the link has not yet locked.
   - **Disabled** – Alignment Mode is disabled.
5 The **Max Hold RSL (dBm)** field displays the best RSL measured since last Max Hold RSL reset or device power up. The **Reset** button is located to the right of this field.
6 The **CW Mode Spectrum** table displays the current RSL per frequency. This same information is displayed in graphical format beneath the table. In the **CW Mode Spectrum Graph**, the currently locked frequency and RSL are displayed in yellow.
7 Click **Apply** to save any configuration changes.

3.2 Assigning IP Addresses in the Network

Before connection over the radio hop is established, it is of high importance that you assign the PTP 850E unit a dedicated IP address, according to an IP plan for the total network. See Changing the Management IP Address.

By default, a new PTP 850E unit has the following IP settings:

IP address: 192.168.1.1

Subnet mask: 255.255.255.0



Caution

If the connection over the link is established with identical IP addresses, an IP address conflict will occur and remote connection may be lost.

3.3 Establishing a Connection

Connect the PTP 850E unit to a PC by means of a Twisted Pair cable. The cable is connected to the MGT port on the PTP 850E and to the LAN port on the PC. Refer to the Installation Guide for the type of unit you are connecting for cable connection instructions.

3.4 PC Setup

To obtain contact between the PC and the PTP 850E unit, it is necessary to configure an IP address on the PC within the same subnet as the PTP 850E unit. The default PTP 850E IP address is 192.168.1.1. Set the PC address to e.g. 192.168.1.10 and subnet mask to 255.255.255.0. Note the initial settings before changing.



Note

The PTP 850E IP address, as well as the password, should be changed before operating the system. See Changing the Management IP Address and Changing Your Password.

1. Select **Control Panel** > **All Control Panel Items** > **Network and Sharing Center**.
2. Click **Change the adapter settings**.
3. Select **Local Area Connection** > **Properties** > **Internet Protocol Version 4 (TCP/IP)**, and set the following parameters:

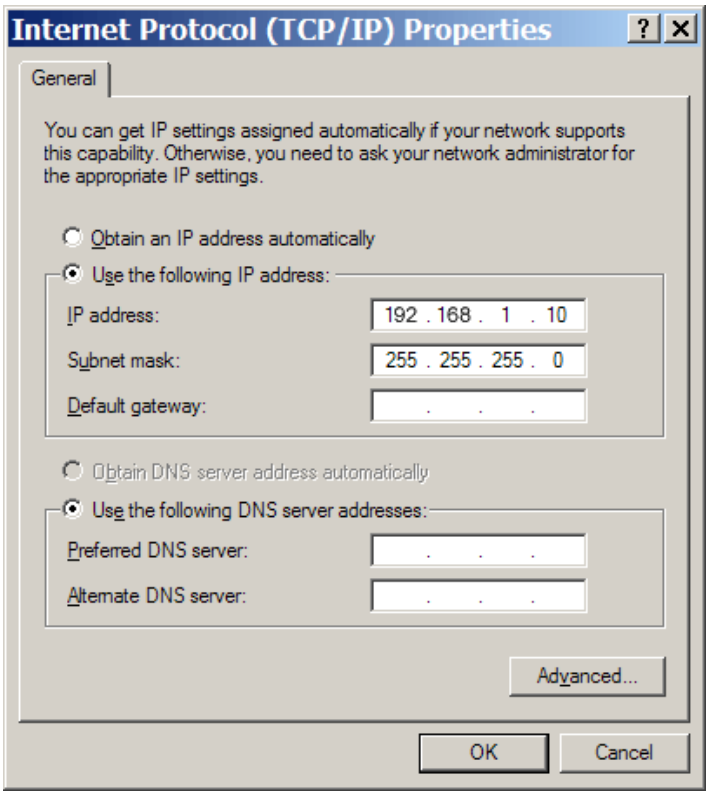
IP address: 192.168.1.10

Subnet mask 255.255.255.0

No default gateway

4. Click **OK** to apply the settings.

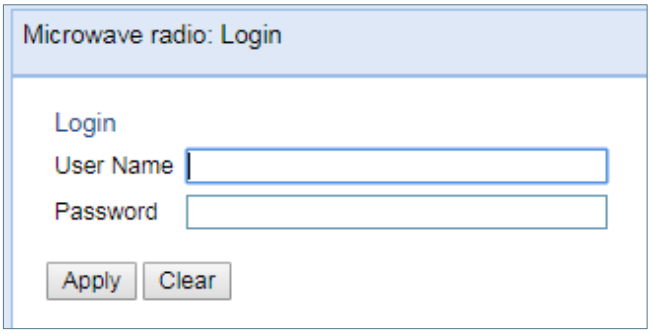
Figure 33 Internet Protocol Properties Window



3.5 Logging on

1. Open an Internet browser (Internet Explorer or Mozilla Firefox).
2. Enter the default IP address “192.168.1.1” in the Address Bar. The Login page opens.

Figure 34 Login Page



3. In the Login window, enter the following:

User Name: **admin**

Password: **admin**

4. Click **Apply**.

Logging in Without Knowing the IP Address

If the unit's IP address has been changed from its default of 192.168.1.1, and you do not know the new IP address, you can log into the unit by establishing a connection directly to the CPU. This requires a Cambium Networks proprietary Ethernet cable. This cable should be ordered from Cambium Networks, according to the following table.

Table 9: Cable for Direct CPU Connection

Product	Cable Marketing Model	Cable Description
PTP 850C	SPL-ETH-CBL	CABLE,RJ45 TO 2XRJ45F, 0.54M,CAT-5E,FOR ETH
PTP 850E	DP to RJ45 MNG CABLE	CABLE,DP TO RJ45F,0.2M,FOR FIELD DEBUG
PTP 850S	PTP 820_Mini-MNG-CBL_ESP	CABLE,MiniDP TO RJ45F,0.2M,FOR FIELD DEBUG. ESP

For PTP 850E, as an alternative to the proprietary cable described above, you can use a cable with the following pinouts:

Side A – DisplayPort		Diff. Pair	Side B- RJ-45 Socket	
PROT_TX_P	15	Pair 1	PROT_TX_P	1
PROT_TX_N	17		PROT_TX_N	2
PROT_RX_P	18	Pair 2	PROT_RX_P	3
PROT_RX_N	19		PROT_RX_N	6
Shell		Shield	Shell	

For PTP 850S, as an alternative to the proprietary cable described above, you can use a cable with the following pinouts:

P1	WIRE	P2
14	TWISTED PAIR 1	3
16		6
18	TWISTED PAIR 2	1
20		2
SHELL	SHIELD	SHELL

To log in using this cable:

1 Disconnect the management cable from the PTP 850E.

2 The IP address of the CPU is 192.0.2.1. To connect, set up a new Local Area Connection with an IP address as follows:

- IP address: 192.0.2.3
- Subnet mask 255.255.255.240
  - No default gateway

3 Connect the single end of the cable to the Protection port of the PTP 850 unit.

- For PTP 850C: The Management/Protection port (P6).
- For PTP 850E: The Protection port (P6).
- For PTP 850S: The EXT port (P4).

4 Connect Channel 2 of the cable to the LAN port on the PC.

5 The system will prompt you for a user name and password.

6 Enter the user name and password. The default user name and password are:

- User Name: **admin**
- Password: **admin**

7 Click **Apply**.

After a connection is established, you can view or configure the unit's IP address using the Web EMS. See Changing the Management IP Address.

3.6 Changing Your Password

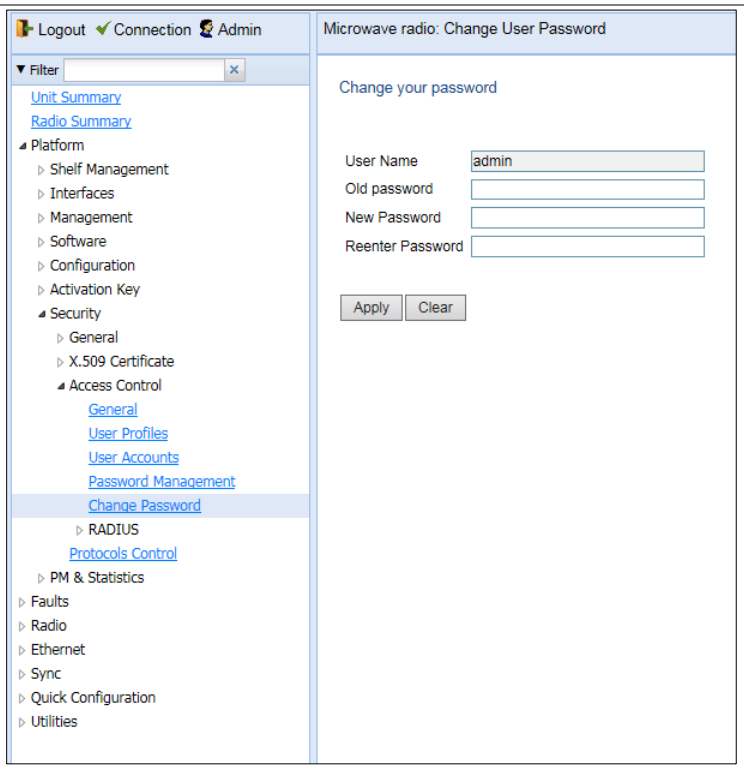
It is recommended to change your default Admin password as soon as you have logged into the system.

In addition to the Admin password, there is an additional password protected user account, “root user”, which is configured in the system. The root user password and instructions for changing this password are available from Cambium Networks Customer Support. It is strongly recommended to change this password.

To change your password:

2. Select **Platform** > **Security** > **Access Control** > **Change Password**. The Change User Password page opens.

Figure 35 Change User Password Page



3. In the **Old password** field, enter the current password. For example, upon initial login, enter the default password (**admin**).

4. In the **New password** field, enter a new password. If **Enforce Password Strength** is activated (see Configuring the Password Security Parameters), the password must meet the following criteria:

Password length must be at least eight characters.

Password must include characters of at least three of the following character types: lower case letters, upper case letters, digits, and special characters. For purposes of meeting this requirement, upper case letters at the beginning of the password and digits at the end of the password are not counted.

A password cannot be repeated within five changes of the password.

5. Click **Apply**.

In addition to the Admin password, there is an additional password protected user account, “root user”, which is configured in the system. The root user password and instructions for changing this password are available from Cambium Networks Customer Support. It is strongly recommended to change this password.

3.7 Applying a Pre-Defined Configuration File

PTP 850E units can be configured from the Web EMS in a single step by applying a pre-defined configuration file. A pre-defined configuration file can be prepared for multiple PTP 850E units, with the relevant configuration details specified and differentiated per-unit.

Pre-defined configuration files can include all the parameters necessary to configure basic links, including:

Platform parameters:

- ETSI to ANSI conversion
- General unit parameters, such as unit name, location, and contact person

- Activation Key (or Demo mode) configuration
- IP configuration (IPv4 and IPv6)
- NTP configuration
- Basic SNMP Parameters (Enable/Disable, Read and Write Communities)
- Time services configuration

Interface configuration:

- Radio
- Ethernet
- Radio protection

Advanced radio configuration

- XPIC

Services configuration

- Management
- Point-to-Point
- Multipoint

The pre-defined configuration file is generated by Cambium Global Services and provided as a service.

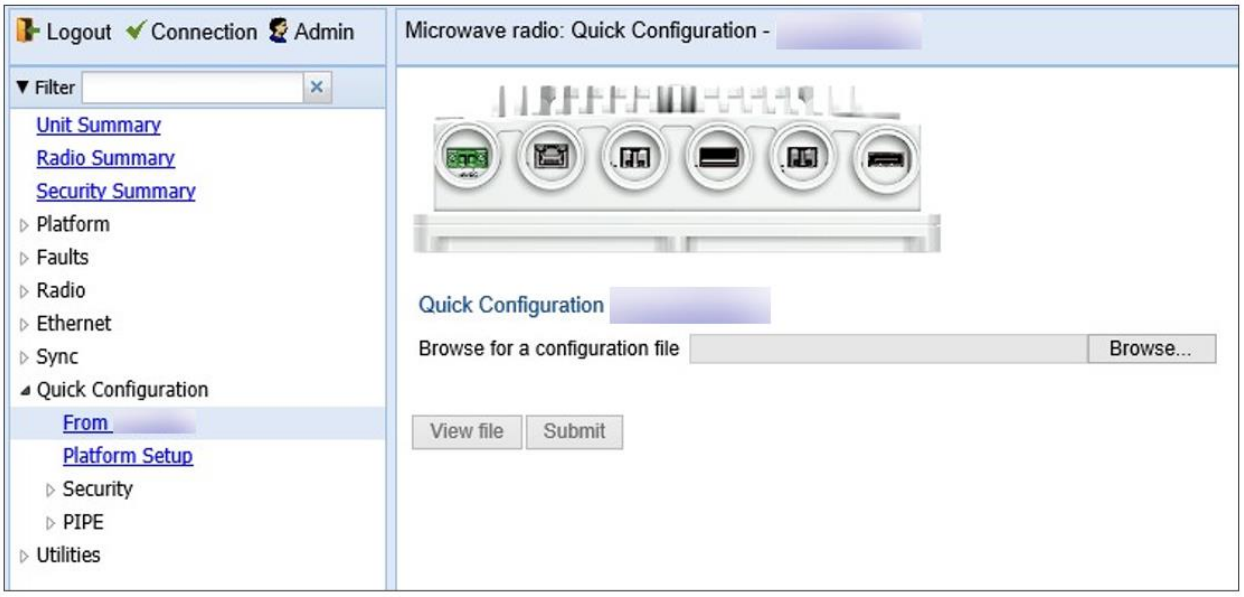
The pre-defined configuration file must be compatible with the System release version the PTP 850E device is running. Configuration files must also be compatible with the type of device. For example, a configuration file created for PTP 820E cannot be applied to an PTP 850E device.

For further information on the creation of pre-defined configurations, consult your Cambium representative.

To apply a pre-defined configuration file:

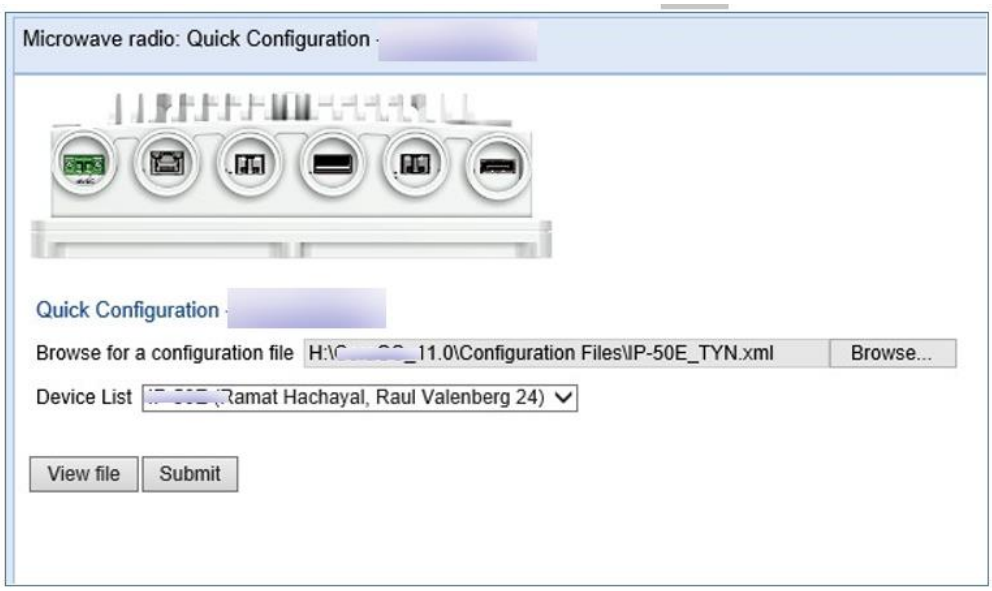
1 Select **Quick Configuration > From File**. The Quick Configuration – From File page opens.

Figure 36 Quick Configuration – From File Page



2 Click Browse, and select the configuration file for your unit.

Figure 37 Quick Configuration – From File Page – Configuration File Loaded



3 In the **Device List** field, select the unit you are configuring.

Note

Although the configuration file may contain parameters for multiple

types of devices, only devices of the same product type as the unit you are configuring are displayed in this field.

4 Optionally, click **View file** to display the configuration file (read-only).

5 To initiate the configuration, click **Submit**. Progress is updated in the Quick Configuration – From File page.

When the configuration is complete, the unit reboots.

Note

If the pre-defined configuration file included a new IP address for the unit, make sure to configure an IP address on the PC or laptop you are using to perform the configuration within the same subnet as the PTP 850E unit's new IP address.

3.8 Performing Quick Platform Setup

The Platform Setup page in the Web EMS centralizes the main configurable items from several Web EMS pages in a single location:

Unit Parameters (Name, Contact Person, Location, Longitude, and Latitude)

IPv4 Address, Subnet Mask, and Default Gateway

NTP Enable/Disable

Demo Activation Key Enable/Disable

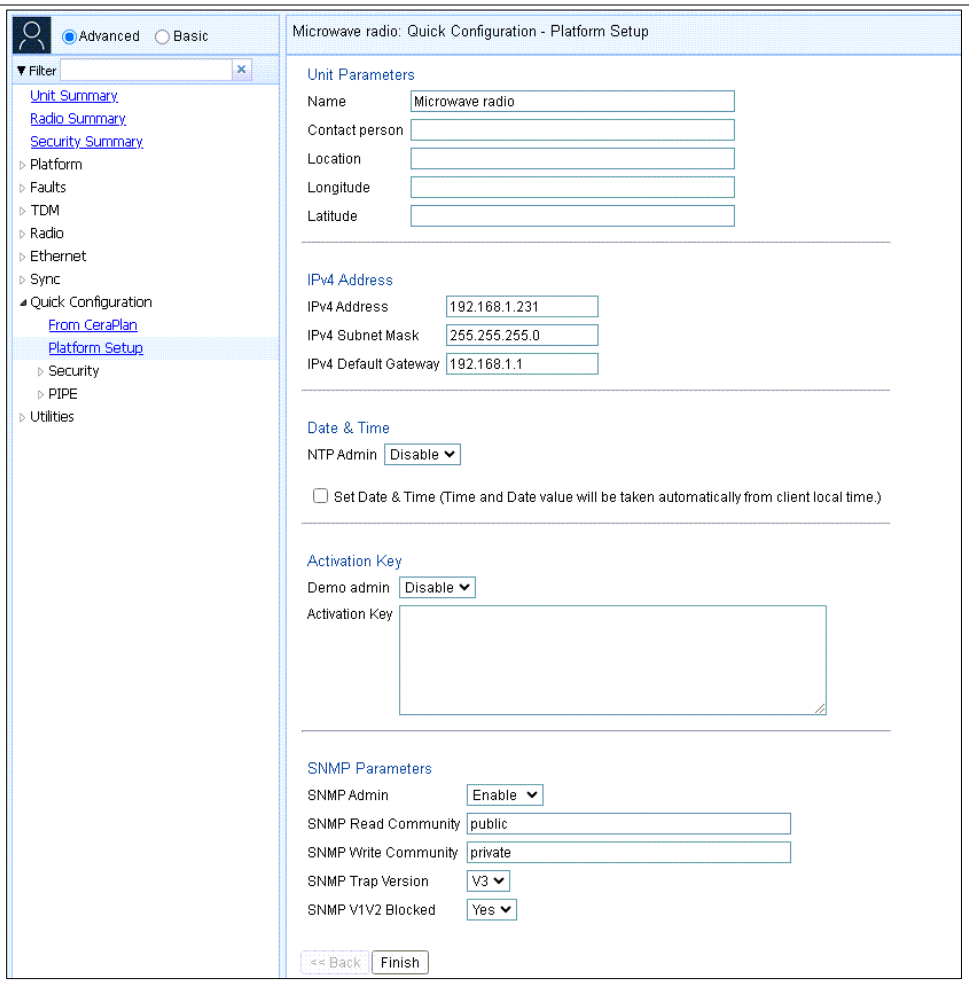
SNMP Parameters

These items enable you to configure the basic platform parameters quickly, in a single Web EMS page. Combined with the quick link configuration wizards, this enables you to configure a new link in the field quickly and efficiently, to the point where the link is up and functioning and any necessary advanced configurations can be performed remotely without the need to physically access the PTP 850E unit.

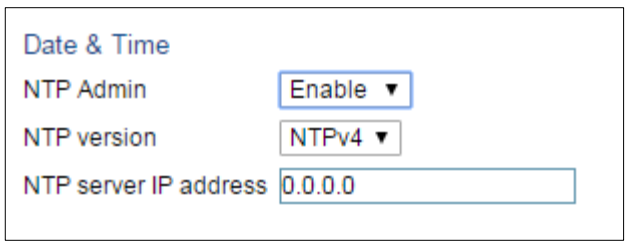
To use the Platform Setup page:

1. Select **Quick Configuration** > **Platform Setup**. The Quick Configuration – Platform Setup page opens.

Figure 38 Quick Configuration – Platform Setup Page



1. The Unit Parameters section is optional. For details on each field, see Configuring Unit Parameters.
2. In the IPv4 Address section, configure the unit's management IP address, subnet mask, and, optionally, a default gateway. If you want to use an IPv6 address, see Changing the Management IP Address.
3. In the Date & Time section, you can enable Network Time Protocol (NTP). NTP distributes Coordinated Universal Time (UTC) throughout the system, using a jitter buffer to neutralize the effects of variable latency.
   If you select **Enable**, the **NTP version** and **NTP server IP address** fields are also displayed, enabling you to configure the NTP parameters. For details on these fields, see Configuring NTP.



4. In the Activation Key section, you can enable or disable Demo mode in the **Demo admin** field. Demo mode enables all features for 60 days. When demo mode expires, the most recent valid activation key goes into effect. The 60-day period is only counted when the system is powered up. 10 days before demo mode expires, an alarm is raised indicating that demo mode is about to expire.
   If you set **Demo admin** to **Disable**, the Activation Key field is displayed. Enter a valid activation key in this field. For a full explanation of activation keys, see Optionally, in the **Description** field, enter descriptive information about the unit.

1. In the **IPv4 address** field, enter an IP address for the unit. You can enter the address in IPv4 format in this field, and/or in IPv6 format in the **IPv6 Address** field. The unit will receive communications whether they are sent to its IPv4 address or its IPv6 address.
2. If you entered an IPv4 address, in the **IPv4 Subnet mask** field, enter the subnet mask.
3. Optionally, in the **IPv4 Default gateway** field, enter the default gateway address.
4. In the **IPv6 Assignment Mode** field, you can configure dynamic IPv6 assignment via DHCP by selecting **Automatic (DHCP)**. For instructions, see Enabling Dynamic IPv6 Addresses Via DHCPv6.

   Note: **By default, the IPv6 Assignment Mode** field is set to **Manual**.

5. If you are configuring IPv6 in Manual mode, in the **IPv6 Address** field, enter an IPv6 address for the unit. You can enter the address in IPv6 format in this field, and/or in IPv4 format in the **IPv4 IP Address** field. The unit will receive communications whether they are sent to its IPv4 address or its IPv6 address.
6. If you entered an IPv6 address, enter the IPv6 prefix length in the **IPv6 Prefix-Length** field.
7. Optionally, if you entered an IPv6 address, enter the default gateway in IPv6 format in the **IPv6 Default Gateway** field.
8. Click **Apply**.

   Note: **For an explanation of the IPv6 Link Local Address** field, see Enabling Dynamic IPv6 Addresses Via DHCPv6.

3.9 Enabling Dynamic IPv6 Addresses Via DHCPv6

Related Topics:

- Defining the IP Protocol Version for Initiating Communications
- Configuring the Remote Unit's IP Address

Optionally, you can configure the device to obtain its IPv6 address automatically from a DSCP server. To configure the device to IPv6 Automatic mode, you must enable Automatic mode in the Local Networking Configuration page.

Once IPv6 Automatic mode is configured, the manually configured IPv6 address is stored but not used by the device. It is used again if and when IPv6 Automatic mode is disabled. Before enabling IPv6 Automatic mode, you should record the IPv6 Link Local Address, which is displayed in the Local Networking Configuration page. The Link Local IPv6 address can be used to re-connect to the device if the DHCPv6 server is unavailable.

After enabling IPv6 Automatic mode, the address obtained automatically from the DHCPv6 server can be used to re-connect to the device. You can also use the device's IPv4 address.

Once you have re-established the management connection, you can view the IPv6 configuration the device has obtained from the DHCP server in the Local Networking Configuration page.

To enable IPv6 Automatic mode:

1 Select **Platform > Management > Networking > Local**. The Local Networking Configuration page opens.

Note: To display the same page in Basic mode, without the IP Family Configuration option, select **Platform > IP Configuration**.

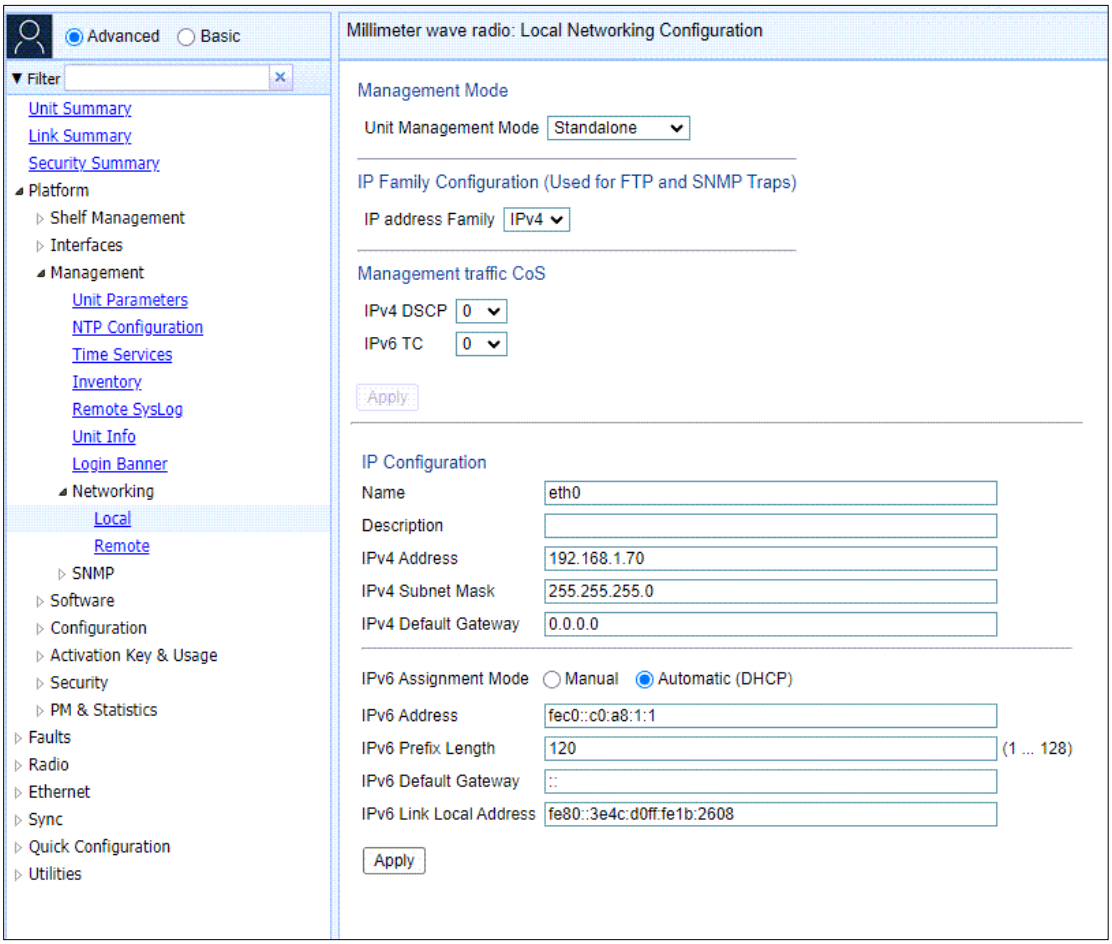


Figure 42: Local Networking Configuration Page (IPv6 Automatic Mode)

2 Record the address displayed in the **IPv6 Link Local Address** field to ensure that you can restore the management connection to the device after enabling IPv6 Automatic mode.
3 In the **IPv6 Assignment Mode** field, select **Automatic (DHCP)**.
4 Click **Apply**. Management will be lost until the device obtains a new IP address from the DHCP server. However, you can still access the device via its IPv4 address or the IPv6 Link Local Address.
5 For configurations with unit redundancy, make sure to perform copy-to-mate as soon as the management connection is restored, to ensure that in case of switchover, the IPv6 address of the Standby unit is aligned with that of the Active unit.

In the event that the Standby unit is to be moved to a different setup, to act as either the Active or Standby unit in that setup, it is recommended to first clear the DUID (DHCP Unique Identifier) in order to prevent duplicate DUIDs in the new setup. This must be done via CLI, using the following command:

```
root> platform management ip reset ipv6-duid
```

Note: The DUID is used in IPv6 to provide unique identification for devices.

5. Configuring DSCP/TC for Management

In certain situations when using in-band management, management data and user traffic are not separated by VLANs. This happens if both are untagged or use the same VLAN.

In such cases, you can assign a DSCP (IPv4) or TC (IPv6) value to management data in order to distinguish it from user traffic. While ingress management packets will have whatever DSCP/TC they were originally assigned, when they egress from the CPU they will carry the assigned DSCP or TC. This enables you to ensure that management packets from the device have priority and will continue to be sent even when there is congestion.

Note: By default, the DSCP/TC value assigned to management traffic egressing the device is 0.

The following settings are required for these DSCP/TC settings to work properly:

- For all logical interfaces, the **Trust VLAN UP bits** parameter must be set to **Un-Trust**.
- For the management service, the **CoS Mode** must be set to **Preserve-SP-COS-Decision**.
- If the device is the main unit in a Link Bonding configuration, add service points for the Management service on the interfaces passing traffic to the paired units, with the same VLAN used for management.

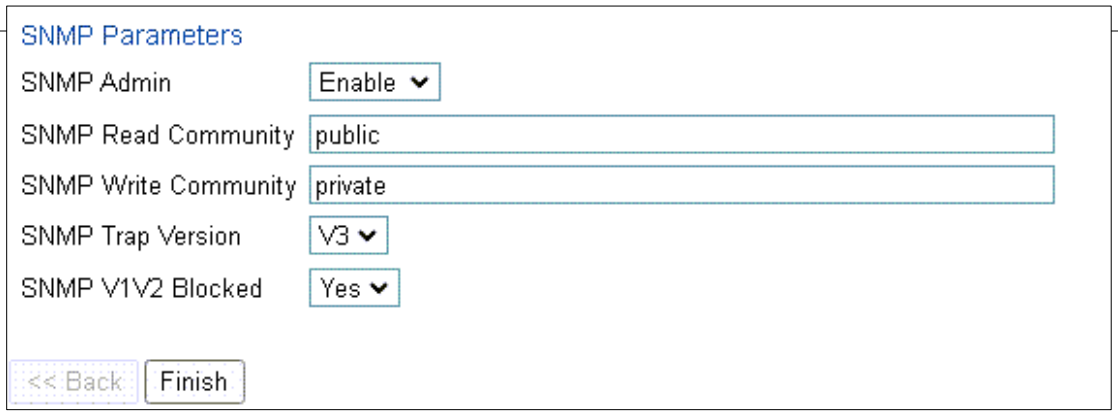
To configure DSCP/TC for management:

1 Select **Platform** > **Management** > **Networking** > **Local**. The Local Networking Configuration page opens.
2 In the **IPv4 DSCP** field, select a DSCP value for management connections that use IPv4 protocol.
3 In the **IPv6 TC** field, select a TC value for management connections that use IPv6 protocol.
4 Click **Apply** underneath the **IPv6 TC** field.

6. Configuring the Activation Key.

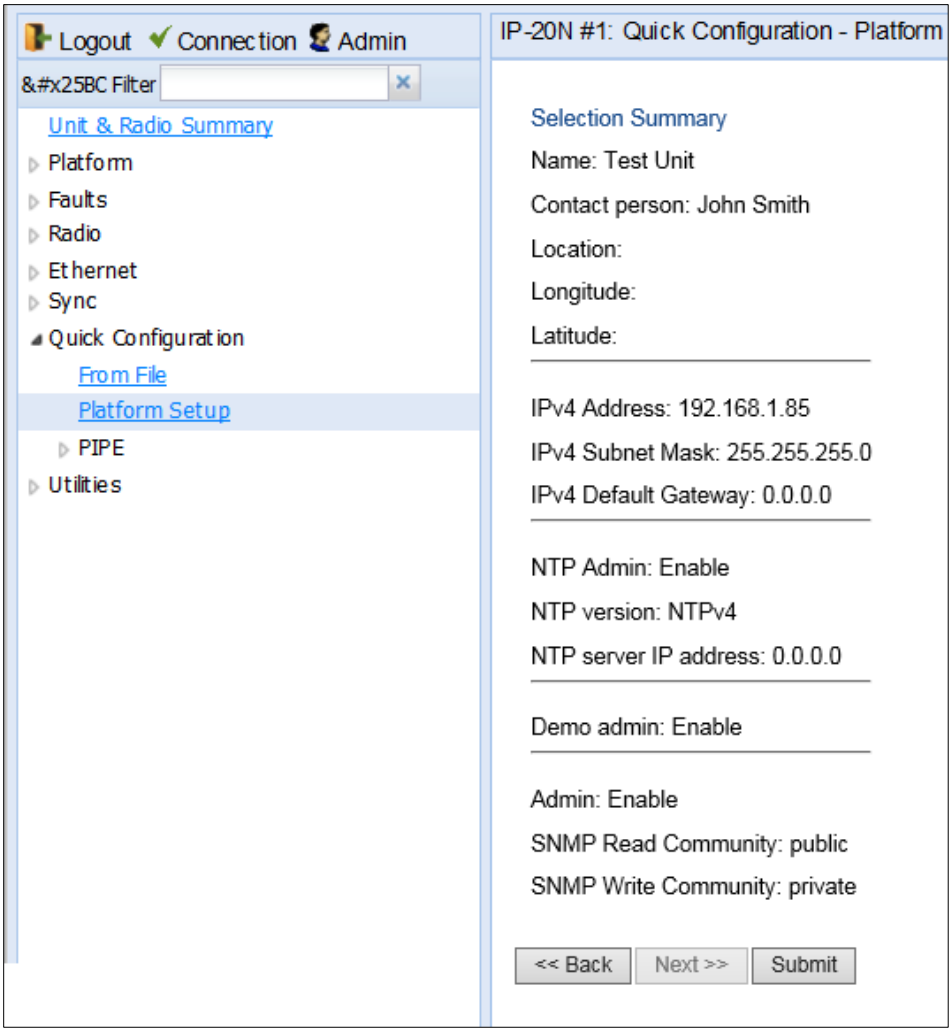


7. In the **SNMP Parameters** section, you can set whether to enable or disable SNMP monitoring in the **SNMP Admin** field, and set the **SNMP Read Community** and **SNMP Write Community**. You can also configure the **SNMP Trap Version**. By default, this is set to **V3** and the **SNMP V1V2 Blocked** field is set to **Yes** so that only SNMPv3 access is enabled.



8. Click **Finish**. The Selection Summary page opens. To go back and change any of the parameters, click **Back**. To implement the new parameters, click **Submit**.

Figure 39 Quick Configuration– Platform Setup Summary Page



3.10 Configuring In-Band Management

You can configure in-band management in order to manage the unit remotely via its radio and/or Ethernet interfaces.



Note

Before configuring in-band management, it is recommended to review the configuration recommendations for in-band management.

Each PTP 850 unit includes a pre-defined management service. The Service ID for this service is:

- PTP 850S: 257
- PTP 850C and PTP 850E

The management service is a multipoint service that connects the two local management ports and the network element host CPU in a single service. In order to enable in-band management, you must add at least one service point to the management service, in the direction of the remote site or sites from which you want to access the unit for management.



Note

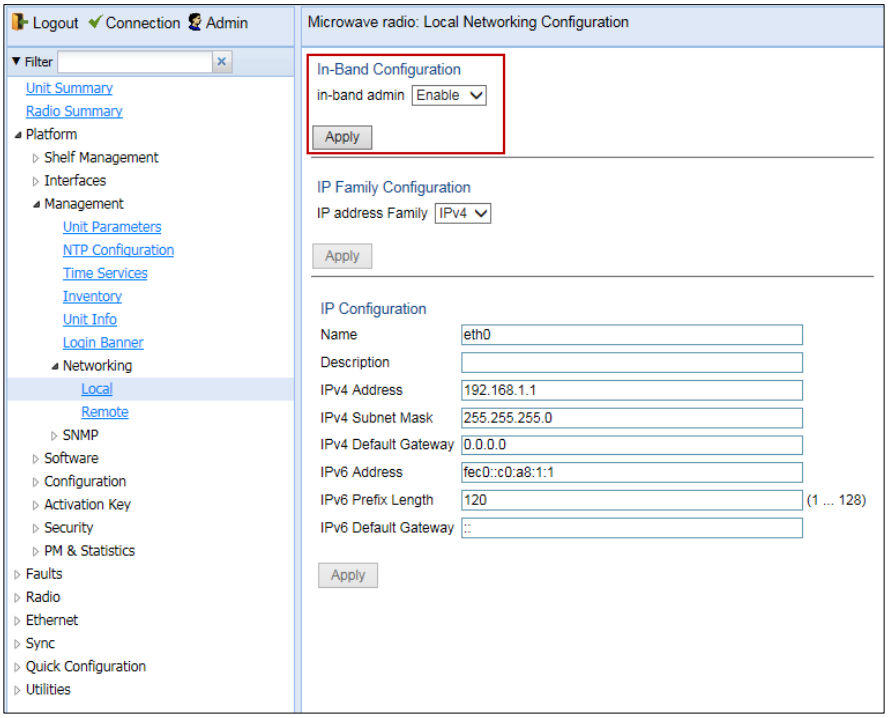
In order to use in-band management, it must be supported on the external switch.

For instructions on adding service points, see Configuring Service Points.

After adding service points, you must enable in-band management. To enable in-band management:

1. Select **Platform** > **Management** > **Networking** > **Local**. The Local Networking Configuration page opens.

Figure 40 Local Networking Configuration Page – In-Band Management



2. In the **In-Band Admin** field, select **Enable**.
3. Click **Apply** underneath the **In-Band Admin** field.

3.11 Changing the Management IP Address

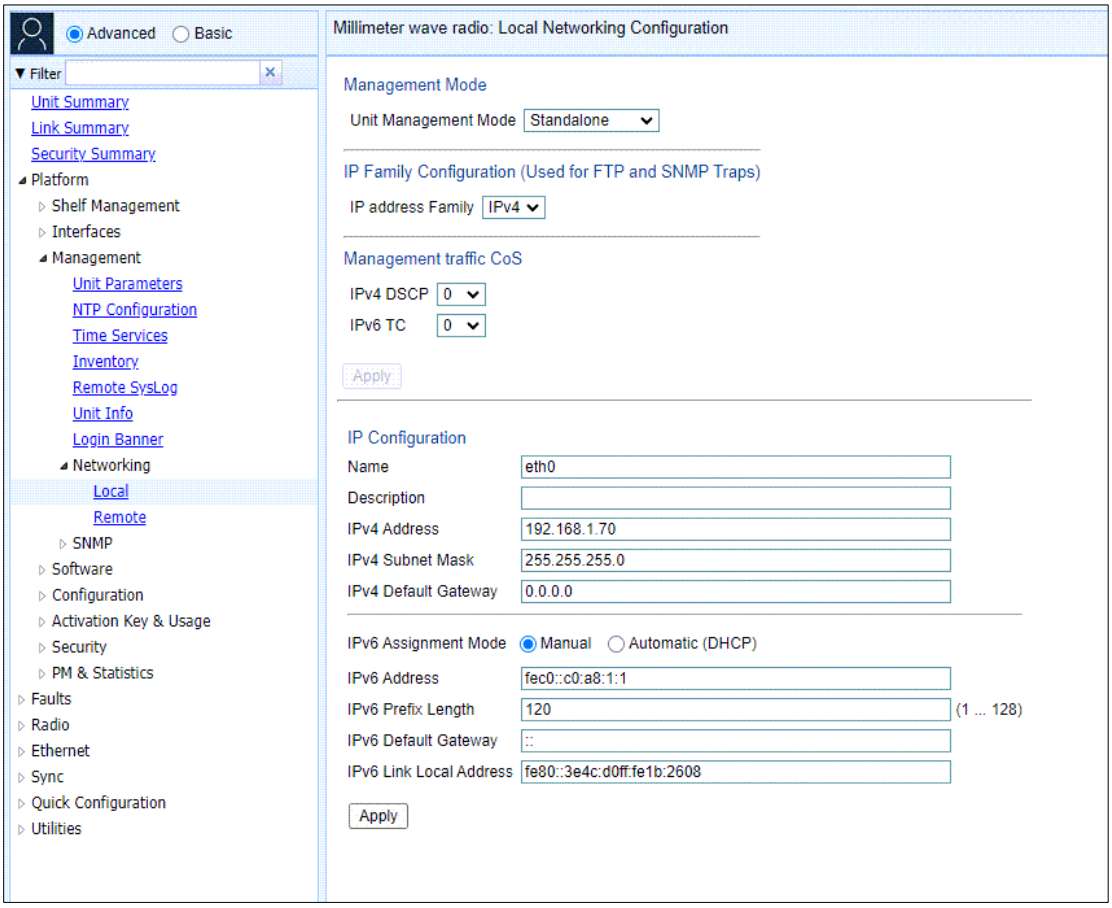
Related Topics:

- Configuring In-Band Management
- Defining the IP Protocol Version for Initiating Communications
- Configuring the Remote Unit's IP Address

To change the management IP address of the local unit:

9. Select **Platform > Management > Networking > Local**. The Local Networking Configuration page opens. IP address configuration is performed in the IP Configuration area of the page.

Figure 41 Local Networking Configuration Page



10. Optionally, in the **Name** field, enter a name for the unit.
11. Optionally, in the **Description** field, enter descriptive information about the unit.
12. In the **IPv4 address** field, enter an IP address for the unit. You can enter the address in IPv4 format in this field, and/or in IPv6 format in the **IPv6 Address** field. The unit will receive communications whether they are sent to its IPv4 address or its IPv6 address.
13. If you entered an IPv4 address, in the **IPv4 Subnet mask** field, enter the subnet mask.
14. Optionally, in the **IPv4 Default gateway** field, enter the default gateway address.
15. In the **IPv6 Assignment Mode** field, you can configure dynamic IPv6 assignment via DHCP by selecting **Automatic (DHCP)**. For instructions, see Enabling Dynamic IPv6 Addresses Via DHCPv6.

    Note: **By default, the IPv6 Assignment Mode** field is set to **Manual**.

16. If you are configuring IPv6 in Manual mode, in the **IPv6 Address** field, enter an IPv6 address for the unit. You can enter the address in IPv6 format in this field, and/or in IPv4 format in the **IPv4 IP Address** field. The unit will receive communications whether they are sent to its IPv4 address or its IPv6 address.
17. If you entered an IPv6 address, enter the IPv6 prefix length in the **IPv6 Prefix-Length** field.
18. Optionally, if you entered an IPv6 address, enter the default gateway in IPv6 format in the **IPv6 Default Gateway** field.
19. Click **Apply**.

    Note: **For an explanation of the IPv6 Link Local Address** field, see Enabling Dynamic IPv6 Addresses Via DHCPv6.

3.12 Enabling Dynamic IPv6 Addresses Via DHCPv6

Related Topics:

- Defining the IP Protocol Version for Initiating Communications
- Configuring the Remote Unit's IP Address

Optionally, you can configure the device to obtain its IPv6 address automatically from a DSCP server. To configure the device to IPv6 Automatic mode, you must enable Automatic mode in the Local Networking Configuration page.

Once IPv6 Automatic mode is configured, the manually configured IPv6 address is stored but not used by the device. It is used again if and when IPv6 Automatic mode is disabled. Before enabling IPv6 Automatic mode, you should record the IPv6 Link Local Address, which is displayed in the Local Networking Configuration page. The Link Local IPv6 address can be used to re-connect to the device if the DHCPv6 server is unavailable.

After enabling IPv6 Automatic mode, the address obtained automatically from the DHCPv6 server can be used to re-connect to the device. You can also use the device's IPv4 address.

Once you have re-established the management connection, you can view the IPv6 configuration the device has obtained from the DHCP server in the Local Networking Configuration page.

To enable IPv6 Automatic mode:

1 Select **Platform > Management > Networking > Local**. The Local Networking Configuration page opens.

Note: To display the same page in Basic mode, without the IP Family Configuration option, select **Platform > IP Configuration**.

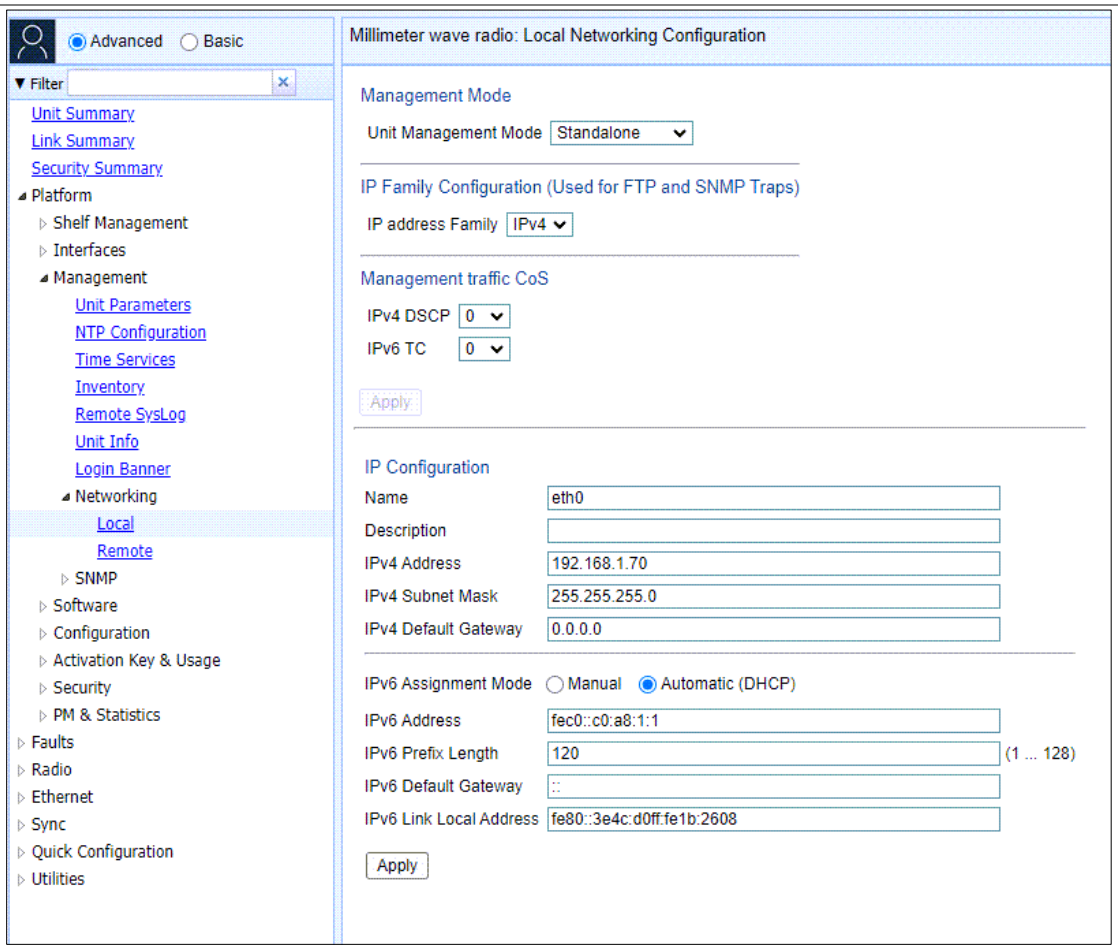


Figure 42: Local Networking Configuration Page (IPv6 Automatic Mode)

2 Record the address displayed in the **IPv6 Link Local Address** field to ensure that you can restore the management connection to the device after enabling IPv6 Automatic mode.
3 In the **IPv6 Assignment Mode** field, select **Automatic (DHCP)**.
4 Click **Apply**. Management will be lost until the device obtains a new IP address from the DHCP server. However, you can still access the device via its IPv4 address or the IPv6 Link Local Address.
5 For configurations with unit redundancy, make sure to perform copy-to-mate as soon as the management connection is restored, to ensure that in case of switchover, the IPv6 address of the Standby unit is aligned with that of the Active unit.

In the event that the Standby unit is to be moved to a different setup, to act as either the Active or Standby unit in that setup, it is recommended to first clear the DUID (DHCP Unique Identifier) in order to prevent duplicate DUIDs in the new setup. This must be done via CLI, using the following command:

```
root> platform management ip reset ipv6-duid
```

Note: The DUID is used in IPv6 to provide unique identification for devices.

3.13 Configuring DSCP/TC for Management

In certain situations when using in-band management, management data and user traffic are not separated by VLANs. This happens if both are untagged or use the same VLAN.

In such cases, you can assign a DSCP (IPv4) or TC (IPv6) value to management data in order to distinguish it from user traffic. While ingress management packets will have whatever DSCP/TC they were originally assigned, when they egress from the CPU they will carry the assigned DSCP or TC. This enables you to ensure that management packets from the device have priority and will continue to be sent even when there is congestion.

Note: By default, the DSCP/TC value assigned to management traffic egressing the device is 0.

The following settings are required for these DSCP/TC settings to work properly:

- For all logical interfaces, the **Trust VLAN UP bits** parameter must be set to **Un-Trust**.
- For the management service, the **CoS Mode** must be set to **Preserve-SP-COS-Decision**.
- If the device is the main unit in a Link Bonding configuration, add service points for the Management service on the interfaces passing traffic to the paired units, with the same VLAN used for management.

To configure DSCP/TC for management:

1. Select **Platform** > **Management** > **Networking** > **Local**. The Local Networking Configuration page opens.
2. In the **IPv4 DSCP** field, select a DSCP value for management connections that use IPv4 protocol.
3. In the **IPv6 TC** field, select a TC value for management connections that use IPv6 protocol.
4. Click **Apply** underneath the **IPv6 TC** field.

3.14 Configuring the Activation Key

This section includes:

- Activation Key Overview
- Viewing the Activation Key Status Parameters
- Entering the Activation Key
- Activating Demo Mode

Displaying a List of Activation-Key-Enabled Features

PTP 850 offers a pay-as-you-grow concept in which future capacity growth and additional functionality can be enabled with activation keys. Each device contains a single unified activation key cipher.

New PTP 850 units are delivered with a default activation key that enables you to manage and configure the unit. Additional feature and capacity support requires you to enter an activation key cipher in the Activation Key Configuration page. Contact your vendor to obtain your activation key cipher.



Note

To obtain an activation key cipher, you may need to provide the unit's serial number. You can display the serial number in the Web EMS Inventory page. See Displaying Unit Inventory.

3.14.1 Activation Key Overview

PTP 850E offers a pay-as-you-grow concept in which future capacity growth and additional functionality can be enabled with activation keys. Each device contains a single unified activation key cipher.

Alternatively, a Smart Activation Key is available for simplified and centralized activation key management, using a Smart Activation Key server to manage licensing for multiple devices.

Note: This and the following sections describe how to manage activation keys without using the Smart Activation Key.

New PTP 850E units are delivered with a default activation key that enables you to manage and configure the unit. Additional feature and capacity support requires you to enter an activation key cipher in the Activation Key Configuration page. Contact your vendor to obtain your activation key cipher.



Note

To obtain an activation key cipher, you may need to provide the unit's serial number. You can display the serial number in the Web EMS Inventory page.

Each required feature and capacity should be purchased with an appropriate activation key. It is not permitted to enable features that are not covered by a valid activation key. In the event that the activation-key-enabled capacity and feature set is exceeded, an Activation Key Violation alarm occurs and the Web EMS displays a yellow background and an activation key violation warning. After a 48-hour grace period, all other alarms are hidden until the capacity and features in use are brought within the activation key's capacity and feature set.

In order to clear the alarm, you must configure the system to comply with the activation key that has been loaded in the system. The system automatically checks the configuration to ensure that it complies with the activation-key-enabled features and capacities. If no violation is detected, the alarm is cleared.

When entering sanction state, the system configuration remains unchanged, even after power cycles. However, the alarms remain hidden until an appropriate activation key is entered or the features and capacities are re-configured to be within the parameters of the current activation key.

Demo mode is available, which enables all features for 60 days. When demo mode expires, the most recent valid activation key goes into effect. The 60-day period is only counted when the system is powered up. 10 days before demo mode expires, an alarm is raised indicating that demo mode is about to expire.

3.14.2 Viewing the Activation Key Status Parameters

To display the current activation key status parameters:

1. Select **Platform > Activation Key > Activation Key Configuration**. The Activation Key Configuration page opens.

Figure 43 Activation Key Configuration Page

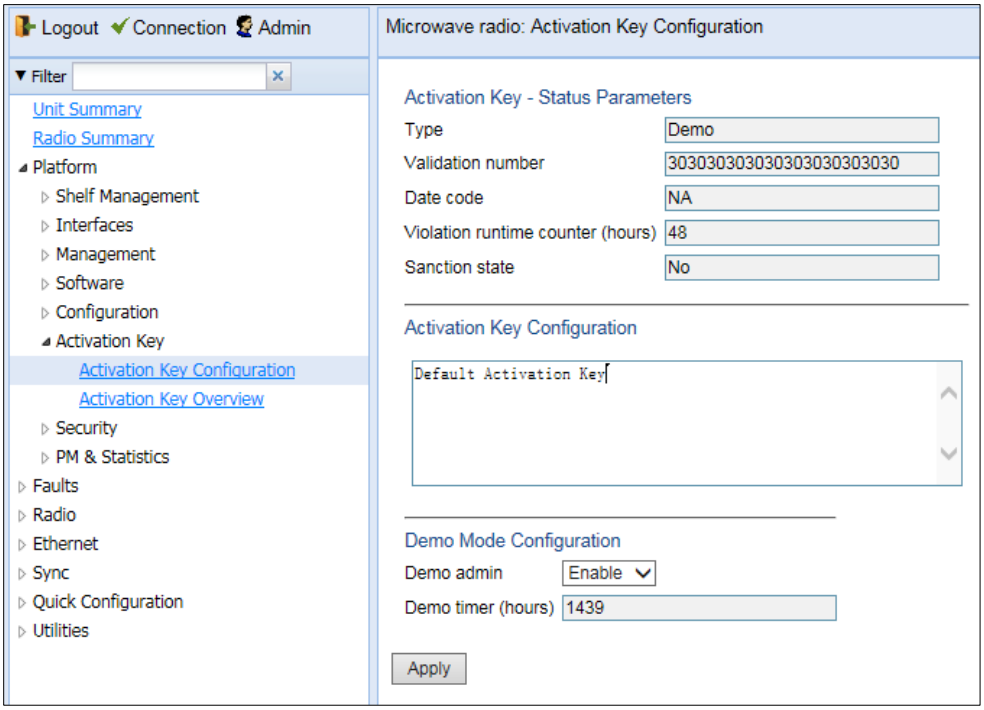


Table 8 Activation Key Status Parameters

Parameter	Definition
Type	Displays the current activation key type.
Validation number	Displays a random, system-generated validation number.
Date code	Displays a date code used for validation of the current activation key cipher.
Violation runtime counter (hours)	In the event of an Activation Key Violation alarm, this field displays the number of hours remaining in the 48-hour activation key violation grace period.
Sanction state	If an Activation Key Violation alarm has occurred, and the 48-hour activation key violation grace period has expired without the system having been brought into conformance with the activation-key-enabled capacity and feature set, Yes appears in this field to indicate that the system is in an Activation Key Violation sanction state. All other alarms are hidden until the capacity and features in use are brought within the activation-key-enabled capacity and feature set.

3.14.3 Entering the Activation Key

1. To enter a new activation key:
2. Select **Platform > Activation Key > Activation Key Configuration**. The Activation Key Configuration page opens (Figure 43).
3. Enter the activation key cipher you have received from the vendor in the Activation Key field. The activation key cipher is a string that enables all features and capacities that have been purchased for the unit.
4. Click **Apply**.

If the activation key cipher is not legal (e.g., a typing mistake or an invalid serial number), an Activation Key Loading Failure event is sent to the Event Log. When a legal activation key cipher is entered, an Activation Key Loaded Successfully event is sent to the Event Log.

Activating a Demo Activation Key

3.14.4 To activate demo mode:

1. Select **Platform > Activation Key > Activation Key Configuration**. The Activation Key Configuration page opens (Figure 44).
2. In the **Demo admin** field, select **Enable**.
3. Click **Apply**.

The Demo timer field displays the number of hours that remain before the demo activation key expires.

3.14.5 Activation Key Reclaim

If it is necessary to deactivate an PTP 850E device, whether to return it for repairs or for any other reason, the device's activation key can be reclaimed for a credit that can be applied to activation keys for other devices.

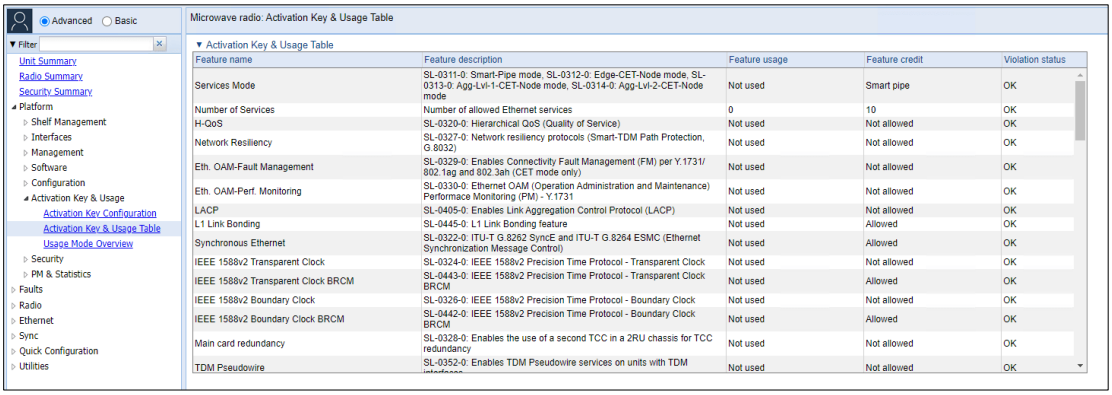
Where the customer has purchased upgrade activation keys, credit is given for the full feature or capacity, not for each individual upgrade. For example, if the customer purchased two capacity activation keys for 300M and later purchased one upgrade activation key to 350M, credit is given as if the customer had purchased one activation key for 350M and one activation key for 300M.

3.14.6 Displaying a List of Activation-Key-Enabled Features

To display the status of activation key coverage for features and capacities in the PTP 850:

1. Select **Platform > Activation Key > Activation Key Overview**. The Activation Key Overview page opens.

Figure 44 Activation Key Overview Page



The Activation Key Overview page displays the activation-key-enabled features and capacities for the PTP 850, and indicates the activation key status of each feature according to the activation key currently implemented in the unit.

Note

Some of the features listed in the Activation Key Overview page may not be supported in the currently installed software version.

Table 9 Activation Key-Enabled-Features Table Parameters

Parameter	Definition
Feature ID	A unique ID that identifies the feature.
Feature name	The name of the feature.
Feature Description	A description of the feature.

Parameter	Definition
Activation key-enabled feature usage	Indicates whether the activation-key-enabled feature is actually being used.
Activation key-enabled feature credit	Indicates whether the feature is allowed under the activation key that is currently installed in the unit.
Activation key violation status	Indicates whether the system configuration violates the currently installed activation key with respect to this feature.

Table 10 Activation Key-Enabled-Features Description

Activation Key Name	Description
Services Mode	Enables Carrier Ethernet Transport (CET) and a number of Ethernet services, depending on the type of activation key: • Edge CET Node – Up to 8 EVCs. • Aggregation Level 1 CET Node – Up to 64 EVCs. • Aggregation Level 2 CET Node – Up to 1024 EVCs. • Any CET activation key also enables the following: • A GbE traffic port in addition to the port provided by the default activation key, for a total of 2 GbE traffic ports. • Full QoS for all services including basic queue buffer management (fixed queues buffer size limit, tail-drop only) and eight queues per port, no H-QoS. • One activation key is required per device.
Number of Services	Indicates how many services are allowed according to the Services Mode activation key, and how many are actually configured on the device.
H-QoS	Enables H-QoS. This activation key is required to add service-bundles with dedicated queues to interfaces. Without this activation key, only the default eight queues per port are supported. One activation key is required per device.
Network Resiliency	Enables the following network resiliency protocols: G.8032 One activation key is required per device.
Eth. OAM– Fault Management	Enables Connectivity Fault Management (FM) per Y.1731 (CET mode only). One activation key is required per device.
Eth. OAM– Performance Monitoring	Not relevant in the current System Release.
LACP	Enables Link Aggregation Control Protocol (LACP). One activation key is required per device.
L1 Link Bonding	Enables configuration of Link Bonding groups in which the PTP 850C or PTP 850E is the main unit. Only the main unit requires an activation key.

Activation Key Name	Description
Synchronous Ethernet	Enables the ITU-T G.8262 SyncE and ITU-T G.8264 ESMC synchronization unit. This activation key is required in order to provide end-to-end synchronization distribution on the physical layer. This activation key is also required to use Synchronous Ethernet (SyncE). One activation key is required per device.
IEEE 1588v2 Transparent Clock	Not relevant for PTP 850C and PTP 850E.
IEEE 1588v2 Transparent Clock BRCM	Enables IEEE-1588 Transparent Clock. One activation key is required per device.
IEEE 1588v2 Boundary Clock	Not relevant for PTP 850C and PTP 850E.
IEEE 1588v2 Boundary Clock BRCM	Enables IEEE-1588 Boundary Clock. One activation key is required per device.
Main Card Redundancy	Not relevant for PTP 850 products.
TDM Pseudowire	Not relevant for PTP 850 products.
Frame cut-through	Not relevant for PTP 850 products.
Secured Management	Enables secure management protocols (SSH, HTTPS, SFTP, SNMPv3, TACACS+, and RADIUS).
Netconf/YANG	Enables management protocol Netconf on the device. One activation key is required per device.
Ethernet traffic ports – 100Mbps	Enables the use of 100Mbps ports. Two Ethernet ports are enabled by default without requiring any activation key. A separate activation key is required per port.
Ethernet traffic ports – 1GbE/2.5GbE	Enables the use of 1GbE/2.5GbE ports. One GbE port is enabled by default without requiring any activation key. A separate activation key is required per port.
Ethernet traffic ports – 10GbE	Enables the use of 10GbE ports. A separate activation key is required per port.

Activation Key Name	Description
Ethernet traffic ports – 40GbE	Enables the use of a 40GbE port. Only relevant for PTP 850E.
ACM	Adaptive Coding Modulation. A separate activation key is required per radio.
CHBW-1.75M	Not relevant for PTP 850 products.
Header De-Duplication	Not relevant for PTP 850 products.
XPIC	Cross Polarization Interference Cancellation. A separate activation key is required per radio member.
Millimeter Wave XPIC (NA)	Not relevant for PTP 850 products.
Multi Carrier ABC	Multi-Carrier ABC. A separate activation key is required per radio member.
MIMO	Not relevant for PTP 850 products.
SD	Not relevant for PTP 850 products.
ASD	Not relevant for PTP 850 products.
AFR 1+0	Not relevant for PTP 850 products.
ACMB	Adaptive Coding Modulation Channel Bandwidth. A separate activation key is required per radio Only relevant for PTP 850E.
AES Encryption	Enables the use of AES-256 encryption for full radio payload encryption. A separate activation key is required per carrier. Note that: • If no AES activation key is configured for the unit and the user attempts to enable AES on a radio carrier, in addition to an Activation Key Violation alarm the feature will remain inactive and no encryption will be performed. • After entering an AES activation key, the user must reset the unit before AES can be activated. Unit reset is only necessary for the first AES activation key. If AES activation keys are acquired later for additional radio carriers, unit reset is not necessary.
2nd Core Activation	Enables the second carrier of an PTP 850C. A separate activation key is required per radio.
2nd RX Core Activation	Not relevant for PTP 850 products.
2nd Core Activation RFU-D	Not relevant for PTP 850 products.

Activation Key Name	Description
2nd Core Activation HP	Not relevant for PTP 850 products.
2nd Modem Activation	Not relevant for PTP 850 products.
RFU Port Activation	Not relevant for PTP 850 products.
Capacity 10Mbps	Displays the number of radio carriers for which there is permission to use up to 10 Mbps. This is the default level, so every radio carrier on the device has this capacity level.
mmW Capacity 10Mbps	Displays the number of mmW radio carriers for which there is permission to use up to 10 Mbps. This is the default level, so every radio carrier on the device has this capacity level.
Capacity 50 Mbps	Displays the number of radio carriers for which there is permission to use up to 50 Mbps.
mmW Capacity 50 Mbps	Displays the number of mmW radio carriers for which there is permission to use up to 50 Mbps. This is the default level, so every radio carrier on the device has this capacity level.
Capacity 100Mbps	Displays the number of radio carriers for which there is permission to use up to 100 Mbps.
mmW Capacity 100Mbps	Displays the number of mmW radio carriers for which there is permission to use up to 100 Mbps.
Capacity 150Mbps	Displays the number of radio carriers for which there is permission to use up to 150 Mbps.
mmW Capacity 150Mbps	Displays the number of mmW radio carriers for which there is permission to use up to 150 Mbps.
Capacity 200Mbps	Displays the number of radio carriers for which there is permission to use up to 200 Mbps.
mmW Capacity 200Mbps	Displays the number of mmW radio carriers for which there is permission to use up to 200 Mbps.
Capacity 225Mbps	Displays the number of radio carriers for which there is permission to use up to 225 Mbps.

Activation Key Name	Description
mmW Capacity 225Mbps	Displays the number of mmW radio carriers for which there is permission to use up to 200 Mbps.
Capacity 250Mbps	Displays the number of radio carriers for which there is permission to use up to 250 Mbps.
mmW Capacity 250Mbps	Displays the number of mmW radio carriers for which there is permission to use up to 200 Mbps.
Capacity 300Mbps	Displays the number of radio carriers for which there is permission to use up to 300 Mbps.
mmW Capacity 300Mbps	Displays the number of mmW radio carriers for which there is permission to use up to 200 Mbps.
Capacity 350Mbps	Displays the number of radio carriers for which there is permission to use up to 350 Mbps.
mmW Capacity 350Mbps	Displays the number of mmW radio carriers for which there is permission to use up to 350 Mbps.
Capacity 400Mbps	Displays the number of radio carriers for which there is permission to use up to 400 Mbps.
mmW Capacity 400Mbps	Displays the number of mmW radio carriers for which there is permission to use up to 400 Mbps.
Capacity 450Mbps	Displays the number of radio carriers for which there is permission to use up to 450 Mbps.
mmW Capacity 450Mbps	Displays the number of mmW radio carriers for which there is permission to use up to 450 Mbps.
Capacity 500Mbps	Displays the number of radio carriers for which there is permission to use up to 500 Mbps.
mmW Capacity 500Mbps	Displays the number of mmW radio carriers for which there is permission to use up to 500 Mbps.
Capacity 650Mbps	Displays the number of radio carriers for which there is permission to use up to 650 Mbps.

Activation Key Name	Description
mmW Capacity 650Mbps	Displays the number of mmW radio carriers for which there is permission to use up to 650 Mbps.
Capacity 1Gbps	Displays the number of radio carriers for which there is permission to use up to 1 Gbps.
mmW Capacity 1Gbps	Displays the number of mmW radio carriers for which there is permission to use up to 1 Gbps.
Capacity 1.6Gbps	Displays the number of radio carriers for which there is permission to use up to 1.6 Gbps.
mmW Capacity 1.6Gbps	Displays the number of mmW radio carriers for which there is permission to use up to 1.6 Gbps.
Capacity 2Gbps	Displays the number of radio carriers for which there is permission to use up to 2 Gbps.
mmW Capacity 2Gbps	Displays the number of mmW radio carriers for which there is permission to use up to 2 Gbps.
mmW Capacity 2.5Gbps	Displays the number of radio carriers for which there is permission to use up to 2.5 Gbps.
mmW Capacity 3Gbps	Displays the number of radio carriers for which there is permission to use up to 3 Gbps.
mmW Capacity 4Gbps	Displays the number of radio carriers for which there is permission to use up to 4 Gbps.
mmW Capacity 5Gbps	Displays the number of radio carriers for which there is permission to use up to 5 Gbps.
mmW Capacity 6Gbps	Displays the number of radio carriers for which there is permission to use up to 6 Gbps.
mmW Capacity 7Gbps	Displays the number of radio carriers for which there is permission to use up to 7 Gbps.
mmW Capacity 8Gbps	Displays the number of radio carriers for which there is permission to use up to 8 Gbps.

Activation Key Name	Description
mmW Capacity 9Gbps	Displays the number of radio carriers for which there is permission to use up to 9 Gbps.
mmW Capacity 10Gbps	Displays the number of radio carriers for which there is permission to use up to 10 Gbps.
Capacity 10Mbps	Displays the number of mmW radio carriers for which there is permission to use up to 10 Mbps. This is the default level, so every radio carrier on the device has this capacity level.
ASP and LLF	Enables the use of Link Loss Forwarding (LLF) with Automatic State Propagation (ASP). Without the activation key, only one LLF ID can be configured. This means that only one ASP pair can be configured per radio interface or radio group. One activation key is required per device.
Multiband	Multiband. Two activation keys are required per Multiband node, on the PTP 850E. One of these activation keys is for the radio port, the other is for the Ethernet port carrying traffic to the unit paired with the PTP 850E. No activation key is required for the unit paired with the PTP 850E.1
L1 Link Bonding	Enables configuration of Link Bonding groups in the following configurations: • In 4+0 Layer 1 Link Bonding configurations, the main unit requires a Link Bonding activation key. • In Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP, the PTP 850C requires a Link Bonding activation key. • In Multiband groups using Layer 1 Link Bonding, the PTP 850E requires a Link Bonding activation key.
Anti-Theft	Not relevant for PTP 850 products.
Web customer view	Not relevant in the current System Release.
Front Panel RFU Activation	Not relevant for PTP 850 products.
Advanced Security Key	Enables Syslog Encryption and NTP Authentication.

[1] Note that for Multiband configurations that use Link Bonding, an L1 Link Bonding is required rather than a Multiband activation key.

Activation Key Name	Description
E-Stabilizer Advanced Features	Enables activation of automatic tracking mode and performance monitoring (PTP 850E only)
E-Band High TX Power	Not relevant for PTP 850C and PTP 850E.
Advanced high capacity MC-ABC (>=20 Gbps)	Not relevant for PTP 850C and PTP 850E.
Single Sign-On	Enables single sign-on (SSO).

3.15 Setting the Time and Date (Optional)

Related Topics:

Configuring NTP

PTP 850 uses the Universal Time Coordinated (UTC) standard for time and date configuration. UTC is a more updated and accurate method of date coordination than the earlier date standard, Greenwich Mean Time (GMT).

Every PTP 850 unit holds the UTC offset and daylight savings time information for the location of the unit. Each management unit presenting the information uses its own UTC offset to present the information in the correct time.



Note

If the unit is powered down, the time and date are saved for 96 hours (four days). If the unit remains powered down for longer, the time and date may need to be reconfigured.

To display and configure the UTC parameters:

1. Select **Platform** > **Management** > **Time Services**. The Time Services page opens.

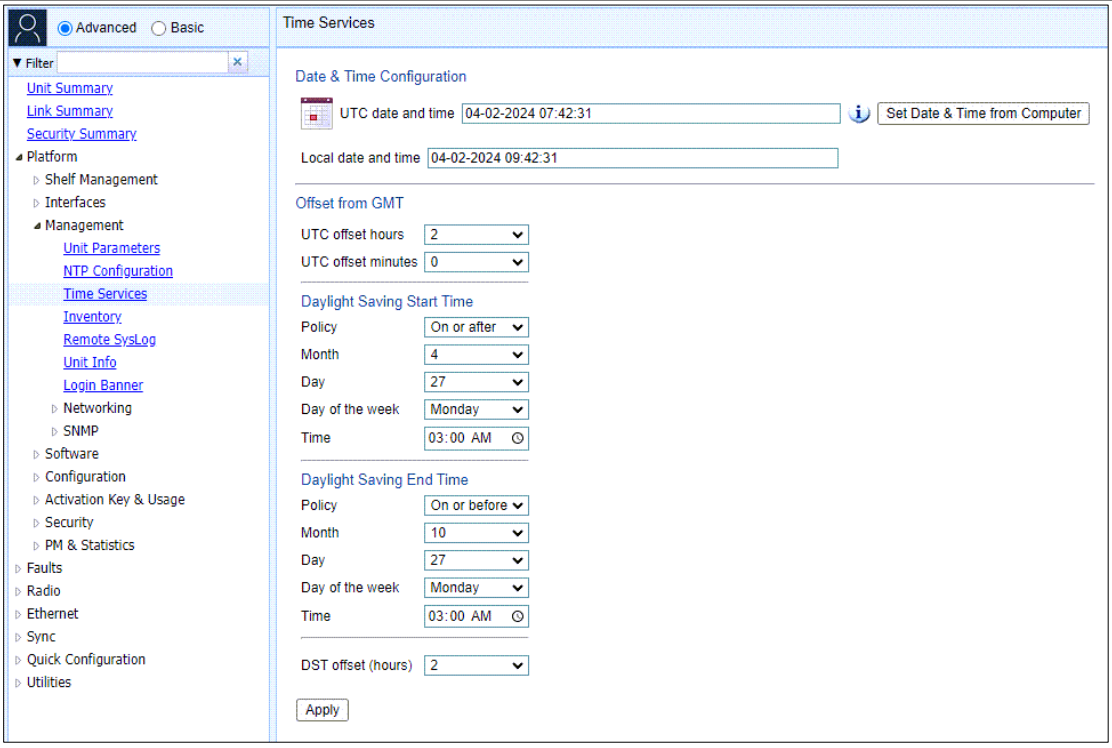


Figure 45 Time Services Page

2. Configure the fields listed in Table 11 Time Services Parameters.
3. Click **Apply**.

Table 11 Time Services Parameters

	Parameter	Definition
Date and Time Configuration	UTC date and time	The UTC date and time.
	Local date and time	The calculated local date and time, based on the local clock, Universal Time Coordinated (UTC), and Daylight Savings Time (DST) configurations.
Offset from GMT	UTC offset hours	The required hours offset (positive or negative) relative to GMT. This is used to offset the clock relative to GMT, according to the global meridian location.

	Parameter	Definition
	UTC offset minutes	The required minutes offset (positive or negative) relative to GMT. This is used to offset the clock relative to GMT, according to the global meridian location.

Daylight Saving Start Time	Policy	Enables you to create a rule for the beginning of Daylight Saving Time (DST). Options are: • **Fixed date**: When this option is selected, only the **Month**, **Day**, and **Time** fields appear. DST starts on the specified month, day, and time. • **On or after**: DST starts on the first occurrence of the specified day of the week immediately after the specified Month and Day. For example, if **Day of the week** is set to **Friday**, DST starts the first Friday after the specified month and day. If the **Month** and **Day** fall on a Friday, DST starts on that month and day. • **On or before**: DST starts on the first occurrence of the configured day of the week immediately before the specified Month and Day. For example, if **Day of the week** is set to **Friday**, DST starts the last Friday before the specified month and day. If the **Month** and **Day** fall on a Friday, DST starts on that month and day. • **Last**: When this option is selected, only the **Month**, **Day of the Week**, and **Time** fields appear. DST starts on the last occurrence of the specified day of the

	Parameter	Definition
		week in the specified month. The default value is **Fixed date**.
	Month	This parameter operates according to the selected Policy, as described above. The default value is **1** (January).
	Day	This parameter operates according to the selected Policy, as described above. The default value is **1**.
	Day of the Week	This parameter operates according to the selected Policy, as described above. The default value is **Sunday**.
	Time	The Time at which DST begins. The default value is **02:00 AM**.

Daylight Saving End Time	Policy	Enables you to create a rule for the end of DST. Options are: • **Fixed date**: When this option is selected, only the **Month**, **Day**, and **Time** fields appear. DST ends on the specified month, day, and time. • **On or after**: DST ends on the first occurrence of the configured day of the week immediately after the specified Month and Day. For example, if **Day of the week** is set to **Friday**, DST ends the first Friday after the specified month and day. If the **Month** and **Day** fall on a Friday, DST ends on that month and day. • **On or before**: DST ends on the first occurrence of the specified day of the week immediately before the specified Month and Day. For example, if **Day of the week** is set to **Friday**, DST ends the last Friday before the specified month and day. If the **Month** and **Day** fall on a Friday, DST ends on that month and day. • **Last**: When this option is selected, only the **Month**, **Day of the Week**, and **Time** fields appear. When this option is selected, DST ends on the last occurrence of the specified day of the week in the specified month.

	Parameter	Definition
		The default value is **Fixed date**.
	Month	This parameter operates according to the selected Policy, as described above. The default value is **1** (January).
	Day	This parameter operates according to the selected Policy, as described above. The default value is **1**.
	Day of the Week	This parameter operates according to the selected Policy, as described above. The default value is **Sunday**.
	Time	The Time at which DST ends. The default value is **02:00 AM**.

	Parameter	Definition
	DST offset	The required offset, in hours, for Daylight Savings Time. Only positive offset is supported.

3.16 Enabling the Interfaces (Interface Manager)

By default:

Ethernet traffic interfaces are disabled and must be manually enabled.

The Ethernet management interface is enabled.

Radio interfaces are enabled.



Note

In release 11.1, Ethernet Slot 1, Ports 2 through 7 are supported. Port 2 can only be used in Multiband configurations to connect the PTP 850E with the paired unit.

The QSFP port (Port 4), is displayed as follows.

In a 4x1/10G configuration the QSFP port can provide four Ethernet interfaces: Ethernet Slot 1, Port 3, Ethernet Slot 1, Port 4, Ethernet Slot 1, Port 5, and Ethernet Slot 1, Port 6. In this configuration, a QSFP transceiver is attached to the QSFP port, and an MPO-MPO cable is connected between the transceiver and a splitter on the other side of the link. The splitter splits the traffic between four Ethernet cables connecting the splitter to the customer equipment.

The QSFP port can also be used with a QSFP-to-SFP adaptor to provide a 1x1/10G configuration. In this configuration, the port is displayed as Ethernet Slot 1, Port 3.

To enable or disable interfaces:

1. Select **Platform > Interfaces > Interface Manager**. The Interface Manager page opens, displaying all of the system's traffic and management interfaces.

Figure 46 Interface Manager Page-PTP 850C

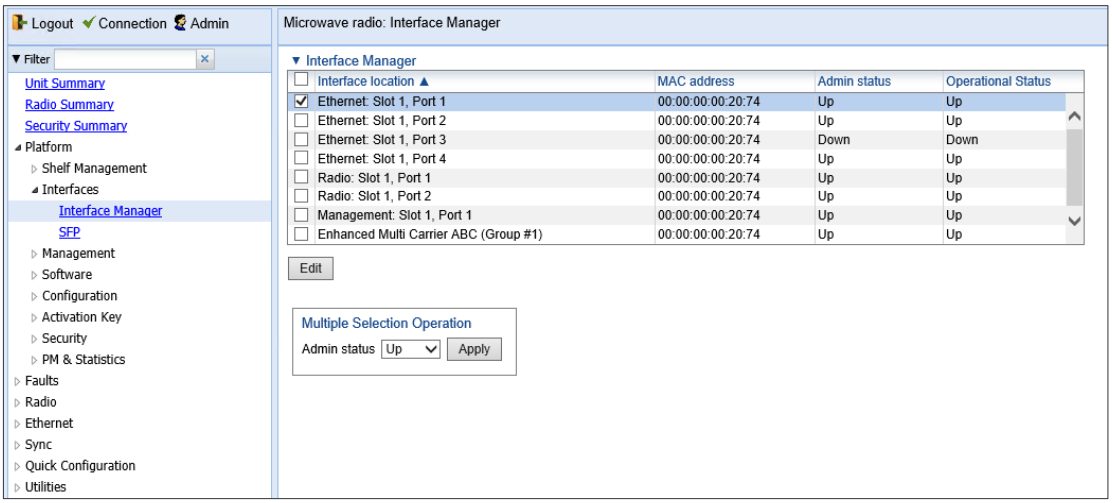


Figure 47 Interface Manager Page-PTP 850E

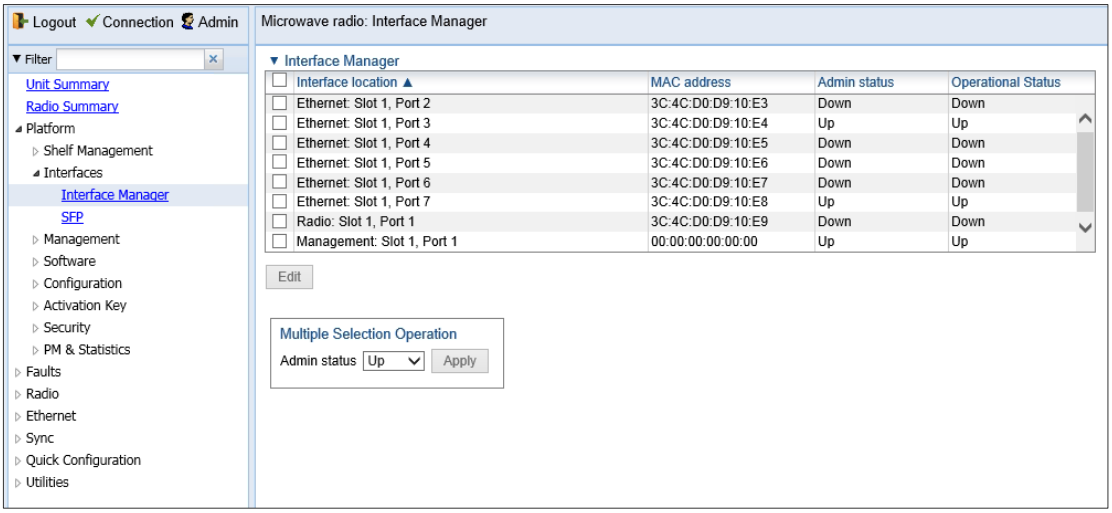
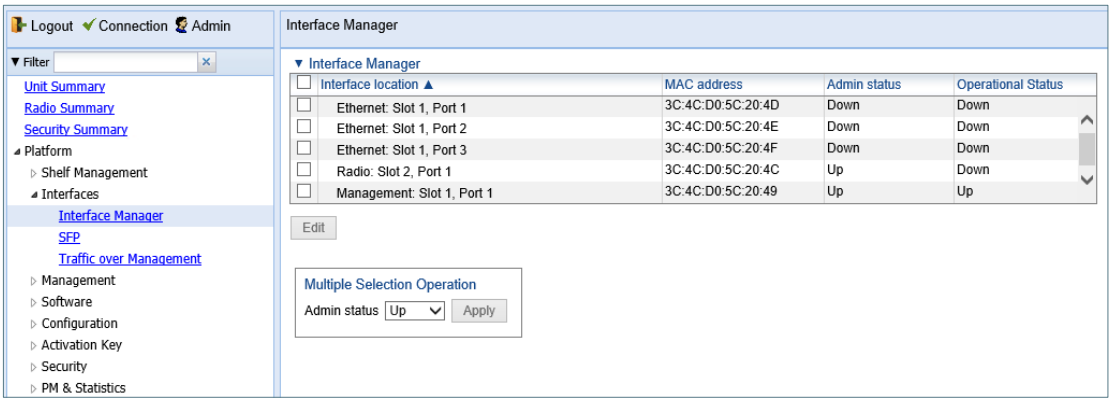


Figure 48 Interface Manager Page-PTP 850S

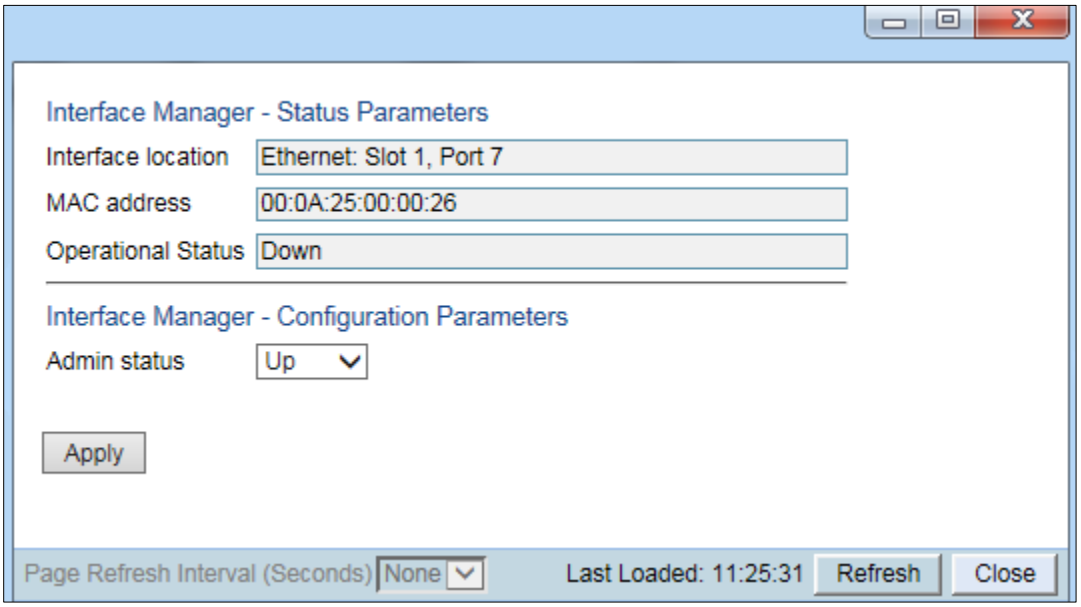


If an alarm is currently raised on an interface, an alarm icon appears to the left of the interface location. For example, an alarm is raised on the Radio interface. To display details about the alarm or alarms in tooltip format, hover the mouse over the alarm icon.

To enable or disable an individual interface:

1. Select the interface in the Interface Manager table.
2. Click **Edit**. The Interface Manager – Edit page opens.

Figure 49 Interface Manager – Edit Page

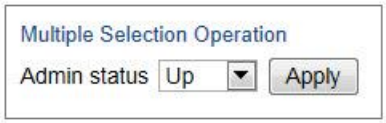


3. In the Admin status field, select **Up** to enable the interface or **Down** to disable the interface.
4. Click **Apply**, then **Close**.

To enable or disable multiple interfaces:

1. Select the interfaces in the Interface Manager table or select all the interfaces by selecting the check box in the top row.
2. In the **Multiple Selection Operation** section underneath the Interface Manager Table, select Admin status – Up or **Admin status – Down**.

Figure 50 Multiple Selection Operation Section (Interface Manager Page)



3. Click **Apply**.

Note

The **Operational Status** field displays the current, actual operational state of the interface (**Up** or **Down**).

PTP 850E Management Interface

The management interface on PTP 850E (Port 2) can be used for traffic as well as management and PoE. This increases the number of available Ethernet traffic ports and enables customers to configure setups in which a single cable is used to carry management, traffic, and power from the customer equipment to the PTP 850E device.

In most respects, this port can be used like other Ethernet traffic ports, including:

- Support for Auto Negotiation
- Support for synchronization
- Support for LLDP
- Support for Y.1731 CFM-SOAM
- Support for LACP
- Support for RMON

Because this interface is used for management, a management service (Service ID 1025) and a service point (Service Point ID 30) are configured on the interface and should not be removed.

Note: One case in which Service Point ID 30 must be removed is Multiband with Link Bonding with PTP 850E and a third-party device where the devices are connected via the PTP 850E's Management port and an electrical port on the third-party device. In this case, make sure to follow the procedure described in Procedure for Configuring Management When Using the PTP 850E Management Port with a Link Bonding Configuration to avoid losing management.

In addition, an L3 shaper (ID 256) is configured on the interface. This shaper can and must be deleted in order to use the port for traffic. See Removing the L3 Shaper.

Upon upgrade to Release 12.0 or higher, the port speed remains what it was previously. If a reset to default settings is performed, the port speed is set to 1 Gbps.

Note that if the PTP 850E is in a unit redundancy configuration in which a splitter cable is being used to connect the management ports (P2) of the two PTP 850E units and an external management station for local management, the port speed must be set to 100 Mbps, since the cable does not support 1 Gbps. This setting will not be affected by upgrading to Release 12.0 or higher.

Note: The management port cannot be used for traffic in Unit Redundancy configurations.

For instructions on setting the port speed, see Configuring Ethernet Interfaces.

The following limitations exist for this port:

- Cannot belong to LAG groups
- Does not support MSTP and G.8032
- Automatic State Propagation can only be used in Safe mode

To use the PTP 850E management port for traffic, you should perform the following configurations as described in more detail in the following sections:

- Remove the L3 Shaper.
- Modify the management service point.
- Enable the LOC alarm (Alarm ID 401) for the management port. By default, this alarm is disabled on the management port and must be manually enabled when using the port for traffic.

3.16.1.1 Removing the L3 Shaper

To use the management port for traffic, you must remove the L3 shaper from the port. This must be done via CLI using the following commands:

```
root>ethernet interfaces mng slot 1 port 1
eth type mng [1/1]>logical-port-shaper delete
```

To display the shaper's configuration, use the following command:

```
eth type mng [1/1]>logical-port-shaper show configuration
```

3.16.1.2 Modifying the Management Service Point

In order to ensure that the port can be used for traffic services, the Attached Interface Type of the management service point should be modified from its default value of dot1q-Untagged. Leaving the management service point as Untagged will result in untagged data traffic being classified into the management service. This should be avoided.

The management service point can be changed to dot1q with a specific C-VLAN, or to s-tag or QinQ, giving you the flexibility to configure services on the interface according to the expected user traffic. See Editing a Service Point.

A special CLI command is available to change the Attached Interface Type and VLAN settings of the service point. This command must be entered in service view, and is only available for the management service on units in which the management port is being used for both management and traffic.

Use the following command to enter service view:

```
root> ethernet service sid 1025
```

Use the following command to change the Attached Interface Type of the management service point to QinQ:

```
service[1025]> sp subtype edit qinq spid 30 s-vlan-id <1-4094|untag> c-
vlan-id <1-4094|untag>
```

Use the following command to change the Attached Interface Type of the management service point to s-tag:

```
service[1025]> sp subtype edit s-tag spid 30 s-vlan-id <1-4094|untag>
```

Use the following command to change the Attached Interface Type of the management service point back to its default value of dot1q, or to modify the service point's VLAN:

```
service[1025]> sp subtype edit dot1q spid 30 c-vlan-id <1-4094|untag>
```

Note that if this service point is tagged, you will be able to select the management port in the Quick Configuration wizards (see Configuring a Link Using the Quick Configuration Wizard). If it is untagged, the management port will not be visible in these wizards, and link configurations using this port will have to be configured manually.

For general information about service points, see Configuring Service Points.

Specifically, it is recommended to perform the following service configuration changes:

- Change the VLAN encapsulation of the management service point from Untagged to a specific VLAN.
- Configure a PIPE service point for data traffic on the management port. This service point should be untagged (e.g., dot1q-untagged or Bundle-C with "Untagged" as the C-VLAN encapsulation).

Note: As long as the management service point is configured as dot1q-Untagged, you will be unable to configure the PIPE service point.

Be very careful when reconfiguring this service point to ensure continued management access. Make sure that if you change the management service point's VLAN tagging, management traffic is then tagged with the same VLAN as the management service point.

Note: To avoid the problem of changing the tagging of management traffic in the middle of the service point reconfiguration process, it is recommended to perform this process if possible by accessing the unit via the EXT port, with a special cable. For details, see Error! Reference source not found..

3.16.1.3 Enabling the LOC Alarm

To enable the LOC alarm:

1 Select **Platform > Interfaces > Traffic over Management**. The Traffic over Management page opens.

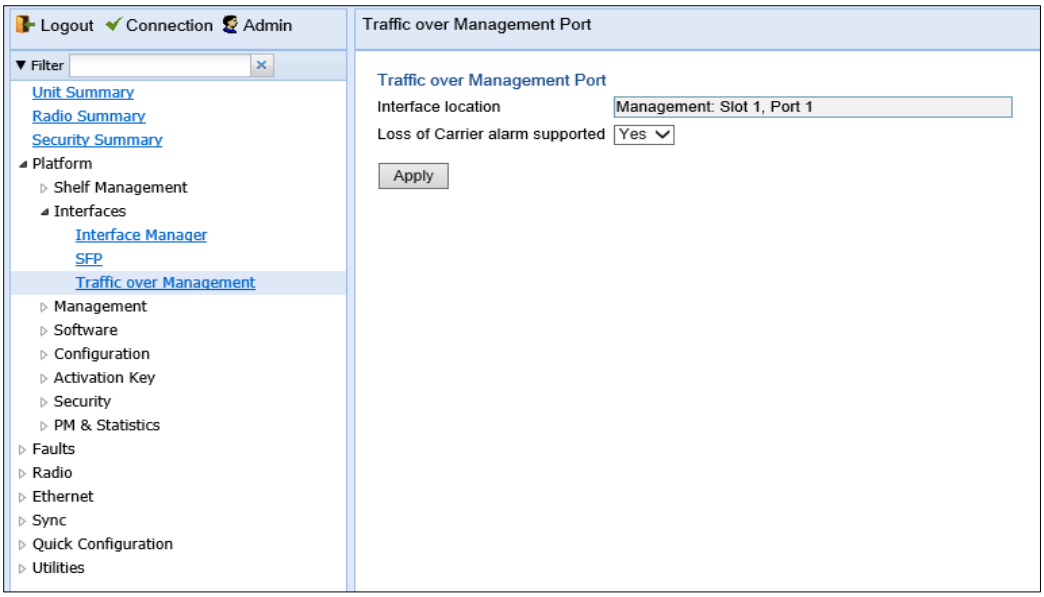


Figure 51: Traffic over Management Page

2 In the **Loss of Carrier Alarm Supported** field, select **Yes**.
3 Click **Apply**.

3.17 Configuring the Radio (MRMC) Script(s)

Related Topics:

Displaying MRMC Status

Multi-Rate Multi-Constellation (MRMC) radio scripts define how the radio utilizes its available capacity. Each script is a pre-defined collection of configuration settings that specify the radio's transmit and receive levels, link modulation, channel spacing, and bit rate. Scripts apply uniform transmit and receive rates that remain constant regardless of environmental impact on radio operation.

Note

The list of available scripts reflects activation-key-enabled features. Only scripts within your activation-key-enabled capacity will be displayed.

To display the MRMC scripts and their basic parameters and select a script:

1. Select one of the following, depending on the regulatory framework in which you are operating:

To display ETSI scripts, select **Radio > MRMC > Symmetrical Scripts > ETSI**.

To display ANSI (FCC) scripts, select **Radio > MRMC > Symmetrical Scripts > FCC**.

The MRMC Symmetrical Scripts page opens. For a description of the parameters displayed in the MRMC Symmetrical Scripts page, see *Configuring the Radio (MRMC) Scripts (s).*

Note

For detailed information on the exact scripts and profiles available per channel and configuration, refer to the Release Notes for the release version you are using.

Figure 52 MRMC Symmetrical Scripts Page-PTP 850C

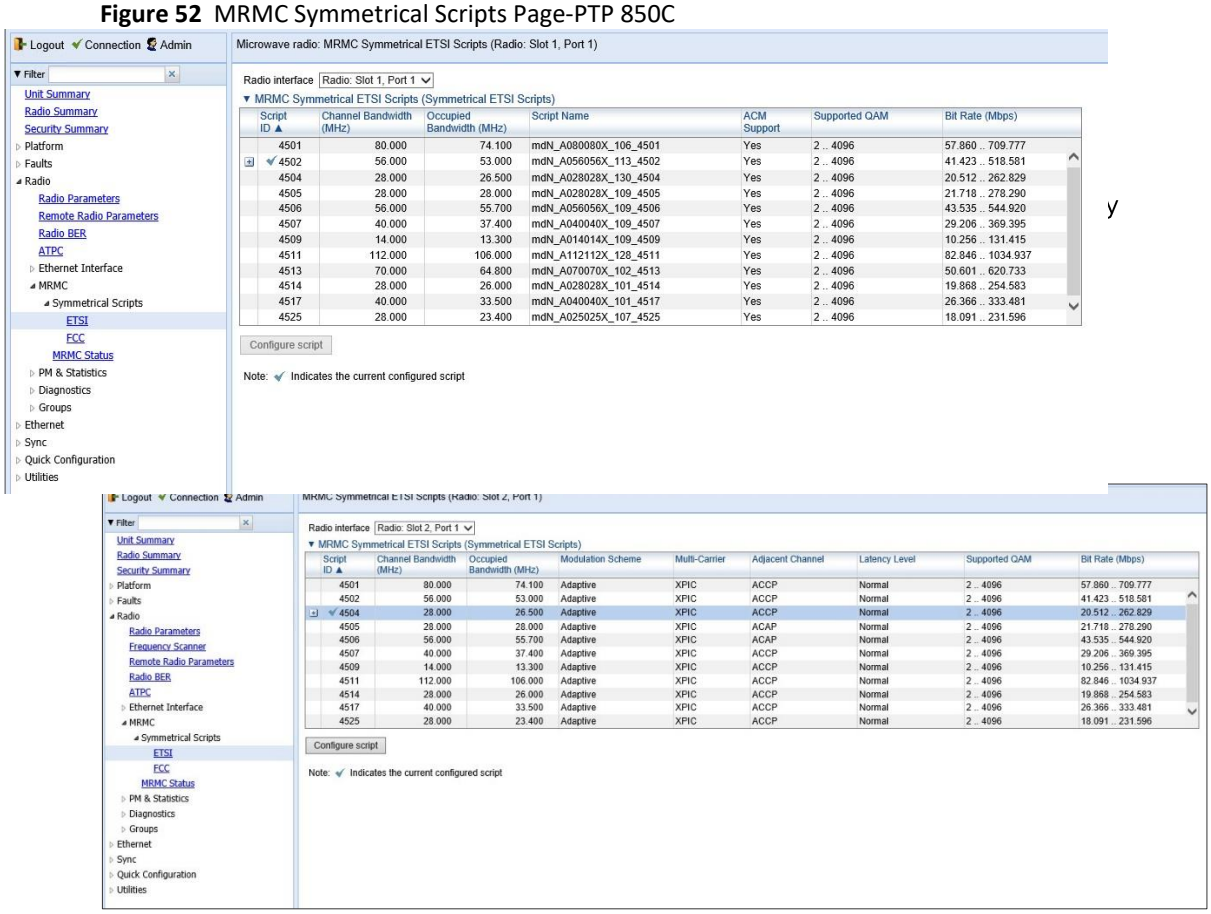
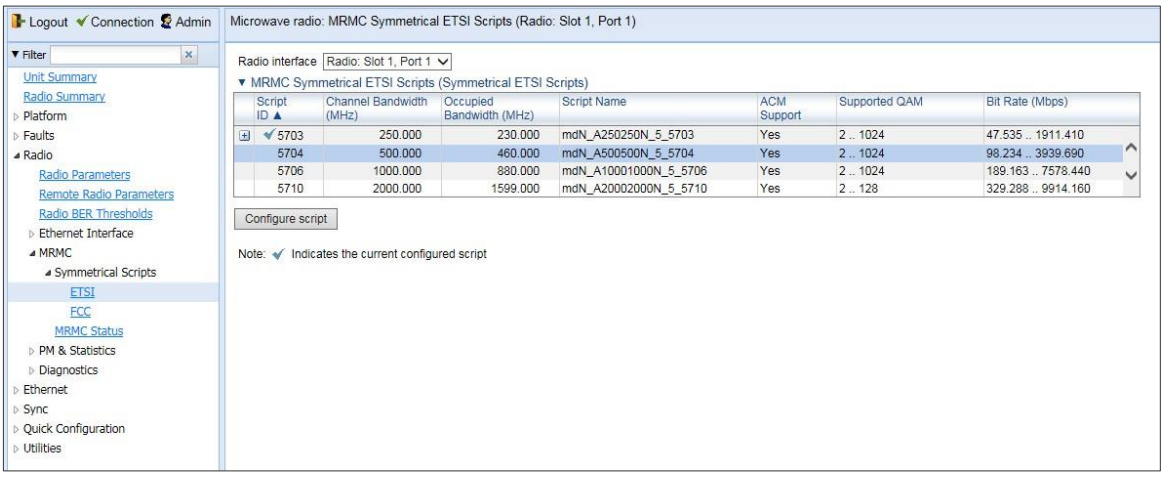
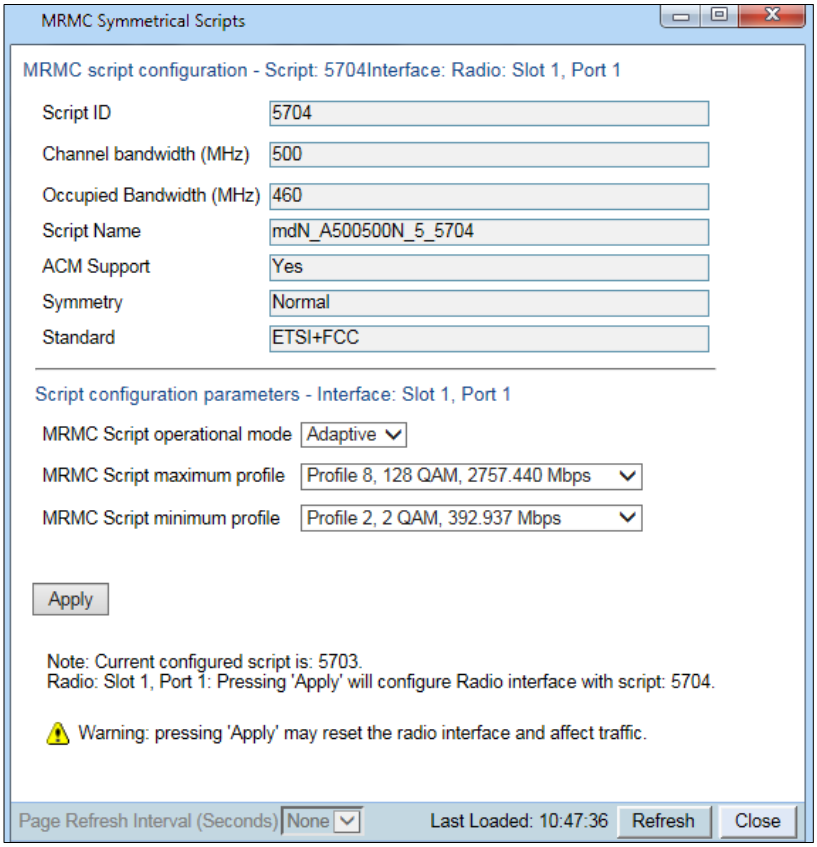


Figure 54 MRMC Symmetrical Scripts Page-PTP 850E



3. Click **Configure Script**. A separate MRMC Symmetrical Scripts page opens similar to the page shown below.

Figure 55 **MRMC Symmetrical Scripts Page – Configuration**



4. In the **MRMC Script operational mode** field, select the ACM mode: **Fixed** or **Adaptive**.

Fixed ACM mode applies constant Tx and Rx rates. However, unlike regular scripts, with a Fixed ACM script you can specify a maximum profile to inhibit inefficient transmission levels.

In Adaptive ACM mode, Tx and Rx rates are dynamic. An ACM-enabled radio system automatically chooses which profile to use according to the channel fading conditions. If you select **Adaptive**, two fields are displayed enabling you to select minimum and maximum ACM profiles.

5. Define the script profile or profiles

If you selected **Fixed** ACM mode, select the ACM profile in the **MRMC Script profile** field.

If you selected **Adaptive** ACM mode, select the maximum and minimum ACM profiles in the **MRMC Script maximum profile** and the **MRMC Script minimum profile** fields.

6. Click **Apply**.



Note

Changing the script resets the radio interface and affects traffic. Changing the maximum or minimum profile does not reset the radio interface.

Table 12 MRMC Symmetrical Scripts Page Parameters

Parameter	Definition
Script ID	A unique ID assigned to the script in the system.
Channel Bandwidth (MHz)	The script's channel bandwidth (channel spacing).
Occupied Bandwidth (MHz)	The script's occupied bandwidth.
Script Name	The name of the script.
ACM Support	Indicates whether the script supports ACM. All PTP 850E scripts support ACM.
Supported QAMModulation Scheme	MRMC Symmetrical Scripts Main Page only: Displays the range of modulation levels, in QAM, supported by the script.PTP 850S only. Indicates whether the script supports Adaptive Coding Modulation (ACM). In ACM mode, a range of profiles determines Tx and Rx rates. This enables the radio to modify its transmit and receive levels in response to environmental conditions.
Bit Rate (Mbps)Multi-Carrier	MRMC Symmetrical Scripts Main PagePTP 850S only: Displays. Indicates the rangeMulti-Carrier status of bit rates, in Mbps, supported by the script. (XPIC, MIMO, or Single-Carrier).
Adjacent Channel	PTP 850C only. Displays the script’s adjacent channel polarization mode.
Latency Level	Always displays Normal.
Supported QAM	MRMC Symmetrical Scripts Main Page only: Displays the range of modulation levels, in QAM, supported by the script.

Parameter	Definition
Bit Rate (Mbps)	MRMC Symmetrical Scripts Main Page only: Displays the range of bit rates, in Mbps, supported by the script.
Symmetry	MRMC Symmetrical Scripts Configuration Page only: Indicates that the script is symmetrical (Normal). Only symmetrical scripts are supported in the current release.
Standard	MRMC Symmetrical Scripts Configuration Page only: Indicates whether the script is compatible with ETSI or FCC (ANSI) standards, or both.
MRMC Script operational mode	MRMC Symmetrical Scripts Configuration Page only: The ACM mode: **Fixed** or **Adaptive**. • Fixed ACM mode applies constant TX and RX rates. However, unlike regular scripts, with a Fixed ACM script you can specify a maximum profile to inhibit inefficient transmission levels. • In Adaptive ACM mode, TX and RX rates are dynamic. An ACM-enabled radio system automatically chooses which profile to use according to the channel fading conditions.
MRMC Script profile	MRMC Symmetrical Scripts Configuration Page, Fixed ACM mode only: The profile in which the system will operate.
MRMC Script maximum profile	MRMC Symmetrical Scripts Configuration Page, Adaptive ACM mode only: The maximum profile for the script. For example, if you select a maximum profile of 5, the system will not climb above profile 5, even if channel fading conditions allow it.
MRMC Script minimum profile	MRMC Symmetrical Scripts Configuration Page, Adaptive ACM mode only: The minimum profile for the script. For example, if you select a minimum profile of 3, the system will not go below profile 3 regardless of the channel fading conditions. The minimum profile cannot be greater than the maximum profile, but it can be equal to it. **Note:** The default minimum profile is 2.

3.17.1 Radio Profiles

Note: The maximum profile varies per script. For details, refer to the Release Notes for the System relase version you are using.

Radio Profiles for PTP 850C and PTP 850S

Profile	Modulation
Profile 0	BPSK
Profile 1	QPSK
Profile 2	8 QAM
Profile 3	16 QAM
Profile 4	32 QAM
Profile 5	64 QAM
Profile 6	128 QAM
Profile 7	256 QAM
Profile 8	512 QAM
Profile 9	1024 QAM (Strong FEC)
Profile 10	1024 QAM (Light FEC)
Profile 11	2048 QAM
Profile 12	4096 QAM

Radio Profiles for PTP 850E

For 62.5 channels, Profile 0 is BPSK with the normal (62.5 MHz) channel spacing, Profile 1 is QPSK, and so on.

For 125 MHz channels, Profile 0 is BPSK with ½ channel spacing. Profile 1 is BPSK with the normal channel spacing (125 MHz), Profile 1 is QPSK, and so on. An ACMB activation key is required for Profile 0.

Table 13 Available Radio Profiles – PTP 850E (62.5 MHz and 125 MHz)

Profile	Modulation – Script 5701 (62.5 MHz)	Modulation – Script 5702 (125 MHz)
Profile 0	BPSK – full channel spacing	BPSK – ½ full channel spacing
Profile 1	4 QAM	BPSK – full channel spacing
Profile 2	8 QAM	4 QAM
Profile 3	16 QAM	8 QAM
Profile 4	32 QAM	16 QAM
Profile 5	64 QAM	32 QAM
Profile 6	128 QAM	64 QAM
Profile 7	256 QAM	128 QAM
Profile 8	512 QAM	256 QAM
Profile 9	-	512 QAM

For channels of 250 MHz and higher, Profiles 0 and 1 require a special activation key (SL-ACMB). These profiles are used with ACMB, which is an enhancement of ACM that provides further flexibility to mitigate fading at BPSK by reducing the channel spacing to one half or one quarter of the original channel bandwidth when fading conditions make this appropriate.

Table 14 Available Radio Profiles – PTP 850E (250 MHz to 2000 MHz – XPIC)

Profile	Modulation
Profile 0	BPSK ¼ channel spacing
Profile 1	BPSK ½ channel spacing

Profile	Modulation
Profile 2	BPSK-full channel spacing
Profile 3	4 QAM
Profile 4	8 QAM
Profile 5	16 QAM
Profile 6	32 QAM
Profile 7	64 QAM
Profile 8	128 QAM
Profile 9	256 QAM
Profile 10	512 QAM

3.18 Running the Frequency Scanner (PTP 850E)



Note

This section is only relevant for PTP 850E.

To facilitate optimal operation in frequency scenarios, PTP 850E includes a frequency scanner that enables you to scan a defined frequency range and determine the current interference level for each channel.

The frequency scanner can be used both in the initial provisioning of the link and at any time after the link has been provisioned. The scanner determines the interference level for each RX channel. Using this information, you can select the channels with the least interference, and configure the unit's frequency accordingly.

When the frequency scan begins, the unit stops receiving traffic until the scan is complete. This means the link is effectively down while the frequency scanner is operating. Once the frequency scan operation has been completed, either at the end of a Single Mode scan or by user action in the case of a Continuous scan, the link is automatically restored at the same frequency settings as before the scan.

Note

The frequency scanner does not automatically change the link's frequency settings. These settings must be changed manually. The frequency scanner simply provides information you can use in determining the proper frequency configuration.

To perform a frequency scan:

1 Select **Radio > Frequency Scanner**. The Frequency Scanner page opens.

Figure 56 Frequency Scanner Page – Continuous Mode

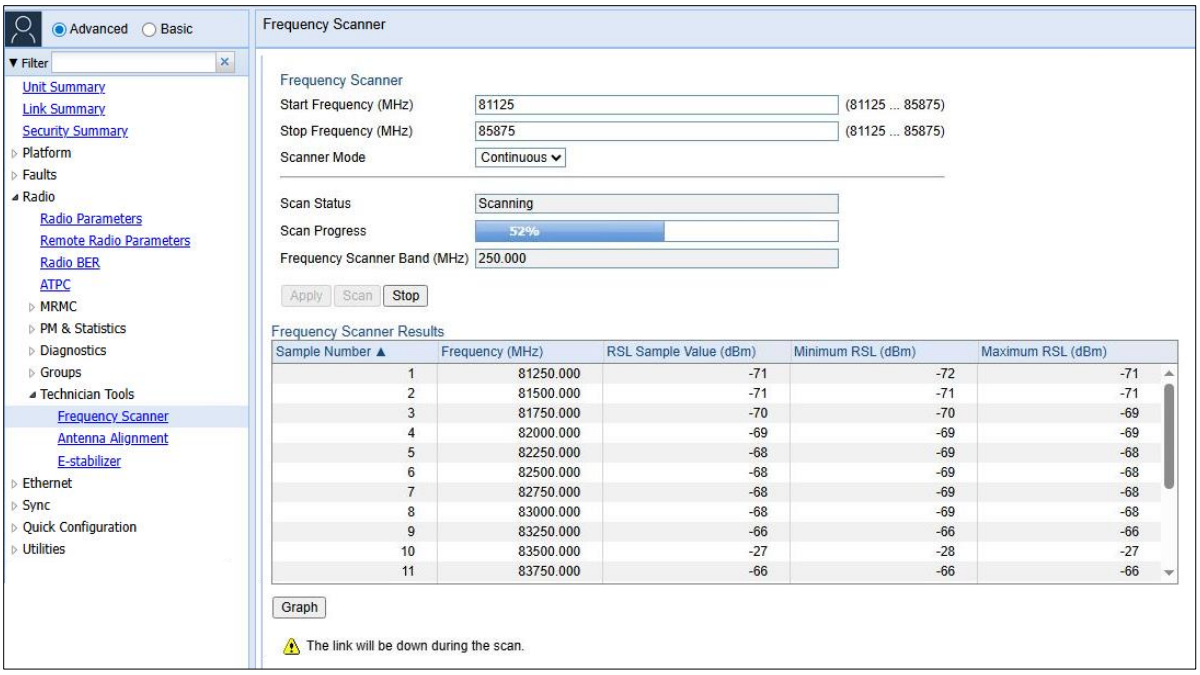
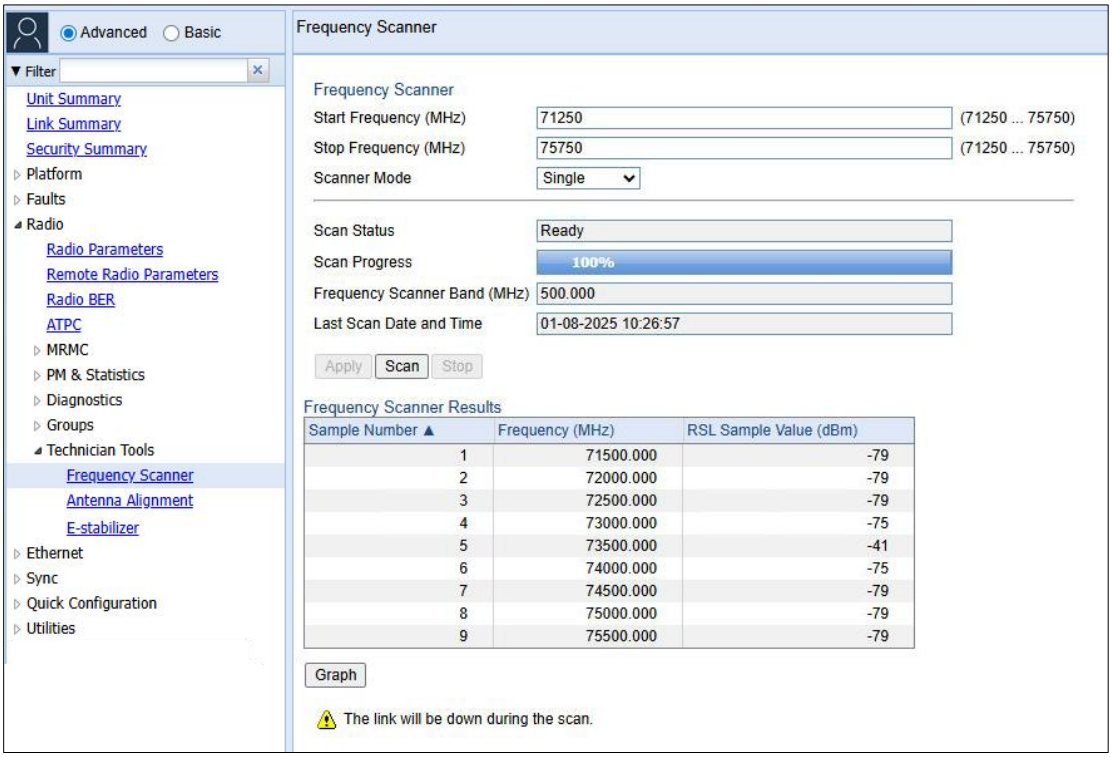


Figure 57 Frequency Scanner Page – Single Mode



2 Enter a range for the scan (in MHz) by entering the lower frequency of the range in the **Start Frequency** field and the upper frequency of the range in the **Stop Frequency** field. The range of permissible values is 81000-86000 MHz on the high side and 71000-76000 MHz on the low side
3 In the **Scanner Mode** field, select from the following options:

- **Continuous Mode** – The frequency scanner scans each channel in the script, and repeats the scan continuously until you manually stop the scan by clicking **Stop**. For each channel, the Web EMS will display the minimum, maximum, and most recently measured interference levels, in both table and graph formats.
- **Single Mode** – The frequency scanner scans each channel in the script once, over the defined frequency range. For each channel, the Web EMS will display the measured interference level.

Note

When running the Frequency Scanner on the remote side of a link using in-band management, make sure to run the Frequency Scanner in Single mode, not Continuous mode. Since the link is down during the scan, management to the remote site is lost, so that if the scan is run in Continuous mode, it will not be possible to de-activate the Frequency Scanner.

4 Click **Apply** to save the scan configuration.
5 Click **Scan**:

- The **Scan Progress** field displays the scan's progress, in percentage of the defined spectrum that has been scanned. In Continuous Mode, the **Scan Progress** field rises to 100 when the defined spectrum has been scanned, returns to 0, and continues to advance from 0 to 100 for each scan until you click **Stop**. In Single Mode, the **Scan Progress** field rises to 100 and stays at 100 once the defined spectrum has been scanned.
- The **Frequency Scanner Band** field displays the frequency channel configured in the current MRMC script.
- The **Last Scan Date and Time** field displays the date and time of the most recently completed frequency scan.

Scan results are displayed in table format, and can also be displayed in graph format. In Single Mode, results are displayed after the scan is completed. In Continuous Mode, results are displayed after the scan has completed one cycle over the defined spectrum, and are automatically updated as the scan proceeds.

Below figure shows the results of a Continuous Mode scan on an PTP 820V in table format. Below figure shows the results of a Single Mode scan on an PTP 850E in table format. For each RX channel in the defined frequency range, the table displays the following columns:

- Frequency (MHz) – The starting frequency in the scanned channel.
- RSL Sample Value (dBm) – In Single Mode, the RSL value measured for the scanned channel. In Continuous Mode, the latest RSL value measured for the scanned channel.
- Minimum RSL (dBm) – In Continuous Mode, the lowest RSL value measured for the scanned channel. In Single Mode, the same as the RSL Sample Value.
- Maximum RSL (dBm) – In Continuous Mode, the highest RSL value measured for the scanned channel. In Single Mode, the same as the RSL Sample Value.

You can also display the scan results in graph format by clicking **Graph**. The Graph page presents the scan results in graphical format, with the frequency on the horizontal axis and the RSL on the vertical axis.

The Graph page has the following tabs:

- RSL Sample Value (dBm) – In Single Mode, the RSL value measured for the scanned channel. In Continuous Mode, the latest RSL value measured for the scanned channel.
- Minimum RSL (dBm) – In Continuous Mode, the lowest RSL value measured for the scanned channel. In Single Mode, the same as the RSL Sample Value.
- Maximum RSL (dBm) – In Continuous Mode, the highest RSL value measured for the scanned channel. In Single Mode, the same as the RSL Sample Value.

Figure 58 Frequency Scanner Results – Graph Format (Continuous Mode)

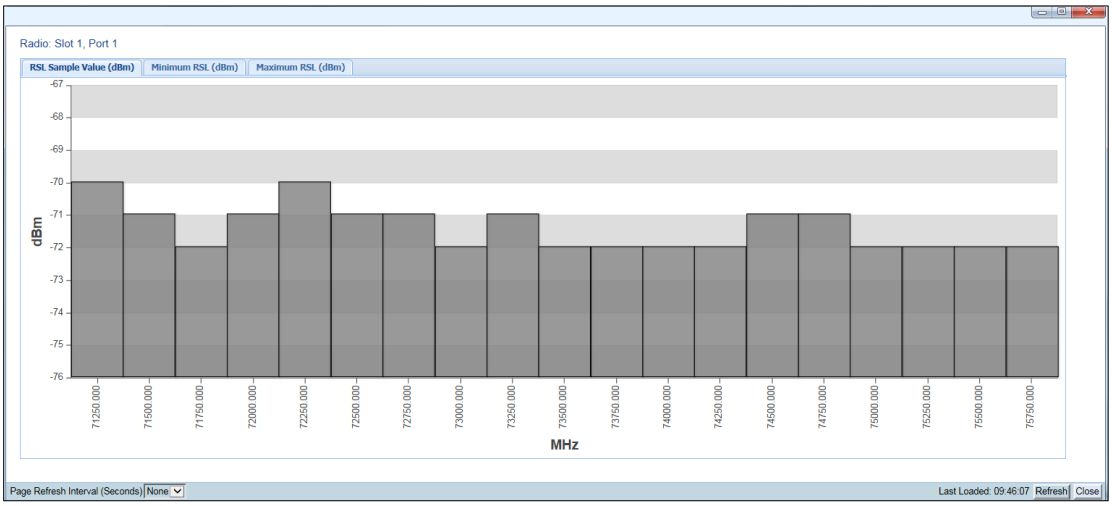
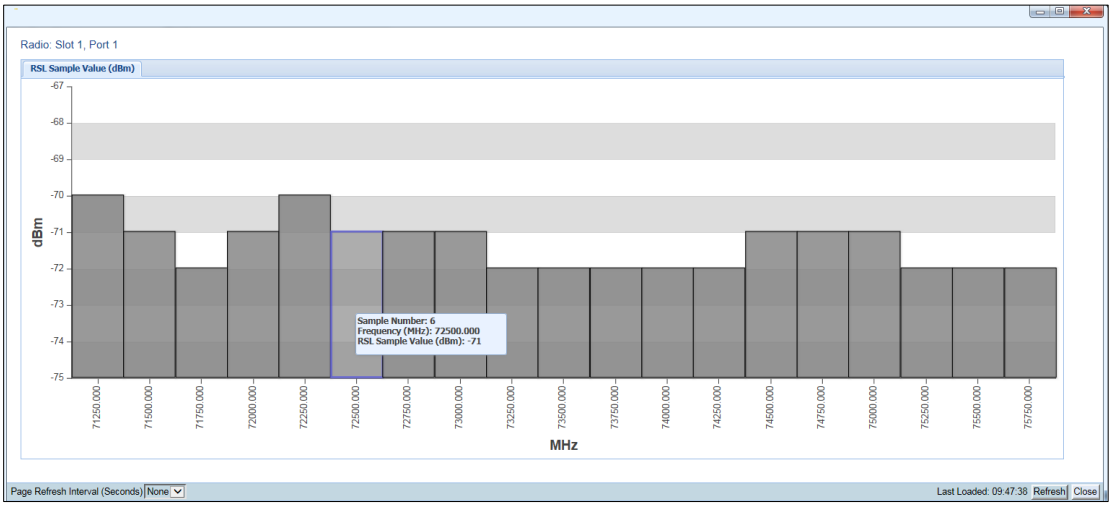


Figure 59 Frequency Scanner Results – Graph Format (Single Mode)



3.19 Configuring the Radio Parameters

In order to establish a radio link, you must:

1. Verify that the radio is muted (the **TX Mute Status** should be **On**).
2. Configure the radio frequencies.



Note:

Even if you are using the default frequencies, it is mandatory to actually configure the frequencies.

3. Configure the TX level.
4. Click **Apply** to apply these configurations.



Note:

If you are using the default values and did not change any other parameters on the Radio Parameters page, the **Apply** button will be grayed out. To activate the **Apply** button, change any parameter on the page, then change it back to the desired value.

5. Set **TX Mute** to **Unmute**.
6. Click **Apply** to apply the unmute.
7. Verify that the radio is unmuted (the **TX Mute Status** should be **Off**).

You can do these tasks, perform other radio configuration tasks, and display the radio parameters in the Radio Parameters page.

To configure the radio parameters:

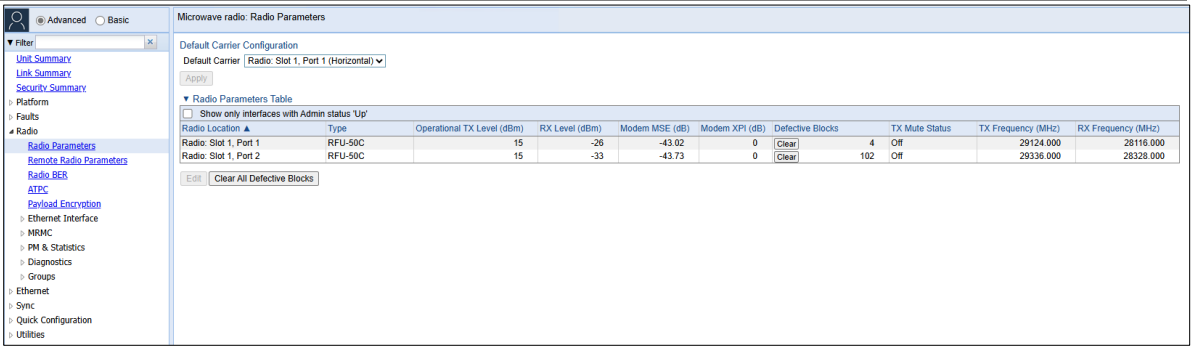
1 Select **Radio > Radio Parameters:**

Note: This page is only available in Advanced mode. However, the basic radio parameters can also be configured during link configuration with a Quick Configuration wizard. See Configuring a Link Using the Quick Configuration Wizard. You can also configure the basic radio parameters in Basic mode by selecting **Interfaces > Interface Manager**, selecting a radio interface, and clicking **Radio Parameters**.

- For PTP 850C, the Radio Parameters Table opens. Select the carrier you want to configure and click **Edit** to display the Radio Parameters page for that carrier.

  For PTP 850C, the **Default Carrier** field is available in the Radio Parameters Table and enables you to use the Horizontal carrier (Port 1) or the Vertical carrier (Port 2) for 1+0 configurations. By default, Horizontal is selected. If you are configuring a Vertical 1+0 configuration, select **Radio: Slot 1, Port 2 (Vertical)** in the **Default Carrier** field, then click **Apply**. Make sure the **Default Carrier** field matches the physical configuration of the device (Horizontal or Vertical).

Note: You cannot change the default carrier if there are services configured on either of the carriers or if either or both carriers belong to a Multi-Carrier ABC group.



- For PTP 850E, the Radio Parameters page opens right away.

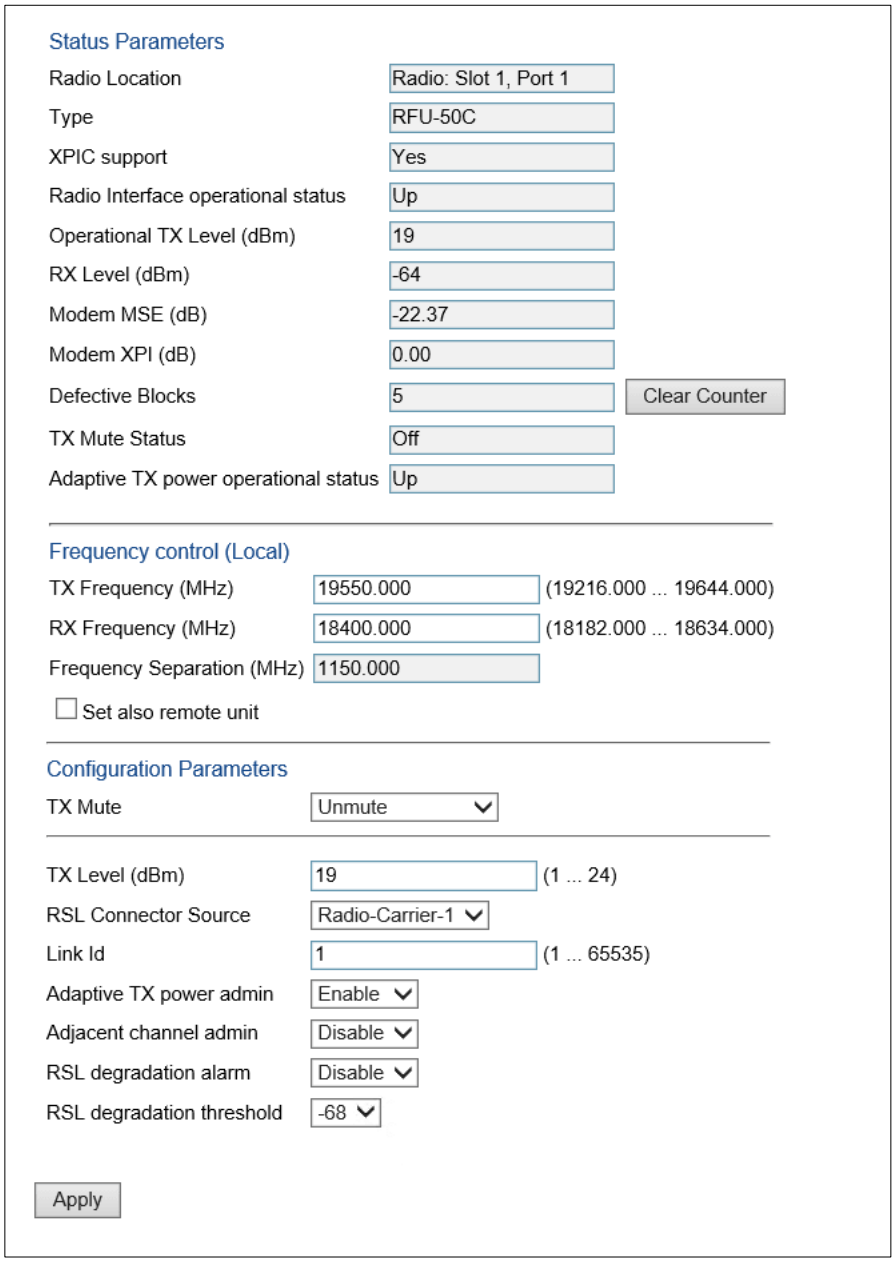


Figure 60: Radio Parameters Page

2 Set the radio frequency in the **Frequency control (Local)** section:

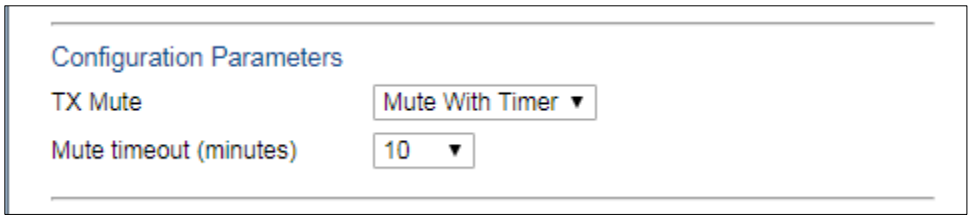
i In the **TX Frequency (MHz)** field, set the transmission radio frequency in MHz.
ii In the **RX Frequency (MHz)** field, set the received radio frequency in MHz.
iii Click **Apply**. The system automatically calculates and displays the frequency separation in the **Frequency Separation (MHz)** field, based on the configured TX and RX frequencies.
iv Optionally, select **Set also remote unit** to apply the frequency settings to the remote unit as well as the local unit.

Notes: If the carrier belongs to an AMCC (XPIC) group, you must disable the group before changing the TX or RX frequency.

3 Set the other radio parameters in the **Configuration parameters** section:

i To mute the TX output of the radio carrier, select **Mute** in the **TX Mute** field. To unmute the TX output of the radio carrier, select **Unmute**. To configure a timed mute, select **Mute with Timer**.

If you select **Mute with Timer**, an additional field appears: **Mute timeout (minutes)**. This field defines a timer for the mute, in minutes (1-1440). When the timer expires, the mute automatically ends. This provides a fail-safe mechanism for maintenance operations that eliminates the possibility of accidently leaving the radio muted after the maintenance has been completed. By default, the timer is 10 minutes.



Note: In contrast to an ordinary mute, a timed mute is not persistent. This means that if the unit is reset, the radio is not muted when the unit comes back online, even if the timer had not expired. Also, in Unit Redundancy configurations, a timed mute is not copied to the mate unit or radio, and no mismatch alarm is raised if a timed mute is configured on only one radio in the protection pair.

ii In the **TX Level (dBm)** field, enter the desired TX signal level (TSL). The range of values depends on the frequency and RFU type. When **Adaptive TX power admin** is configured to **Enable**, this field determines the maximum TX level, as described below.
iii The **RSL Connector Source** field (PTP 850C only) is used when you are measuring the RSL at the unit's RSL port, and determines which receiver's RSL is measured at the RSL port:

- **Main** – Reserved for future use.
- **Diversity** – Reserved for future use.
- **Radio-Carrier-1** – Select this to measure the RSL of radio carrier 1.
- **Radio-Carrier-2** – Select this to measure the RSL of radio carrier 2.

Note: The voltage at the RSL port is 1.XX where XX is the RSL level. For example: 1.59V means an RSL of -59 dBm. Note that the voltage measured at the RSL port is not accurate and should be used only as an aid).

Note that the voltage measured at the RSL port is not accurate and should be used only as an aid).

iv In the **Link ID** field, enter a unique link identifier from 1 to 65535. The Link ID identifies the link, in order to distinguish it from other links. If the Link ID is not the same at both sides of the link, a Link ID Mismatch alarm is raised.

v The **Adaptive TX power admin** field enables or disables Adaptive TX Power. When Adaptive TX Power is enabled, the radio adjusts its TX power dynamically based on the current modulation. When the modulation is at a high level, the TX power is adjusted to the level required with the high modulation. If the modulation goes down to a lower level, the TX power increases to compensate for the lower modulation. The TX level configured in the **TX Level (dBm)** field determines the maximum TX level, but the actual TX level as shown in the **Operational TX Level (dBm)** field can be expected to be lower when the radio is operating at high modulations requiring less TX power.
To enable Adaptive TX power, select **Enable**. The **Adaptive TX power operational status** field should now indicate **Up** to indicate that the feature is fully functional.

Note: Adaptive TX Power only operates when the MRMC script is configured to Adaptive mode. If the script is configured to Fixed mode (or Adaptive mode with the Minimum and Maximum Profile set to the same value), you can set **Adaptive TX Power** to **Enable**, but the **Adaptive TX power operational status** field will indicate **Down**.

vi In certain adjacent channel configurations with PTP 850C, interference from the adjacent channel may prevent the link from reaching the maximum ACM profile that might otherwise be available.

In addition, if the TX is muted, and Adaptive TX Power is enabled on the remote side, the remote side will reach LOF and its increased TX power may lead to poor MSE on the local adjacent receiver.

Therefore, if these problems exist on an PTP 850C using an adjacent channel configuration, it is recommended to set **Adjacent channel admin** to **Enable**. For all other products and configurations, leave the default value of **Disable**.

Note: Enabling or disabling Adjacent Channel mode may cause a brief loss of traffic.

vii In the **RSL degradation alarm** field, select **Enable** if you want the unit to generate an alarm in the event that the RSL falls beneath the threshold defined in the **RSL degradation threshold** field. The range of values is -99 to 0. By default, the alarm is disabled, with a default degradation threshold of -68 dBm. The RSL degradation alarm is alarm ID 1610, *Radio Receive Signal Level is below the configured threshold*.
The alarm is cleared when the RSL goes above the configured threshold. The alarm is masked if the radio interface is disabled, the radio does not exist, or a communication-failure alarm (Alarm ID #1703) is raised.

Note: The **RSL Connector Source** field is not relevant for PTP 850E.

For a description of the read-only parameters in the **Status parameters** section .

3.20 Creating Service(s) for Traffic

In order to pass traffic through the PTP 850E, you must configure Ethernet traffic services. For configuration instructions, see Configuring Ethernet Service(s).

3.21 Configuring CPRI

Optionally, PTP 850E can be used with a CPRI module. The CPRI module is inserted in the PTP 850E's QSFP port (P4), and provides up to 10 Gbps capacity for CPRI traffic. The CPRI module converts CPRI signals to Ethernet and Ethernet to CPRI in

accordance with Radio over Ethernet (RoE) standard IEEE 1914.3 and CPRI specification v7.0. For more details, see the Technical Description for PTP 850E.

Note: Support for CPRI is planned for future release.

CPRI Configuration Overview

Note: For instructions how to install the CPRI module in the PTP 850E, refer to the Installation Guide for PTP 850E.

Before configuring the QSFP port (P4) for CPRI, make sure the following preconditions are met for the logical ports that correspond to P4 (Ethernet Slot 1, Port 3, Ethernet Slot 1, Port 4, Ethernet Slot 1, Port 5, and Ethernet Slot 1, Port 6):

- In the Interface Manager, the ports must all be set to **Admin Status** = **Down**.
- None of the ports belong to a group (e.g., LAG).
- None of the ports are used as a synchronization source.
- No service point is attached to any of the ports.
- 1588 Boundary Clock is not configured on any of the ports.

Once these conditions are met, the following configurations must be made for P4:

- Set the QSFP mode to CPRI.
- Create an Ethernet service for CPRI traffic.
- Configure Synchronization for CPRI traffic.
- Configure the CPRI parameters.
- Enable the CPRI port.
- Configure Synchronization for CPRI traffic
- Create an Ethernet service for CPRI traffic

Setting the QSFP Mode to CPRI

To set the QSFP mode of the QSFP port to CPRI:

- Select Platform > Interfaces > QSFP. The QSFP Module Configuration page opens.

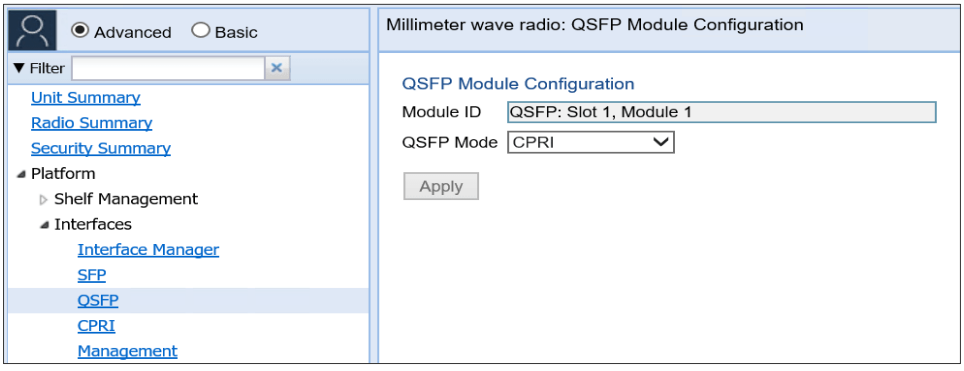


Figure 51: QSFP Module Configuration Page – CPRI

- Select **CPRI**.
- Click **Apply**.

After this step has been performed, the logical ports that correspond to P4 (Ethernet Slot 1, Port 3, Ethernet Slot 1, Port 4, Ethernet Slot 1, Port 5, and Ethernet Slot 1, Port 6) no longer appear in the various Web EMS pages that display port status and configuration. Instead, the following appears to represent the port:

- CPRI Slot 1 Port 1

Creating an Ethernet Service for CPRI Traffic

You must configure a point-to-point Ethernet service with the following service points to carry CPRI traffic:

- Create a service point on the radio interface.
- Create a service point on the CPRI interface (CPRI Slot 1 Port 1)

It is recommended to use pre-defined service point Option #8 (PIPE, dot1q). See

Configuring Ethernet Service(s).

Configuring Synchronization for CPRI Traffic

Synchronization for the CPRI module should be configured as follows:

- If the CPRI module is connected to a Baseband Unit (BBU), CPRI Slot 1 Port 1 should be configured as the lowest priority synchronization source.
- If the CPRI module is connected to the Remote Radio Head (RRH, also known as the Remote Radio Unit, RRU), Radio Slot 1 Port 1 should be configured as the lowest priority synchronization source.

Configuring the CPRI Parameters

To configure the CPRI parameters:

- Select Platform > Interfaces > CPRI. The CPRI Configuration page opens.

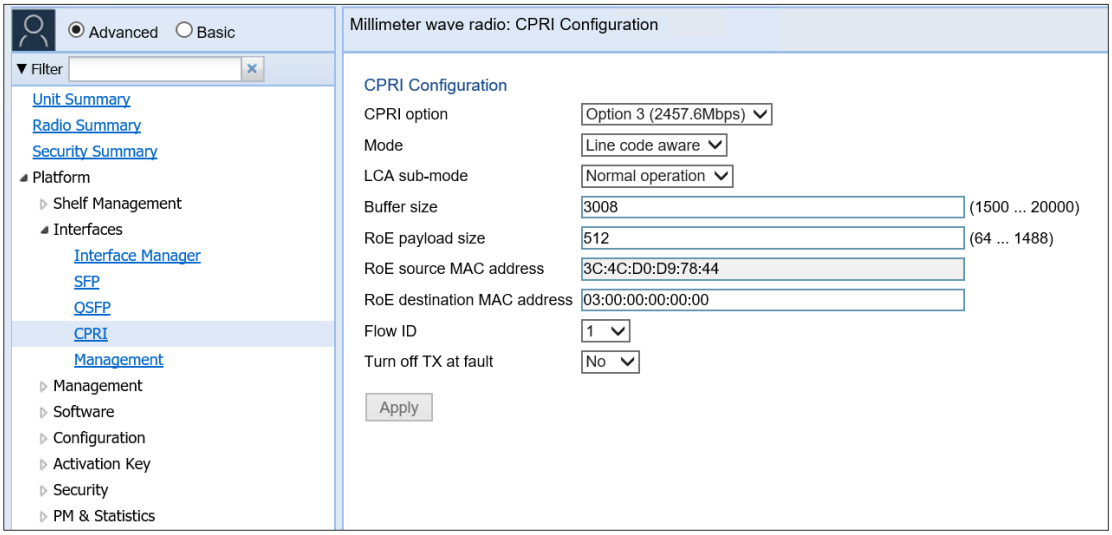


Figure 52: CPRI Configuration Page

- In the CPRI option field, select the bit rate option for the CPRI module. This parameter must be set to the same value on both sides of the CPRI link.

The following options are available:

- **Option 3 (2457.6Mbps)** – 2457.6Mbps, 8B/10B line coding
- **Option 5 (4915.2Mbps)** – 4915.2Mbps, 8B/10B line coding
- **Option 7 (9830.4Mbps)** – 9830.4Mbps, 8B/10B line coding (default)

Option 4 and **Option 6** also appear in the drop-down list, but these

- In the **Mode** field, select the system mode. This parameter must be set to the same value on both sides of the CPRI link.

The following options are available:

- **Line code aware** – (default)
- **Tunneling** – Only works with **Normal operation** as the **LCA sub-mode**. Does not work with **Option 7**.

- In the **LCA sub-mode** field, select the sub-mode. This parameter must be set to the same value on both sides of the CPRI link.

The following options are available:

- **Normal operation** – (default)
- **Special character** – Only works with **Line code aware** as the **Mode**.

- In the **Buffer size** field, configure the number of bytes that must be in the buffer before a CPRI signal is transmitted. This parameter must be set to the same value on both sides of the CPRI link.

Enter a multiple of 16, within the range of 1500 and 20000. The default value is 3008.

It is recommended to increase the buffer size if the traffic from either side is not continuous, but rather, comes in bursts.

- In the **RoE payload size** field, configure the RoE payload length, in bytes. This includes only CPRI data, not the RoE header. The default value is 512. This parameter must be set to the same value on both sides of the CPRI link.

The available options depend on the **Mode** and **LCA sub-mode**, as follows:

- When the **Mode** is **Line code aware** and the **LCA sub-mode** is **Normal operation**, supported values are 256, 512, and 1024.
- When the **Mode** is **Line code aware** and the **LCA sub-mode** is **Special character**, supported values are 512 and 1024.
- When the **Mode** is **Tunneling** and the **LCA sub-mode** is **Normal operation**, supported values are multiples of 16 within a range of 64 to 1488.

The **RoE source MAC address** field is read only, and displays the MAC

- In the **RoE destination MAC address** field, enter the following:
- If the CPRI module is connected to a BBU, enter the MAC address of the CPRI module connected to the RRH.
- If the CPRI module is connected to a RRH, enter the MAC address of the CPRI module connected to the BBU.

- In the **Flow ID** field, select an ID to be used in the RoE conversion. Options are 0-10. The default is 1. This parameter must be set to the same value on both sides of the CPRI link.
- In the **Turn off TX at fault** field, select **No** (default) or **Yes**.

If this parameter is set to **Yes**, the TX is turned off if a fault is discovered.

- Click **Apply**.

Enabling the CPRI Port

You must enable the CPRI port (CPRI Slot 1 Port 1) in the Interface Manager.

You must enable the CPRI port (CPRI Slot 1 Port 1) in the Interface Manager.

To enable the CPRI port:

1 Select **Platform** > **Interfaces** > **Interface Manager**. The Interface Manager page opens, displaying all of the system's traffic and management interfaces.

Note: To display the same page in Basic mode, select **Interfaces** > **Interface Manager**.

2 Select CPRI Slot 1 Port 1 and click **Interface Admin**. The Interface Manager Parameters page opens.

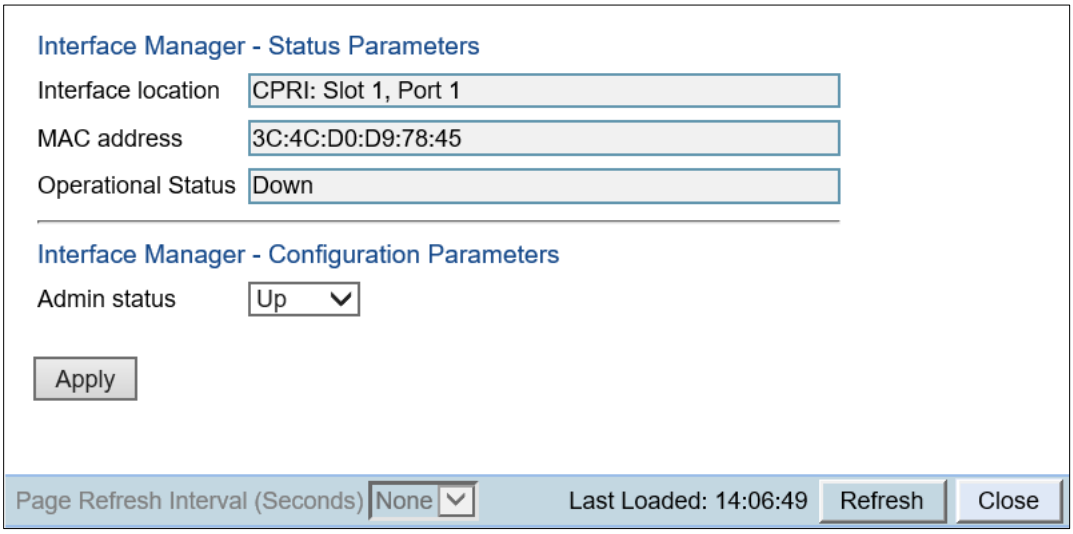


Figure 61: Interface Manager Page – Enabling the CPRI Port

3 In the **Admin Status** field, select **Up**.
4 Click **Apply**.

For general information on configuring interfaces, see Enabling the Interfaces (Interface Manager).

Configuring Synchronization for CPRI Traffic

Synchronization for the CPRI module should be configured as follows:

- If the CPRI module is connected to a Baseband Unit (BBU), CPRI Slot 1 Port 1 should be configured as the lowest priority synchronization source.
- If the CPRI module is connected to the Remote Radio Head (RRH, also known as the Remote Radio Unit, RRU), Radio Slot 1 Port 1 should be configured as the lowest priority synchronization source.

To configure the CPRI module connected to the BBU:

1 Select **Sync** > **Sync Source**. The Sync Source page opens.

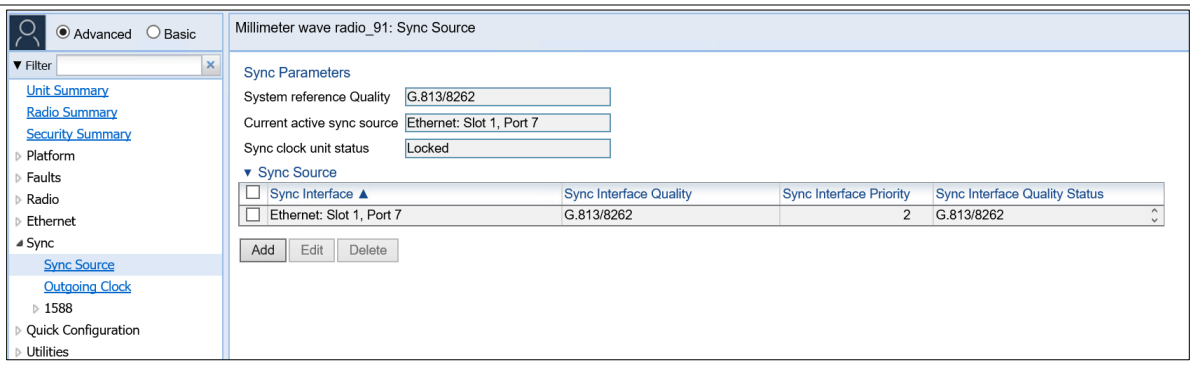


Figure 62: Sync Source Page

2 In the Sync Source page, click **Add**. The Sync Source – Add page opens.

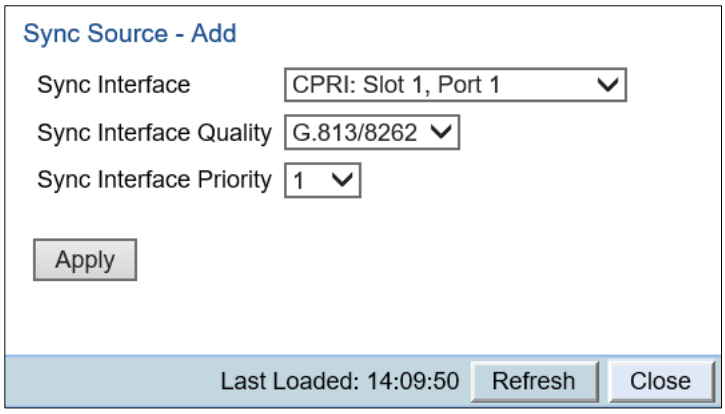


Figure 63: Sync Source – Add Page (CPRI – BBU)

3 In the **Sync Interface** field, select **CPRI Slot 1 Port 1**.
4 In the **System Interface Quality** field, select **G.813/8262**.
5 In the **System Interface Priority** field, select **1**.
6 Click **Apply**.

To configure the CPRI module connected to the RRH:

1 Select **Sync** > **Sync Source**. The Sync Source page opens (Figure 62).
2 In the Sync Source page, click **Add**. The Sync Source – Add page opens.

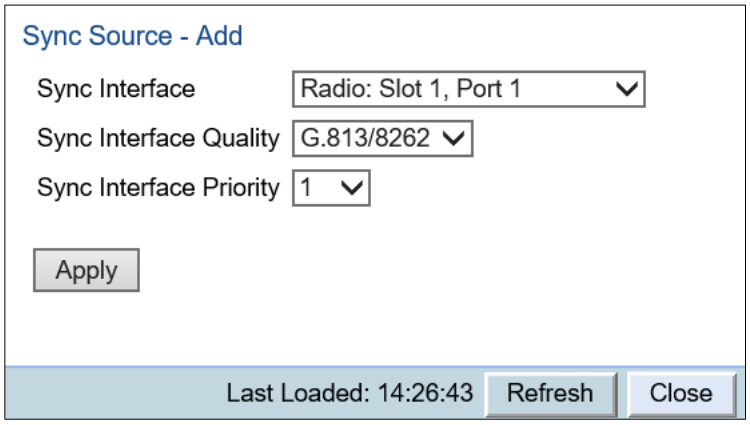


Figure 64: Sync Source – Add Page (CPRI – RRH)

3 In the **Sync Interface** field, select **Radio Slot 1 Port 1**.
4 In the **System Interface Quality** field, select **G.813/8262**.
5 In the **System Interface Priority** field, select **1**.

6 Click **Apply**.

For general information about configuration a sync source, see Configuring the Sync Source.

Creating an Ethernet Service for CPRI Traffic

You must configure a point-to-point Ethernet service with the following service points to carry CPRI traffic:

- Create a service point on the radio interface.
- Create a service point on the CPRI interface (CPRI Slot 1 Port 1)

It is recommended to use pre-defined service point Option #8 (PIPE, dot1q).

To create the required Ethernet service:

1 Select **Ethernet > Services**. The Ethernet Services page opens.

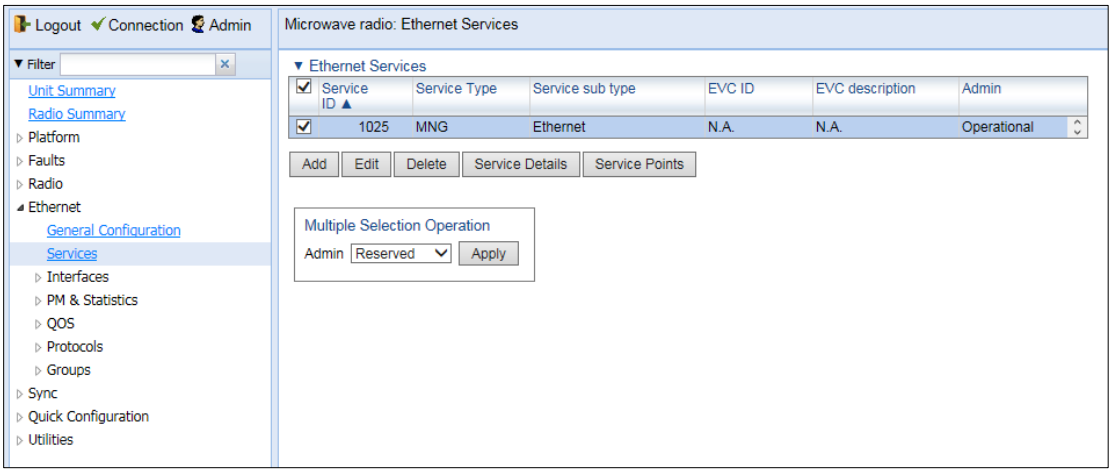


Figure 65: Ethernet Services Page

2 In the Ethernet Services page, click **Add**. The Ethernet Services – Add page opens.

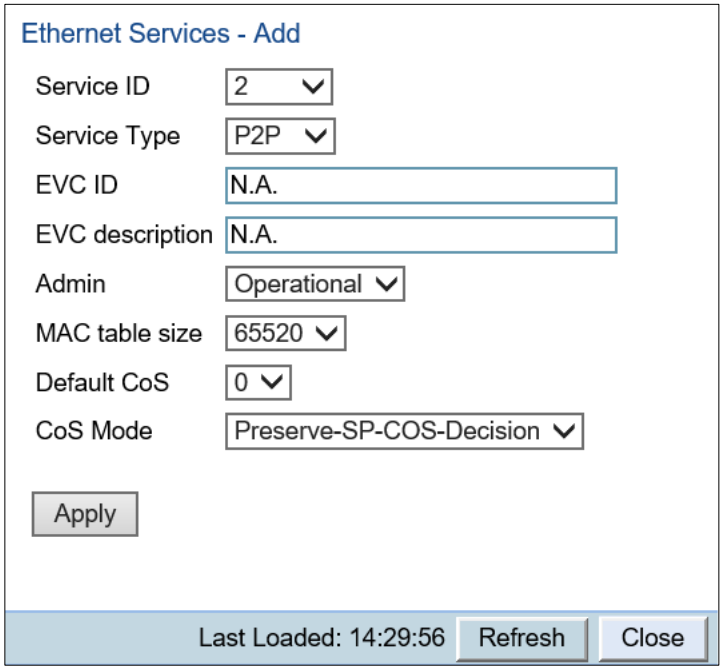


Figure 66: Ethernet Services - Add page (CPRI)

3 In the **Service ID** field, select a unique ID for the service. You can choose any unused value from 1 to 4095. Once you have added the service, you cannot change the Service ID. Service ID 1025 is reserved for a pre-defined management service.
4 In the **Service Type** field, select **P2P.**
5 Optionally, in the **EVC ID** field, enter an Ethernet Virtual Connection (EVC) ID (up to 20 characters). This parameter does not affect the network element's behavior, but is used by the NMS for topology management.
6 Optionally, in the **EVC Description** field, enter a text description of the service (up to 64 characters). This parameter does not affect the network element's behavior, but is used by the NMS for topology management.
7 In the **Admin** field, select **Operational**.
8 In the **MAC table size** field, enter the maximum MAC address table size for the service. The MAC address table is a source MAC address learning table used to forward frames from one service point to another. You can select from the value range 16 – 65,520, in multiples of 16.
This maximum only applies to dynamic, not static, MAC address table entries.

Note: Additional configuration of the MAC address table can be performed via the CLI. See Defining the MAC Address Forwarding Table for a Service.

9 In the **Default CoS** field, enter a default Class of Service (CoS) value (0-7). This value is assigned to frames at the service level if CoS Mode is set to Default-CoS. Otherwise, this value is not used, and frames retain whatever CoS value they were assigned at the service point or logical interface level.
10 In the **CoS Mode** field, select one of the following options. This parameter determines whether or not frames passing through the service have their CoS modified at the service level. The CoS determines the priority queue to which frames are assigned.

- **Default CoS** – Frames passing through the service are assigned the default CoS defined above. This CoS value overrides whatever CoS may have been assigned at the service point or interface level.
- **Preserve-SP-COS-Decision** – The CoS of frames passing through the service is not modified by the service's default CoS.

11 Click **Apply**, then **Close** to close the Ethernet Services - Add page.

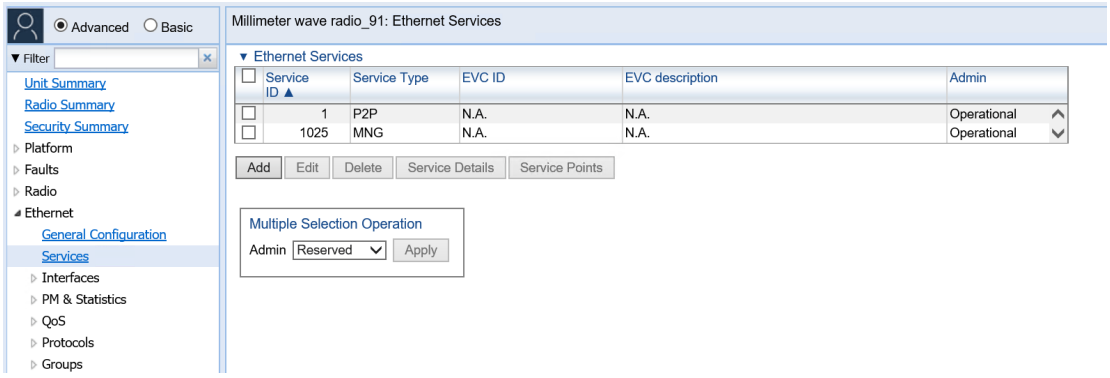


Figure 67: Ethernet Services Page – CPRI Service

12 In the Ethernet Services page, select the service you just configured.
13 Click **Service Points**. The Ethernet Service Points page opens.

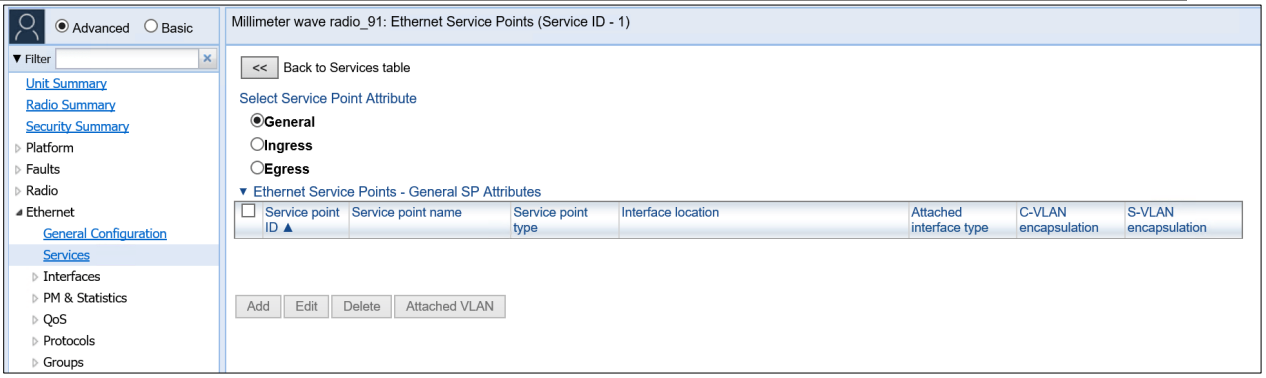


Figure 68: Ethernet Service Points Page (Empty)

14 Click **Add**. The Ethernet Service Points – Add page opens.

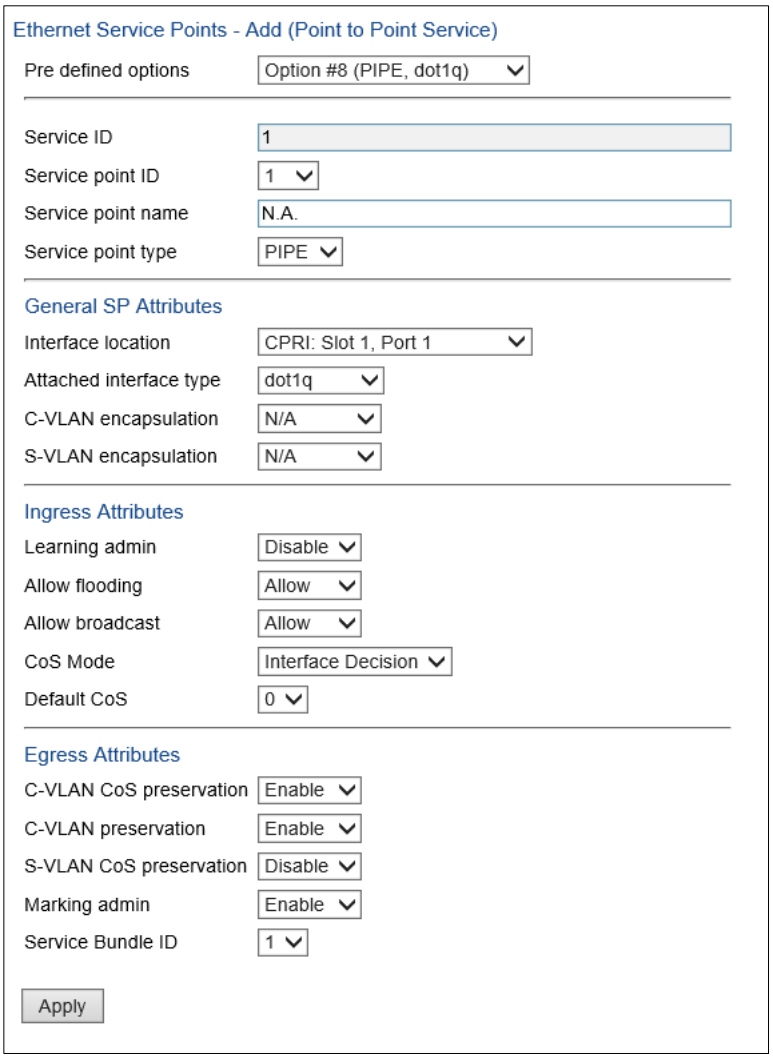


Figure 69: Ethernet Service Points - Add Page (CPRI Service Point on CPRI Port)

15 In the **Pre defined options** field, select **Option #8 (PIPE, dot1q)**.
16 In the **Interface location** field, select **CPRI: Slot 1, Port 1**.
17 Leave the values of the other fields with their default parameters according to **Option #8 (PIPE, dot1q)**.
18 Click **Apply**, then **Close**.

19 Repeat Steps 14 through 18 to create a second service point. However, in the **Interface location** field, select **Radio: Slot 1, Port 1**.

Once you have completed this procedure, the Ethernet Service Points page should appear as shown in Figure 70.

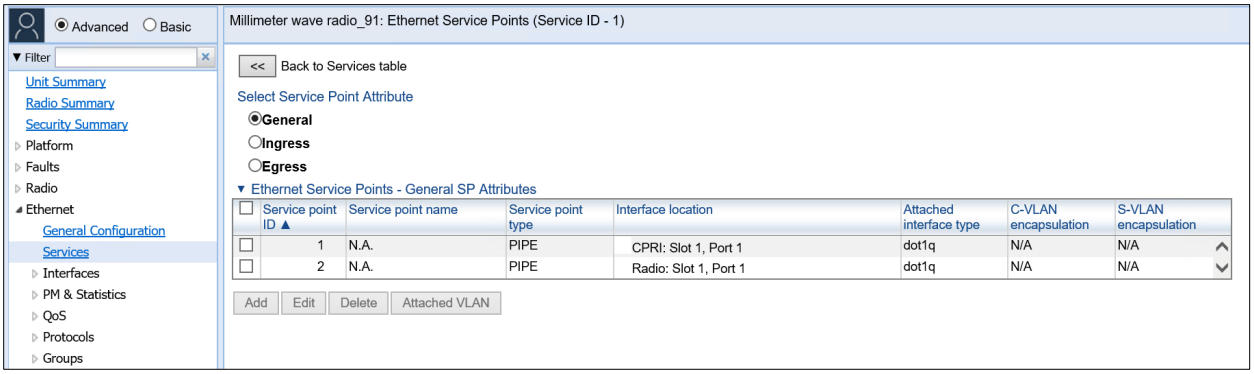


Figure 70: Ethernet Service Points Page (Populated for CPRI Service)

For general information about configuration Ethernet services and service points, see Configuring Ethernet Service(s).

3.22 Operating in FIPS Mode

Notes: FIPS 140-3 compliance is only available with System release 12.7.

PTP 850C and PTP 850E can be configured to be FIPS 140-3-compliant in specific hardware and software configurations, as described in this section.

Requirements for FIPS Compliance

For a full list of FIPS requirements, refer to the *FIPS 140-3 Non-Proprietary Security Policy*, available upon request. It is the responsibility of the customer to ensure that these requirements are met.

For an PTP 850C and PTP 850E node to be FIPS-compliant, the unit must be FIPS-compliant hardware. A FIPS-compliant PTP 850C or PTP 850E unit has a unique part number ending in the letters AF, in the following format:

- PTP 850C-***-AF
- PTP 850E-***-AF

Note: To display the part numbers of the hardware components of your PTP 850 unit.

Unit redundancy configurations can be configured to be FIPS 140-3-compliant. This requires encryption of the protection link between the two units.

Three special labels, included with the PTP 850C or PTP 850E radio kit, must be affixed to a FIPS-compliant PTP 850C or PTP 850E unit once the diplexer unit has been attached to the radio unit. These labels are tamper-evident and must be applied in such a way that it is not possible to remove the diplexer unit from the radio unit without also removing a label and leaving evidence that the label was tampered with. The labels must be replaced if the radio or diplexer is replaced. Replacement labels can be ordered from Cambium Networks, part number BS-0341-2. Tamper-evident labels should be inspected for integrity at least once every six months.

When applying a FIPS label, make sure to follow these guidelines:

- Use caution to avoid touching the adhesive in such a way as to leave fingerprints and damage the labels.
- The curing time (drying time) for the labels is at least sixty minutes.
- When replacing a label, gently cut the label, replace the module, and apply a new label in place of the previous label.

For additional information, refer to the Installation Guide for the product you are using.

Enabling FIPS Mode

To set the unit to operate in FIPS mode:

1 Select **Platform** > **Security** > **General** > **Configuration**. The Security General Configuration page opens.

Note: This page is only available in Advanced mode.

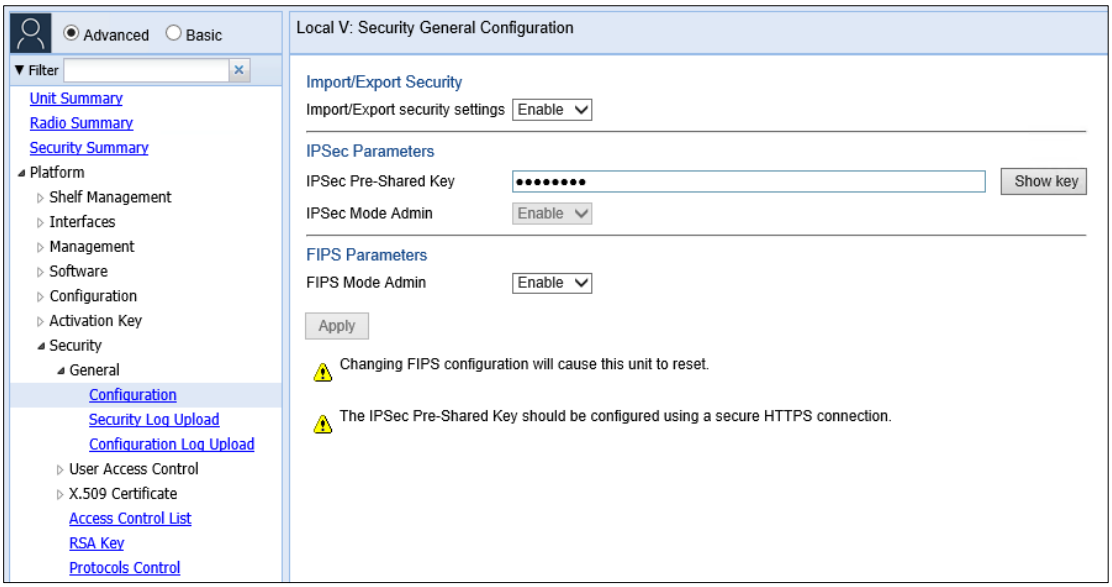


Figure 71: Security General Configuration Page

2 The **Import/Export security settings** field determines whether security configurations are included in configuration backup files. To enhance unit security, it is recommended to select **Disable** in this field, so that security configurations will *not* be included in backup files. When you are finished, click **Apply**.
3 In the **FIPS admin configuration** field, select **Enable**.
4 Click **Apply**. Changing the FIPS configuration causes a unit reset. After this or any other system reset in FIPS mode, the length of time before users can log back into the system is longer than usual due to FIPS-related self-testing.

Note: Note that when FIPS is enabled in a link with unit redundancy or, for PTP 850E, 2+0 XPIC, this state is propagated to the mate unit, causing reset of both units. Note also that when FIPS is enabled in a link with unit redundancy, IPsec encryption is automatically enabled on the external protection link. For details, see Encrypting the Protection Link.

After enabling FIPS:

- The MD5 option for SNMPv3 is blocked.

For a full list of FIPS requirements, including software configuration requirements, refer to the FIPS 140-3 Non-Proprietary Security Policy, available upon request.

Note that whenever one of the following occurs with FIPS mode enabled (Admin = Enable), a Key Derivation Function self-test (Known Answer Test - KAT) is initiated:

- SNMP is enabled or disabled.
- An SNMPv3 user is added or removed
- IPsec mode is enabled (Admin = Enable)
- The IPsec pre-shared key is changed

If the Key Derivation Function self-test fails, the unit is automatically rebooted. If the self-test fails again after reboot has been completed, another reboot is initiated and a soft-zeroization takes place, as part of which all sensitive security parameters are erased from the device's persistent storage and FIPS mode is disabled.

3.22.1 Initial Configuration of FIPS-Compliant Unit Redundancy Configuration

For unit redundancy configurations, the external protection link must be encrypted using IPsec. This encrypts all IP packets that pass between the management ports of the two PTP 850 units.

To set up a unit redundancy configuration that is FIPS 140-3-compliant, you must follow these steps:

1 Configure and enable unit redundancy on both units.
2 Enable FIPS on both PTP 850 units. See Enabling FIPS Mode.
When you enable FIPS mode, IPsec encryption will automatically be enabled on the protection link, using the default protection pre-shared key. Alarm 5113 will be raised.
3 Verify that there is no Configuration Mismatch alarm by checking in the **Faults > Current** Alarms page. If a Configuration Mismatch alarm is present, you must clear the alarm before configuring a new pre-shared key. Otherwise, the key will not be copied to the Standby unit.

Note: You can use the following CLI command to display a list of mismatched parameters:

```
root> platform management protection show mismatch details
```

4 Configure a new pre-shared key on the active unit. For instructions, see Encrypting the Protection Link.

3.22.2 Replacing a Unit in a FIPS-Compliant Unit Redundancy Configuration

If it becomes necessary to replace a unit in a FIPS 140-3-compliant unit redundancy configuration, you must pre-configure the replacement unit as follows:

1 Enable FIPS on the replacement unit. See Enabling FIPS Mode.
2 Configure the protection pre-shared key on the replacement unit. See Initial Configuration of FIPS-Compliant Unit Redundancy Configuration, Step 3.
3 Configure and enable unit redundancy on the replacement unit.
4 Perform copy-to-mate.

3.23 Encrypting the Protection Link

Optionally, you can encrypt the protection link using IPSec. This encrypts all IP packets that pass between the Protection ports of the two PTP 850 units.

IPSec uses a 32-character pre-shared key. The pre-shared key is a 32-byte symmetric encryption key. The same pre-shared key must be configured on both ends of the encrypted link. The default value of the pre-shared key is:

```
protectionpresharedkey0123456789
```

You should make sure to change the default value when enabling IPSec encryption. If the default value is not changed, the following alarm is triggered:

- 5113 – IPSec Pre-Shared Key has the default value

If you are encrypting the protection link when initially configuring Unit Redundancy, it is recommended to configure encryption *before* enabling Unit Redundancy. In this case, configure IPSec encryption separately on both PTP 850 units on both sides of the link, making sure to use the same pre-shared key.

If you are encrypting the protection link in a configuration in which Unit Redundancy has already been configured, configure IPSec on the Active unit on both sides of the link. The IPSec configuration will be copied automatically to the Standby units.

To configure IPSec encryption of the protection link:

1 Verify that the web interface protocol for accessing the unit is configured to HTTPS. See Enabling HTTPS.
2 Select **Platform** > **Security** > **General** > **Configuration**. The Security General Configuration page opens (Figure 71).
3 In the **IPSec Pre-Shared Key** field, enter the pre-shared key. The key must be *exactly* 32 characters.

Note: If you are configuring IPSec after Unit Redundancy has already been enabled, communication with the Standby unit may be lost for up to a minute while the key is being copied.

4 In the **IPSec Mode Admin** field, select **Enable**.
5 Click **Apply**.

4. Configuration Guide

4.1 System Configurations

This section lists the basic PTP 850C, PTP 850E and PTP 850S system configurations, with links to configuration instructions.

Table 15 System Configurations

Configuration	Supported Products	Link to Configuration Instructions
1+0	All	Configuring a 1+0 Link Using the Quick Configuration Wizard
2+0 Enhanced Multi-Carrier ABC	PTP 850C	Configuring a 2+0 Multi-Carrier ABC Link Using the Quick Configuration Wizard OR Configuring Multi-Carrier ABC
Multiband	PTP 850E	Configuring a Multiband (Enhanced Multi- Carrier ABC) Link Using the Quick Configuration Wizard OR Configuring Multiband
2+0 XPIC	PTP 850C PTP 850E	Configuring XPIC
1+1 HSB Unit Protection	PTP 850E	Configuring 1+1 HSB Unit Protection
Link Aggregation (LAG)	PTP 850C PTP 850E PTP 850S	Configuring Link Aggregation (LAG) and LACP

5. Configuring an PTP 850 Unit Using Basic Mode

This section guides you through the Basic mode Web EMS menu tree. The purpose of this section is to enable Basic mode users to configure an PTP 850 unit, including unit and link parameters, quickly and efficiently. Cross-references are provided to other sections of the User Guide for more detailed explanations and instructions for PTP 850 features and configurations.

This section is divided and ordered according to the Basic mode menu tree:

- *Services* – Enables you to create Ethernet services.
- *Faults* – Includes options to display current alarms and the event log.
- *Performance Monitoring* – Enables you to display radio and Ethernet PMs.
- *Diagnostic & Maintenance* – Enables you to perform diagnostics, troubleshooting, and configuration management.
- Device View – Enables you to reset the unit and restore the unit's factory

default configuration settings.

- *Unit Summary* – Displays unit parameters, current alarms, and unit inventory information on a single page for quick viewing.
- *Quick Configuration* – Enables you to configure links quickly and simply using a collection of Quick Configuration wizards. Also enables you to configure the entire unit by applying a pre-configured System release Plan file.
- *Platform* – Includes pages for configuring the unit, including user access settings, activation keys, software upgrades, unit time, and other unit settings.
- *Interfaces* – Includes an expanded version of the Interface Manager page. From this page, you can enable and disable interfaces, configure radio parameters and MRMC scripts, display radio status, configure the physical parameters of an Ethernet interface, and configure basic ingress classification parameters of an interface.
- *Services* – Enables you to create Ethernet services.
- *Faults* – Includes options to display current alarms and the event log.
- *Performance Monitoring* – Enables you to display radio and Ethernet PMs.
- *Diagnostic & Maintenance* – Enables you to perform diagnostics, troubleshooting, and configuration management.

5.1.1 Device View

Device View is similar to the Chassis Configuration page in Advanced mode. From Device view, you can perform the following actions:

- Reset the unit. See *Performing a Hard (Cold) Reset*.
- Set the unit to its default factory configuration settings.

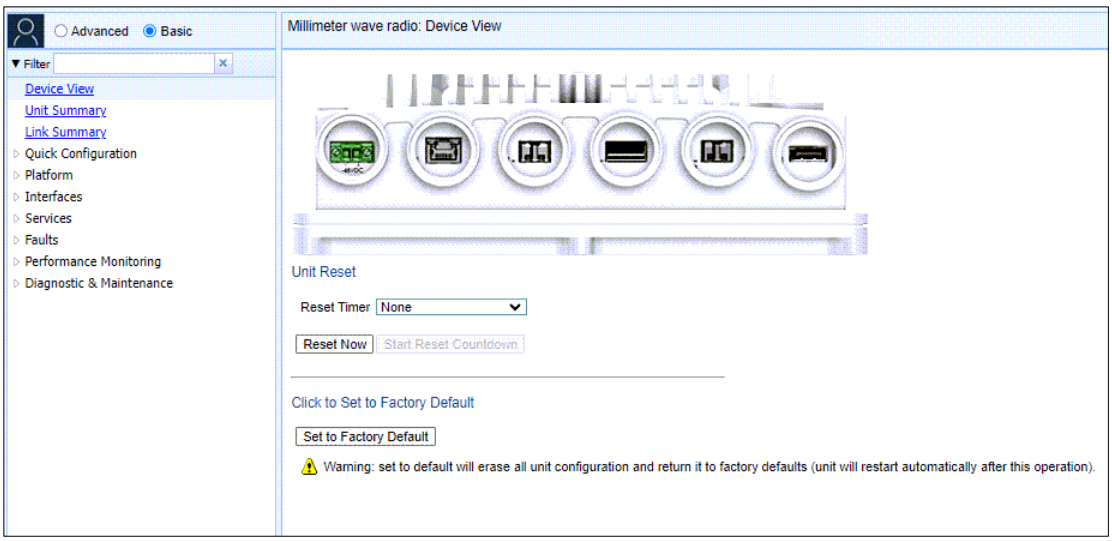


Figure 53: Basic Mode – Device View Page (PTP 850E)

5.1.2 Unit Summary

The Unit Summary page gathers the unit parameters, current alarms, and unit inventory information on a single page for quick viewing. For details, see *The Unit Summary Page*.

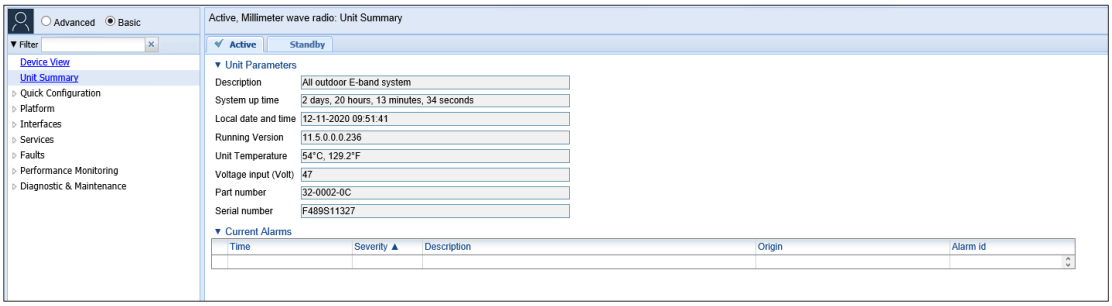


Figure 54: Basic Mode – Unit Summary Page

5.1.3 Quick Configuration

The Quick Configuration menu includes two options for quick configuration of an PTP 850 unit:

- **From System releasePlan** – Enables you apply a pre-defined configuration file that was created using System releasePlan. See *Applying a Pre-Defined Configuration File*.
- **PIPE Wizards** – Opens sub-menus from which you can access a collection of Quick Configuration wizards, that guide you through the process of configuring most types of PTP 850 links, from simple 1+0 links to more complex Multi-Carrier ABC and Multiband links. For a full description of these wizards and step-by-step instructions for using each wizard, see *Configuring a Link Using the Quick Configuration Wizard*.

5.1.4 Platform

From the Platform menu, you can access pages that enable you to configure the unit, including:

- *Unit Parameters Page* – Display and configure unit information, such as unit name and description, language, measurement format, and unit temperature and voltage input.
- *Software Versions & Upgrade Page* – Display the current System release version and perform software upgrades.
- *Time Services Page* – Configure the unit's time and date settings.
- *IP Configuration Page* – Configure the unit's IP address and enable or disable in-band management.
- *Activation Key Page* – Configure the unit's activation key and display current activation key coverage.
- *Security Pages* – Configure unit acess settings, including protocols for accessing the unit, login parameters, users, SNMP settings, and password settings.

Unit Parameters Page

In the Unit Parameters page, you can configure information such as the unit name and description, language, and measurement format. You can also display important information about the unit, such as the current unit temperature and voltage input. For more information, see *Configuring Unit Parameters*.

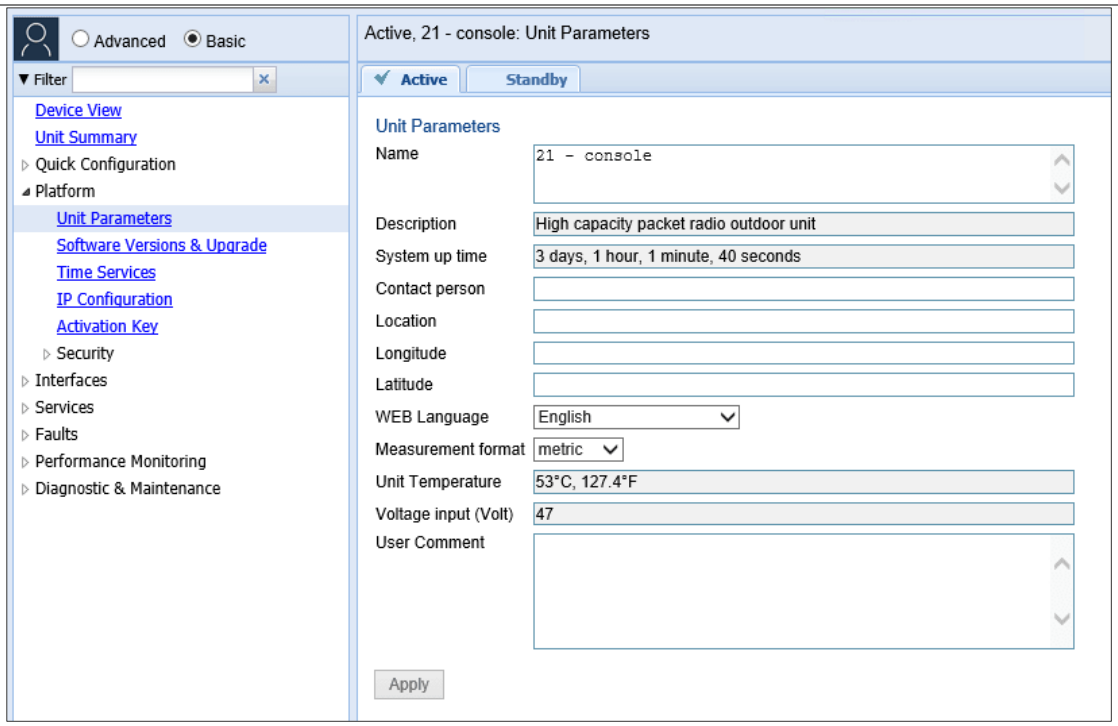


Figure 55: Basic Mode – Unit Parameters Page

Software Versions & Upgrade Page

In the Software Versions & Upgrade page, you can display the current System release version and download and install new versions using HTTP or FTP.

For a full explanation of software management, see *Upgrading the Software*.

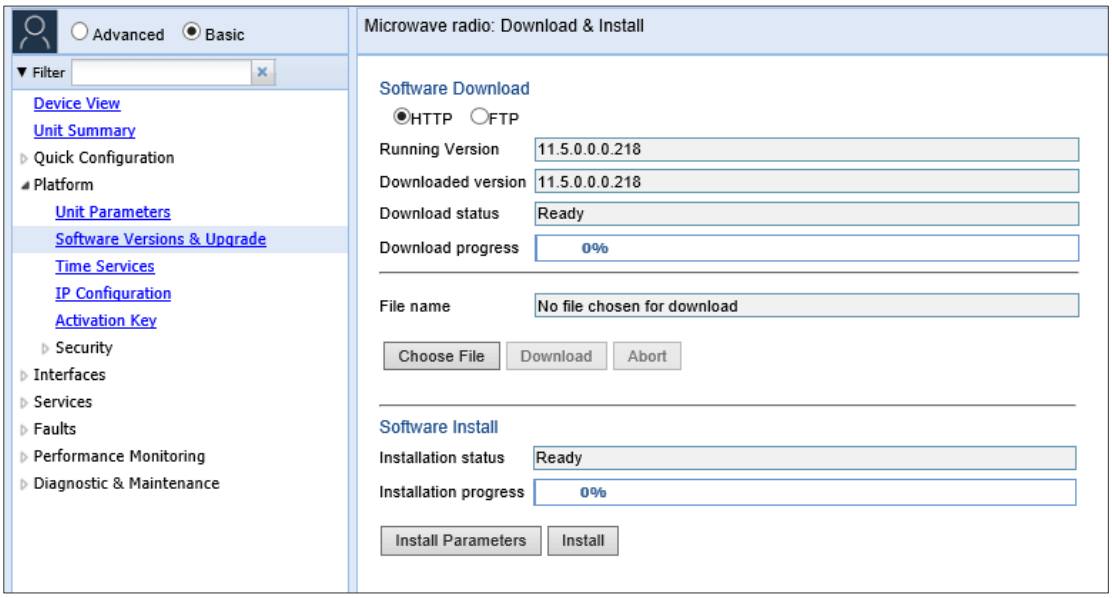


Figure 56: Basic Mode – Software Versions & Upgrade Page

Time Services Page

In the Time Services page, you can configure the unit's time and date settings.

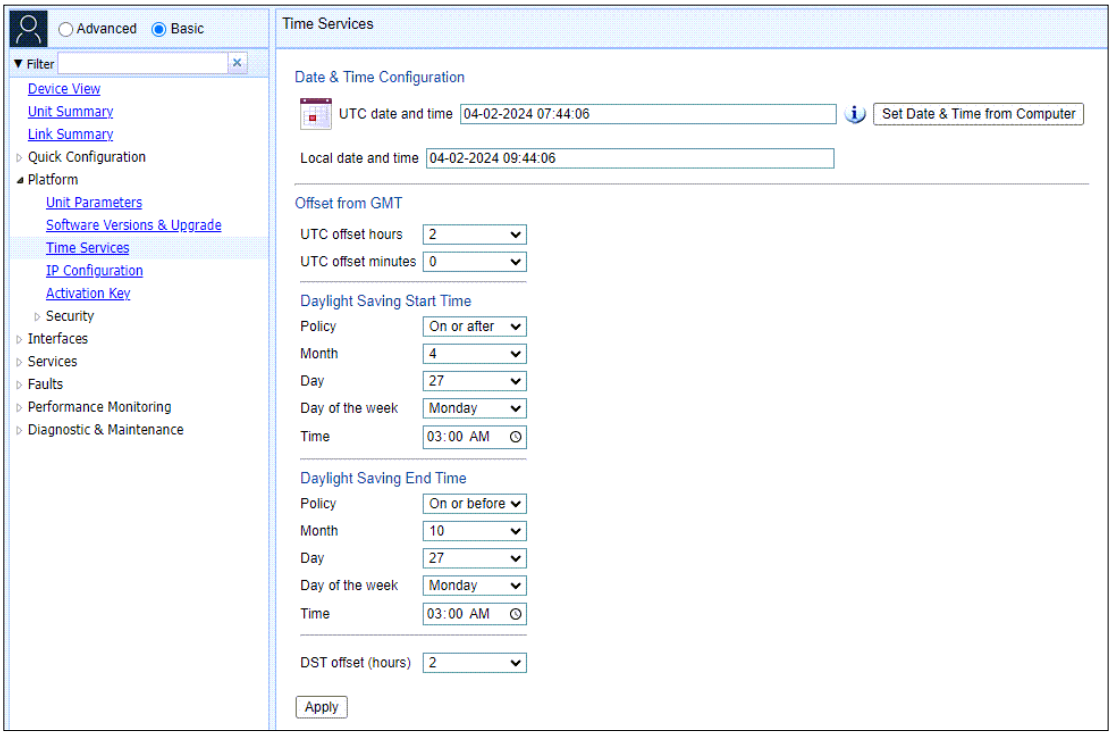


Figure 57: Basic Mode – Time Services Page

IP Configuration Page

In the IP Configuration page, you can configure the unit's IP address and related parameters. You can also enable or disable in-band management.

Note: For PTP 850E devices running System release 12.7 and higher, in-band management is automatically enabled, and the **In-Band Admin** field is not available. This does not prevent the use of local management.

For an explanation of IP configuration, see *Changing the Management IP Address*. For an explanation of in-band management, see *Configuring In-Band Management*.

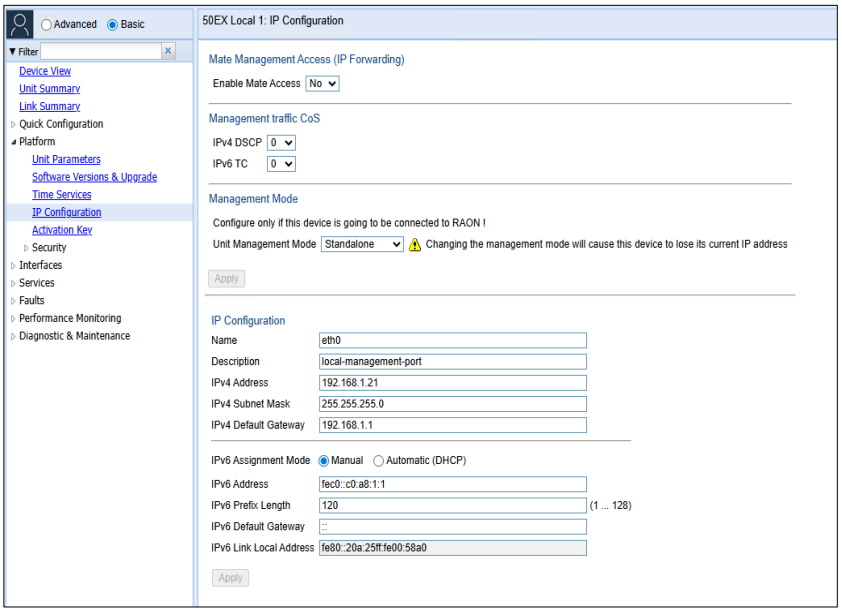


Figure 58: Basic Mode – IP Configuration Page

Activation Key Page

In the Activation Key page, you can configure the unit's activation key. You can also display the status of activation key coverage for features and capacities in the unit.

To display the status of activation key coverage, select **Show Activation Key Overview**. The status details appear at the bottom of the page.

For an explanation of activation key management, see *Configuring the Activation Key*.

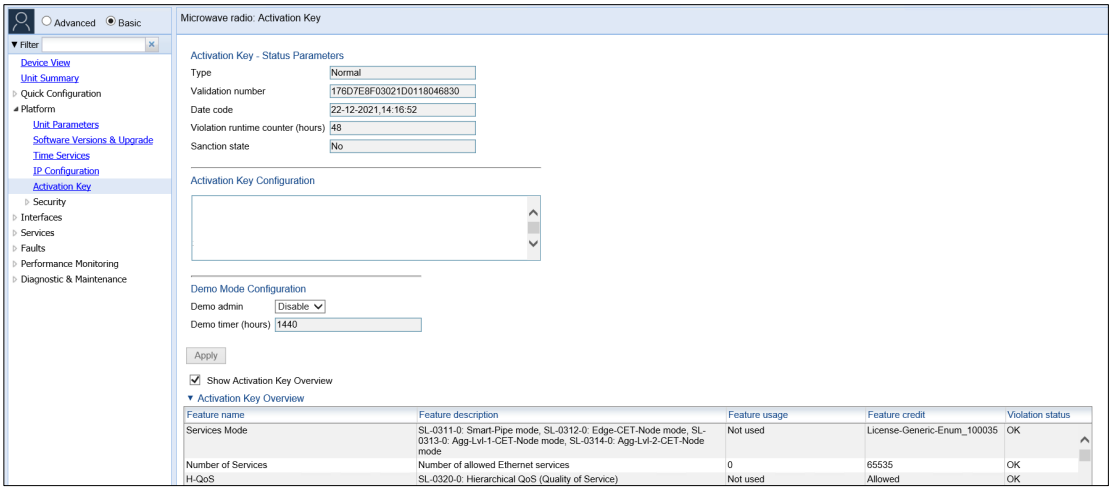


Figure 59: Basic Mode – Activation Key Page

Security Pages

From the Security menu, you can access pages that enable you to configure the unit, including:

- *General Parameters Page* – Enable and disable import and export of security settings, configure the session timeout, and configure a login banner.
- *Protocols Page* – Configure the HTTP type, Telnet blocking, and SNMP parameters.
- *Access Control Page* – Configure users and login settings.

General Parameters Page

In the Security General Parameters page, you can enable and disable import and export of security settings, configure the session timeout, and configure a login banner. For more details about these settings, see *Quick Security Configuration – General Parameters Page*.

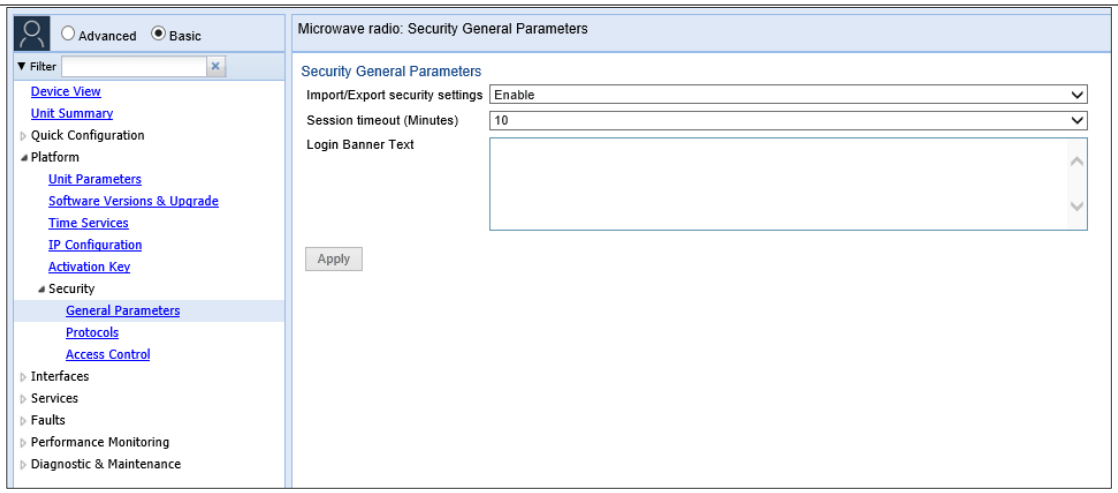


Figure 60: Basic Mode – Security – General Parameters Page

Protocols Page

In the Protocols page, you can configure the HTTP type, Telnet blocking, and SNMP parameters. For more details about these settings, see *Quick Security Configuration – Protocols Page*.

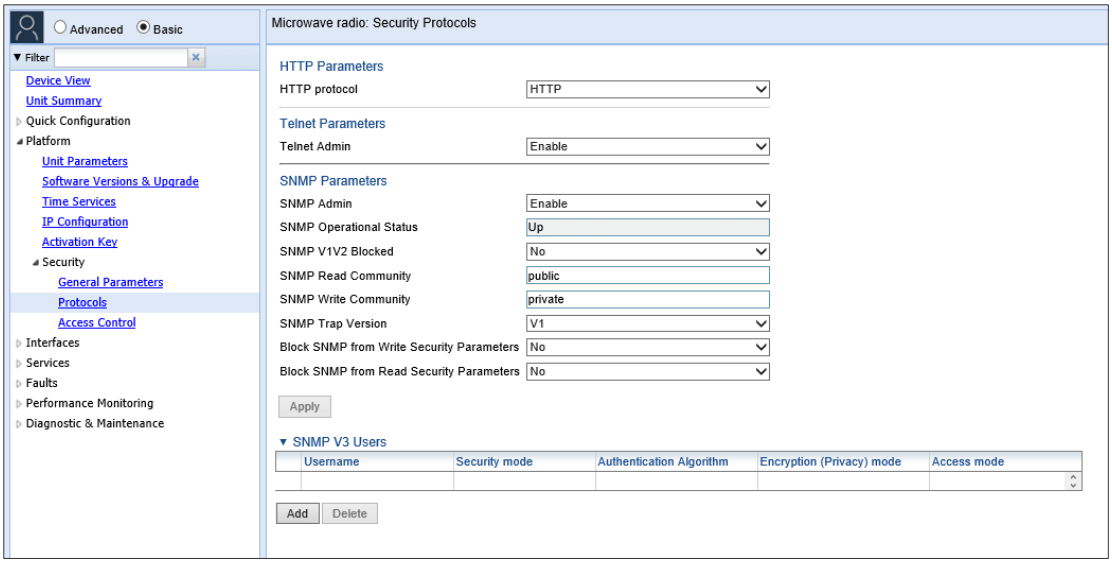


Figure 61: Basic Mode – Security – Protocols Page

Access Control Page

In the Security Access Control page, you can configure users and login parameters.For more information about password and user settings, see *Configuring Users*.



Figure 62: Basic Mode – Security – Security Access Control Page

To configure user profiles, click **Access Control User Profiles**. The Access Control User Profiles page opens. For details, see *Configuring User Profiles*.

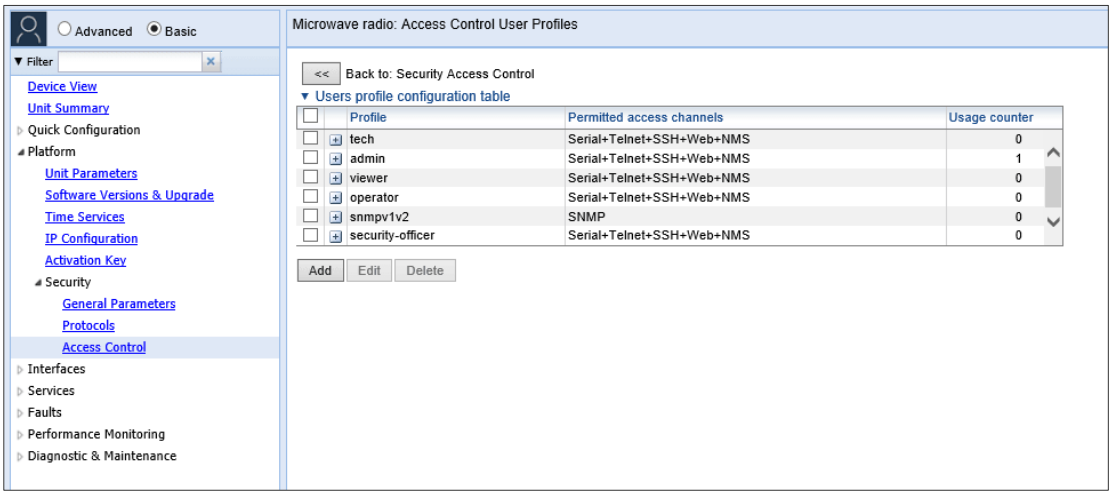


Figure 63: Basic Mode – Security – Access Control User Profiles Page

Interfaces

From the Interfaces menu, you can select **Interface Manager** to display the Interface Manager page.

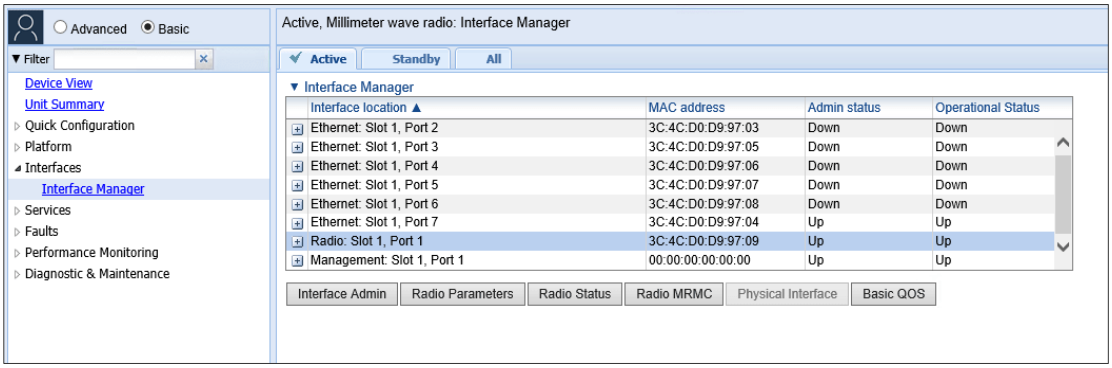


Figure 64: Basic Mode – Interface Manager Page (PTP 850E)

From the Interface Manager page,you can perform the following interface configurations:

1 Enable and disable interfaces – select the interface and click **Interface Admin**. See *Enabling the Interfaces (Interface Manager)*.

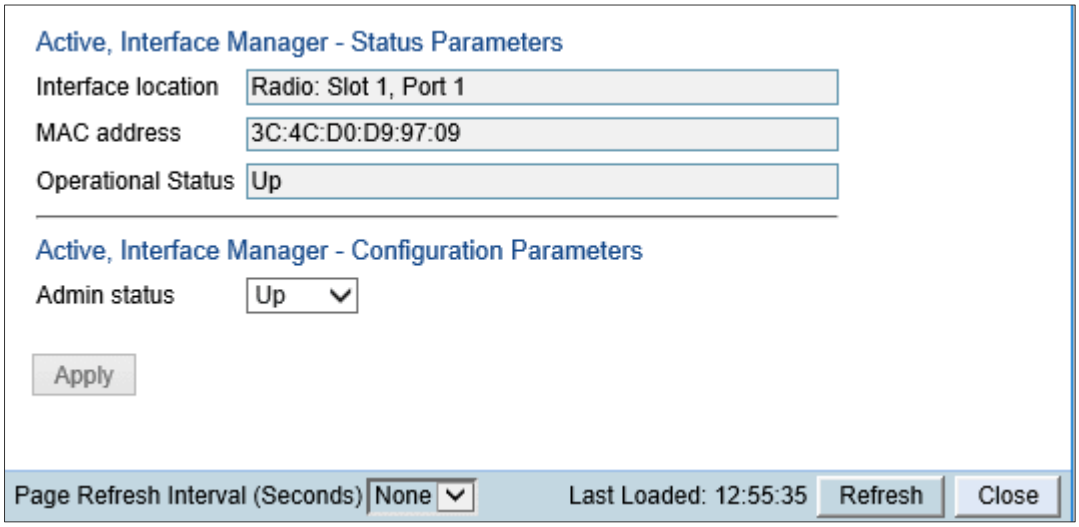


Figure 65: Basic Mode – Interface Manager Page – Interface Admin

2 Configure the radio parameters of a radio interace – select the interface and click **Radio Parameters**. See *Configuring the Radio Parameters*.

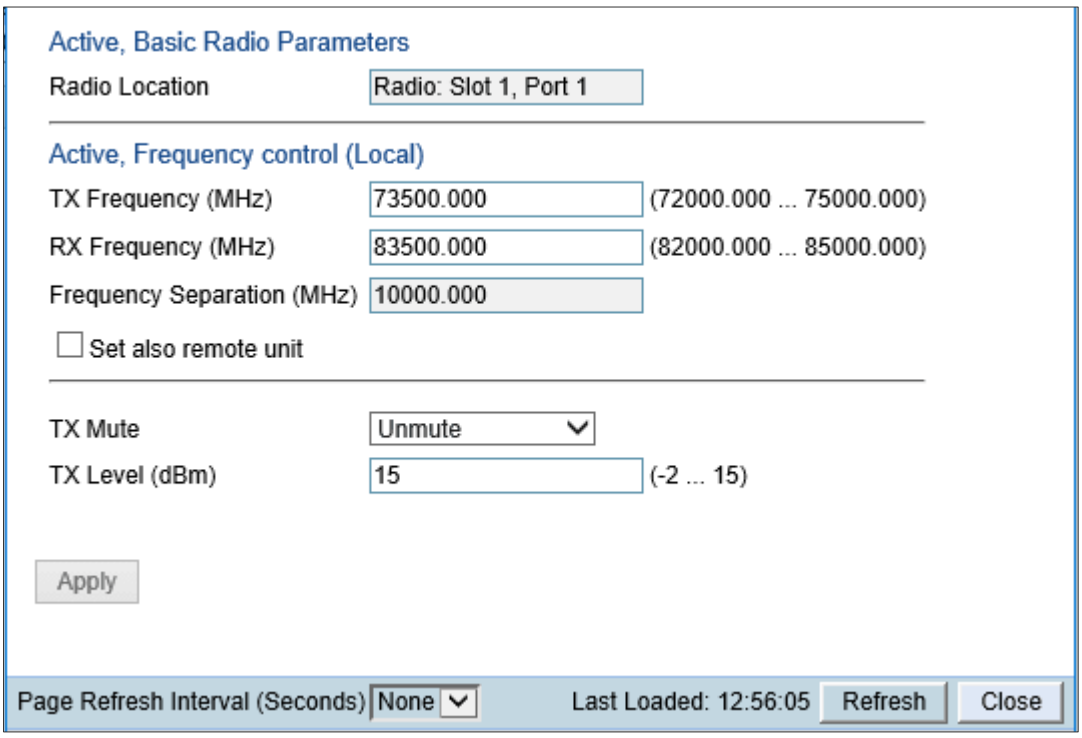


Figure 66: Basic Mode – Interface Manager Page – Radio Parameters (PTP 850E)

3 Configure the MRMC script of a radio interace – select the interface and click **Radio MRMC**. See *Configuring the Radio (MRMC) Script(s)*.

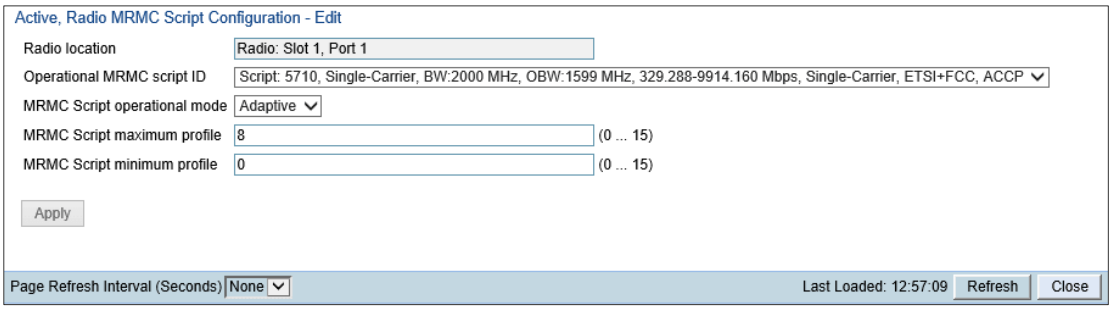


Figure 67: Basic Mode – Interface Manager Page – Radio MRMC (PTP 850E)

4 Display status parameters of a radio interace – select the interface and click **Radio Status**. See *Viewing the Radio Status and Settings*.

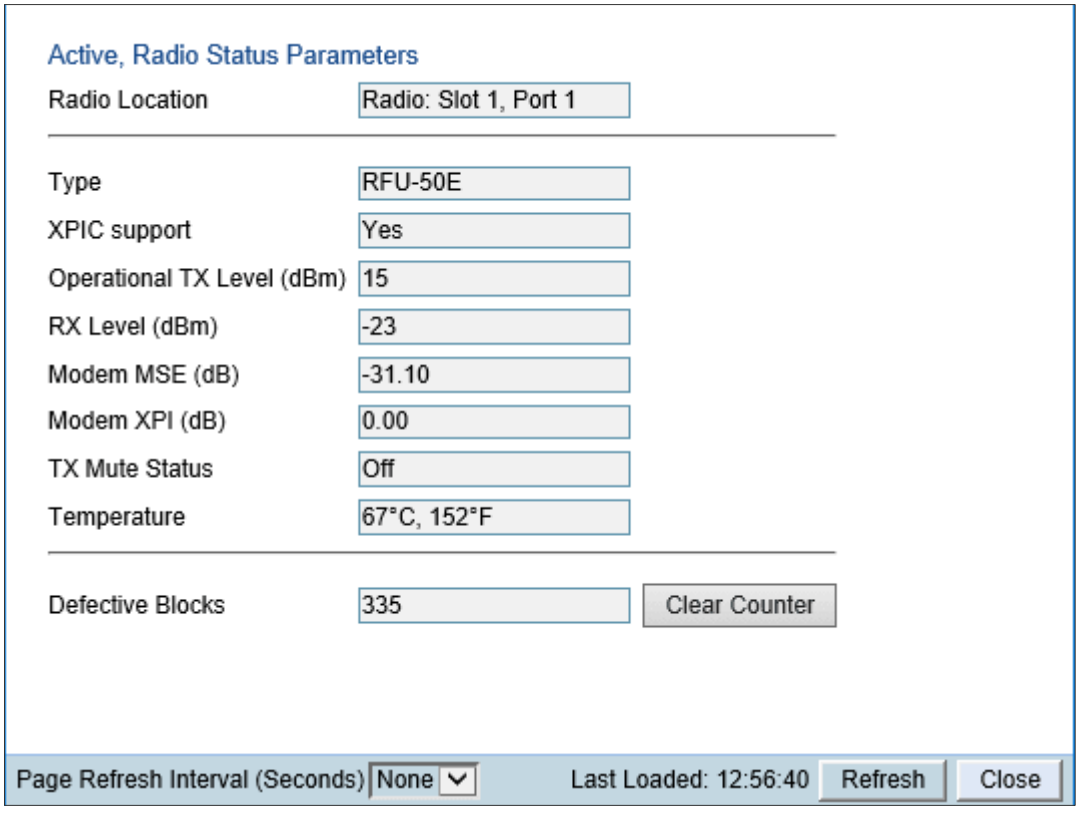


Figure 68: Basic Mode – Interface Manager Page – Radio Status (PTP 850E)

5 Configure the physical parameters of an Ethernet interace or the Management interface – select the interface and click **Physical Interface**. See *Configuring Ethernet Interfaces*.

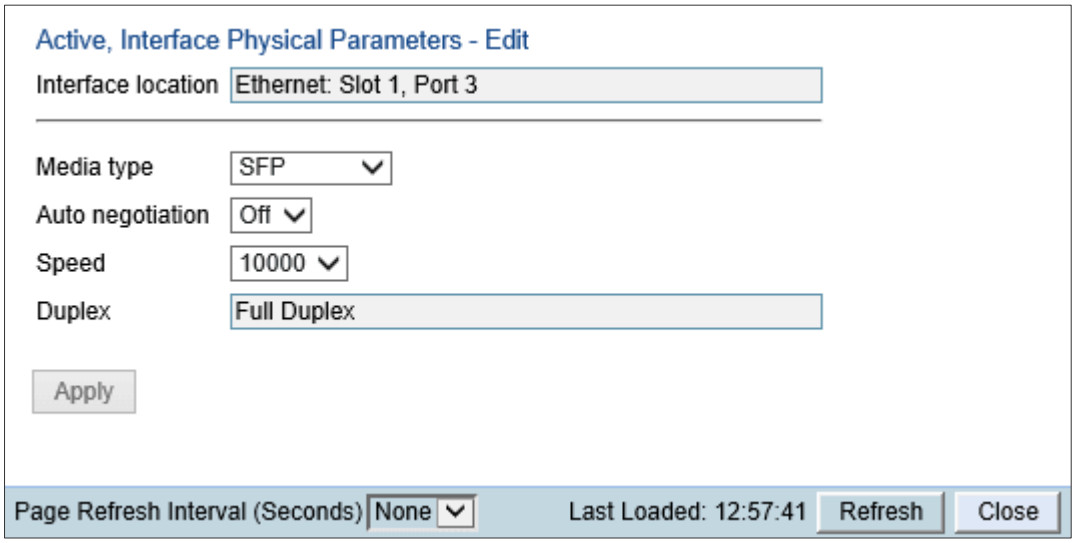


Figure 69: Basic Mode – Interface Manager Page – Physical Interface

6 Configure the basic ingress classification parameters of an interace – select the interface and click **Basic QoS**. See *Configuring Ingress Path Classification on a Logical Interface*.

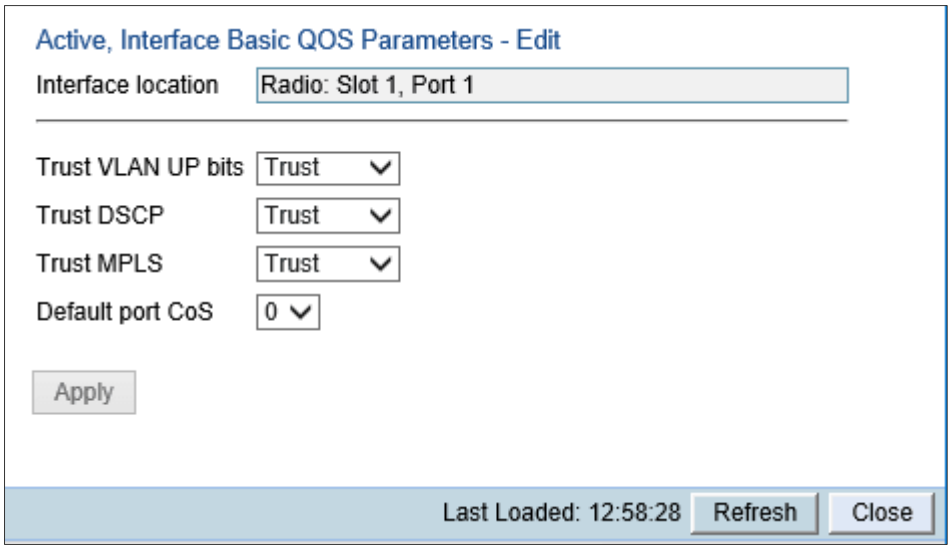


Figure 70: Basic Mode – Interface Manager Page – Basic QoS

Services

The Services menu enables you to create Ethernet services.

To configure Ethernet services, click **Ethernet Services**. For information about configuring Ethernet services, see *Configuring Ethernet Service(s)*.

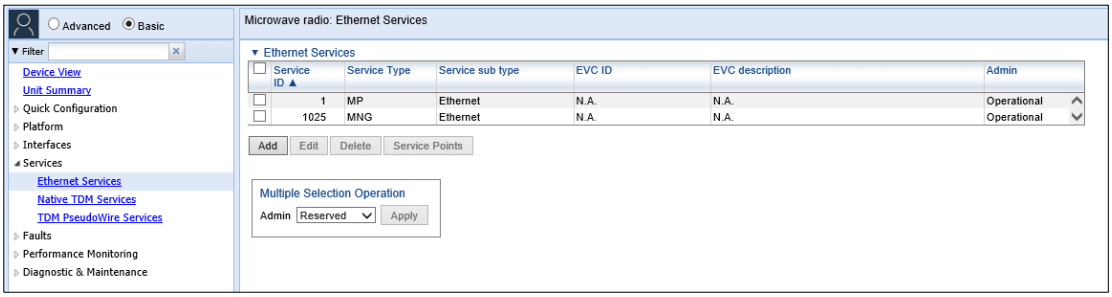


Figure 71: Basic Mode – Ethernet Services

Faults

The Faults menu includes options to display current alarms and the event log.

To display current alarms, click **Current Alarms**. For information about alarms, see *Viewing Current Alarms*.



Figure 72: Basic Mode – Current Alarms

To display the event log, click **Event Log**. For information about the event log, see *Viewing and Saving the Event Log*.

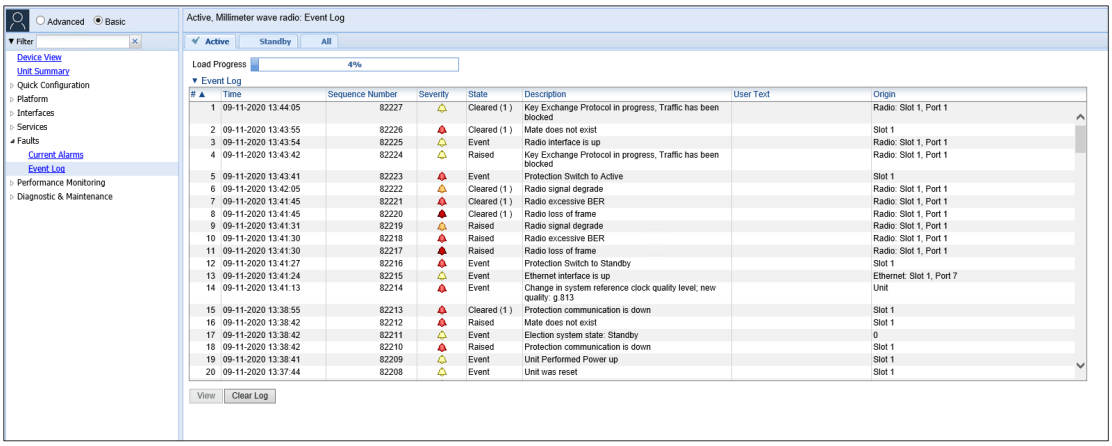


Figure 73: Basic Mode – Event Log

Performance Monitoring

From the Performance Monitoring menu, you can access pages that display important information about link performance, including:

- RMON
- Signal Level
- MSE
- MRMC
- Capacity/Throughput
- Utilization

Note: Link Bonding PMs are only available in Advanced mode.

RMON

To display RMON statistics, click **RMON**. For further information, see *Viewing Ethernet PMs and Statistics*.

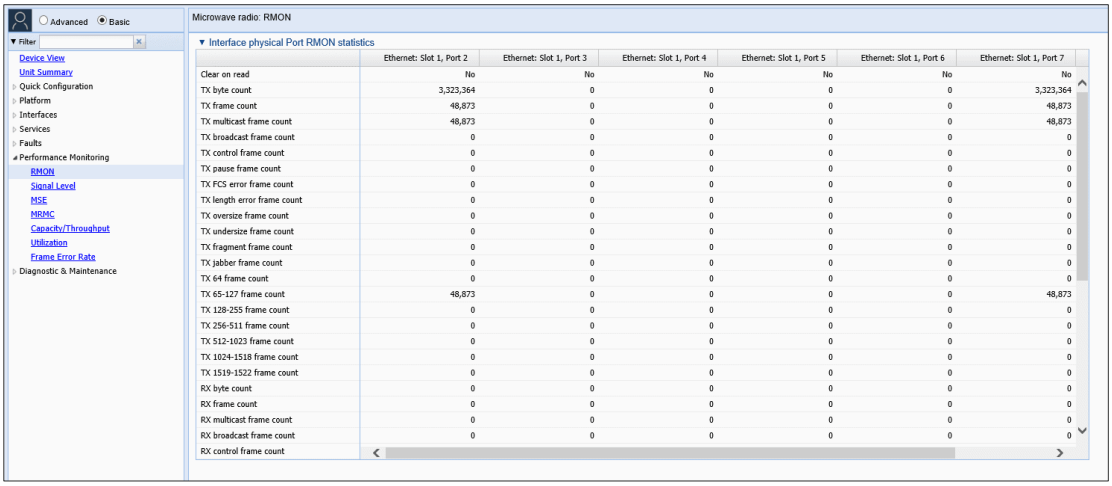


Figure 74: Basic Mode – RMON Page (PTP 850E)

Signal Level

To display Signal Level PMs and define Signal Level PM thresholds, click **Signal Level**. For further information, see *Displaying Signal Level PMs and Configuring Signal Level PM Thresholds*.

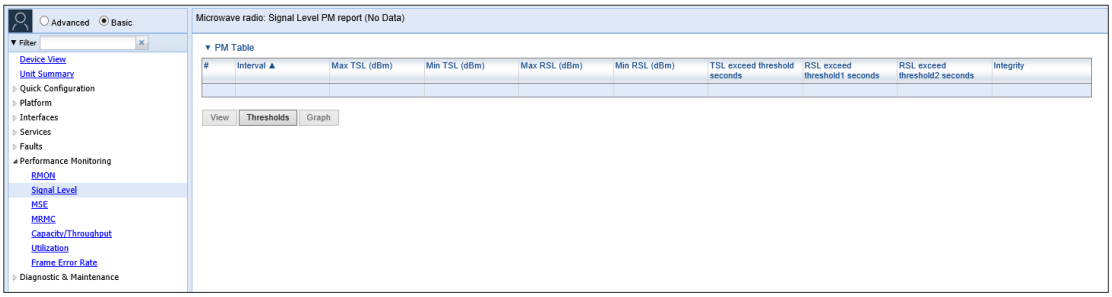


Figure 75: Basic Mode – Signal Level Page

MSE

To display MSE PMs and define MSE PM thresholds, click **MSE**. For further information, see *Displaying MSE PMs and Configuring MSE PM Thresholds*.

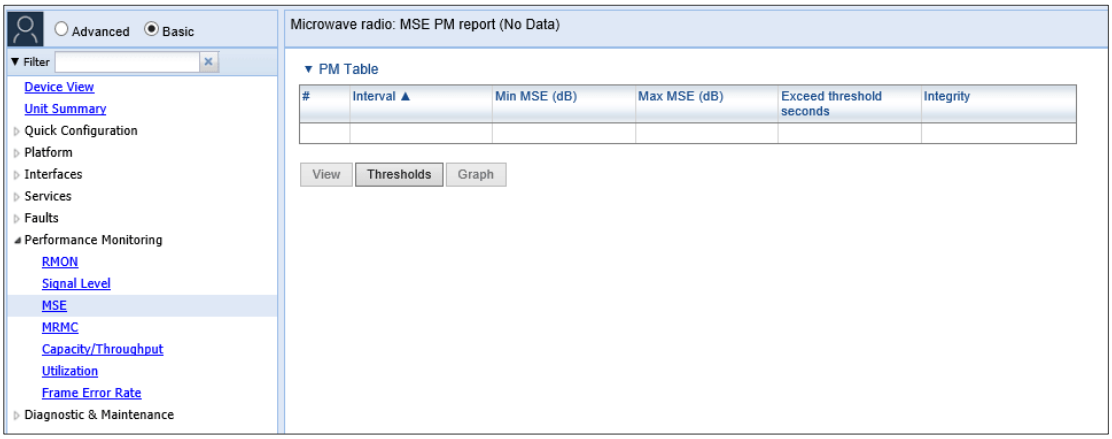


Figure 76: Basic Mode – MSE Page

MRMC

You can display the minimum and maximum ACM profile and the minimum and maximum bitrate (throughput) per 15-minute or daily intervals. You can also define two ACM profile thresholds for each radio carrier, and display the number of seconds per interval that the radio's ACM profile was below each of these thresholds.

To display ACM profile PMs and define ACM profile thresholds, click **MRMC**. For further information, see *Displaying MRMC PMs and Configuring ACM Profile ThresholdsDisplaying Capacity and Throughput PMs*.

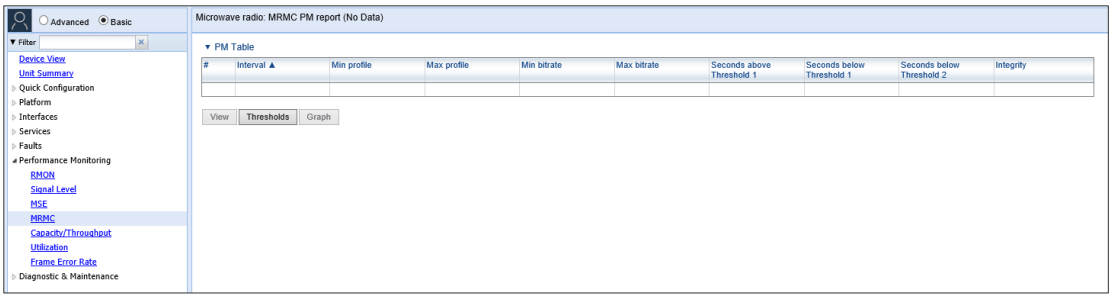


Figure 77: Basic Mode – MRMC Page

Capacity/Throughput

To display capacity and throughput PMs and define capacity and throughput thresholds, click **Capacity/Throughput**. For further information, see *Displaying Capacity and Throughput PMs*.

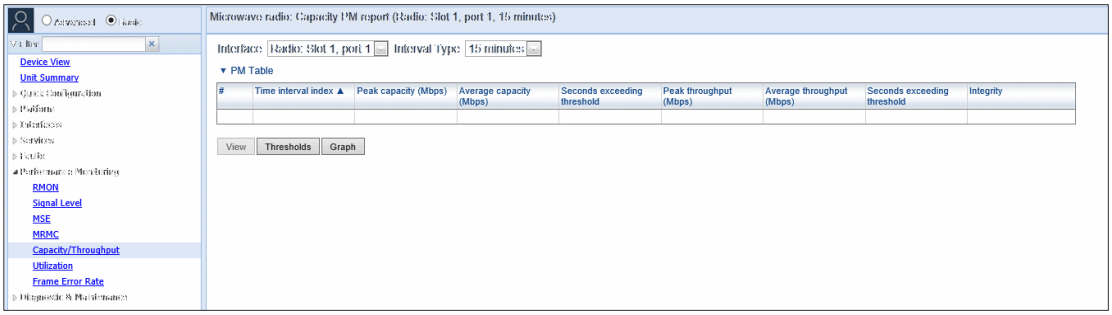


Figure 78: Basic Mode – Capacity/Throughput Page

Utilization

To display utilization PMs and define utilization thresholds, click **Utilization**. For further information, see *Displaying Utilization PMs and Configuring Utilization Thresholds*.

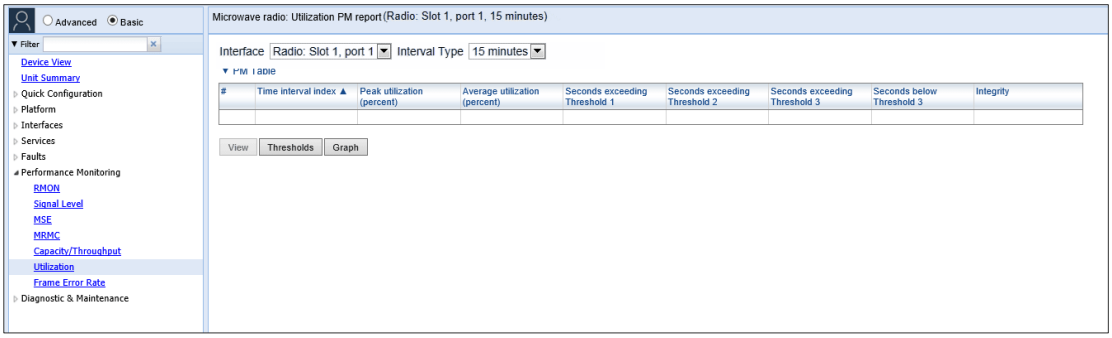


Figure 79: Basic Mode – Utilization Page

Frame Error Rate

To display Frame Error Rate PMs, click **Frame Error Rate**. For further information, see *Displaying Frame Error Rate PMs*.

Note: These PMs are not available for PTP 850C and PTP 850E.

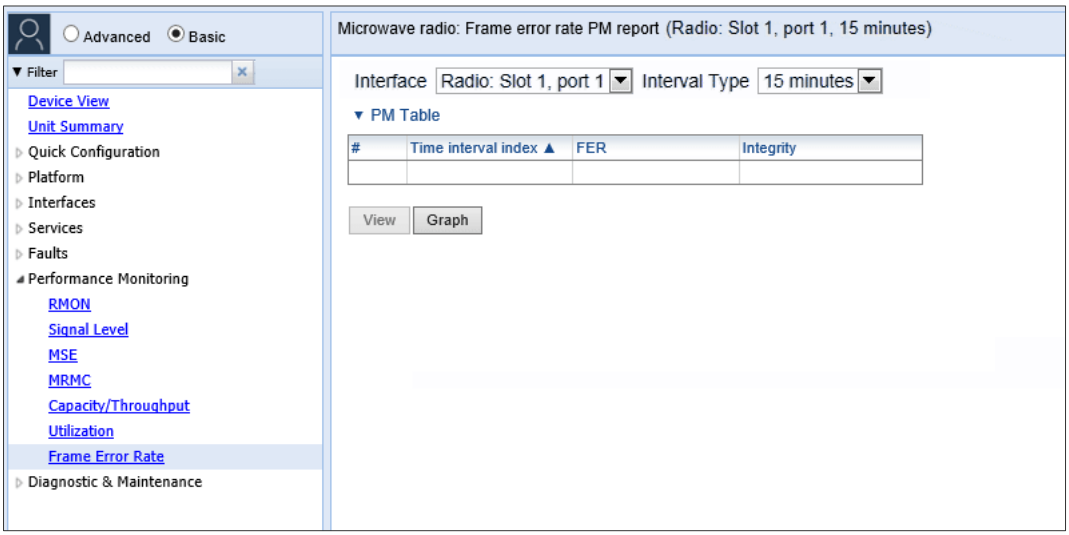


Figure 80: Basic Mode – Frame Error Rate Page

Diagnostic & Maintenance

From the Diagnostic & Maintenance menu, you can access pages that enable you to perform diagnostics, troubleshooting, and configuration management, including:

- *Radio Loopback* – Perform radio loopback
- *Unit Info* – Generate and export a user info file, used primarily for troubleshooting.
- *Configuration Management* – Import and export unit configuration files, used to backup and restore system configurations.

Radio Loopback

Note: To perform radio loopback, the radio must be set to its maximum TX power. For reliable loopback results, the loopback should performed with the modulation at 1024 QAM or lower.

To perform radio loopback, click **Radio Loopback**. For further information, see *Performing Radio Loopback*.

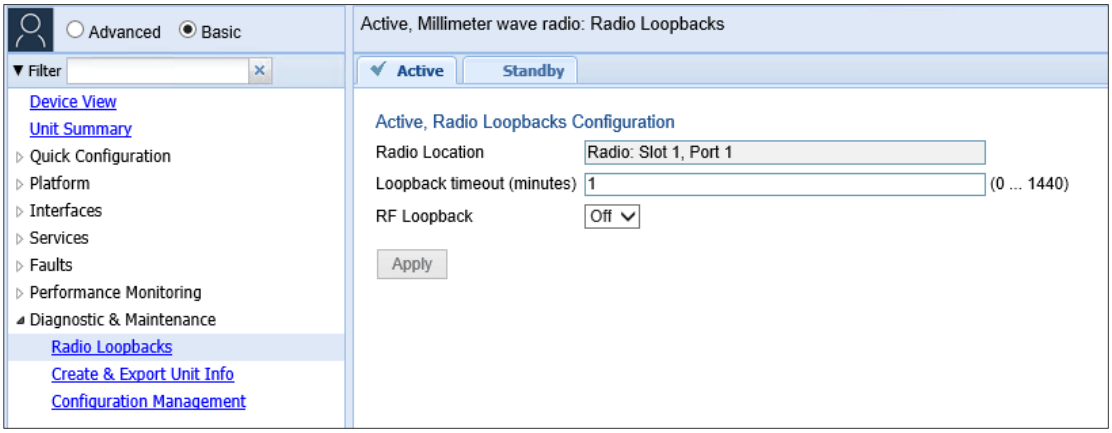


Figure 81: Basic Mode – Radio Loopbacks Page

Unit Info

You can generate a Unit Information file, which includes technical data about the unit. This file can be uploaded and forwarded to customer support, at their request, to help in analyzing issues that may occur.

You can upload the Unit Information file using HTTP, HTTPS, FTP, or SFTP.

> For troubleshooting, it is important that an updated configuration file
>
> be included in User Info files that are sent to customer support. To ensure that an up-to-date configuration file is included, it is recommended to back up the unit's configuration before

To generate a Unit Information file, click **Create & Export Unit Info**. For further information, see *Uploading Unit Info*.

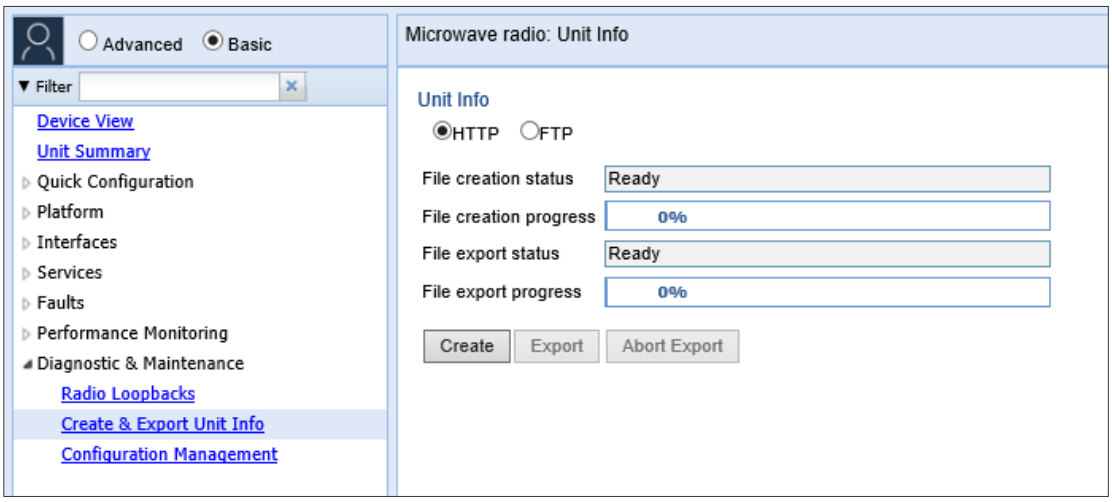


Figure 82: Basic Mode – Unit Info Page

Configuration Management

You can import and export PTP 820 configuration files. This enables you to copy the system configuration to multiple PTP 820 units. You can also backup and save configuration files. Importing and exporting configuration files can be done using HTTP, HTTPS, FTP, or SFTP.

Basic mode combines the actions required to perform configuration management into a single Web EMS page. To display this page, click **Configuration Management**. For further information, see *Backing Up and Restoring Configurations*.

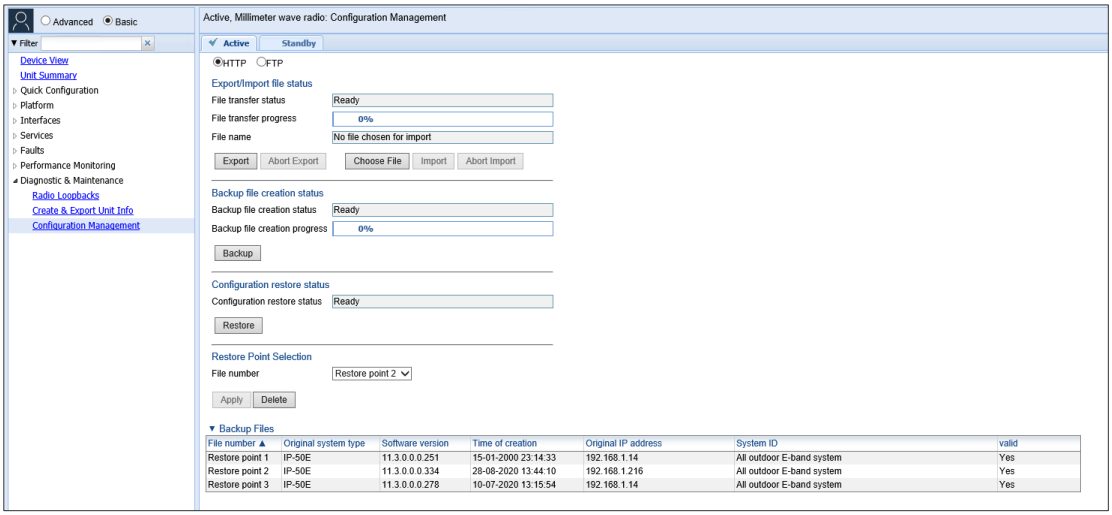


Figure 83: Basic Mode – Configuration Management Page

6. Configuring a Link Using the Quick Configuration Wizard

The Web EMS provides wizards to configure radio links. The wizards guide you through configuration of the basic radio parameters and services necessary to establish a working link. The following link types can be configured with the Quick Configuration wizard:

1+0 – Configures a 1+0 radio link consisting of a user-selected Ethernet (or LAG) and radio interface connected. This link passes traffic between the radio and Ethernet interfaces via a point-to-point service. This wizard can also be used to configure XPIC on the unit. For PTP 850E, XPIC must be configured individually on each PTP 850E unit in the XPIC pair.

Enhanced Multi-Carrier ABC – Configures a 2 + 0 Multi-Carrier ABC group consisting of an Ethernet interface or LAG and the two radio interfaces.

Layer 1 Link Bonding – Configures a link that combines an PTP 850C and either another PTP 850C or an PTP 820C or an PTP 820C-HP, sharing a single Ethernet interface. There are two wizards for this configuration:

Configure as Main (N + 0) – This is used to configure the PTP 850C that is acting as the main unit.

Configure as Attached – This is used to configure the PTP 850C, PTP 820C, or PTP 820C-HP that is acting as the paired (attached) unit. Although the Link Bonding group itself is configured on the main unit, certain configurations are also required on the paired unit to support the Link Bonding configuration. This wizard also enables you to configure the radio, MRMC, and XPIC (optional) parameters on the paired unit.

Multiband – Configures a link that bundles E-Band and microwave radios in a single group that is shared with an Ethernet interface. A Multiband link uses an PTP 850E and an PTP 820C, PTP 820C-HP, PTP 820S, PTP 820N, PTP 820A, or third-party microwave unit. The Multiband group is only configured on the PTP 850E unit. You can use the wizard to configure both the main and the paired units.

Multiband with Layer 1 Link Bonding – Configures a link that bundles an PTP 850E and an PTP 850C, PTP 820C, or PTP 820C-HP in a single group utilizing Layer 1 Link Bonding, and sharing a single Ethernet interface. Instead of a Multiband group, this type of link is based on a Layer 1 Link Bonding group. There are two wizards for this configuration:

Configure as Main (Multiband) – This is used to configure the PTP 850E

Configure as Attached – This is used to configure the PTP 850C, PTP 820C, or PTP 820C-HP that is paired with the PTP 850E. Although the Link Bonding group itself is configured on the PTP 850E, certain configurations are also required on the paired unit to support the Link Bonding configuration. This wizard also enables you to configure the radio, MRMC, and XPIC (optional) parameters on the paired unit.

Note: Multiband configurations with Link Bonding that use PTP 850E with a third-party device should not be configured with the Quick Configuration Wizard, but rather, through the main Link Bonding page.

You cannot add an interface to a link using the Quick Configuration wizard if any service points are attached to the interface prior to configuring the link.

Note: For all configurations, it is recommended that the MRMC script configurations be symmetric on both sides of the link, including the same script and minimum and maximum ACM profiles.

With respect to the management interface of an PTP 850E, if this interface is used for traffic you will be able to select it in the Quick Configuration wizards, but only if the management service point attached to the interface is tagged. If it is untagged, the management port will not be visible in these wizards, and link configurations using this port will have to be configured manually.

6.1.1 Configuring a 1+0 Link Using the Quick Configuration Wizard

Note: For PTP 850C, 1+0 can be configured with either Horizontal polarization (radio carrier 1) or Vertical Polarization (radio carrier 2).

To configure a 1+0 link using the Quick Configuration wizard:

1. Select **Quick Configuration** > **PIPE** > **Single Carrier** > **1+0**. Page 1 of the 1+0 Quick Configuration wizard opens.

Figure 72 1+0 Quick Configuration Wizard – Ethernet Selection (PTP 850C)

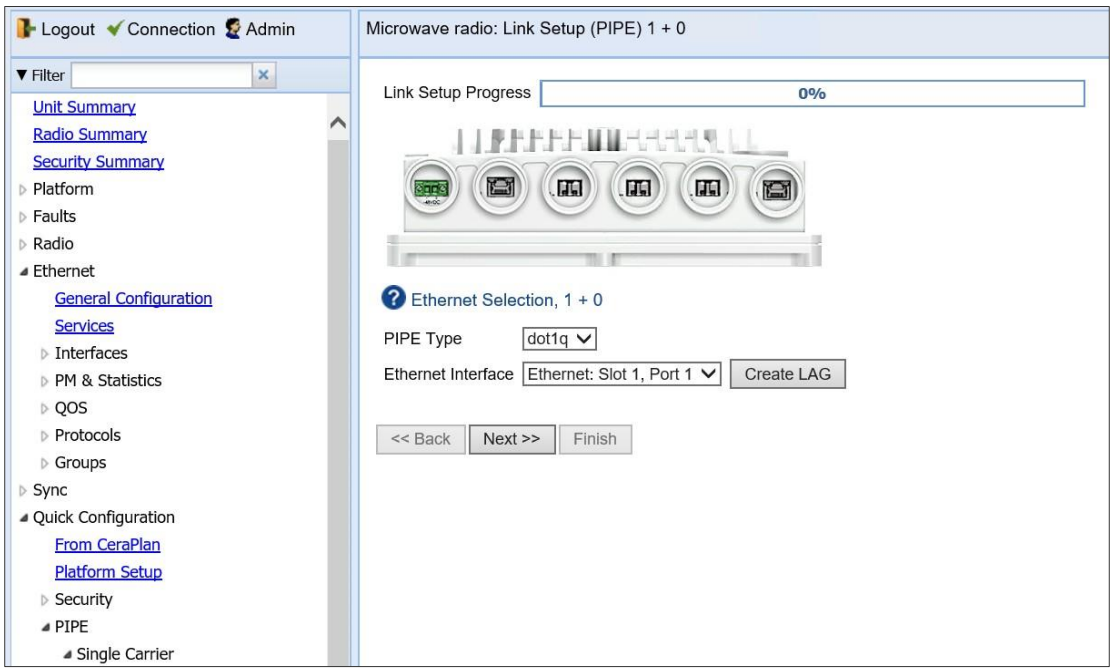


Figure 73 1+0 Quick Configuration Wizard – Ethernet Selection (PTP 850C)

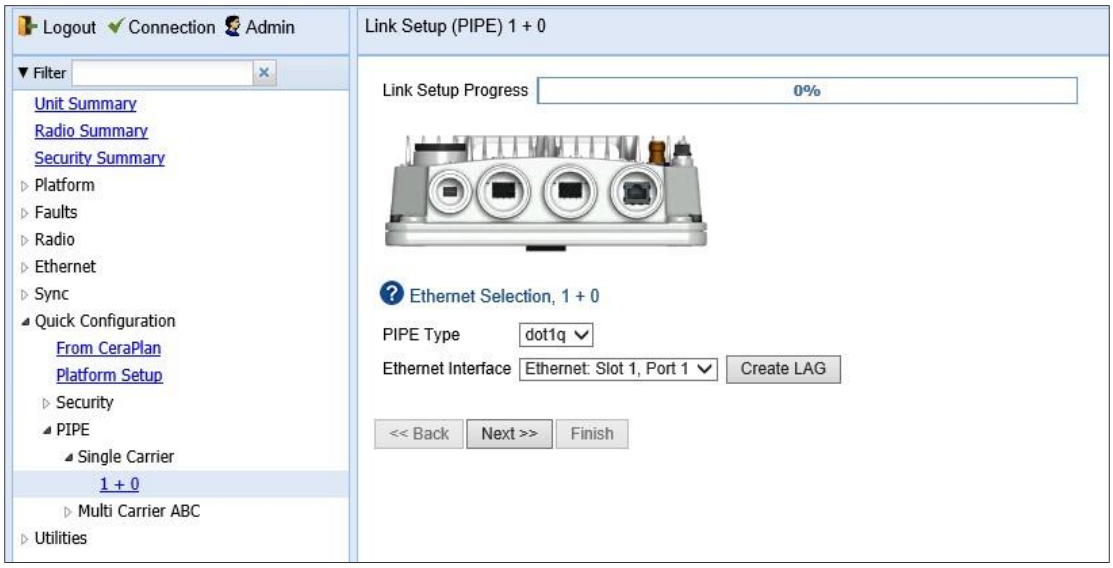
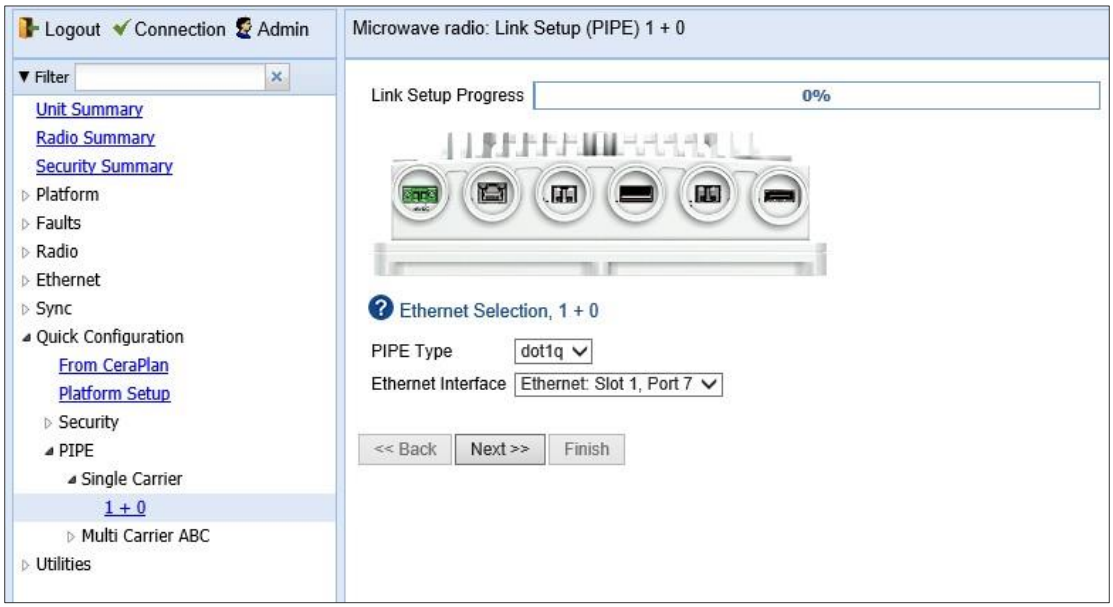


Figure 74 1+0 Quick Configuration Wizard – Ethernet Selection (PTP 850E)



2. In the **PIPE Type** field, select the Attached Interface type for the service that will connect the radio and Ethernet interfaces. Options are:

   dot1q – All C-VLANs and untagged frames are classified into the service.

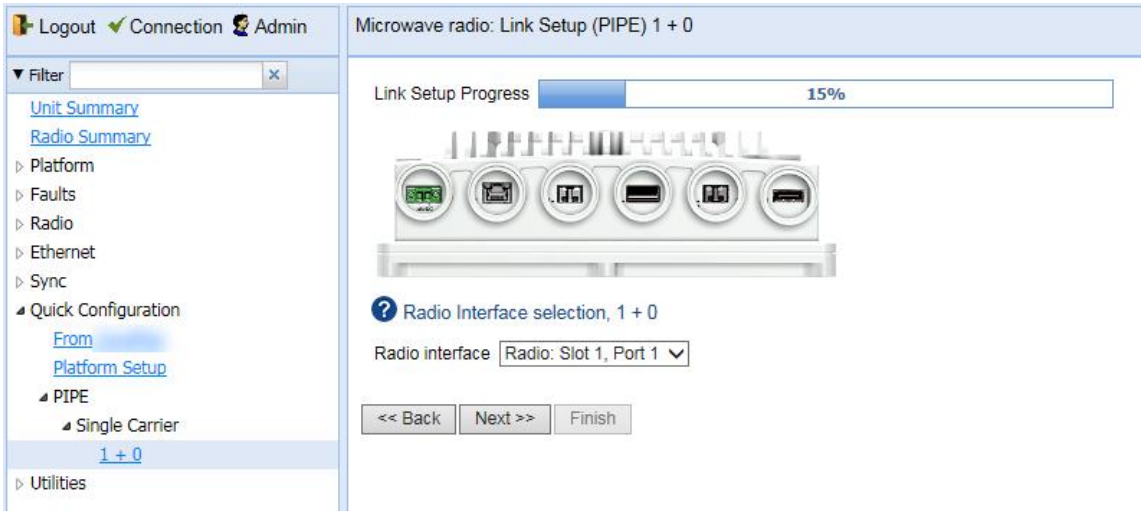
   s-tag – All S-VLANs and untagged frames are classified into the service.

Note

For a full explanation of Ethernet Services, service types, and attached interface types.

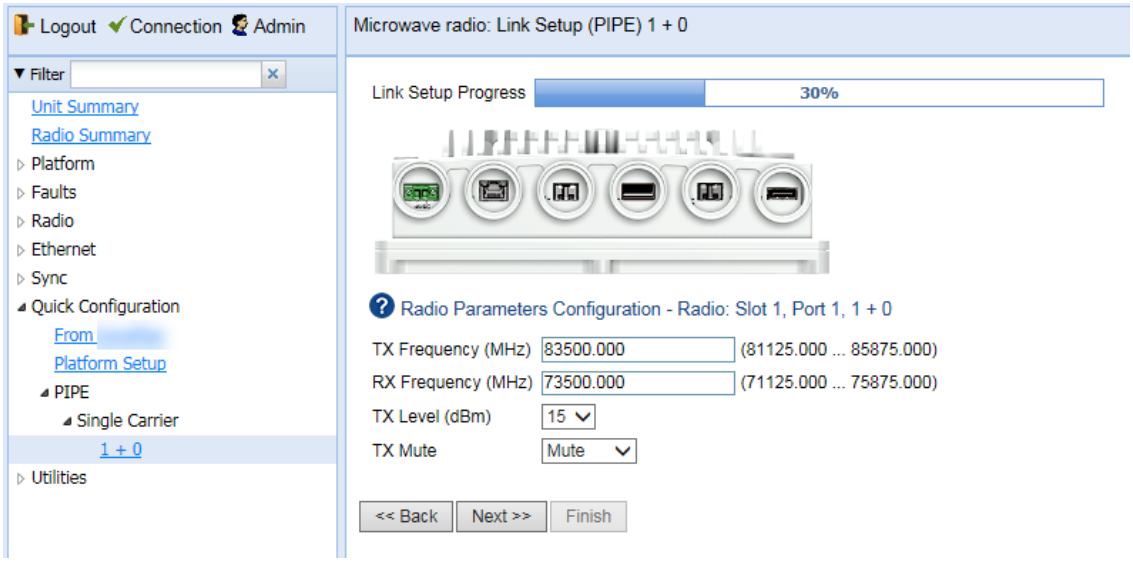
3. In the **Ethernet Interface** field, select an Ethernet interface for the link.
4. Click **Next**. Page 2 of the 1+0 Quick Configuration wizard opens.

Figure 75 1+0 Quick Configuration Wizard – Page 2



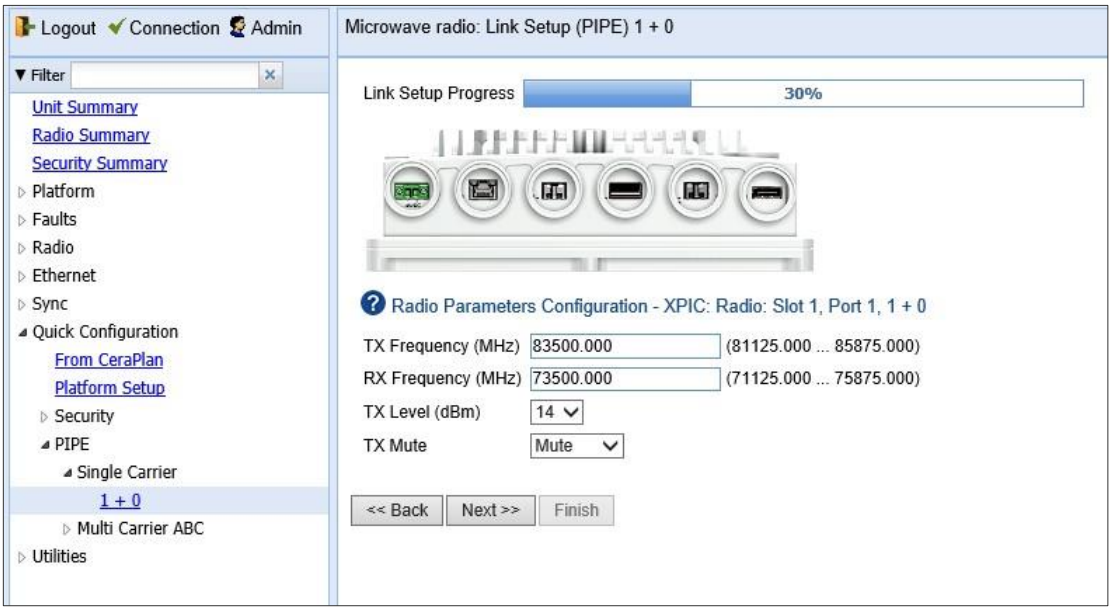
5. In the **Radio Interface** field, select **Radio: Slot 1, Port 1**.
6. Click **Next**. Page 3 of the 1+0 Quick Configuration wizard opens.

Figure 76 1+0 Quick Configuration Wizard – Page 3



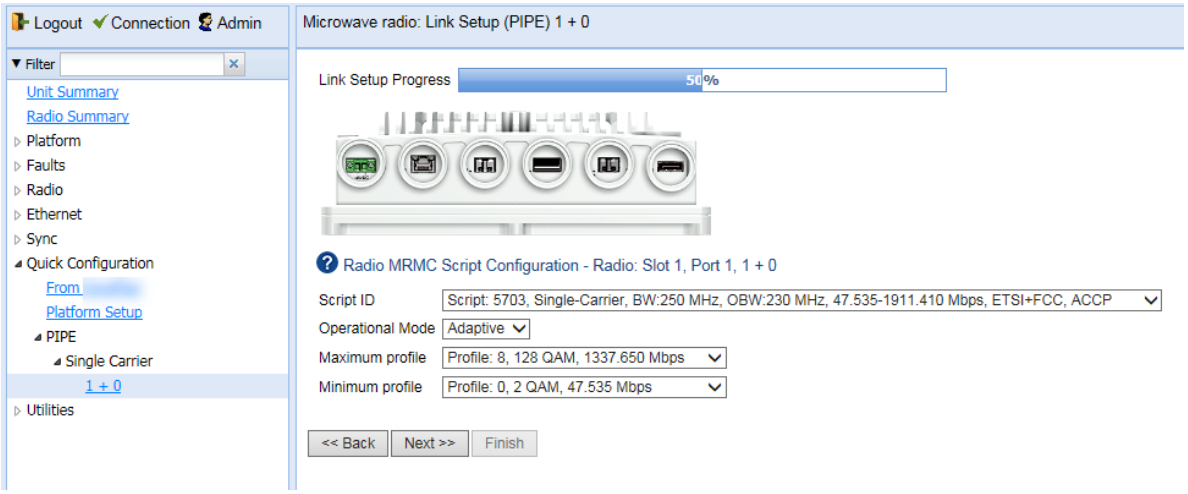
7. If the unit is part of an XPIC link, select XPIC.
8. If you select XPIC, the Member Role field is displayed. In the Member Role field, select Horizontal or Vertical. Make sure the Member Role you select matches the actual polarization of the PTP 850E unit, and that the Member Role you configure in the paired unit is not the same as the role you configure here. For full instructions on configuring an XPIC link, including alignment instructions, see Configuring XPIC.
9. Click Next. Page 4 of the 1+0 Quick Configuration wizard opens.`

Figure 77 1+0 Quick Configuration Wizard – Page 4



10. In the **TX Frequency (MHz)** field, set the transmission radio frequency in MHz.
11. In the **RX Frequency (MHz)** field, set the received radio frequency in MHz.
12. In the **TX Level (dBm)** field, enter the desired TX signal level (TSL). The range of values depends on the frequency and RFU type.
13. To mute the TX output of the radio, select **Mute** in the **TX mute** field. To unmute the TX output of the radio, select **Unmute**.
14. Click **Next**. Page 5 of the 1+0 Quick Configuration wizard opens.

Figure 78 1+0 Quick Configuration Wizard – Page 5



15. In the **Script ID** field, select the MRMC script you want to assign to the radio. For a full explanation of choosing an MRMC script.
    1 In the **Operational Mode** field, select the ACM mode: **Adaptive** or **Fixed**.
        - In Adaptive ACM mode, TX and RX rates are dynamic. An ACM-enabled radio system automatically chooses which profile to use according to the channel fading conditions.
        - Fixed ACM mode applies constant TX and RX rates. However, unlike regular scripts, with a Fixed ACM script you can specify a maximum profile to inhibit inefficient transmission levels.
    2 Do one of the following:

- If you selected **Adaptive** in the **Operational Mode** field, the following two fields are displayed:
- **Maximum profile** – Enter the maximum profile for the script.
- **Minimum profile** – Enter the minimum profile for the script.

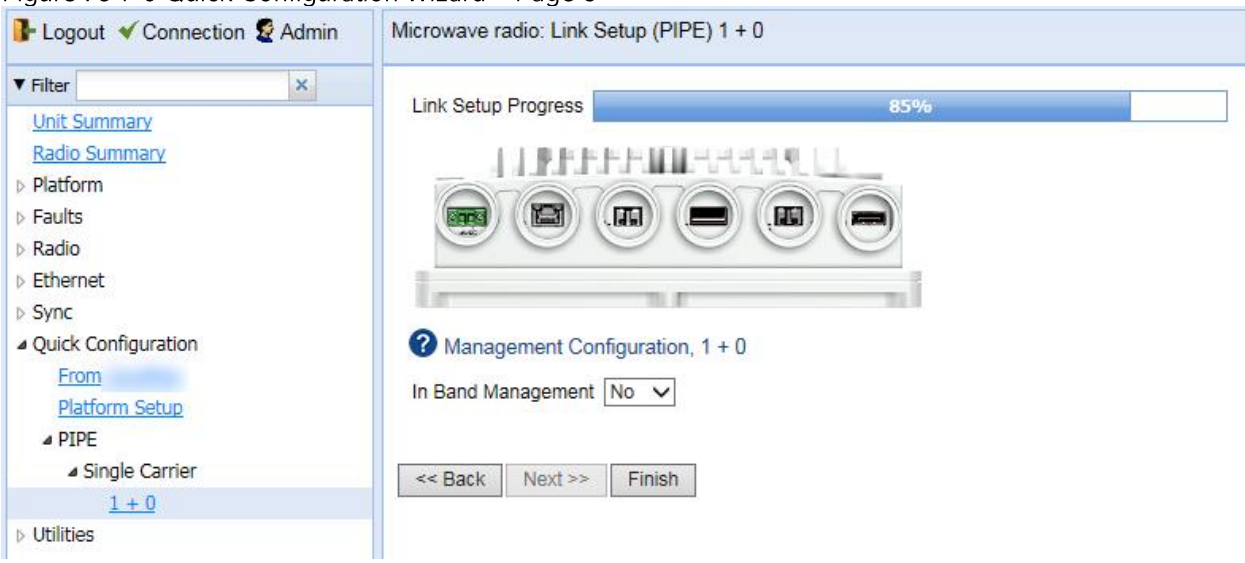
Note

The default minimum profile is 2.

- If you selected **Fixed** in the **Operational Mode** field, the next field is **Profile**. Select the ACM profile for the radio in the **Profile** field.

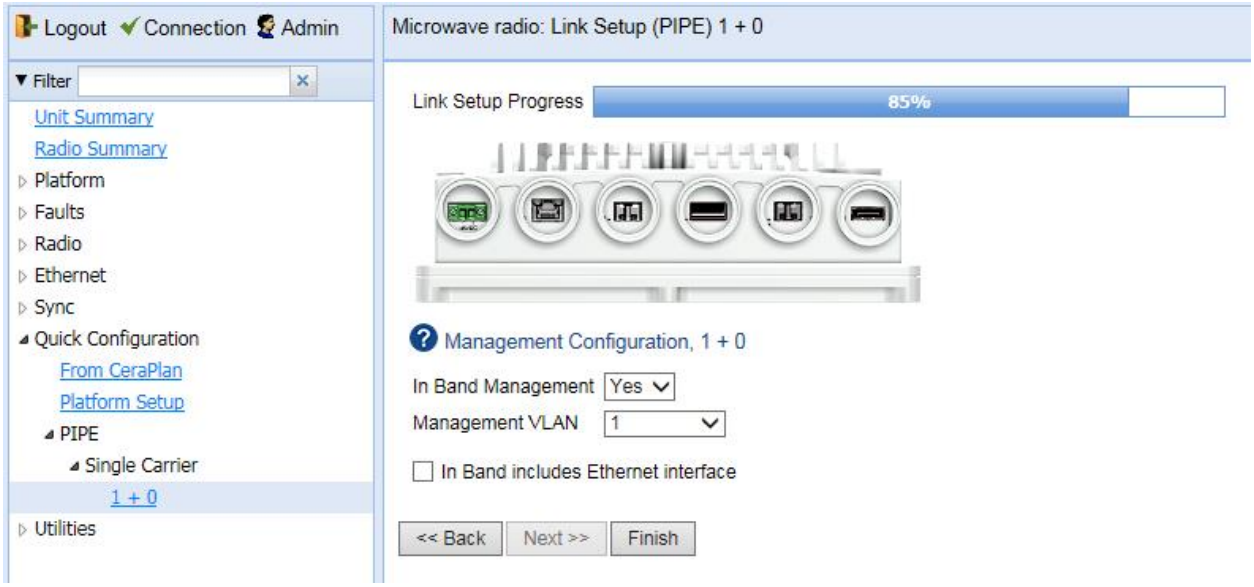
3 Click **Next**. Page 5 of the 1+0 Quick Configuration wizard opens.

Figure 79 1+0 Quick Configuration Wizard – Page 6



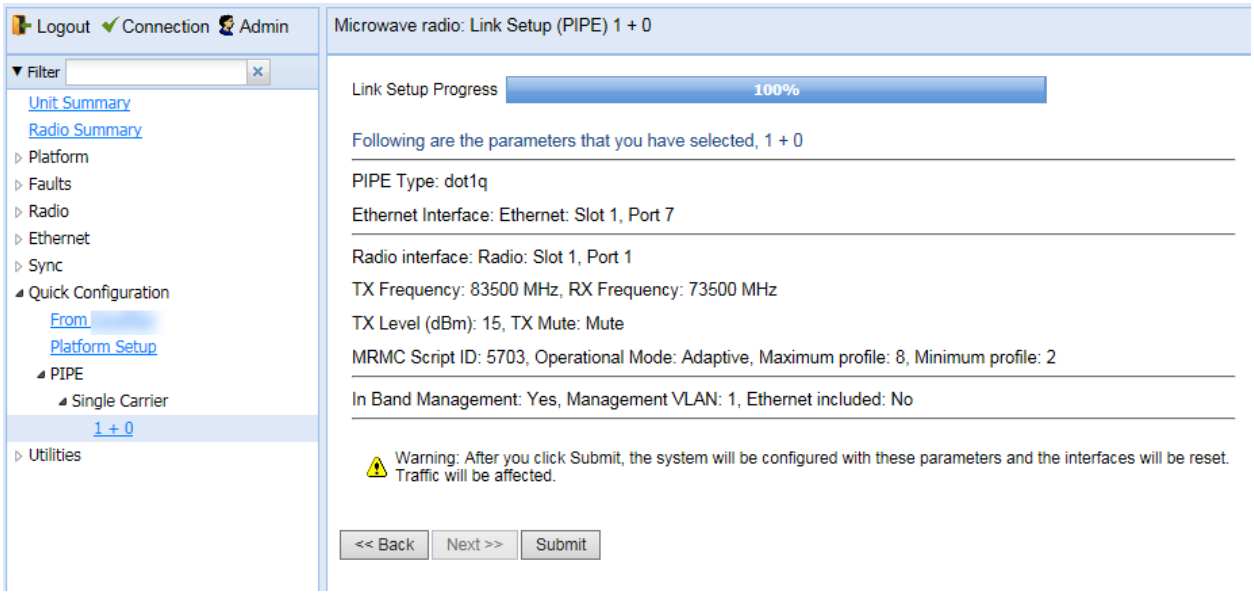
4 In the **In Band Management** field, select **Yes** to configure in-band management, or **No** if you do not need in-band management. If you select **Yes**, the **Management VLAN** field appears.

Figure 80 1+0 Quick Configuration Wizard – Page 5 (In Band Management = Yes)



5 If you selected **Yes** in the **In Band Management** field, select the management VLAN in the **Management VLAN** field.
6 If you want to use the Ethernet interface as well as the radio interface for in-band management, select **In Band includes Ethernet interface**.
7 Click **Finish**. Page 6 of the 1+0 Quick Configuration wizard opens. This page displays the parameters you have selected for the link.

Figure 81 1+0 Quick Configuration Wizard – Page 7 (Summary Page)



8 To complete configuration of the link, click **Submit**. If you want to go back and change any of the parameters, click **Back**. After you click **Submit**, the unit is reset.

6.1.2 Configuring a 2+0 Multi-Carrier ABC Link Using the Quick Configuration Wizard

Note: This section is only relevant for PTP 850C.

For important general information about Multi-Carrier ABC.

To configure a Multi-Carrier ABC group using the Quick Configuration wizard:

1 Select **Quick Configuration** > **PIPE** > **Multi Carrier ABC** > **2+0**. Page 1 of the 2 + 0 Multi Carrier ABC Quick Configuration wizard opens.

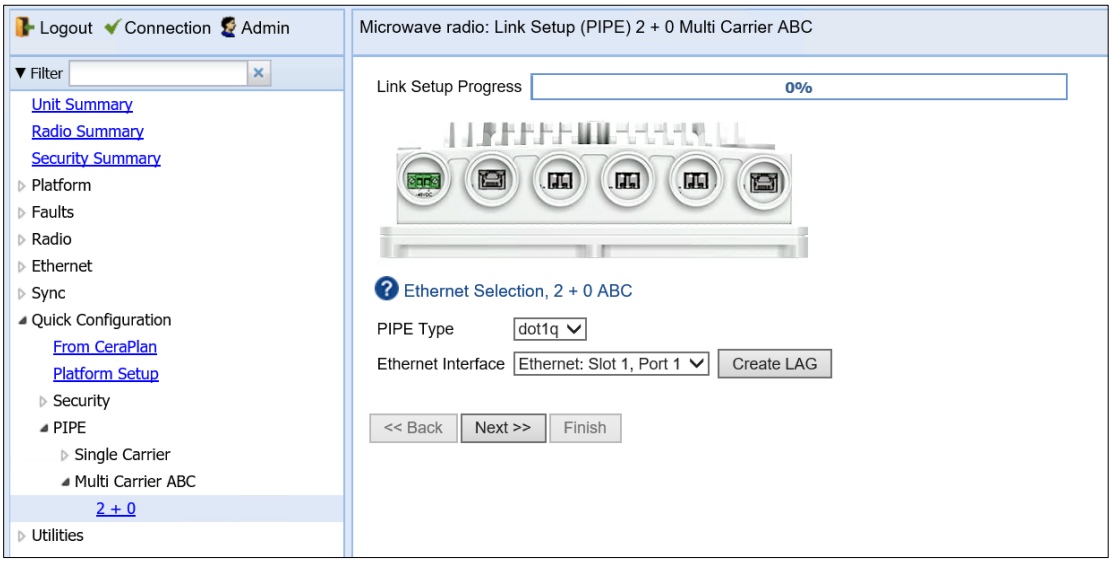


Figure 82: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Ethernet Selection

2 In the **Pipe Type** field, select the Attached Interface type for the service that will connect the Multi-Carrier ABC group and Ethernet interfaces. Options are:

- **s-tag** – All S-VLANs and untagged frames are classified into the service.
- **dot1q** – All C-VLANs and untagged frames are classified into the service.

Note: For a full explanation of Ethernet Services, service types, and attached interface types.

3 In the **Ethernet Interface** field, select an Ethernet interface or a LAG for the group.

Note: To create a LAG, click Create LAG. The Create LAG Group page opens. For instructions on creating LAG groups.

4 Click **Next**. The Radio #1 Selection page opens.

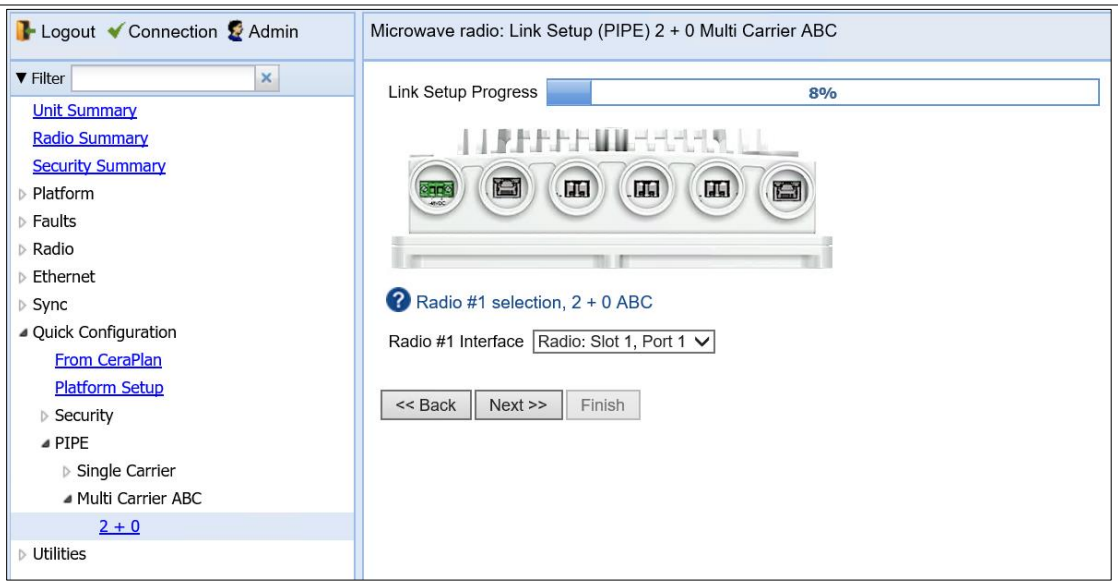


Figure 83: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio #1 Selection Page

5 In the **Radio #1 Interface** field, select the first radio interface for the group.
6 Click **Next**. The Radio #2 Selection page opens.

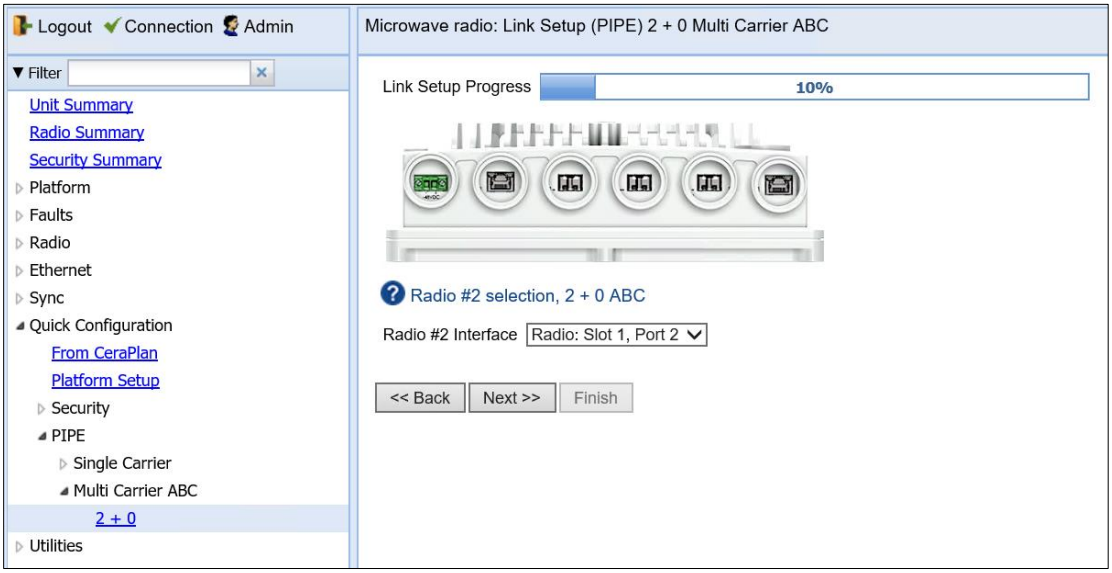


Figure 84: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio #2 Selection Page

7 In the **Radio #2 Interface** field, select the second radio interface for the group.
8 Click **Next**. The Radio XPIC Configuration page opens. If you want to set up an XPIC configuration, select the radio pair. For full instructions on configuring XPIC, including antenna alignment instructions.

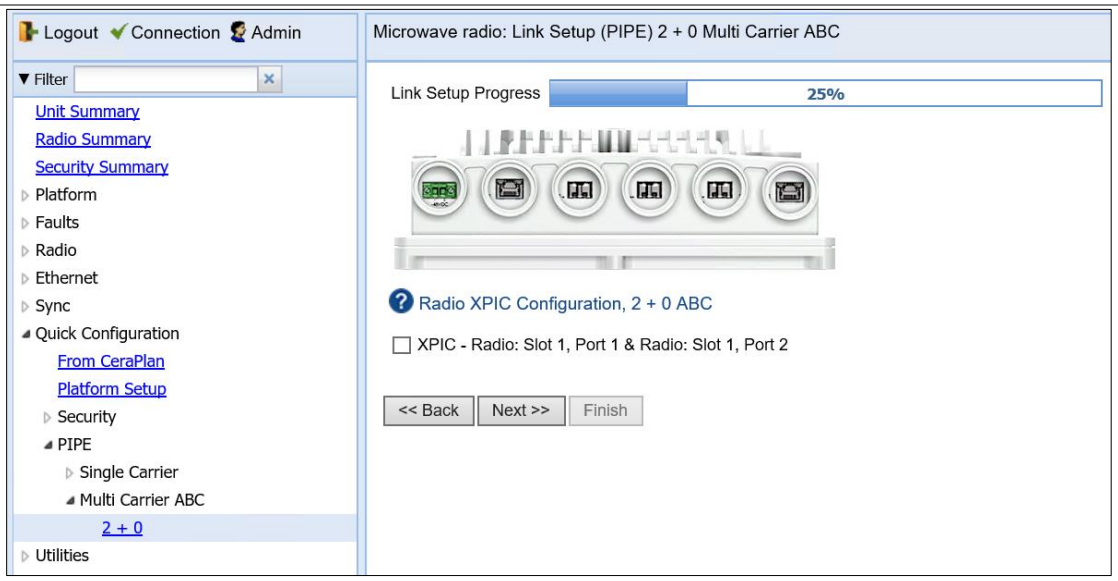


Figure 85: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio XPIC Configuration Page

9 Click **Next**. The Radio Parameters Configuration page opens. You can configure the basic radio parameters for each interface. If you selected XPIC in the Radio XPIC Configuration page, you configure the parameters for the group rather than the individual interfaces.

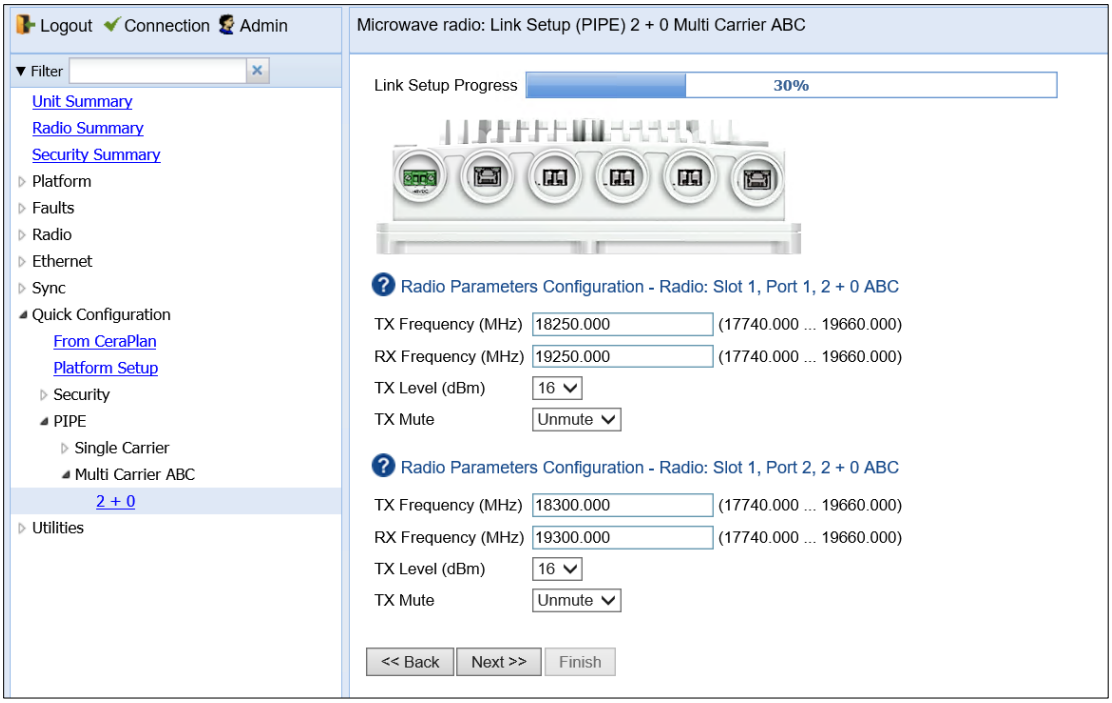


Figure 86: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio Parameters Configuration Page

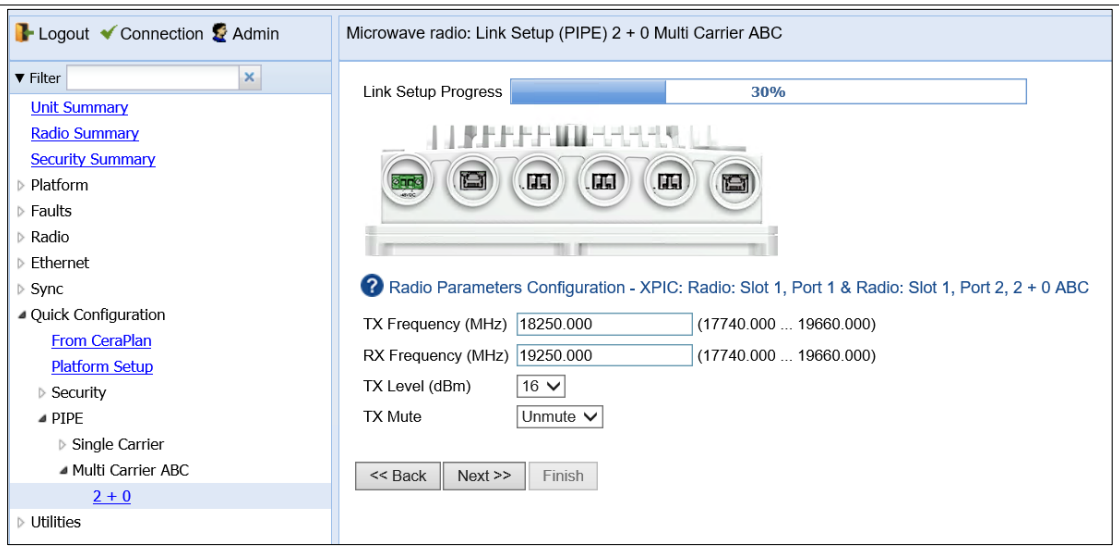


Figure 87: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio Parameters Configuration Page (XPIC)

10 For each interface or XPIC group, configure the following radio parameters.

- i In the **TX Frequency (MHz)** field, set the transmission radio frequency in MHz.
- ii In the **RX Frequency (MHz)** field, set the received radio frequency in MHz.
- iii In the **TX Level (dBm)** field, enter the desired TX signal level (TSL). The range of values depends on the frequency and RFU type.
- iv To mute the TX output of the radio, select **Mute** in the **TX mute** field. To unmute the TX output of the radio, select **Unmute**.

11 Click **Next**. The Radio MRMC Script Configuration page opens. You can configure the MRMC script parameters for each interface. For an XPIC group, you configure the parameters for the group rather than the individual interfaces.

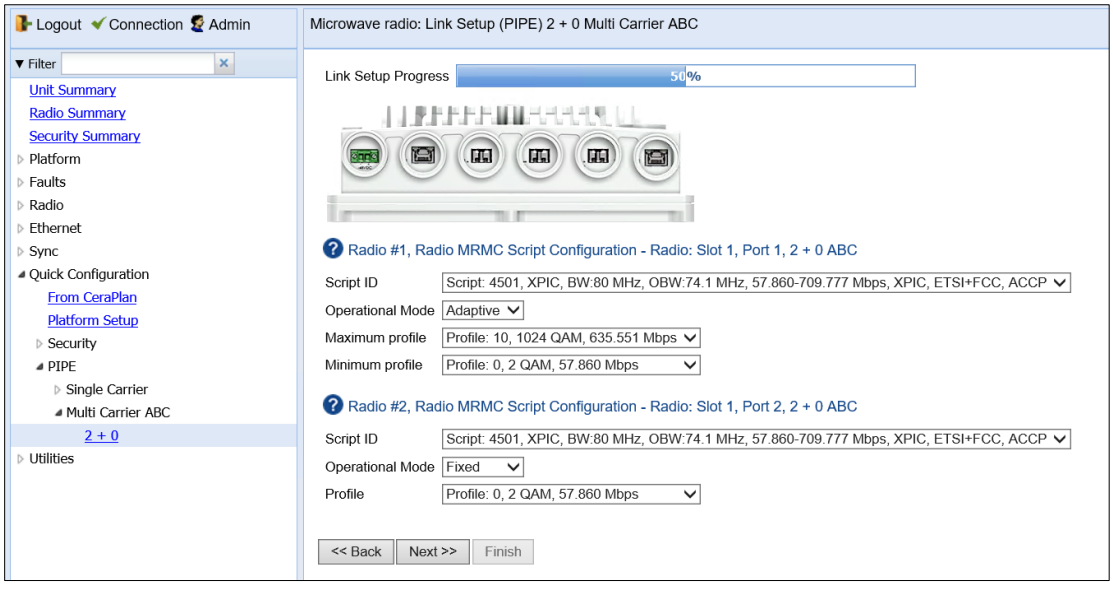


Figure 88: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio MRMC Script Configuration Page

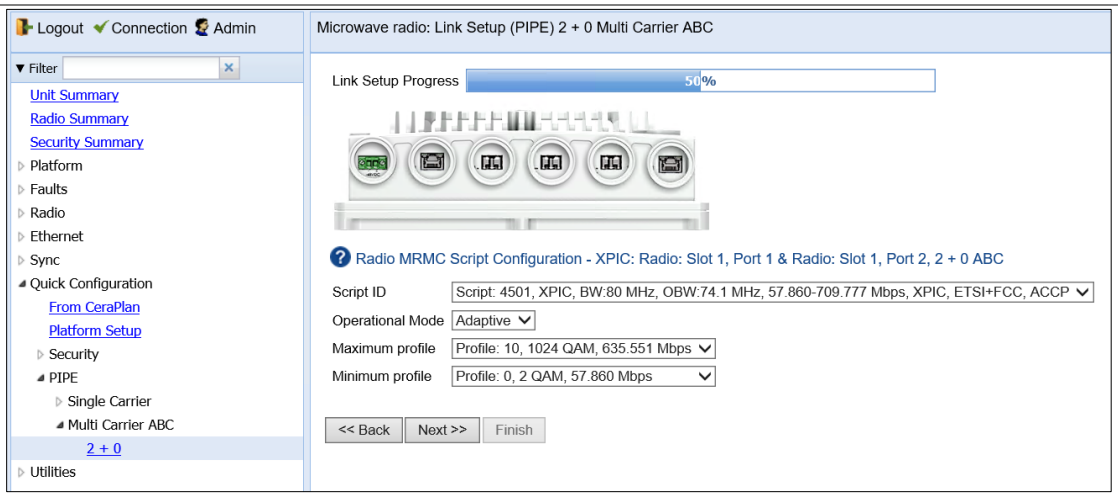


Figure 89: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio MRMC Script Configuration Page – XPIC

12 For each interface or XPIC group, configure the following MRMC script parameters.
13 In the **Script ID** field, select the MRMC script you want to assign to the radio or XPIC group. For a full explanation of choosing an MRMC script.
14 In the **Operational Mode** field, select the ACM mode: **Fixed** or **Adaptive**.

- Fixed ACM mode applies constant TX and RX rates. However, unlike regular scripts, with a Fixed ACM script you can specify a maximum profile to inhibit inefficient transmission levels.
- In Adaptive ACM mode, TX and RX rates are dynamic. An ACM-enabled radio system automatically chooses which profile to use according to the channel fading conditions.

15 Do one of the following:

- If you selected **Fixed** in the **Operational Mode** field, the next field is **Profile**. Select the ACM profile in the **Profile** field.
- If you selected **Adaptive** in the **Operational Mode** field, the following two fields are displayed:
  - **Maximum profile** – Enter the maximum profile for the script.
  - **Minimum profile** – Enter the minimum profile for the script.

16 Click **Next**. The Management Configuration page opens.

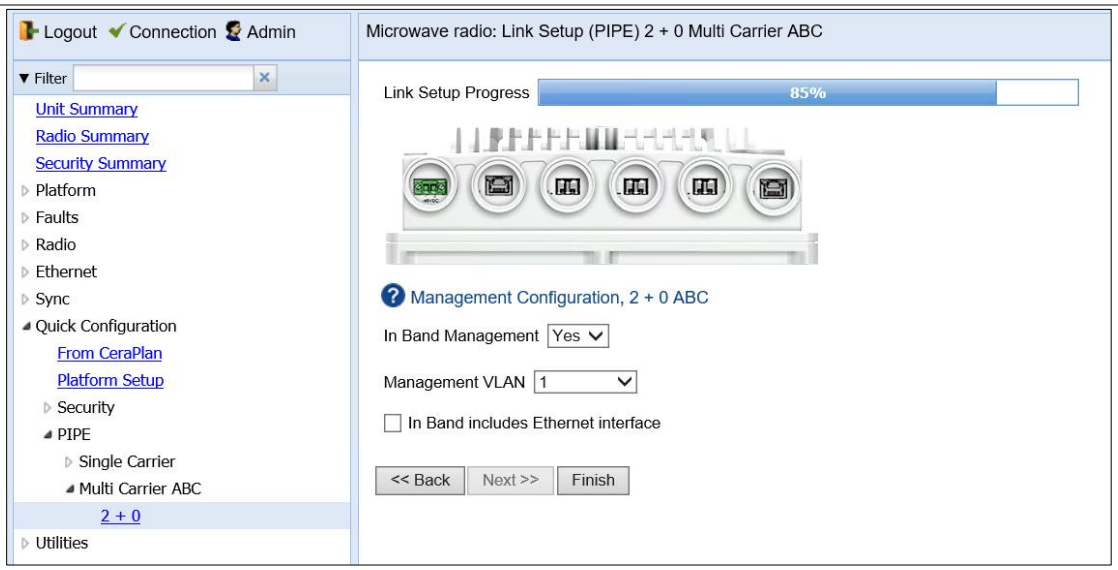


Figure 90: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Management Configuration Page

17 In the **In Band Management** field, select **Yes** to configure in-band management, or **No** if you do not need in-band management. If you select **Yes**, the **Management VLAN** field appears.
18 If you selected **Yes** in the **In Band Management** field, select the management VLAN in the **Management VLAN** field.

Note: You can only select **Untagged** if you are not using IP Forwarding. If you select **Untagged** and you want to configure IP Forwarding later, you will first have to change **Untagged** to a specific VLAN.

19 If you want to use the Ethernet interface as well as the radio interface for in-band management, select **In Band includes Ethernet interface**.
20 Click **Finish**. The Summary page opens. This page displays the parameters you have selected for the group.

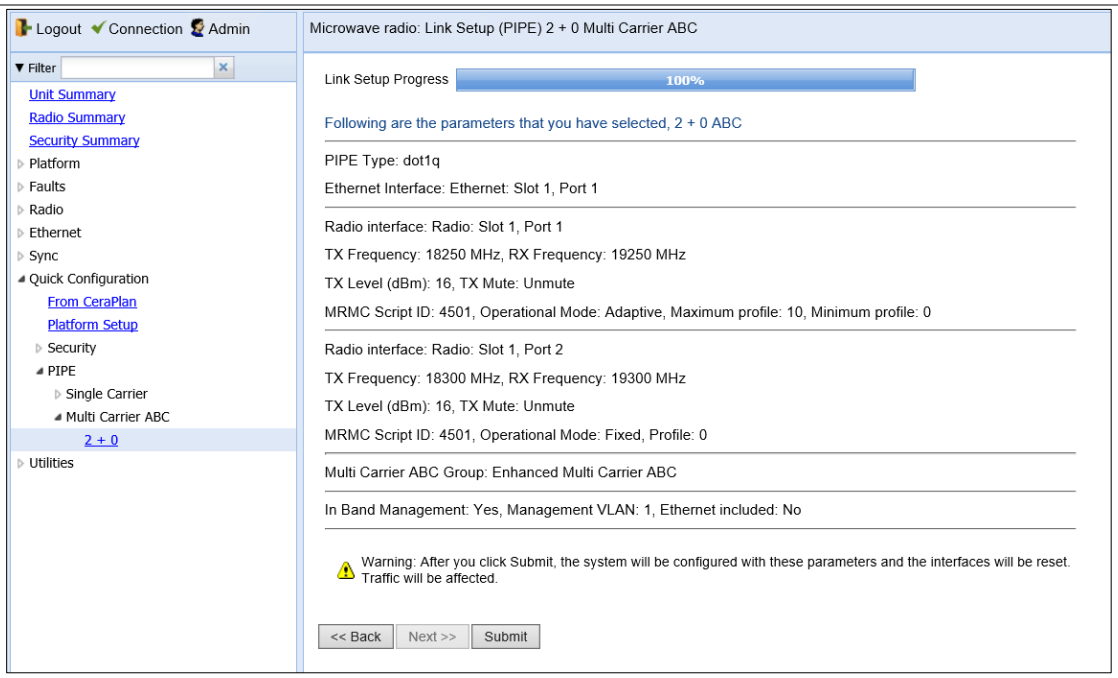


Figure 91: 2 + 0 Multi Carrier ABC Quick Configuration Wizard –Summary Page

21 To complete configuration of the Multi-Carrier ABC group, click **Submit**. If you want to go back and change any of the parameters, click **Back**. After you click **Submit**, the unit is reset.

6.1.3 Configuring a Layer 1 Link Bonding Link Using the Quick Configuration Wizard – Main Unit

This section is applicable for all Link Bonding configurations in which an PTP 850C or PTP 850E is the main unit. An additional Quick Configuration is available to configure the attached unit. See

Configuring a Paired (Attached) Unit in a Layer 1 Link Bonding Group. If the attached unit is an PTP 820C or PTP 820C-HP, see the User Guide for PTP 820 All-Outdoor Products. If the attached unit is an PTP 850CX or PTP 850EX, see the User Guide for PTP 850CX and PTP 850EX.

Multiband configurations with Link Bonding that use PTP 850E with a third-party device should not be configured with the Quick Configuration Wizard but rather, through the main Link Bonding page. See *Configuring 4+0 Layer 1 Link* BondingConfiguring Multiband with Layer 1 Link Bonding.

For important general information about Layer 1 Link Bonding, including required cables and port speeds, see *Layer 1 Link Bonding*4+0 Layer 1 Link Bonding OverviewOverview of Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP.

To configure Layer 1 Link Bonding using the Quick Configuration wizard:

1 Attach and configure the Traffic and (for two-cable configurations) Protocols connections between the two units. 6
2 In the Interface Manager, make sure the port connected to the attached unit for passing traffic between the two units is set to **Admin** = **Down**. See *Enabling the Interfaces (Interface Manager)*.
3 On the main unit, select:
- PTP 850C: Quick Configuration > PIPE > Link Bonding > Configure as Main (N + 0).
- PTP 850E: Quick Configuration > PIPE > Link Bonding > Configure as Main (Multiband)

The Ethernet Selection page of the Quick Configuration wizard opens.

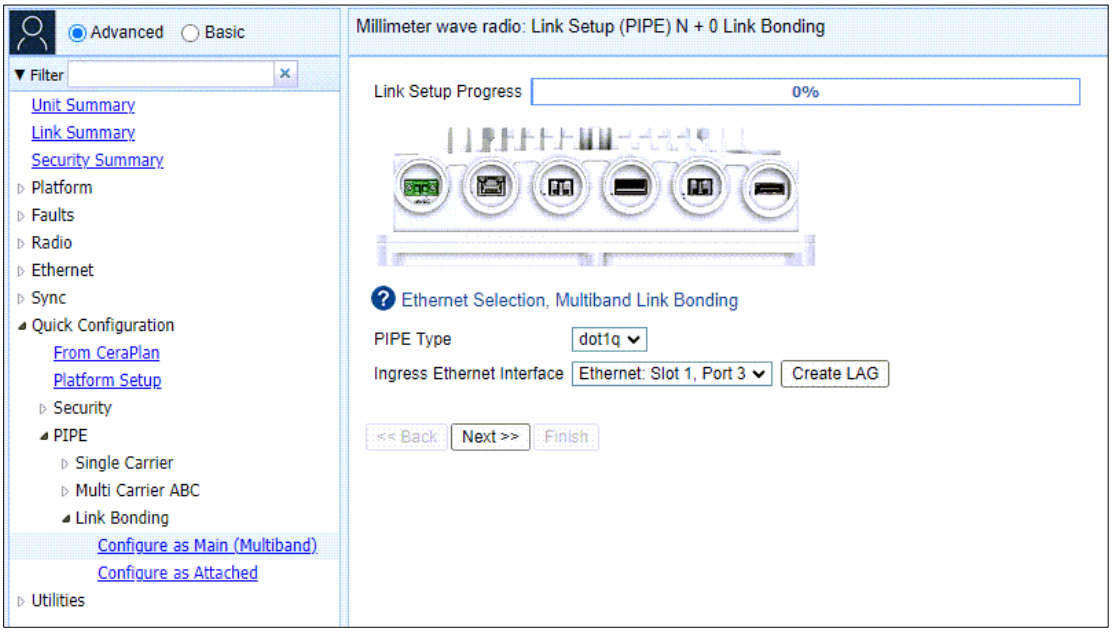


Figure 92: Multiband Link Bonding Quick Configuration Wizard – Ethernet Selection Page (PTP 850E)

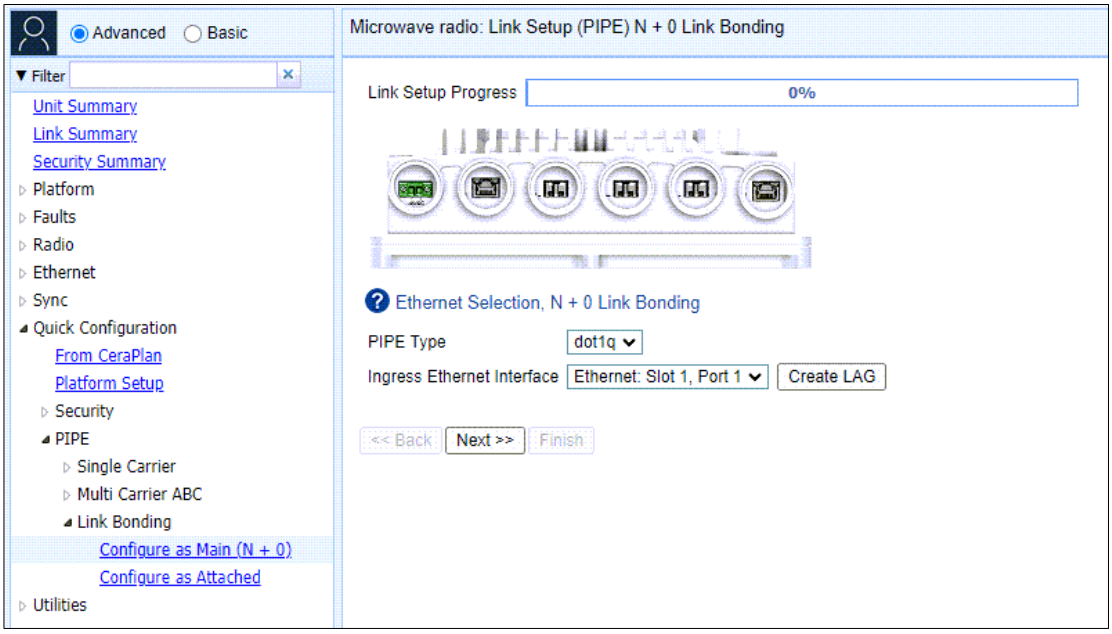


Figure 93: Link Bonding Quick Configuration Wizard – Ethernet Selection Page PTP 850C

4 In the **Pipe Type** field, select the Attached Interface type for the service that will transport traffic between the ingress interface and the Link Bonding group. Options are:

- **s-tag** – All S-VLANs and untagged frames are classified into the service.
- **dot1q** – All C-VLANs and untagged frames are classified into the service.

Note: For a full explanation of Ethernet Services, service types, and attached interface types.

5 In the **Ingress Ethernet Interface** field, select the Ethernet interface connected to the external switch.

- For 4+0 PTP 850C Link Bonding: Ethernet: Slot 1, Port 1 or Port 3
- For Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP: Ethernet: Slot 1, Port 1, Port 3, or Port 4

6 Click **Next**. The Number of Members page of the Link Bonding Quick Configuration wizard opens.

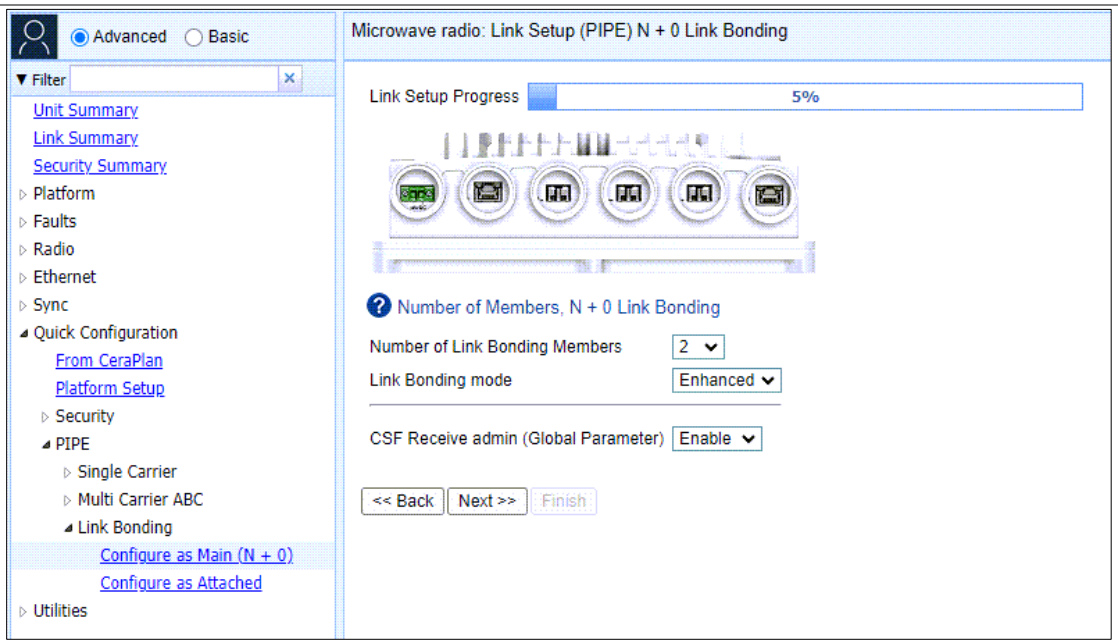


Figure 94: Link Bonding Quick Configuration Wizard – Number of Members Page PTP 850C

7 In the **Number of Link Bonding Members** field, select 2.
8 In the **Link Bonding Mode** field, select **Standard** or **Enhanced**. Enhanced mode is required for configurations that use a single cable to transmit traffic and L2 protocol data between the main and paired units.

Note: For PTP 850C and PTP 850E, most devices support Enhanced Link Bonding mode but some do not. For details.

9 In the **CSF Received Admin (Global Parameter)** field, if you selected Enhanced mode, you must select **Enable**, which is required for Link Bonding Enhanced mode.

If you selected Standard mode, you can select **Enable** or **Disable**.
10 Click **Next**. The Member #1 page of the Link Bonding Quick Configuration wizard opens.

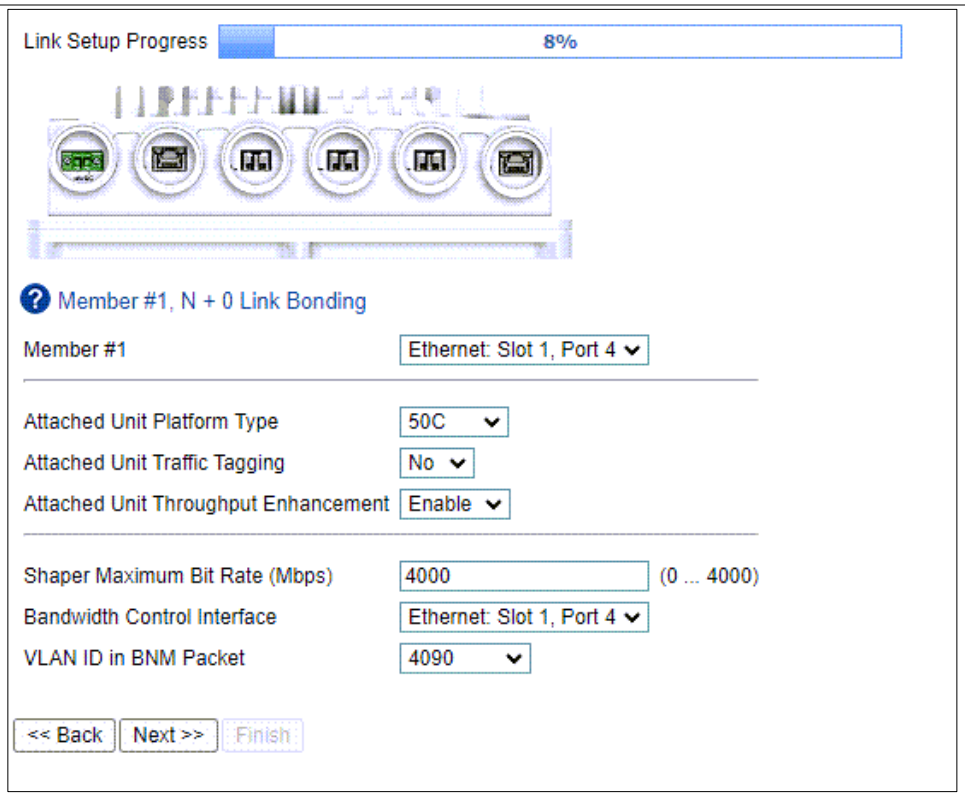


Figure 95: Link Bonding Quick Configuration Wizard – Member #1 Page (4+0 with PTP 850C – Single-Cable Configuration)

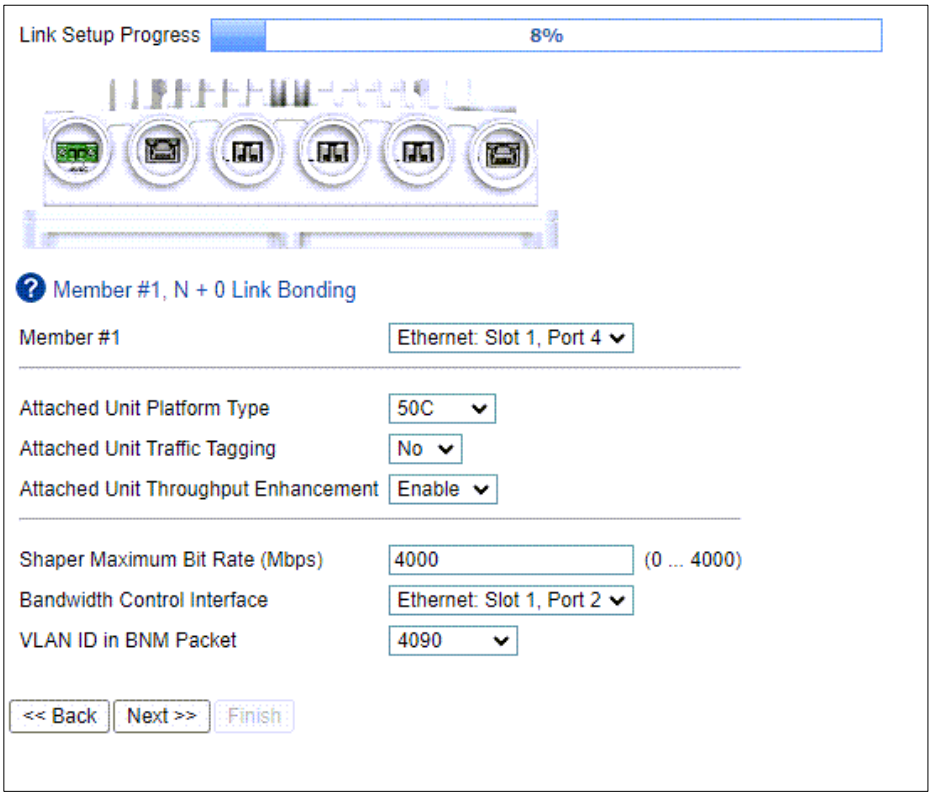


Figure 96: Link Bonding Quick Configuration Wizard – Member #1 Page (4+0 with PTP 850C – Two-Cable Configuration)

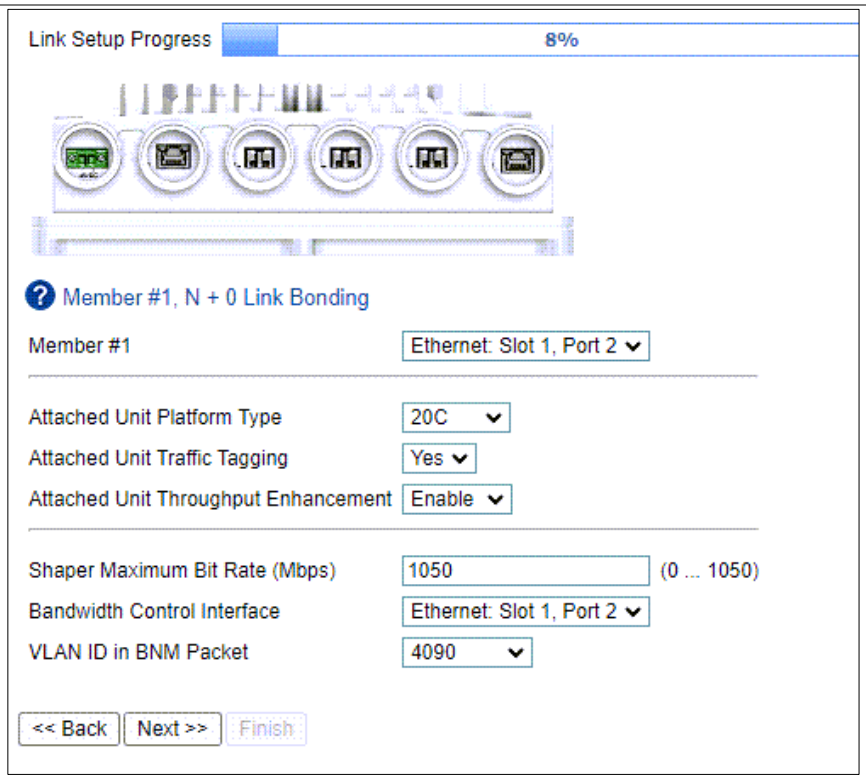


Figure 97: Link Bonding Quick Configuration Wizard – Member #1 Page (PTP 850C with PTP 820C or PTP 820C-HP – Single-Cable Configuration)

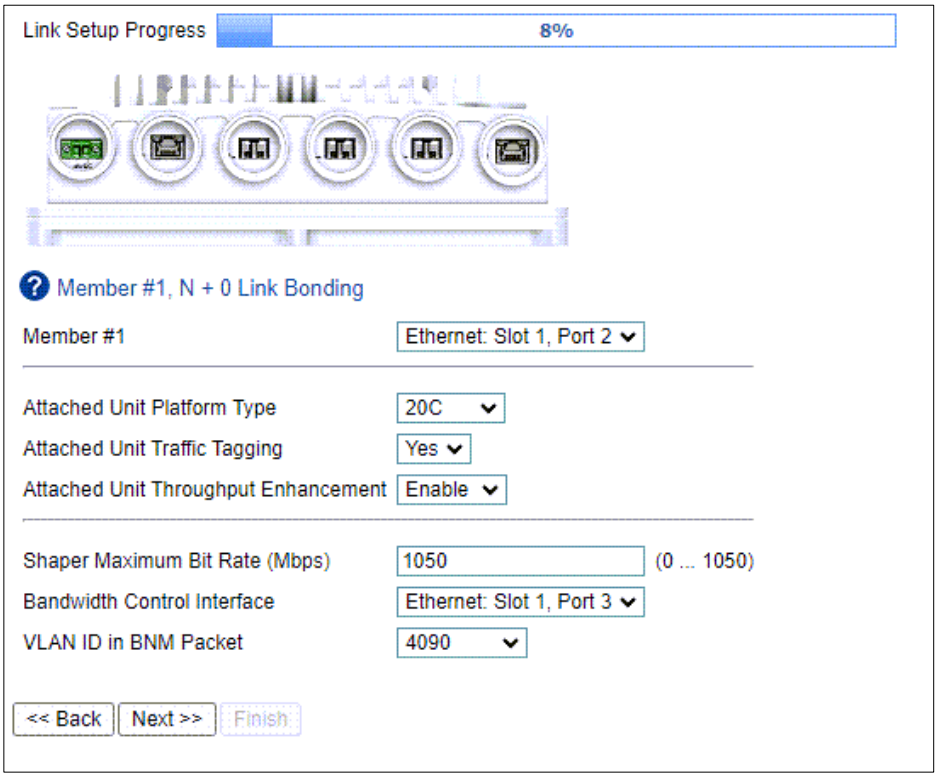


Figure 98: Link Bonding Quick Configuration Wizard – Member #1 Page (PTP 850C with PTP 820C or PTP 820C-HP – Two-Cable Configuration)

11 In the **Member #1** field, select the port connected to the attached unit for passing traffic between the two units.

.

12 In the **Attached Unit Platform Type** field, selected the type of unit paired with the PTP 850C (**PTP 850C** or **PTP 820C**).

13 In the **Attached Unit Traffic Tagging** field:

14 In the **Attached Unit Throughput Enhancement** field, enter **Enable** or **Disable** according to the configuration you intend to do on the paired unit. This enables the main unit to properly calculate the internal Link Bonding parameters.

Note: This field ***does not*** actually configure Throughput Enhancement on the attached unit. You must perform the paired unit's configuration directly on the paired unit itself.

15 In the **Shaper Maximum Bit Rate** field, configure the maximum bit rate. The device uses this value to calculate the L1 Header Compensation. You must set the **Shaper Maximum Bit Rate** field according to the maximum capacity of the link to ensure that the L1 Header Compensation is calculated correctly.

16 In the **Bandwidth Control Interface** field:

- For single-cable configurations, select the same port you selected as Member #1.
- For two-cable configurations, select the port to which the Protocols cable is connected.

17 In the **VLAN ID in BNM Packet** field, select a VLAN ID. You can use any available VLAN ID from 1 to 4090. This is the VLAN use to transfer protocol information between the two units.

18 Click **Next**. The Member #2 page of the Link Bonding Quick Configuration wizard opens.

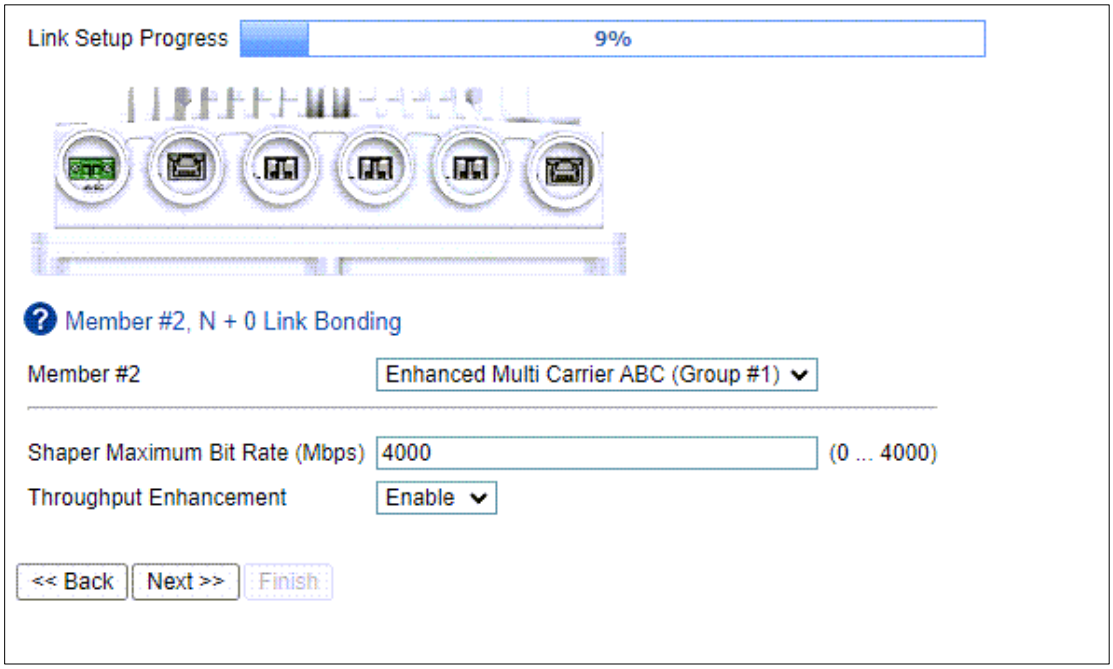


Figure 99: Link Bonding Quick Configuration Wizard – Member #2 Page

19 In the **Member #2** field, select the Multi-Carrier ABC group.

20 In the **Shaper Maximum Bit Rate** field, configure the maximum bit rate. The device uses this value to calculate the L1 Header Compensation. You must set the **Shaper Maximum Bit Rate** field according to the maximum capacity of the link to ensure that the L1 Header Compensation is calculated correctly.

21 In the **Throughput Enhancement** field, you can enable Link Bonding Throughput Enhancement for the main unit. For detailed information about Throughput Enhancement, see:

- For 4+0 Layer 1 Link Bonding with PTP 850C.
- For Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP.

22 Click **Next**. The XPIC page of the Link Bonding Quick Configuration wizard opens.

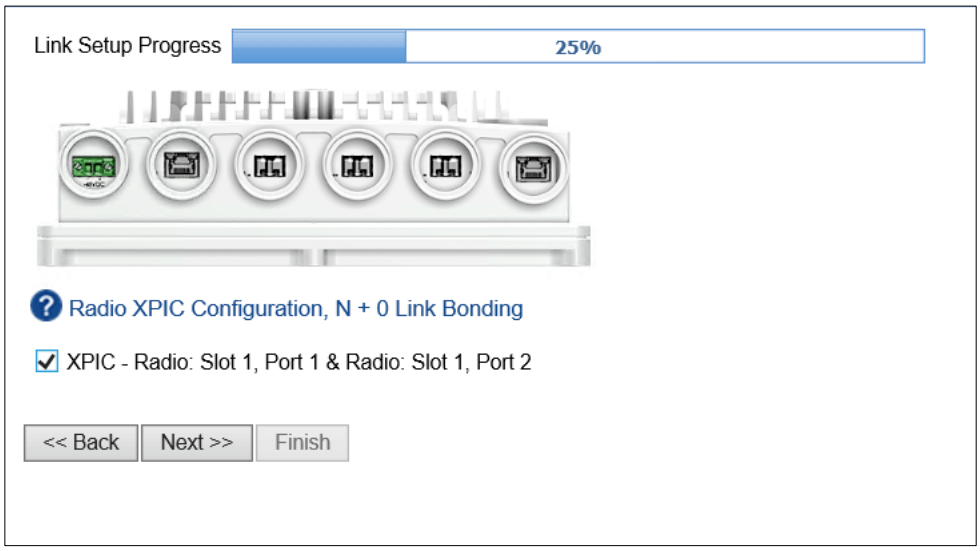


Figure 100: Link Bonding Quick Configuration Wizard – XPIC Page

23 To configure the radio carriers of the PTP 850C to operate in XPIC mode, select **XPIC**.

24 Click **Next**. The Radio MRMC Script Configuration page of the Link Bonding Quick Configuration wizard opens.

Note: If you selected XPIC, one set of MRMC parameters are displayed and are applied to both interfaces. If you did not select XPIC, two sets of radio parameters are displayed, one for each radio carrier.

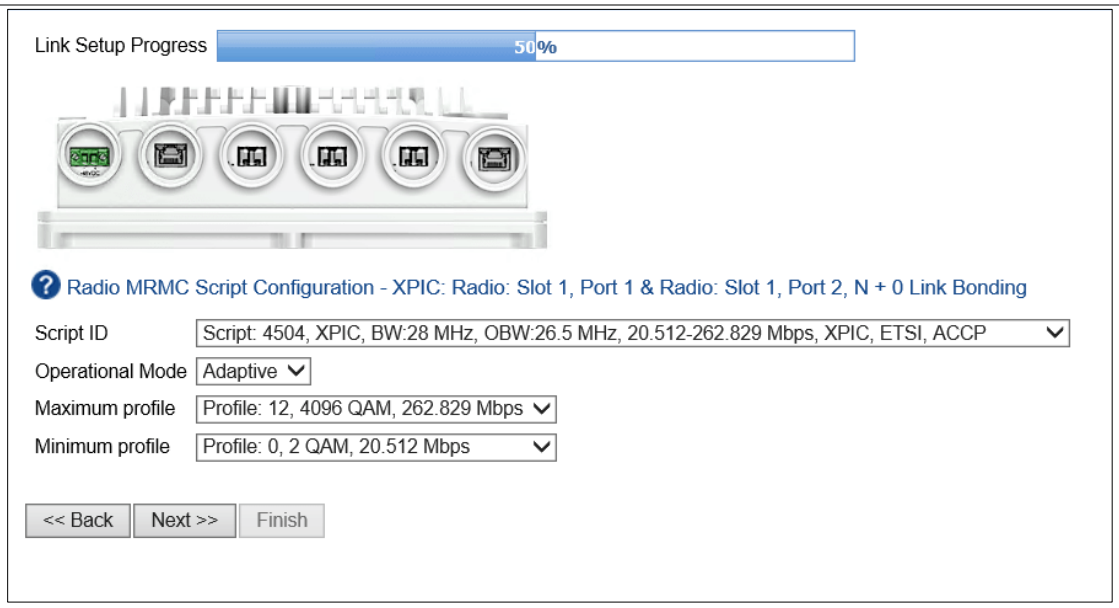


Figure 101: Link Bonding Quick Configuration Wizard – Radio MRMC Script Configuration Page (XPIC Selected)

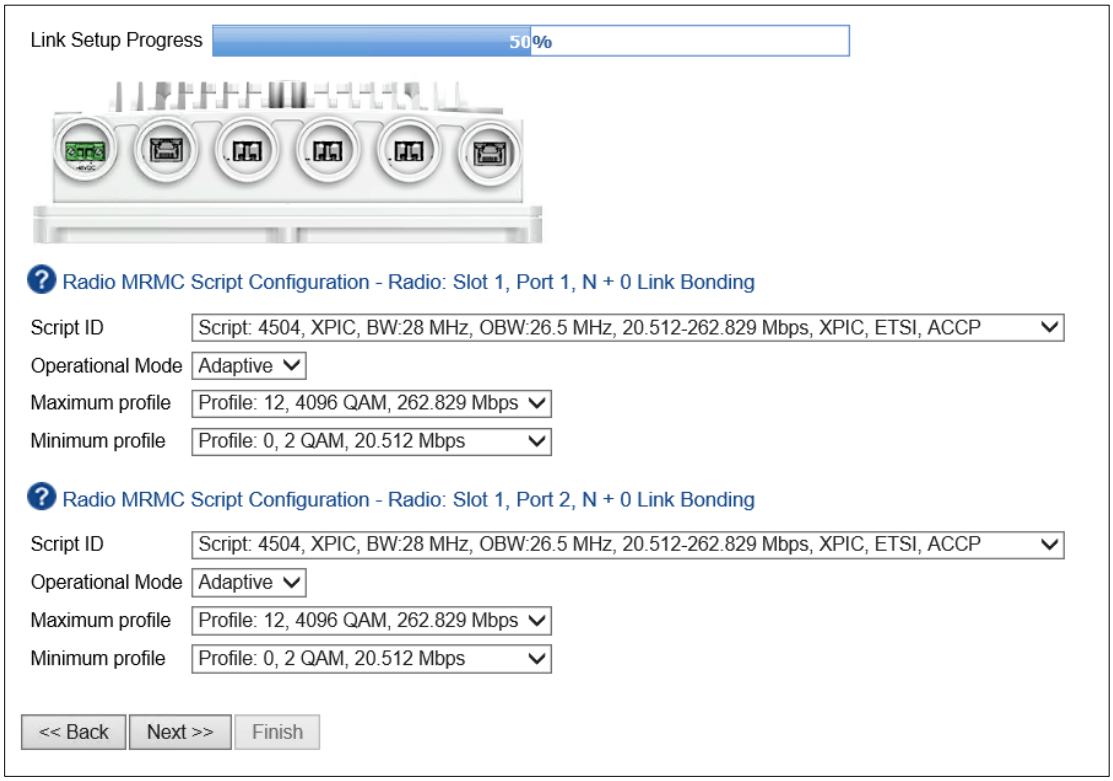


Figure 102: Link Bonding Quick Configuration Wizard – Radio MRMC Script Configuration Page (XPIC not Selected)

25 In the **Script ID** field, select the MRMC script you want to assign to the main Unit's radio interfaces. For a full explanation of choosing an MRMC script.
26 In the **Operational Mode** field, select **Adaptive**. The following two fields are displayed:

- **Maximum profile** – Enter the maximum profile for the script.
- **Minimum profile** – Enter the minimum profile for the script.

Notes: Make sure the **Maximum profile** and **Minimum profile** are set to different values.

27 Click **Next**. The Radio Parameters Configuration page of the Link Bonding Quick Configuration wizard opens.

Note: If you selected XPIC, one set of radio parameters are displayed and are applied to both interfaces. If you did not select XPIC, two sets of radio parameters are displayed, one for each radio carrier.

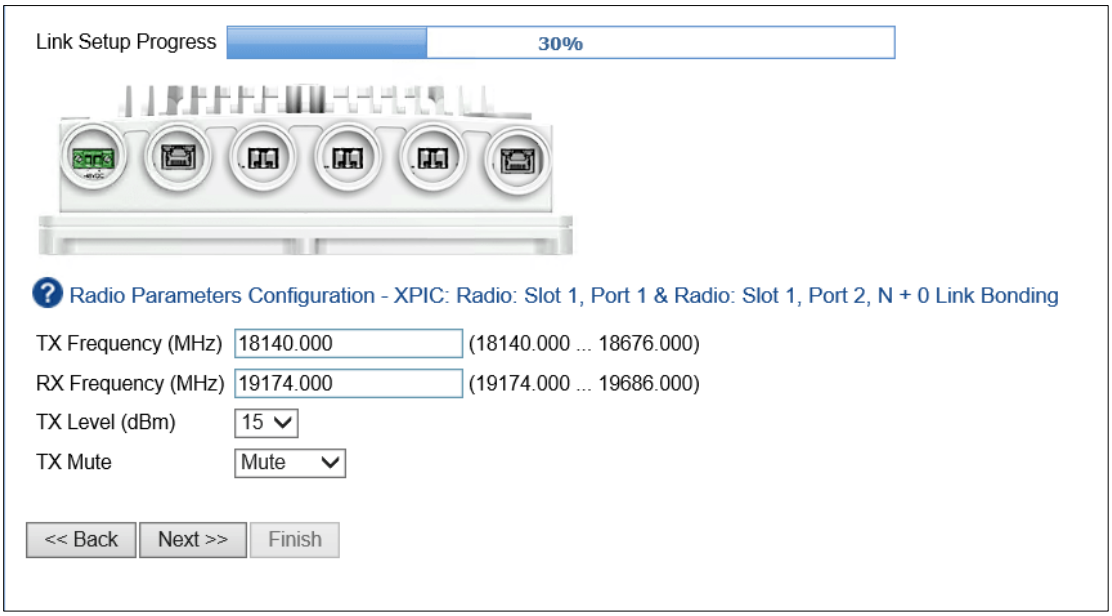


Figure 103: Link Bonding Quick Configuration Wizard – Radio Parameters Configuration Page (XPIC Selected)

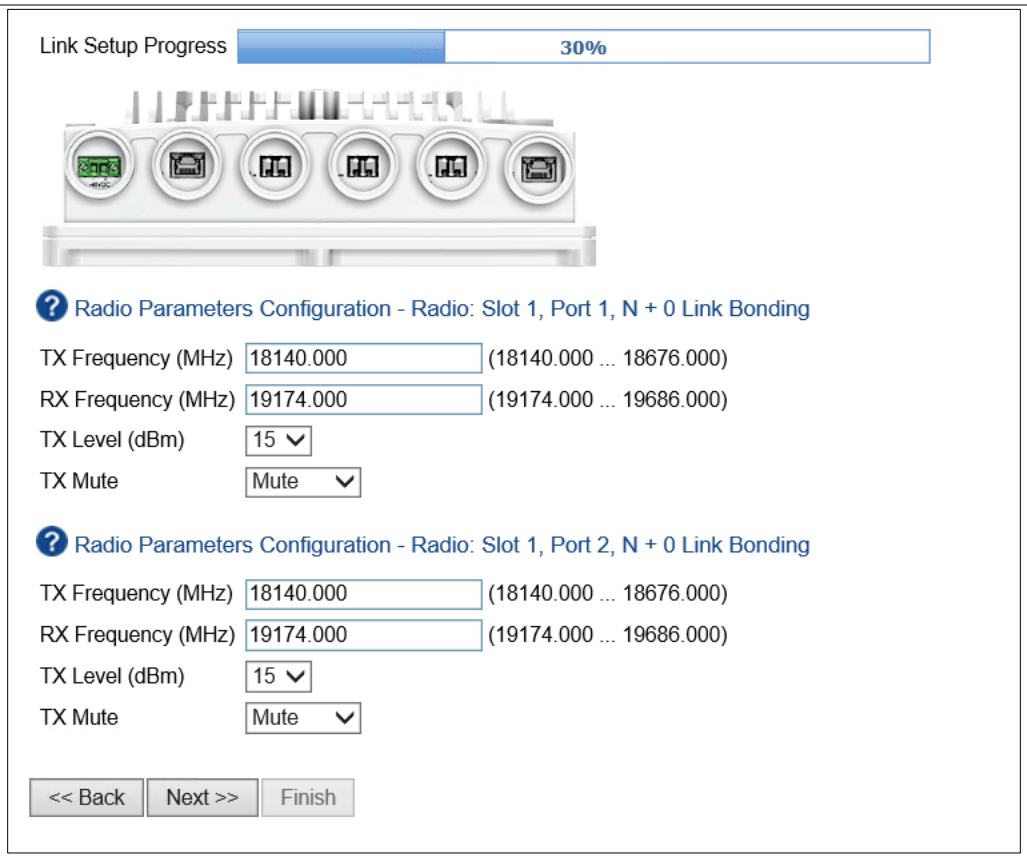


Figure 104: Link Bonding Quick Configuration Wizard – Radio Parameters Configuration Page (XPIC not Selected)

28 Configure the following radio parameters for the main unit's radio interfaces:

i In the **TX Frequency (MHz)** field, set the transmission radio frequency in MHz.
ii In the **RX Frequency (MHz)** field, set the received radio frequency in MHz.
iii In the **TX Level (dBm)** field, enter the desired TX signal level (TSL). The range of values depends on the frequency and RFU type.
iv To mute the TX output of the radio, select **Mute** in the **TX mute** field. To unmute the TX output of the radio, select **Unmute**.

29 Click **Next**. The Management Configuration page of the Link Bonding Quick Configuration wizard opens.

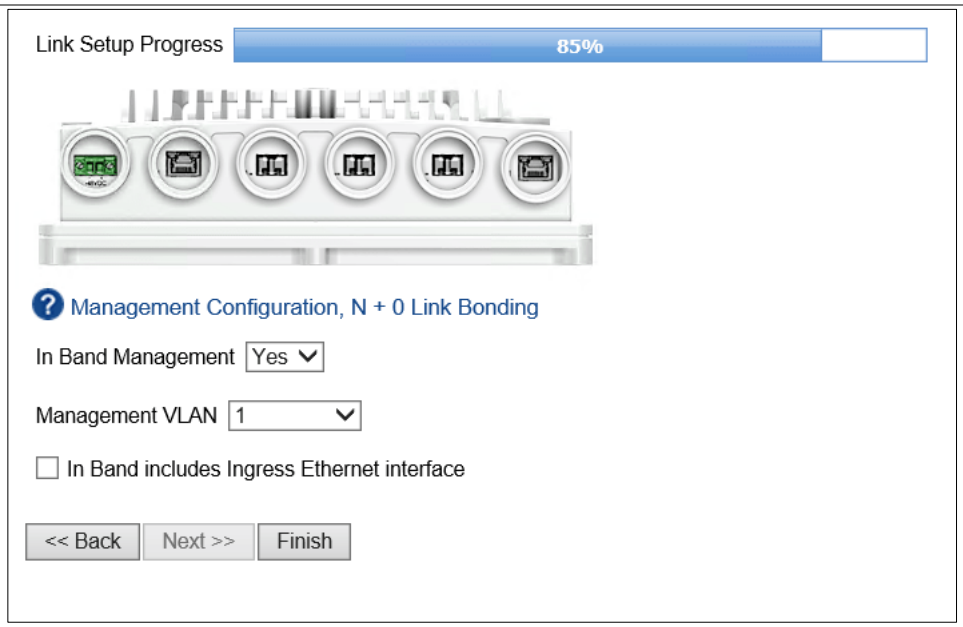


Figure 105: Link Bonding Quick Configuration Wizard – Management Configuration Page

30 In the **In Band Management** field, select **Yes** to configure in-band management, or **No** if you do not need in-band management. If you select **Yes**, the **Management VLAN** field appears.
31 If you selected **Yes** in the **In Band Management** field, select the management VLAN in the **Management VLAN** field.
32 If you want to use the Ethernet interface as well as the radio interface for in-band management, select **In Band includes Ethernet interface**.
33 If you want to manage the paired unit via in-band management, perform the following configurations on the paired unit:

i Enable in-band management.
ii Configure a management service point on the PTP 850C port used to transfer L2 protocol data between the two units.

34 Click **Finish**. The Summary page opens. This page displays the parameters you have selected for the group.

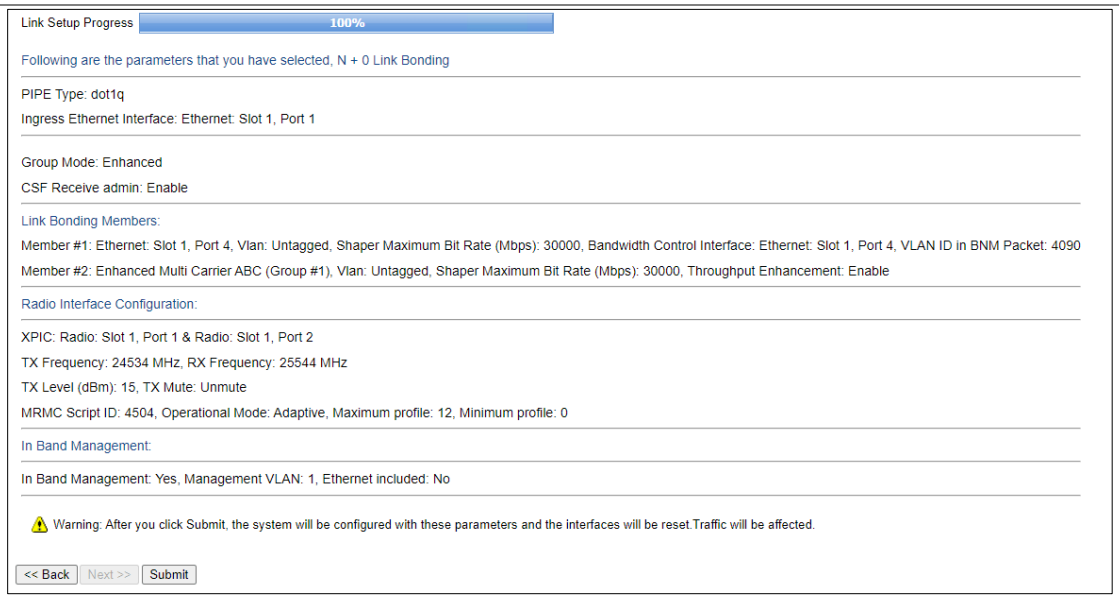


Figure 106: Quick Configuration Wizard – Summary Page (4+0 with PTP 850C)

35 To complete configuration of the Link Bonding group on the main unit, click **Submit**. If you want to go back and change any of the parameters, click **Back**.

36 On the paired unit, you can use the Link Bonding – Configure as Attached wizard to configure Link Bonding parameters for the paired unit, as well as the paired unit's MRMC and radio parameters.

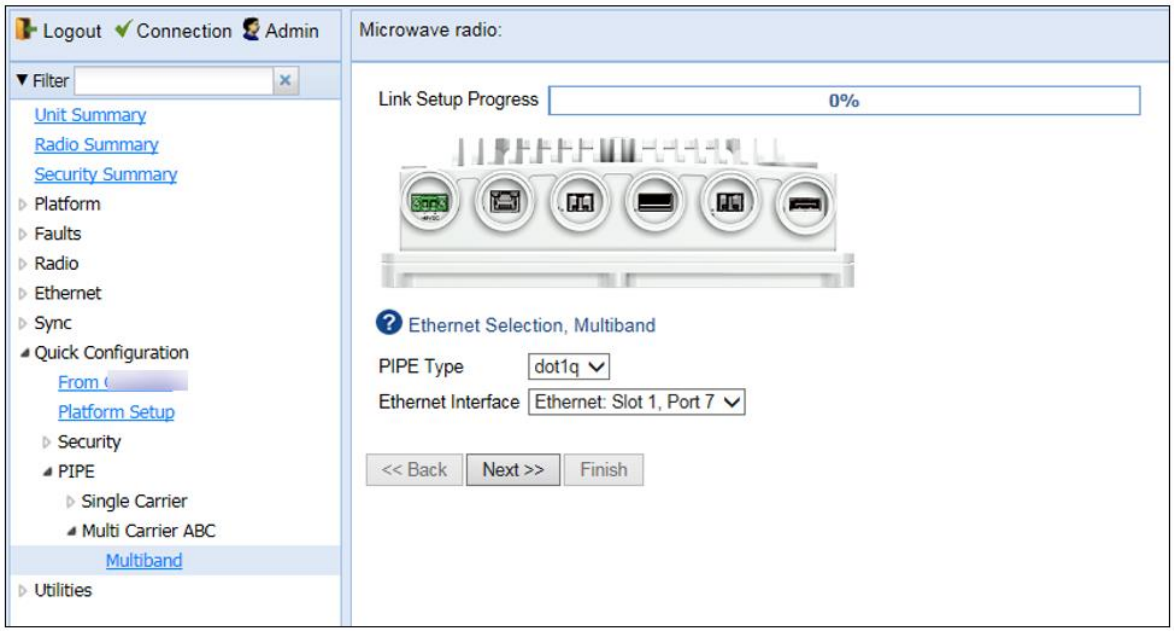
6.1.4 Configuring a Multiband (Enhanced Multi-Carrier ABC) Link Using the Quick Configuration Wizard

For important general information about Multiband links.

To configure a Multiband node using the Quick Configuration wizard:

1. Connect the external switch to any operational traffic port on the PTP 850E.
2. Connect Port 3 (Eth2) on the PTP 850E to the unit paired with the PTP 850E. When the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, use Eth2 on the PTP 820C, PTP 820C-HP, or PTP 820S.
3. Verify that the **Admin** status of Eth2 on the PTP 850E is **Down**.
4. Verify that no service points are configured on the Eth2 port of the PTP 850E. If there are service points on Eth2, remove them.
5. On the PTP 850E, select **Quick Configuration** > **PIPE** > **Multi Carrier ABC** > **Multiband**. Page 1 of the Multiband Quick Configuration wizard opens.

Figure 107 Multiband Quick Configuration Wizard – Page 1



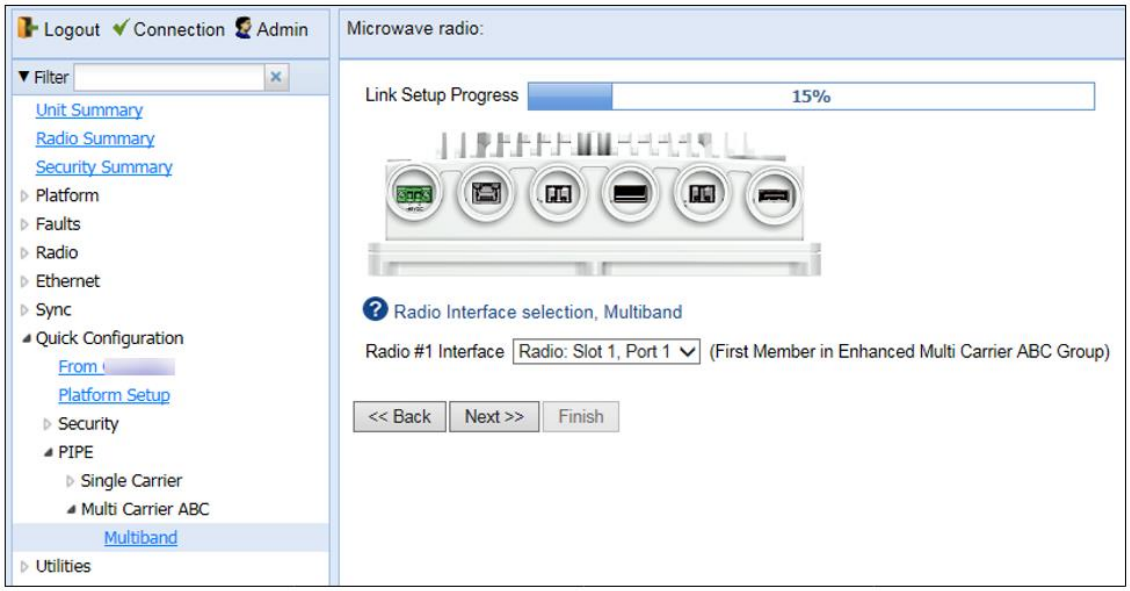
6. In the **Pipe Type** field, select the Attached Interface type for the service that will connect the radio and Ethernet interfaces. Options are:
   - **s-tag** – All S-VLANs and untagged frames are classified into the service.
   - **dot1q** – All C-VLANs and untagged frames are classified into the service.

Note

For a full explanation of Ethernet Services, service types, and attached interface types, see Configuring Ethernet Service(s).

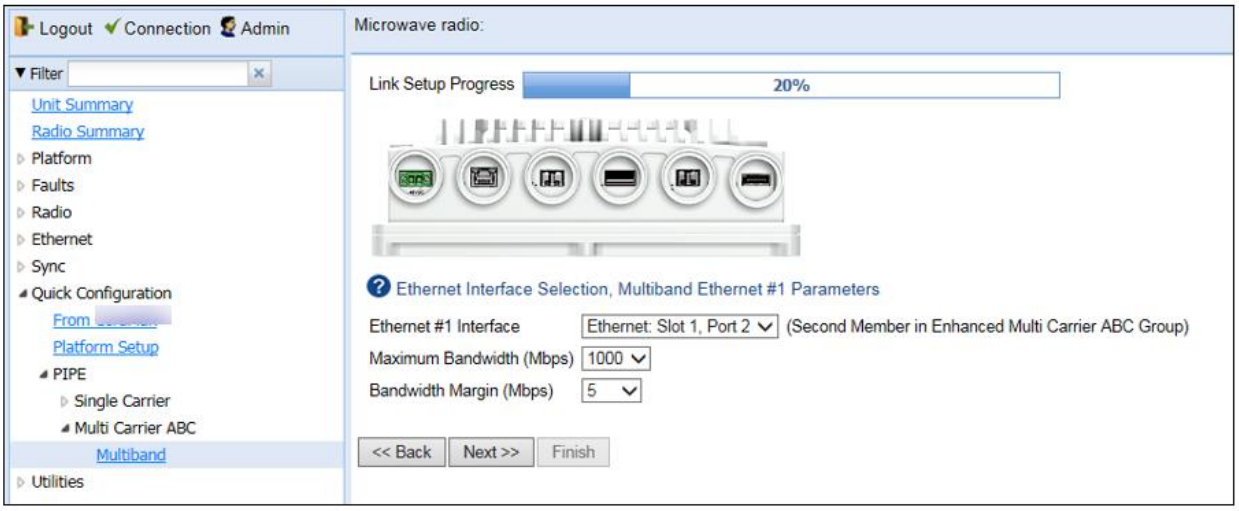
7. In the **Ethernet Interface** field, select the port connected to the external switch.
8. Click **Next**. Page 2 of the Multiband Quick Configuration wizard opens.

Figure 108 Multiband Quick Configuration Wizard – Page 2



9. In the Radio #1 Interface field, select Radio: Slot 1, Port 1.
10. Click Next. Page 3 of the Multiband Quick Configuration wizard opens.

Figure 109 Multiband Quick Configuration Wizard – Page 3



11. In the **Ethernet #1 Interface** field, select Ethernet: Slot 1, Port 2.
12. In the **Maximum Bandwidth (Mbps)** field, select the maximum traffic that the PTP 850E will pass to the paired unit.

    - When using Fixed ACM mode, set this parameter to the actual rate you want the paired unit to broadcast.
    - When using Adaptive ACM mode, set this parameter to the maximum of the paired unit's capacity.

    The default value is 1000 Mbps.

Note

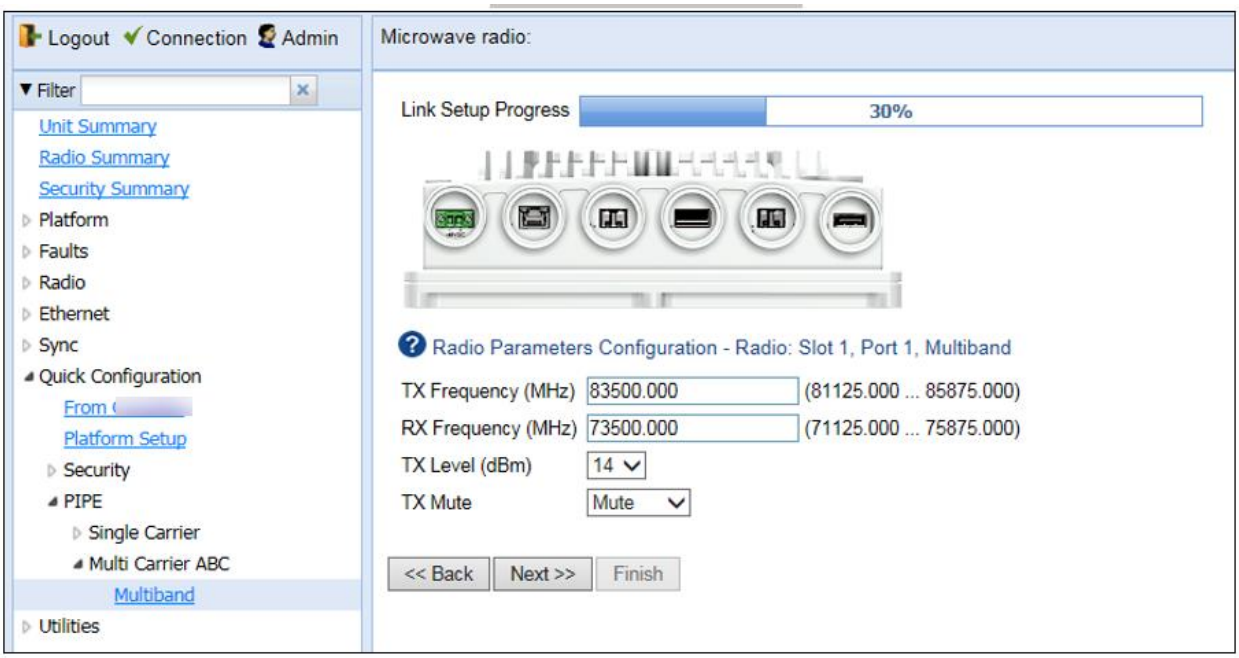
The Maximum Bandwidth represents the L1 capacity of the radio link connected to the Ethernet member. The actual bandwidth that will be available for traffic is less due to overhead.
When using a third-party radio as the paired unit, it is particularly important to set this parameter properly in order to ensure optimal performance. Failure to properly set this parameter may lead to frequent pauses as the queue fills up during low capacity periods, such as when weather conditions cause the ACM profile to drop.

13. In the **Bandwidth Margin (Mbps)** field, select the bandwidth margin, in Mbps. This parameter deducts the specified throughput from the throughput the PTP 850E would otherwise pass to the paired unit. The purpose of this parameter is to provide a margin of safety that will avoid loss of traffic in the event that the ACM profile is reduced on the paired unit. It is recommended to configure this parameter as follows:

    - If the paired unit is an PTP 820 microwave radio or a third-party device with a bandwidth notification mechanism that will inform the PTP 850E of an impending reduction of the ACM profile before the reduction takes place, it is recommended to leave this parameter at its default value of 5 Mbps.
    - If the paired unit is a third-party device without a bandwidth notification mechanism that will inform the PTP 850E of an impending reduction of the ACM profile before the reduction takes place, it is recommended to set this parameter to an amount equal to or greater than the largest throughput differential between any two adjacent profiles for the script configured on the paired unit.

    The range of values is 5 to 100 Mbps.
14. Click Next. Page 4 of the Multiband Quick Configuration wizard opens.

Figure 110 Multiband Quick Configuration Wizard – Page 4

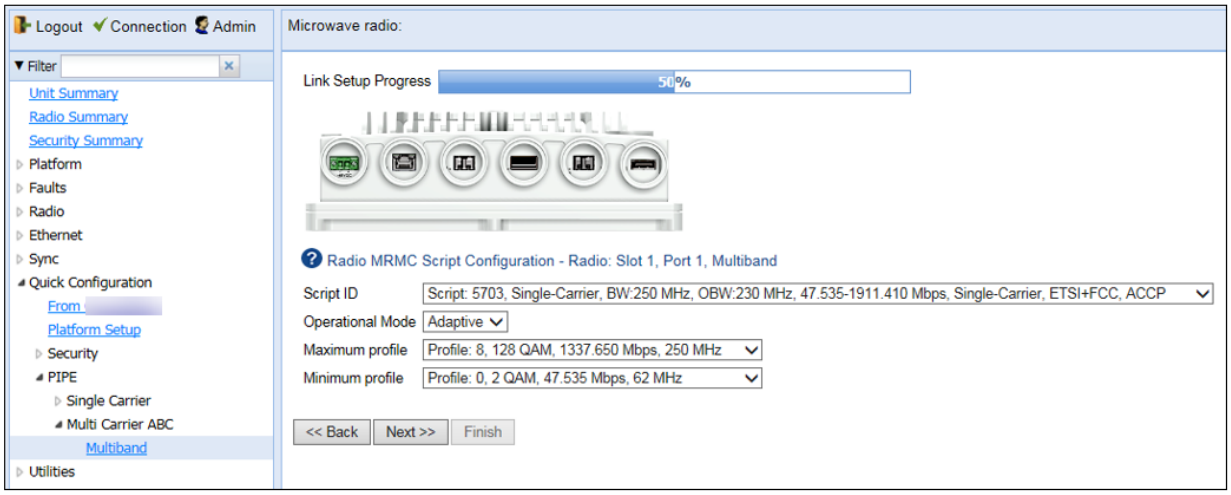


15. Configure the following radio parameters.
    a. In the **TX Frequency (MHz)** field, set the transmission radio frequency in MHz.

b. In the RX **Frequency (MHz)** field, set the received radio frequency in MHz.
c. In the **TX Level (dBm)** field, enter the desired TX signal level (TSL). The range of values depends on the frequency and RFU type.
d. To mute the TX output of the radio, select **Mute** in the **TX mute** field. To unmute the TX output of the radio, select **Unmute**.

16. Click **Next**. Page 5 of the Multiband Quick Configuration wizard opens.

Figure 111 Multiband Quick Configuration Wizard – Page 5



17. In the **Script ID** field, select the MRMC script you want to assign to the radio. For a full explanation of choosing an MRMC script.
18. In the **Operational Mode** field, select **Adaptive**. The following two fields are displayed:

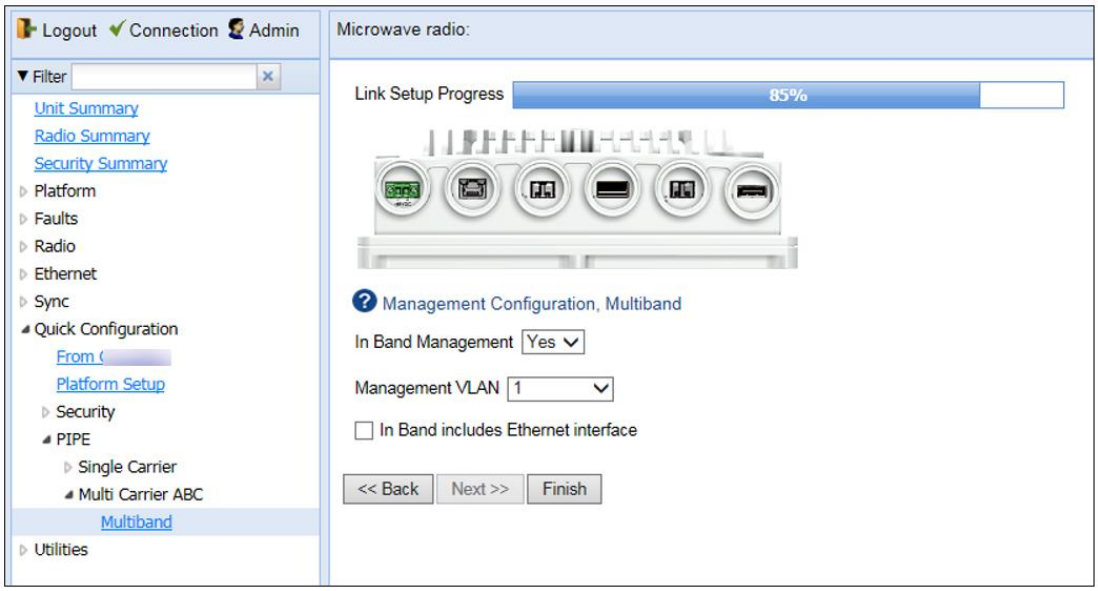
- **Maximum profile** – Enter the maximum profile for the script..
- **Minimum profile** – Enter the minimum profile for the script.

Note

Fixed mode is not supported for Multiband.
For Multiband links, ake sure the Maximum profile and **Mi**nimum profile are set to different values for Multiband links.

19. Click **Next**. Page 6 of the Multiband Quick Configuration wizard opens.

Figure 112 Multiband Quick Configuration Wizard – Page 6



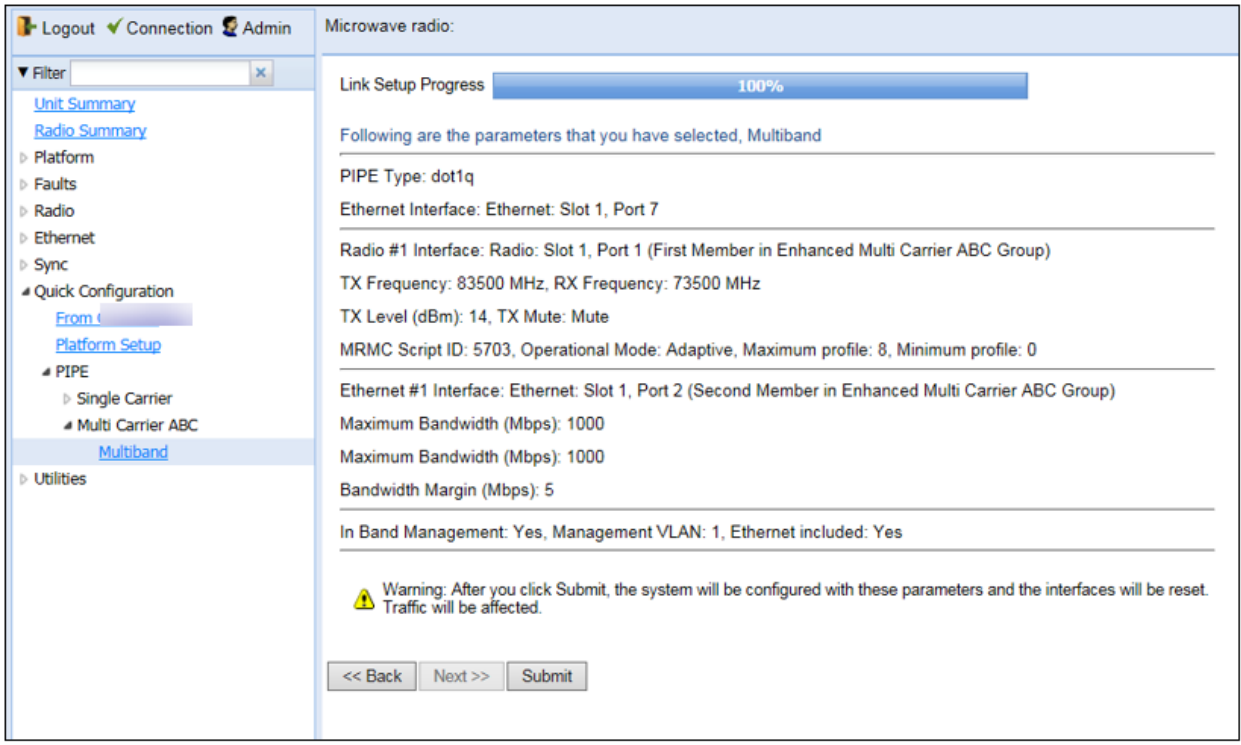
20. In the **In Band Management** field, select **Yes** to configure in-band management, or **No** if you do not need in-band management. If you select **Yes**, the **Management VLAN** field appears.
21. If you selected **Yes** in the **In Band Management** field, select the management VLAN in the **Management VLAN** field.
22. If you want to use the Ethernet interface as well as the radio interface for in-band management, select **In Band includes Ethernet interface**.

Note

If you want to manage the paired unit via the PTP 850E, refer to the instructions in Inband Management via the PTP 850E.

23. Click **Finish**. The Summary page opens. This page displays the parameters you have selected for the group.

Figure 113 Multiband Quick Configuration Wizard – Summary Page



24. To complete configuration of the Multiband group on the PTP 850E, click **Submit**. If you want to go back and change any of the parameters, click **Back**.
25. Enable the Eth2 interface.

When the PTP 850E is paired with an PTP 820 microwave radio, the following must be configured on the PTP 820 microwave radio:

- A **service** must be configured between the Ethernet port connected to the PTP 850E and the radio or Multi-Carrier ABC group being used for the Multiband link.

Note

If the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, the service must be a Pipe service. However, this service must be given higher priority than any other service attached to the interfaces used for Multiband.

- Automatic State Propagation must be configured, with **ASP trigger by remote fault** enabled.
- Radio Bandwidth Notification must be enabled.

For instructions, refer to the User Guide for the PTP 820 product you are using.

When the PTP 850E is paired with a third-party unit, the following must be configured on the third-party unit:

- The unit's switching mechanism must be set to Pipe mode and a Pipe service must be configured between the Ethernet port connected to the PTP 850E and the paired unit's radio or radio group.
- Automatic State Propagation must be configured, with **ASP trigger by remote fault** enabled.
- 802.3X Flow Control must be enabled.
- Ethernet Bandwidth Notification must be enabled

6.1.5 Configuring a Multiband Link with Layer 1 Link Bonding Using the Quick Configuration Wizard – Main Unit

This Quick Configuration wizard is only used with the PTP 850E as main unit. An additional Quick Configuration is available to configure the paired unit. If the paired unit is an PTP 820C or PTP 820C-HP, see the User Guide for PTP 820 All-Outdoor Products.

Multiband configurations with Link Bonding that use PTP 850E with a third-party device should not be configured with the Quick Configuration Wizard but rather, through the main Link Bonding page.

For important general information about Multiband with Layer 1 Link Bonding.

To configure Multiband link with Layer 1 Link Bonding on the main PTP 850E unit using the Quick Configuration wizard:

1 Connect the external switch to the QSFP port (P4, Eth 3 – Eth 6) on the PTP 850E. This port can be configured to operate in QSFP mode (40 Gbps) or SFP+ mode (10 Gbps).
2 Configure the speed as follows:
    - For configurations with PTP 850C, set the traffic ports to 10 Gbps.
    - For configurations with PTP 820C or PTP 820C-HP, set the traffic ports to 1 Gbps.
3 If you are using a separate Protocols cable:
    - For configurations with PTP 850C, configure the port speed of the protocols ports to 2.5 Gbps.
    - For configurations with PTP 820C or PTP 820C-HP, configure the port speed of the protocols ports to 1 Gbps.
4 In the Interface Manager, make sure the port connected to the paired unit for passing traffic between the two units is set to **Admin** = **Down**.
5 Connect an optical cable between the traffic ports. This cable carries traffic and (optionally) L2 protocol data between the two units.
6 Optionally, connect an optical cable between the protocols ports of each unit. This cable carries L2 protocol data between the two units.
7 On the PTP 850E, select **Quick Configuration > PIPE > Link Bonding > Configure as Main (Multiband)**. The Ethernet Selection page of the Quick Configuration wizard opens.

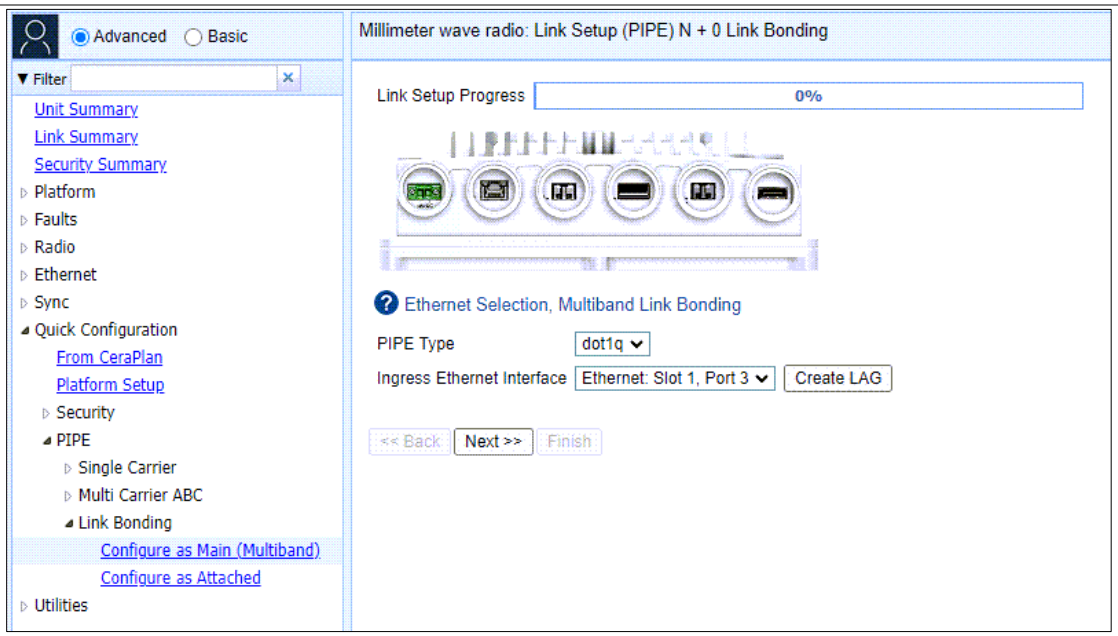


Figure 114: Multiband Link Bonding Quick Configuration Wizard – Ethernet Selection Page

8 In the **Pipe Type** field, select the Attached Interface type for the service that will transport traffic between the ingress interface and the Link Bonding group. Options are:

- **s-tag** – All S-VLANs and untagged frames are classified into the service.
- **dot1q** – All C-VLANs and untagged frames are classified into the service.

Note: For a full explanation of Ethernet Services, service types, and attached interface types,

9 In the **Ingress Ethernet Interface** field, select the Ethernet interface connected to the external switch.

10 Click **Next**. The Number of Members page of the Multiband Link Bonding Quick Configuration wizard opens.

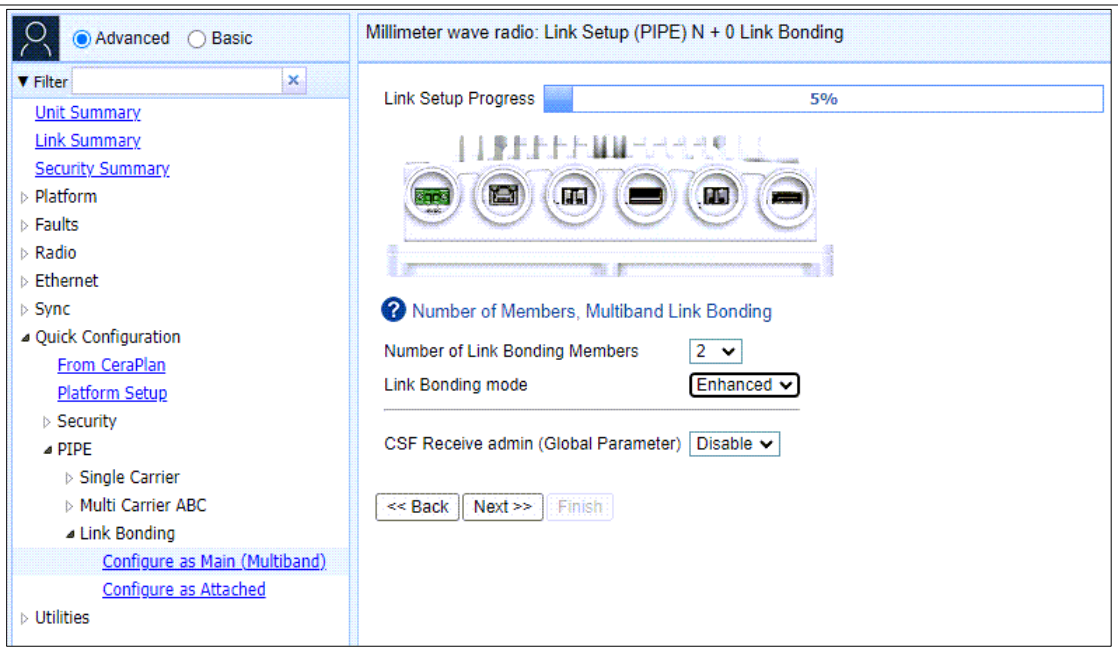


Figure 115: Multiband Link Bonding Quick Configuration Wizard – Number of Members Page

11 In the **Number of Link Bonding Members** field, select 2.
12 In the **Link Bonding Mode** field, select **Standard** or **Enhanced**. Enhanced mode is required for configurations that use a single cable to transmit traffic and L2 protocol data between the main and paired units.

Note: Although most PTP 850C and PTP 850E devices support Enhanced Link Bonding mode, some do not. For details.

13 In the **CSF Received Admin (Global Parameter)** field, if you selected Enhanced mode, you must select **Enable**, which is required for Link Bonding Enhanced mode.
If you selected Standard mode, you can select **Enable** or **Disable**.
14 Click **Next**. The Member #1 page of the Multiband Link Bonding Quick Configuration wizard opens.

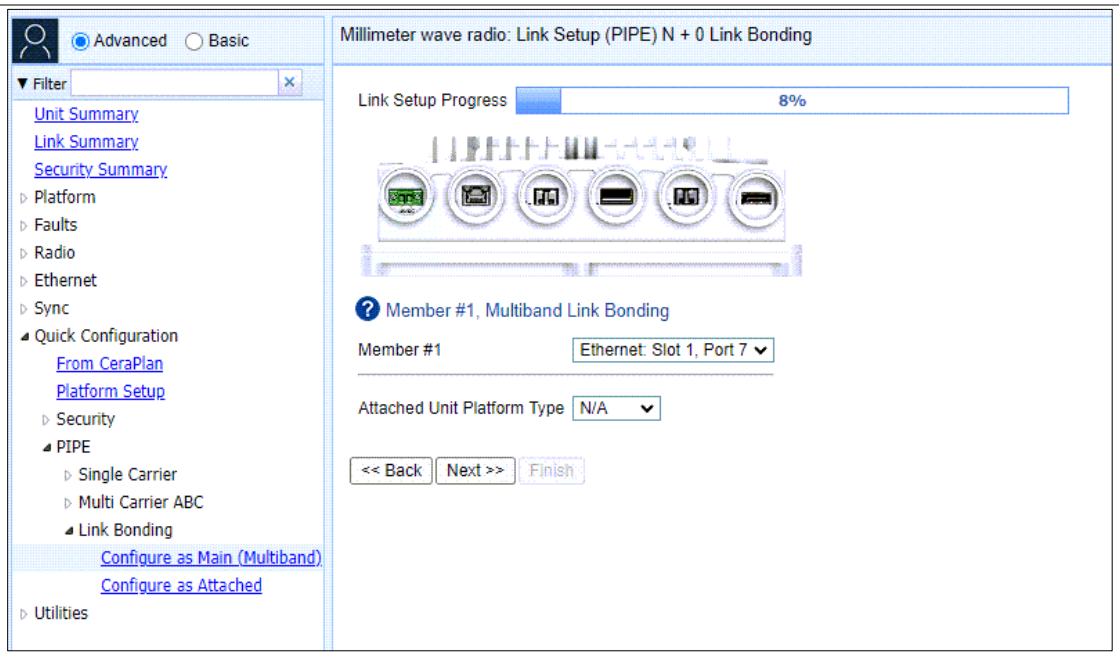


Figure 116: Multiband Link Bonding Quick Configuration Wizard – Member #1 Page

15 In the **Attached Unit Platform Type** field, select the type of device connected to the main unit as the paired (attached) unit.

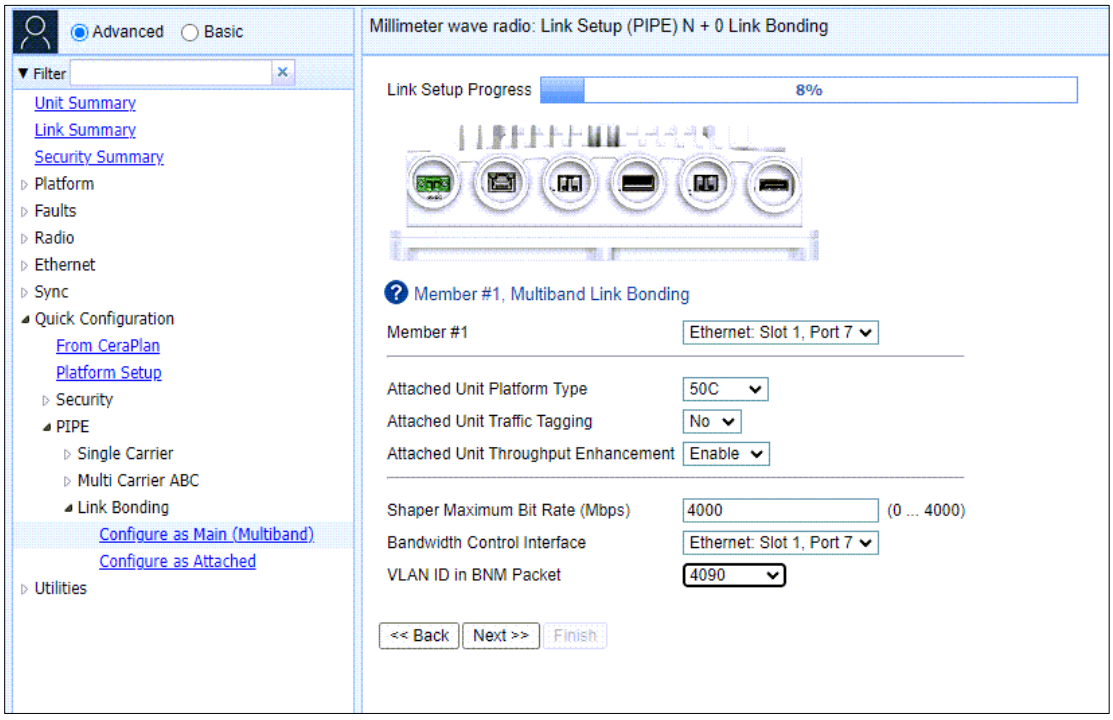


Figure 117: Multiband Link Bonding Quick Configuration Wizard – Member #1 Page (Single-Cable Configuration)

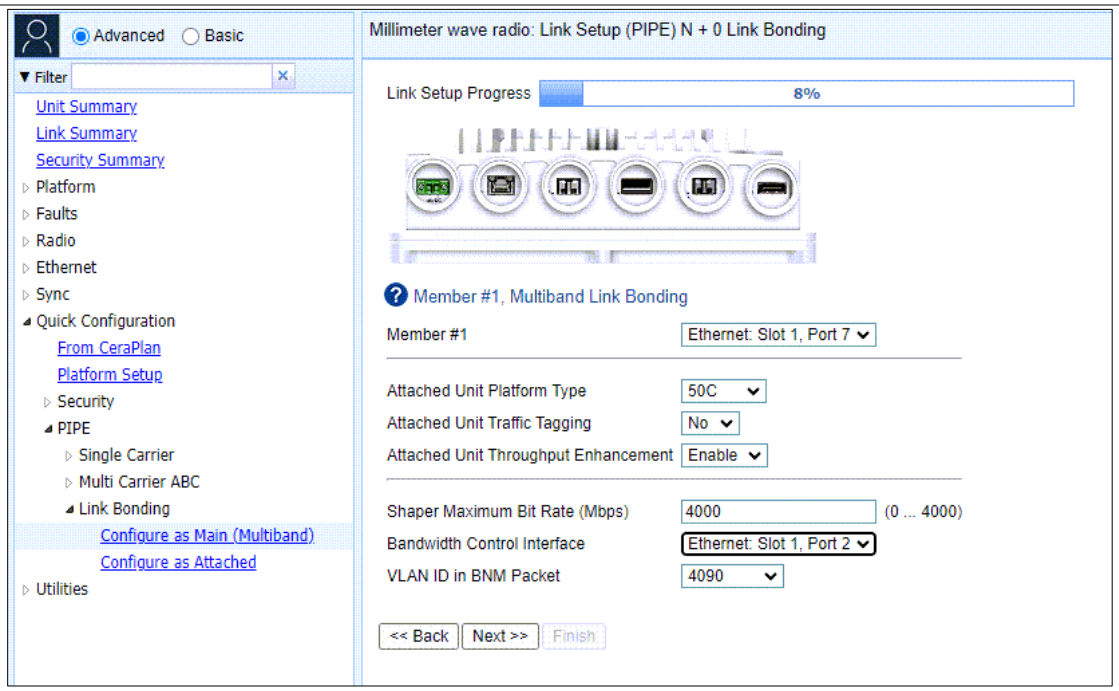


Figure 118: Multiband Link Bonding Quick Configuration Wizard – Member #1 Page (Two-Cable Configuration)

16 In the **Member #1** field, select Ethernet: Slot 1, Port 7. This is the port connected to the paired unit for passing traffic between the two units.
17 In the **Attached Unit Traffic Tagging** field: select **No**.
18 In the **Attached Unit Throughput Enhancement** field, enter **Enable** or **Disable** according to the configuration you intend to do on the paired unit. This enables the main unit to properly calculate the internal Link Bonding parameters.

Important Note: This field ***does not*** actually configure Throughput Enhancement on the attached unit. You must perform the paired unit's configuration directly on the paired unit itself. See

Configuring a Paired (Attached) Unit in a Layer 1 Link Bonding Group.

19 In the **Shaper Maximum Bit Rate** field, configure the maximum bit rate. The device uses this value to calculate the L1 Header Compensation. You must set the **Shaper Maximum Bit Rate** field according to the maximum capacity of the link to ensure that the L1 Header Compensation is calculated correctly.
20 In the **Bandwidth Control Interface** field:

- For single-cable configurations, select the same port as displayed in the Member Location field (**Ethernet: Slot 1, Port 7**)
- For two-cable configurations, select the port to which the Protocols cable is connected.

21 In the **VLAN ID in BNM Packet** field, select a VLAN ID. You can use any available VLAN ID from 1 to 4090. This is the VLAN use to transfer protocol information between the two units.
22 Click **Next**. The Member #2 page of the Multiband Link Bonding Quick Configuration wizard opens.

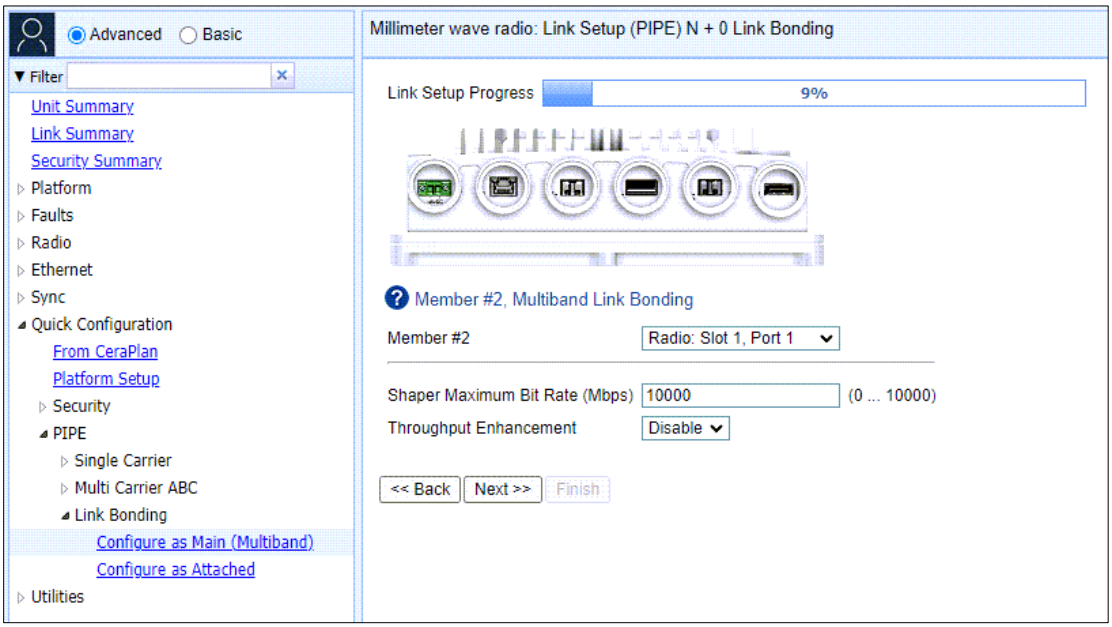


Figure 119: Multiband Link Bonding Quick Configuration Wizard – Member #2 Page

23 In the **Member #2** field, select Radio: Slot 1, Port 1.
24 In the **Shaper Maximum Bit Rate** field, configure the maximum bit rate. The device uses this value to calculate the L1 Header Compensation. You must set the **Shaper Maximum Bit Rate** field according to the maximum capacity of the link to ensure that the L1 Header Compensation is calculated correctly.
25 In the **Throughput Enhancement** field, you can enable Link Bonding Throughput Enhancement for the main unit. For detailed information about Throughput Enhancement.
26 Click **Next**. The Radio MRMC Script Configuration page of the Multiband Link Bonding Quick Configuration wizard opens.

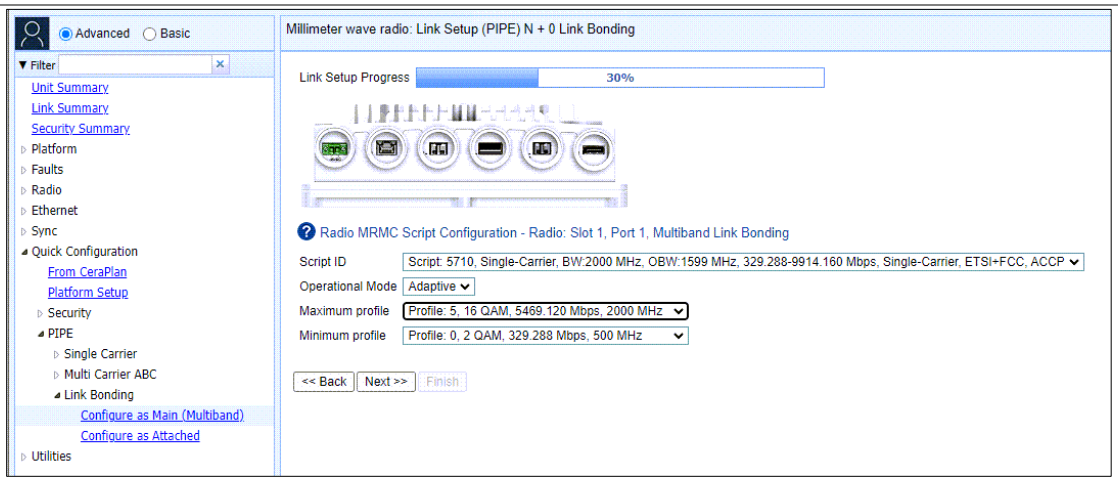


Figure 120: Multiband Link Bonding Quick Configuration Wizard – Radio MRMC Script Configuration Page

27 In the **Script ID** field, select the MRMC script you want to assign to the PTP 850E radio interface. For a full explanation of choosing an MRMC script.

28 In the **Operational Mode** field, select **Adaptive**. The following two fields are displayed:

- **Maximum profile** – Enter the maximum profile for the script.
- **Minimum profile** – Enter the minimum profile for the script.

Notes: Fixed mode is not supported for Multiband.

Make sure the **Maximum profile** and **Minimum profile** are set to different values.

29 Click **Next**. The Radio Parameters Configuration page of the Multiband Link Bonding Quick Configuration wizard opens.

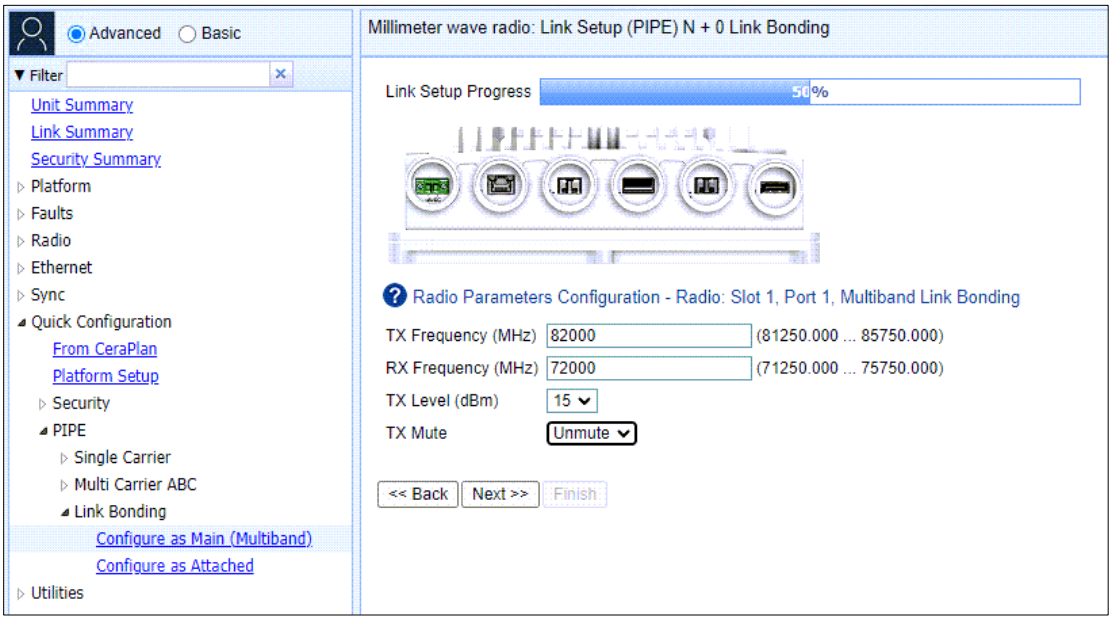


Figure 121: Multiband Link Bonding Quick Configuration Wizard – Radio Parameters Configuration Page

30 Configure the following radio parameters for the PTP 850E radio interface:

i In the **TX Frequency (MHz)** field, set the transmission radio frequency in MHz.
ii In the **RX Frequency (MHz)** field, set the received radio frequency in MHz.
iii In the **TX Level (dBm)** field, enter the desired TX signal level (TSL). The range of values depends on the frequency and RFU type.
iv To mute the TX output of the radio, select **Mute** in the **TX mute** field. To unmute the TX output of the radio, select **Unmute**.

31 Click **Next**. The Management Configuration page of the Multiband Link Bonding Quick Configuration wizard opens.

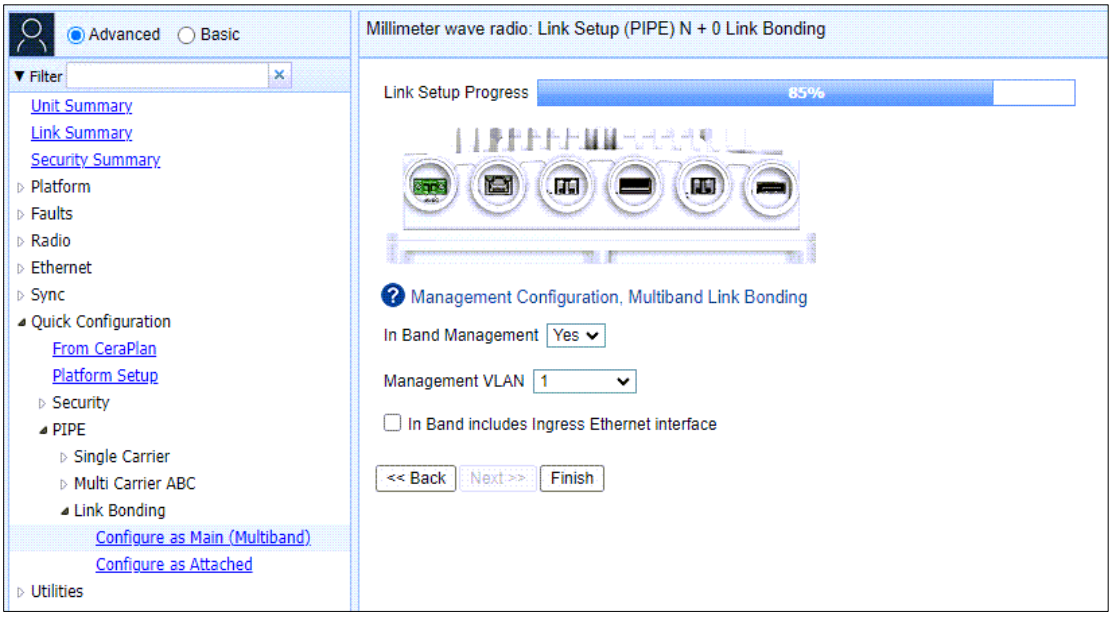


Figure 122: Multiband Link Bonding Quick Configuration Wizard – Management Configuration Page

32 In the **In Band Management** field, select **Yes** to configure in-band management, or **No** if you do not need in-band management. If you select **Yes**, the **Management VLAN** field appears.
33 If you selected **Yes** in the **In Band Management** field, select the management VLAN in the **Management VLAN** field.
34 If you want to use the Ethernet interface as well as the radio interface for in-band management, select **In Band includes Ethernet interface**.
35 If you want to manage the paired unit via in-band management, perform the following configurations on the paired unit:

i Enable in-band management.
ii Configure a management service point on Eth 2.

36 Click **Finish**. The Summary page opens. This page displays the parameters you have selected for the group.

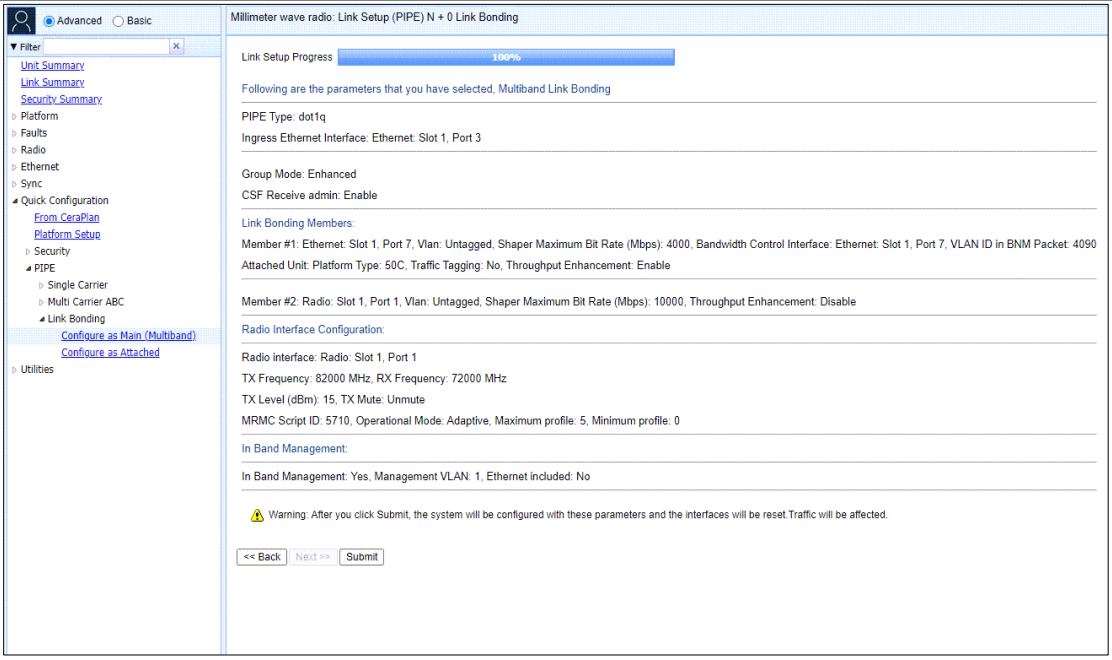


Figure 123: Multiband Quick Configuration Wizard – Summary Page

37 To complete configuration of the Multiband Link Bonding group on the PTP 850E, click **Submit**. If you want to go back and change any of the parameters, click **Back**.

38 In the Interface Manager, set the port connected to the paired unit for passing traffic between the two units to **Admin** = **Up**.

39 On the paired unit, you can use the Link Bonding – Configure as Attached wizard to configure the radio and Link Bonding parameters of the paired unit.

6.1.6 Configuring a Paired (Attached) Unit in a Layer 1 Link Bonding Group

You can use the Link Bonding – Configure as Attached wizard to configure the radio and Link Bonding parameters of a paired unit. This includes all-outdoor units in Link Bonding configurations with other all-outdoor units. It also includes all-outdoor units attached to an PTP 820N/PTP 820A. It does not include third-party devices, which must be configured manually.

Note: For PTP 820C and PTP 820C-HP, refer to the User Guide for PTP 820 All-Outdoor Products.

To configure an attached unit using the Quick Configuration wizard:

1 On the , select **Quick Configuration > PIPE > Link Bonding > Configure as Attached**. The Ethernet Selection page of the Quick Configuration wizard opens.

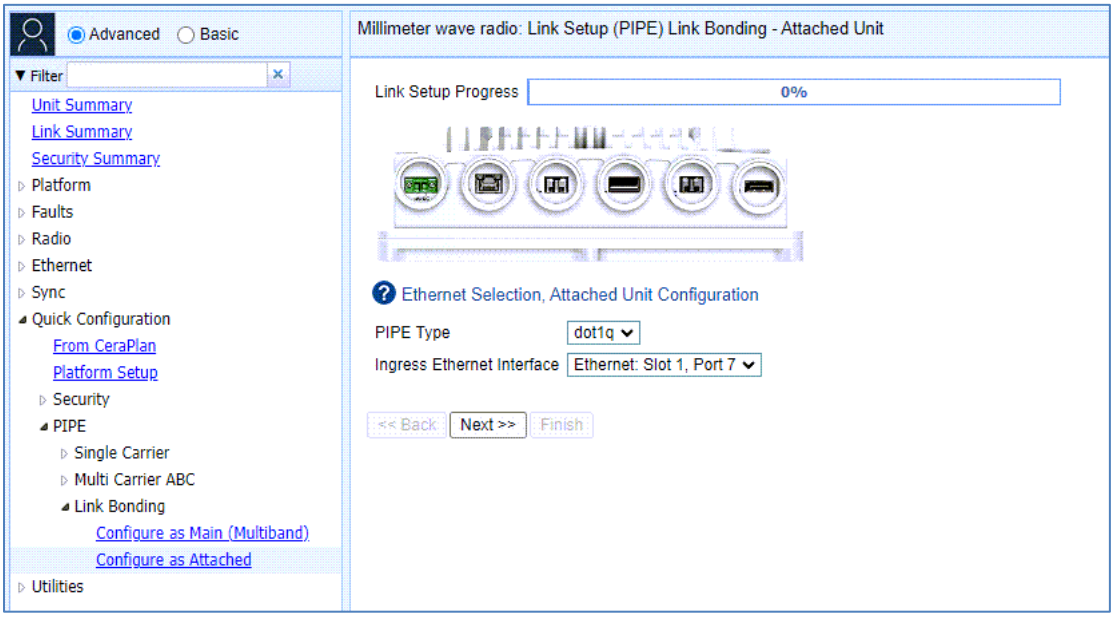


Figure 124: Link Bonding Attached Unit Quick Configuration Wizard – Ethernet Selection Page (PTP 850E)

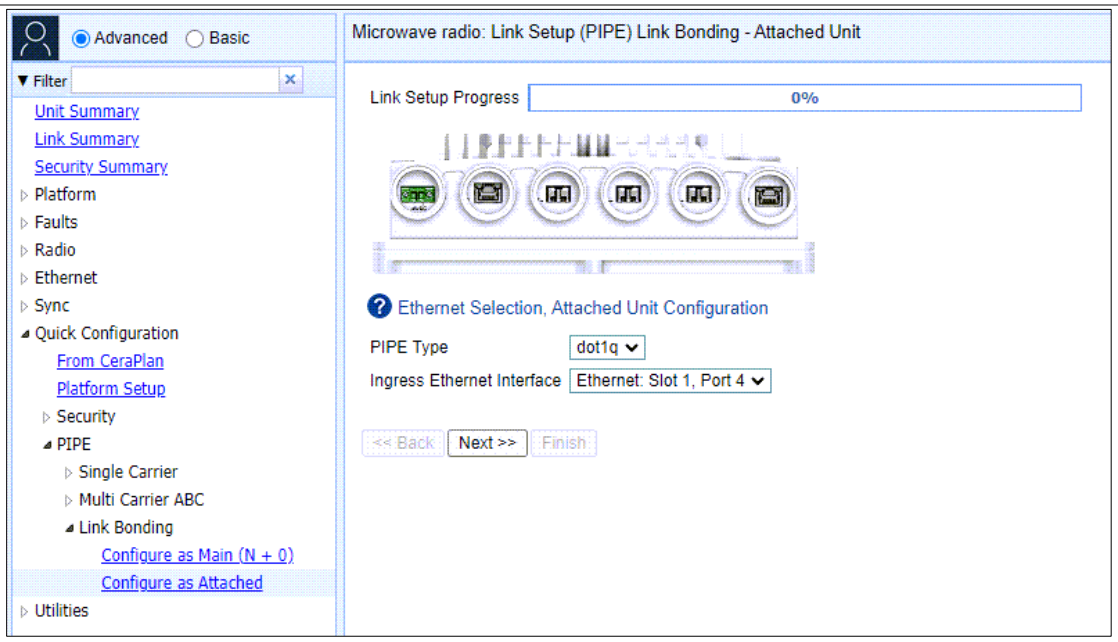


Figure 125: Link Bonding Attached Unit Quick Configuration Wizard – Ethernet Selection Page (PTP 850C)

2 In the **Pipe Type** field, select the Attached Interface type for the service that will transport traffic between the main and paired units. The only available option is **dot1q**.

Note: For a full explanation of Ethernet Services, service types, and attached interface types.

3 In the **Ingress Ethernet Interface** field, select the Ethernet interface on the paired unit connecting the paired unit to the main unit.

4 Click **Next**. The Radio/Multi Carrier ABC Interface page of the Quick Configuration wizard opens.

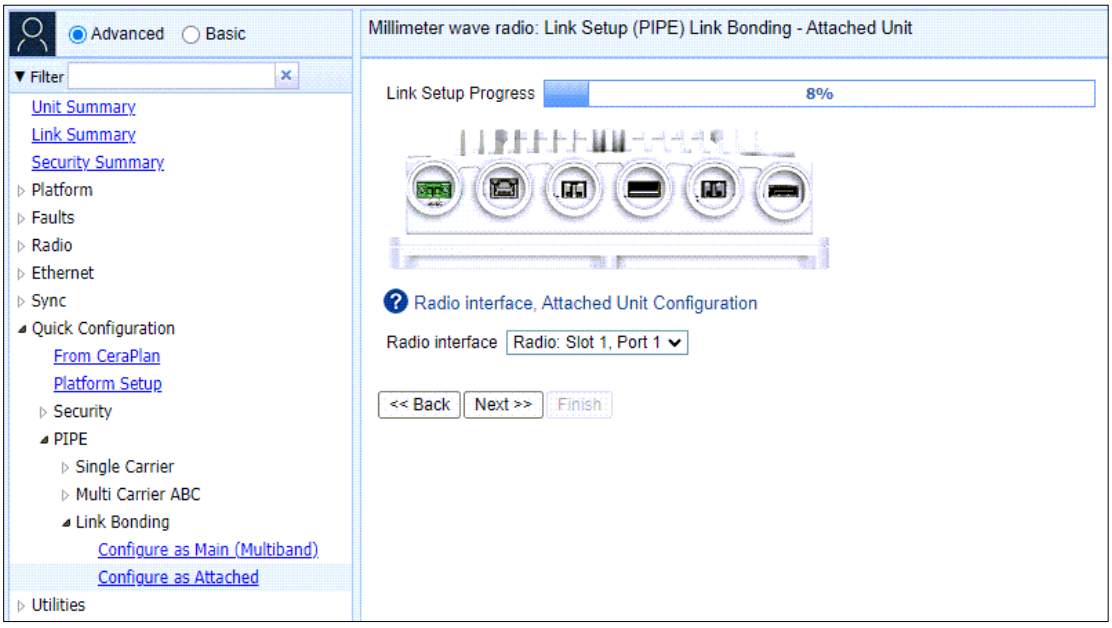


Figure 126: Link Bonding Attached Unit Quick Configuration Wizard – Radio/Multi Carrier ABC Interface Page (PTP 850E)

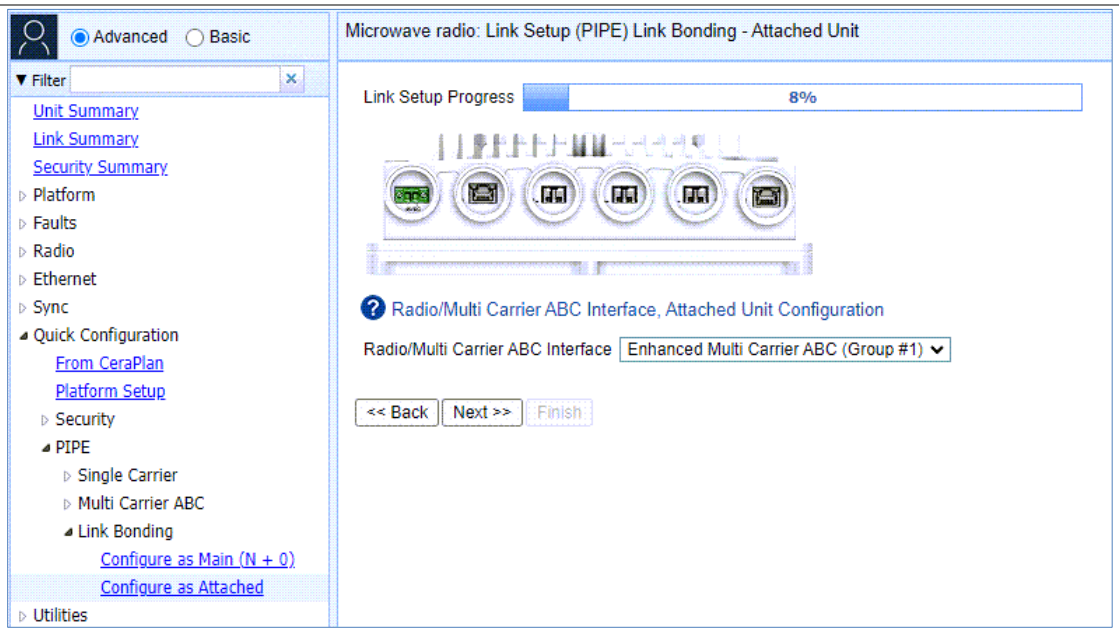


Figure 127: Link Bonding Attached Unit Quick Configuration Wizard – Radio/Multi Carrier ABC Interface Page (PTP 850C)

5 In the **Radio/Multi Carrier ABC Interface** field, select a radio interface or select **Multi-Carrier ABC (Unit, Group #1)** to create a Multi-Carrier ABC group and use it as the radio interface for Link Bonding traffic.
6 Click **Next**. For PTP 850C, the XPIC page of the Quick Configuration wizard opens.

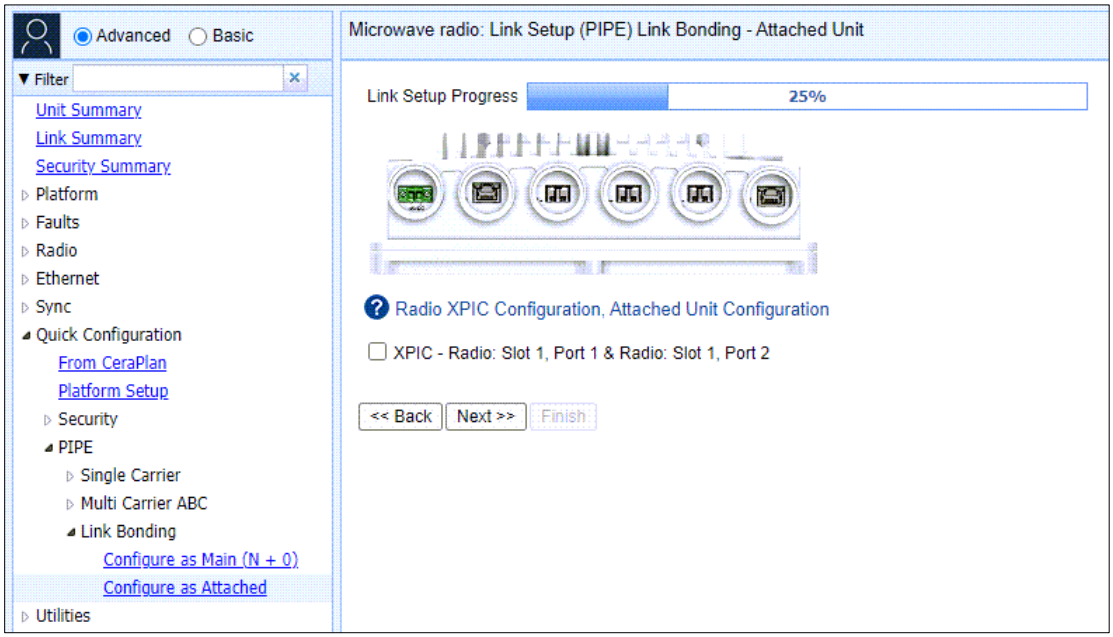


Figure 128: Link Bonding Attached Unit Quick Configuration Wizard – XPIC Page

7 To configure the radio carriers of the unit to operate in XPIC mode, select **XPIC**.
8 Click **Next**. The Radio MRMC Script Configuration page of the Quick Configuration wizard opens.

Note: If you selected XPIC, one set of MRMC parameters are displayed and are applied to both interfaces. If you did not select XPIC, two sets of MRMC parameters are displayed, one for each radio carrier.

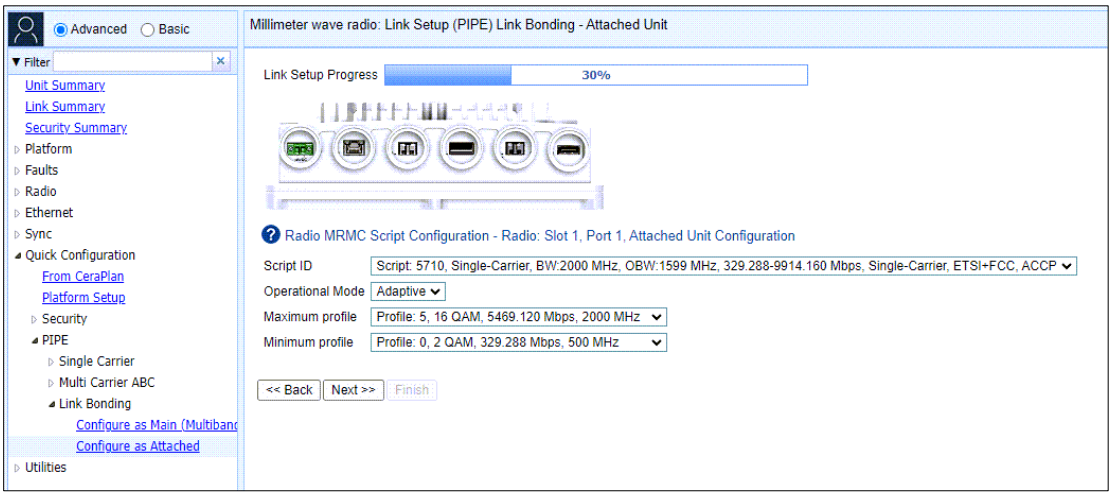


Figure 129: Link Bonding Attached Unit Quick Configuration Wizard – Radio MRMC Script Configuration Page (PTP 850E)

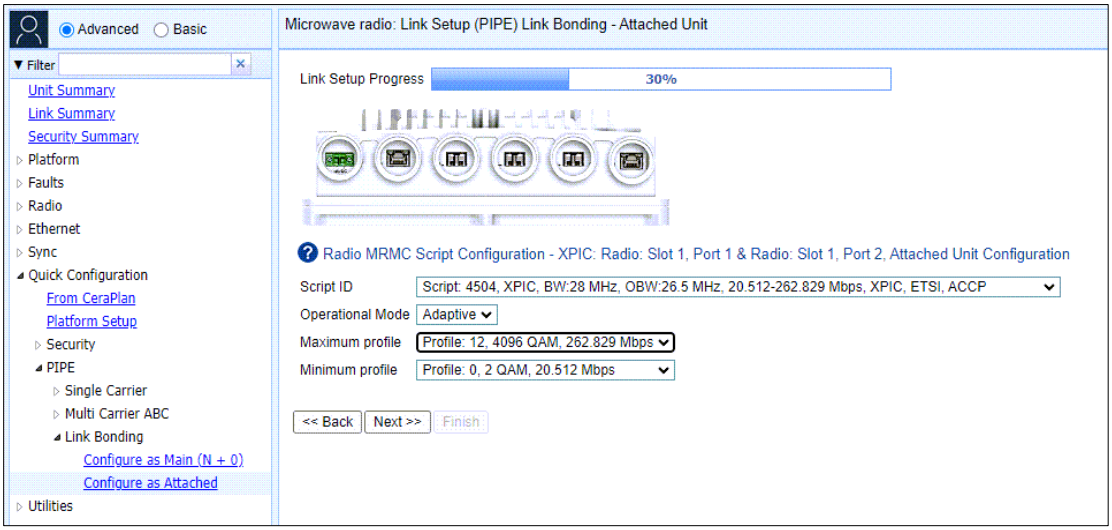


Figure 130: Link Bonding Attached Unit Quick Configuration Wizard – Radio MRMC Script Configuration Page (PTP 850C)

9 In the **Script ID** field, select the MRMC script you want to assign to the PTP 850E radio interface. For a full explanation of choosing an MRMC script.

10 In the **Operational Mode** field, select **Adaptive**. The following two fields are displayed:

- **Maximum profile** – Enter the maximum profile for the script.
- **Minimum profile** – Enter the minimum profile for the script.

Notes: Fixed mode is not supported for Multiband.

Make sure the **Maximum profile** and **Minimum profile** are set to different values.

11 Click **Next**. The Radio Parameters Configuration page of the Quick Configuration wizard opens.

Note: If you selected XPIC, one set of radio parameters are displayed and are applied to both interfaces. If you did not select XPIC, two sets of radio parameters are displayed, one for each radio carrier.

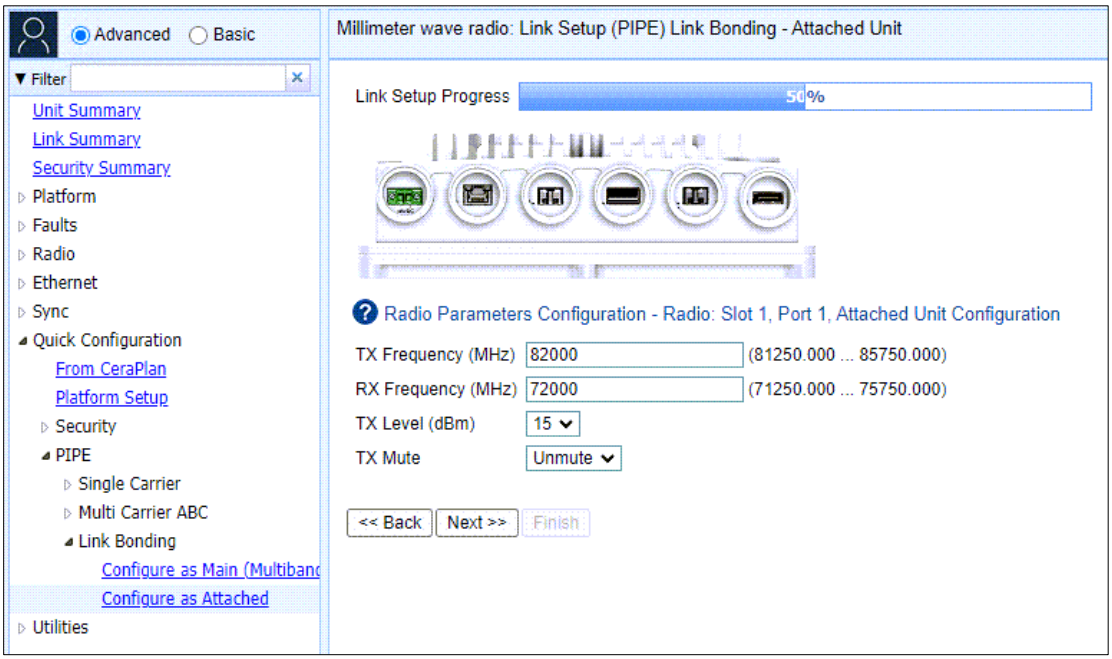


Figure 131: Link Bonding Attached Unit Quick Configuration Wizard – Radio Parameters Configuration Page (PTP 850E)

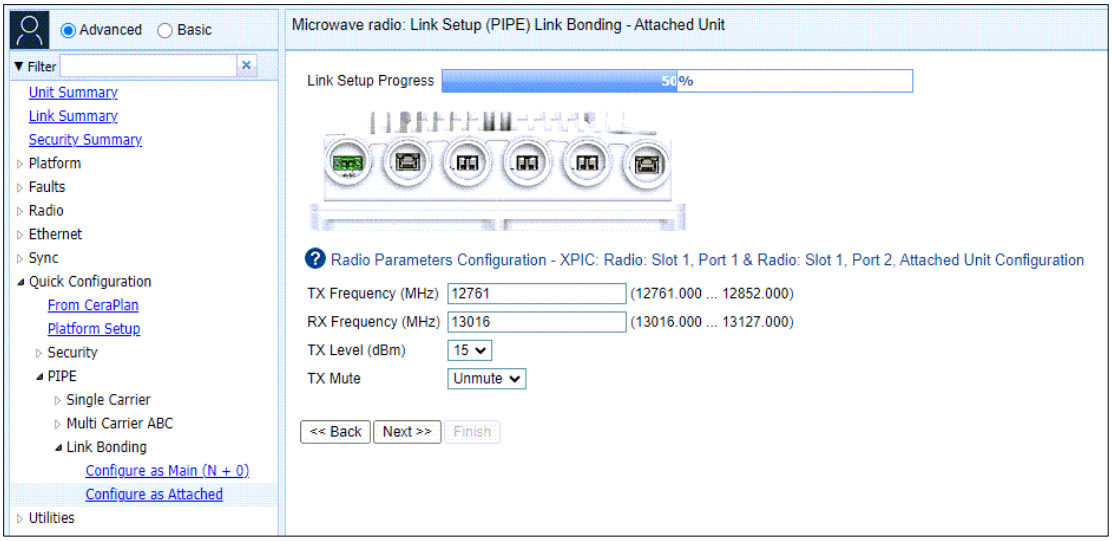


Figure 132: Link Bonding Attached Unit Quick Configuration Wizard – Radio Parameters Configuration Page (PTP 850C)

12 Configure the following radio parameters for the PTP 850E radio interface:

i In the **TX Frequency (MHz)** field, set the transmission radio frequency in MHz.
ii In the **RX Frequency (MHz)** field, set the received radio frequency in MHz.
iii In the **TX Level (dBm)** field, enter the desired TX signal level (TSL). The range of values depends on the frequency and RFU type.
iv To mute the TX output of the radio, select **Mute** in the **TX mute** field. To unmute the TX output of the radio, select **Unmute**.

13 Click **Next**. The Additional Parameters page of the Quick Configuration wizard opens.

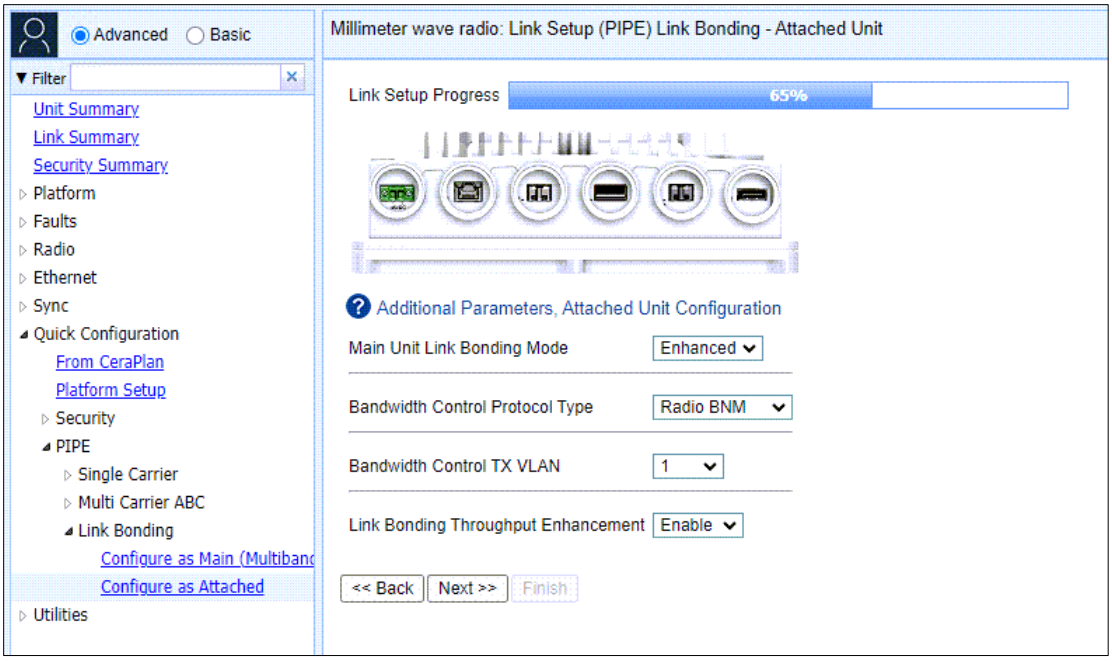


Figure 133: Link Bonding Attached Unit Quick Configuration Wizard – Additional Parameters Page (Enhanced Link Bonding Mode)

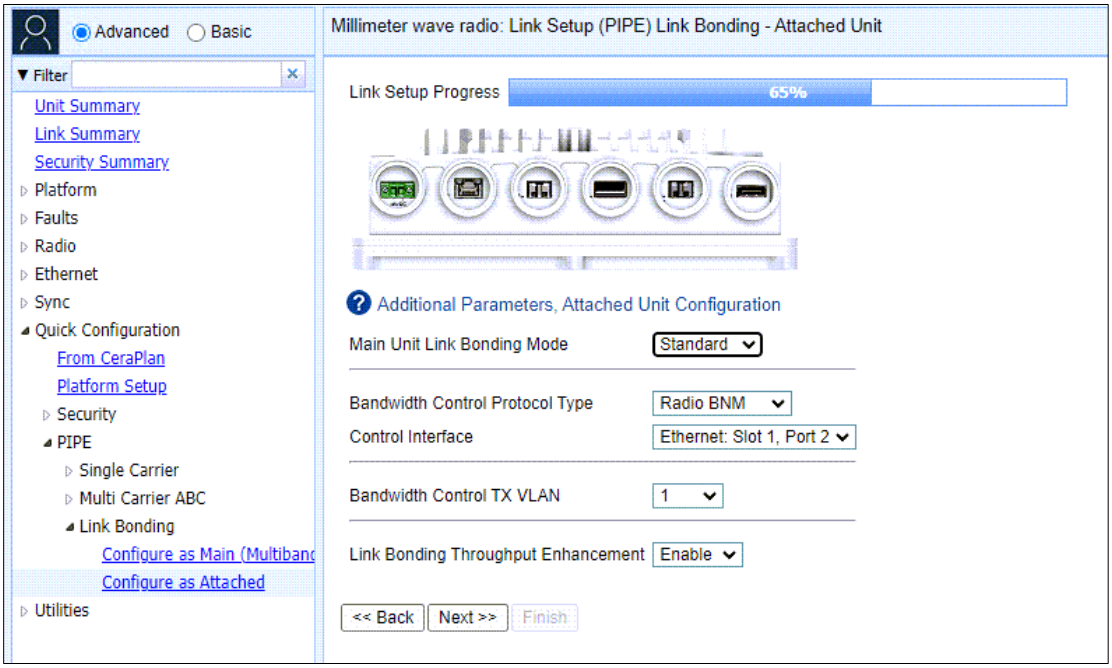


Figure 134: Link Bonding Attached Unit Quick Configuration Wizard – Additional Parameters Page (Standard Link Bonding Mode)

14 In the **Main Unit Link Bonding Mode** field, select **Standard** or **Enhanced**. Make sure to select the same mode as the mode configured on the Main unit.
15 In the **Bandwidth Control Protocol Type** field, select **Radio BNM**.
16 In the **Control Interface** field (Standard Mode only), select the port on the paired unit to which the Protocols cable is connected.

Note: In Enhanced mode, the device automatically assigns the same port configured in the **Ingress Ethernet Interface** field in Step 3.

17 In the **Bandwidth Control TX VLAN** field, select a VLAN ID. You can use any available VLAN ID from 1 to 4090. This is the VLAN used to transfer protocol information between the two units. Make sure to use the same VLAN configured as the **VLAN ID in BNM Packet** in the main unit.

18 In the **Throughput Enhancement** field, you can enable Link Bonding Throughput Enhancement for the paired unit. For detailed information about Throughput Enhancement, see:

- For 4+0 Layer 1 Link Bonding with PTP 850C, see Enabling Link Bonding Throughput Enhancement for 4+0 Layer 1 Link Bonding (CLI)

After configuring a Link Bonding node, it is recommended to enable Link Bonding Throughput Enhancement. Link Bonding Throughput Enhancement is available for the main unit only, not for the paired unit.

Link Bonding Throughput Enhancement is enabled on the main unit's Multi-Carrier ABC group. When it is enabled, the L2 Header Compensation for the group must be reduced by 12.

The Link Bonding Throughput Enhancement and L2 Header Compensation settings must be the same for the main units on both sides of the link. Therefore, the changes should be applied in the following order to ensure that management is not lost:

1 Enable Link Bonding Throughput Enhancement on the remote unit by entering the following commands:

```
root> multi-carrier-abc group-id 1 slot 1 type Enhanced
multi-carrier-abc enhanced-group-id [1] slot [1]> lb-throughput-
enhancement set admin enable
```

2 Enable Link Bonding Throughput Enhancement on the local unit by entering the following commands:

```
root> multi-carrier-abc group-id 1 slot 1 type Enhanced
multi-carrier-abc enhanced-group-id [1] slot [1]> lb-throughput-
enhancement set admin enable
```

3 Modify the L2 Header Compensation (decrease by 12) on the remote unit by entering the following commands:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]>ethernet link-bonding-member group-on-slot enhanced-
abc slot 1 group-id 1
lbg-member[enhanced-abc1/1]>admin set disable
lbg-member[enhanced-abc1/1]> l2-header-compensation edit l1-header-
compensation-enabled <yes|no> l2-header-compensation-value <(-63)-
63>
lbg-member[enhanced-abc1/1]>admin set enable
```

The l2-header-compensation-value parameter should be reduced by 12. For example, if the parameter was set to the default value of 26, change it to 14. To display the current parameter, enter the following command:

```
lbg-member[enhanced-abc1/1]> l2-header-compensation show
```

4 Modify the L2 Header Compensation (decrease by 12) on the local unit by entering the following commands:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]>ethernet link-bonding-member group-on-slot enhanced-abc slot 1 group-id 1
lbg-member[enhanced-abc1/1]>admin set disable
lbg-member[enhanced-abc1/1]> l2-header-compensation edit l1-header-compensation-enabled <yes|no> l2-header-compensation-value <(-63)-63>
lbg-member[enhanced-abc1/1]>admin set enable
```

The l2-header-compensation-value parameter should be reduced by 12. For example, if the parameter was set to the default value of 26, change it to 14. To display the current parameter, enter the following command:

```
lbg-member[enhanced-abc1/1]> l2-header-compensation show
```

- Enabling Link Bonding Throughput Enhancement for 4+0 Layer 1 Link Bonding.
- For Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP.
- For Multiband with Layer 1 Link Bonding.
- For XPIC with Layer 1 Link Bonding.

19 Click **Next**. The Management Configuration page of the Multiband Link Bonding Quick Configuration wizard opens.

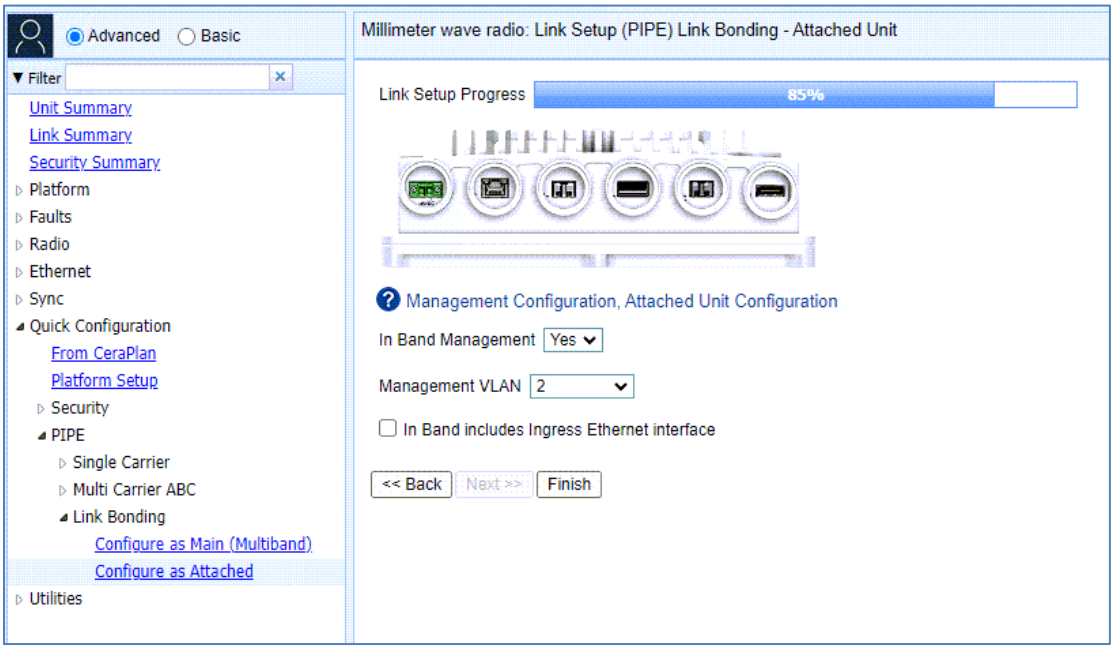


Figure 135: Multiband Link Bonding Quick Configuration Wizard – Management Configuration Page

20 In the **In Band Management** field, select **Yes** to configure in-band management, or **No** if you do not need in-band management. If you select **Yes**, the **Management VLAN** field appears.
21 If you selected **Yes** in the **In Band Management** field, select the management VLAN in the **Management VLAN** field.
22 If you want to use the Ethernet interface as well as the radio interface for in-band management, select **In Band includes Ethernet interface**.
23 Click **Finish**. The Summary page opens. This page displays the parameters you have selected for the group.

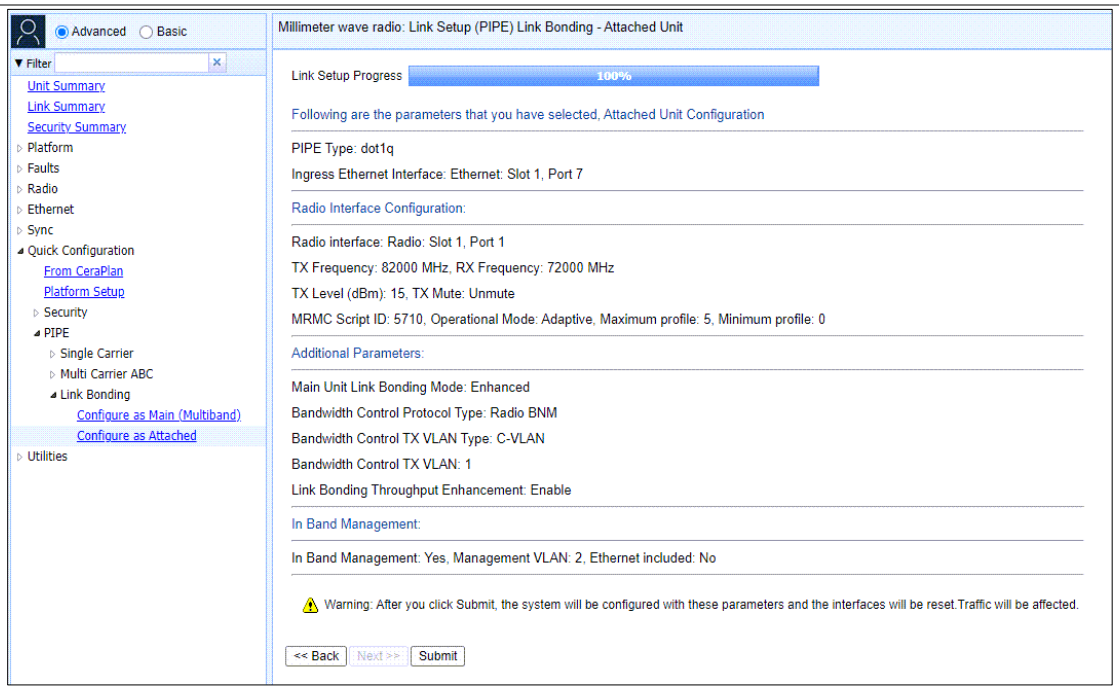


Figure 136: Multiband Quick Configuration Wizard – Summary Page

24 To complete configuration of the attached unit, click **Submit**. If you want to go back and change any of the parameters, click **Back**.

7. Configuring Links, Link Groups, and Unit Redundancy

This section provides instructions for configuring links, link groups, and Unit Redundancy manually, using Advanced mode.

Most link configurations can be configured using Quick Configuration wizards, and it is recommended to do so whenever possible.

This section includes:

- Configuring Multi-Carrier ABC
- Layer 1 Link Bonding Overview
- Configuring 4+0 Layer 1 Link Bonding
- Configuring Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C HP
- Configuring Multiband
- Configuring Multiband with Layer 1 Link Bonding
- Configuring Line Redundancy for Layer 1 Link Bonding Configurations
- Configuring XPIC
- Configuring Unit Redundancy
- Configuring Link Aggregation (LAG) and LACP

Configuring Multi-Carrier ABC

Note: This section is only relevant for PTP 850C.
Multi-Carrier ABC links can also be configured using the Quick Configuration wizard. It is recommended to use the wizard whenever possible.

This section includes:

- Multi-Carrier ABC Overview
- Configuring a Multi-Carrier ABC Group
- Adding and Removing Group Members
- Deleting a Multi-Carrier ABC Group

7.1.1 Multi-Carrier ABC Overview

Multi-Carrier Adaptive Bandwidth Control (ABC) enables multiple separate radio carriers to be shared by a single Ethernet port. This provides an Ethernet link over the radio with the total sum of the capacity of all the radios in the group, while still behaving as a single Ethernet interface. In Multi-Carrier ABC mode, traffic is dynamically divided among the carriers, at the Layer 1 level, without requiring Ethernet Link Aggregation.

Load balancing is performed regardless of the number of MAC addresses or the number of traffic flows. During fading events which cause ACM modulation changes, each carrier fluctuates independently with hitless switchovers between modulations, increasing capacity over a given bandwidth and maximizing spectrum utilization. The result is close to 100% utilization of radio resources in which traffic load is balanced based on instantaneous radio capacity per carrier.

Note that in a Multi-Carrier ABC group in which all carriers are operating at the minimum ACM profile:

- As long as at least one carrier is operating without BER or LOF, the link will continue to pass traffic even if the other carrier is in BER or LOF state. The carrier in BER or LOF state is removed from the group until the BER or LOF state has been resolved.
- If both carriers are in BER or LOF state, traffic will not pass until at least one of the carriers returns to operation without BER or LOF.

One Multi-Carrier ABC group that includes both radio interfaces can be configured per unit. It is recommended to use the same radio script and ACM settings on both radio carriers in the Multi-Carrier ABC group.

Note: The QoS mode of the interface should be *Standard* when adding the interface to a Multi-Carrier ABC group. If the QoS mode is set to *Hierarchical* when it is added to the group, the QoS mode will automatically revert to *Standard*. It will then have to be re-set to *Hierarchical* after it has been added to the group.

Configuring a Multi-Carrier ABC Group

To configure a Multi-Carrier ABC group:

1 Select **Radio > Groups > Multi Carrier ABC**. The Multi Carrier ABC page opens.

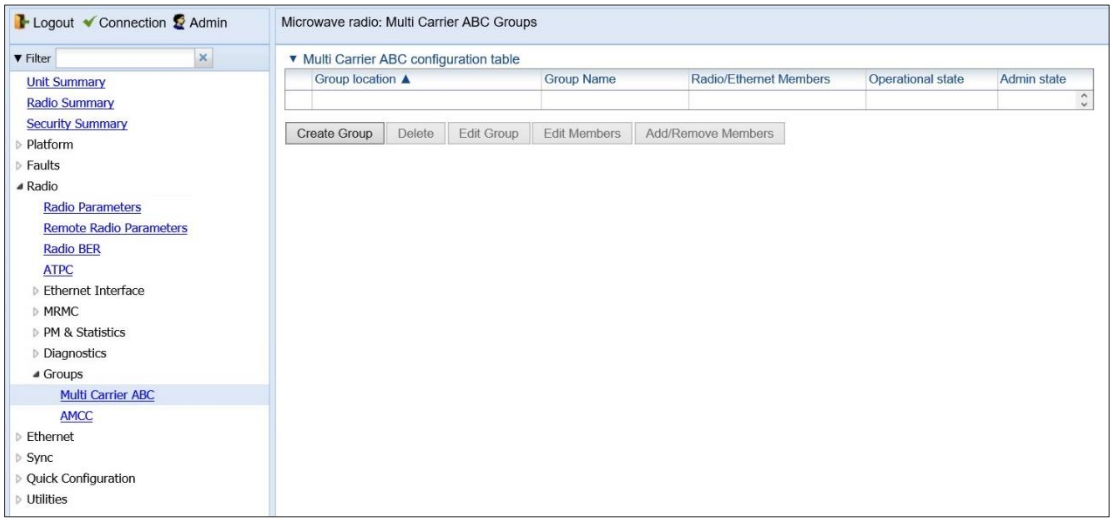


Figure 89: Multi-Carrier ABC Group Page (Empty)

2 Click **Create Group**. The first page of the Create ABC Group wizard opens.

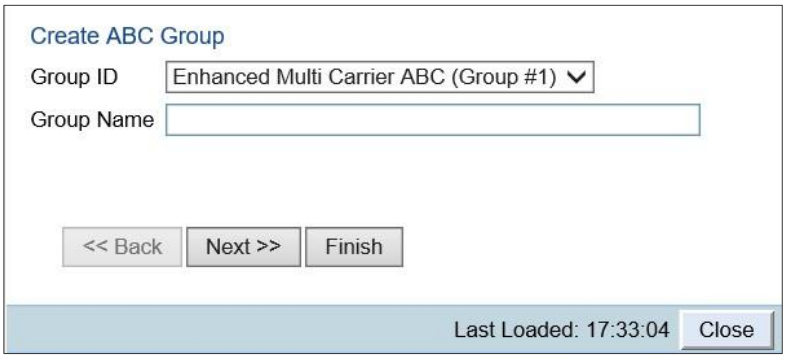


Figure 90: Create ABC Group Wizard – Group Name

3 Optionally, enter a descriptive name for the group in the **Group Name** field.

4 Click **Next**. The next page of the Create Group wizard opens.

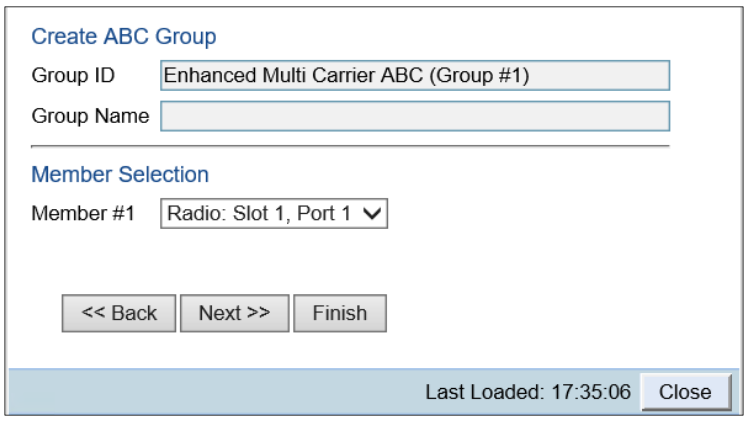


Figure 91: Create ABC Group Wizard – Member Selection 1

5 In the **Member 1** field, select a radio interface.

6 Click **Next**. The next page of the Create Group wizard opens.

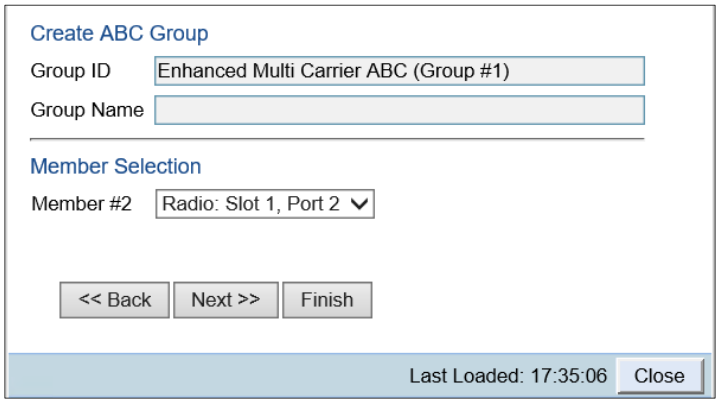


Figure 92: Create ABC Group Wizard – Member Selection 2

7 In the **Member 2** field, select a radio interface.

8 Click **Next**. A summary page opens.

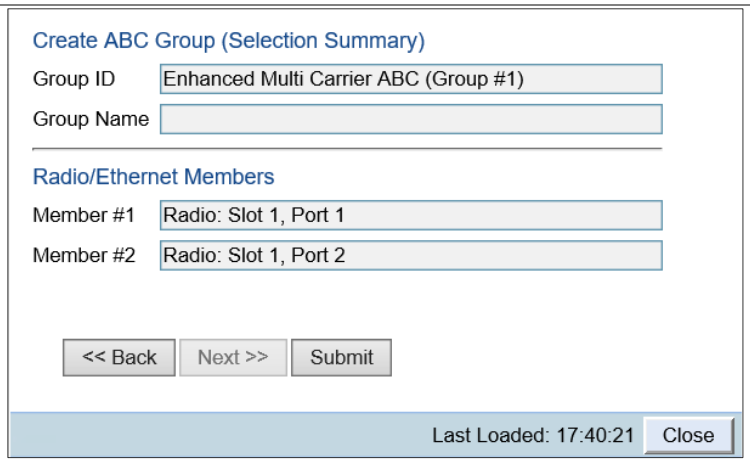


Figure 93: Create ABC Group Wizard – Summary Page

9 Click **Submit**. A message appears indicating whether or not the operation was successful.

10 Click **Close** to close the Create Group wizard. You must click **Submit** before clicking **Close**, or the selections you made will be discarded and the process cancelled.

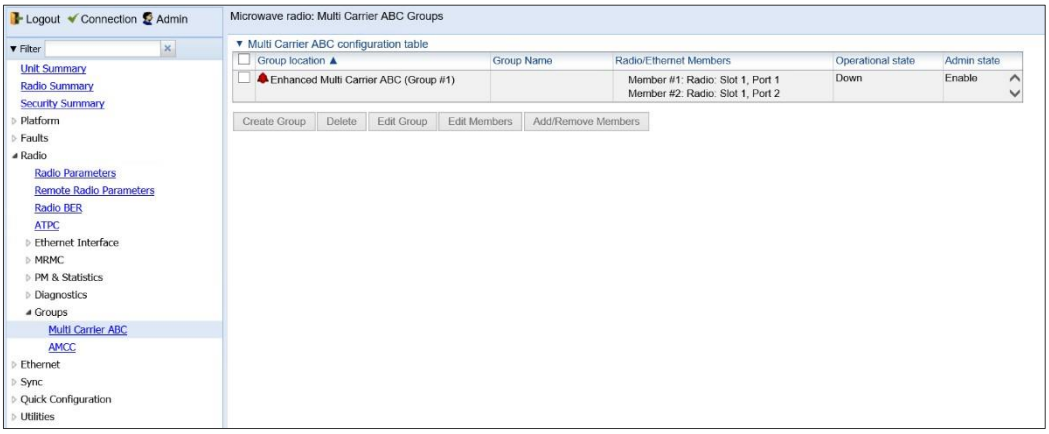


Figure 94: Multi-Carrier ABC Group Page (Populated)

Adding and Removing Group Members

You can add and remove interfaces from the group after creating the group. This is relevant if you want to delete a Multi-Carrier ABC group, since you must remove the members individually before deleting the group.

To remove interfaces:

1 Select the group in the Multi-Carrier ABC table and click **Add/Remove Members**. The Add/Remove Members page opens.

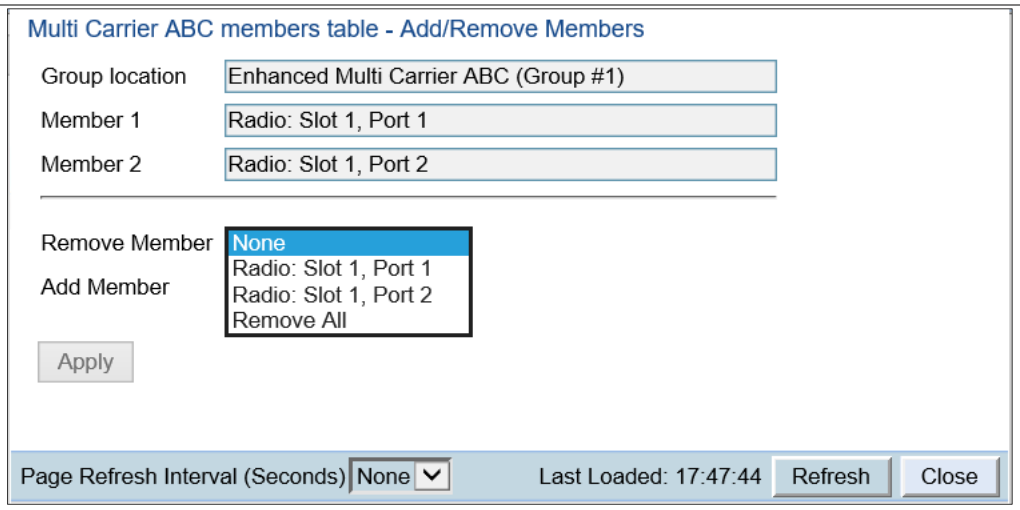


Figure 95: Multi Carrier ABC Group - Add/Remove Members Page

2 Select a member in the **Remove Member** field or select **Remove All**.

3 Click **Apply**.

4 Repeat these steps to remove additional members from the group.

Deleting a Multi-Carrier ABC Group

To delete a Multi-Carrier ABC group:

1 Select **Radio > Groups > Multi Carrier ABC**. The Multi Carrier ABC page opens .

2 Select the group in the Multi-Carrier ABC table and click **Add/Remove Members**. The Add/Remove Members page opens.

3 Remove each member of the group. See *Adding and Removing Group Members*.

4 Click **Close** to close the Multi Carrier ABC – Add/Remove Members page.

5 Select the group and click **Delete**.

7.2 Layer 1 Link Bonding

This section explains Layer 1 Link Bonding and describes the available configurations and how to configure them. This section includes:

- **Error! Reference source not found.**
- **Error! Reference source not found.**
- Configuring 4+0 Layer 1 Link Bonding
- Enabling Link Bonding Throughput Enhancement
- Editing a Link Bonding Group or its Members
- Displaying Statistics for a Link Bonding Group
- Deleting a Link Bonding Group
- L1 and L2 Header Compensation Values
- Configuring Synchronization in a Link Bonding Node
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- Procedure for Configuring Third-Party Devices for Operation in Link Bonding Configurations

7.2.1 Layer 1 Link Bonding Overview

Layer 1 Link Bonding aggregates multiple radio carriers into a single link. The Link Bonding mechanism performs traffic distribution by segmenting and re-assembling the data stream and dividing it among the radio channels in the Link Bonding group. Each segment is a valid Ethernet packet with a proprietary header added.

All-outdoor Link Bonding configurations consist of a “main” unit and a “paired” unit. The main unit is attached to the external switch. A Link Bonding group must be configured on the main unit. The Link Bonding group must include the main Unit’s radio interface (PTP 850E) or Multi-Carrier ABC group (PTP 850C), along with the port carrying traffic between the main unit and the paired unit.

The main unit and the paired unit are connected to each other via a single cable or two cables to carry traffic and L2 protocol data between the two units.

In order to use a single cable for traffic and protocols, the Link Bonding group must be configured to Enhanced mode.

Note: Although most PTP 850C and PTP 850E devices support Enhanced Link Bonding mode, some do not. For details.

Details about which ports to use for the connection between the main and paired units are provided per configuration in the appropriate sections below.

The main unit performs traffic separation. Traffic separation is performed by segmenting and re-assembling the data stream. Each segment is a valid Ethernet packet with a proprietary header added.

Traffic is distributed symmetrically until a member of the Link Bonding group reaches its individual capacity, after which remaining traffic is passed via the remaining group member. If a member of a Link Bonding group goes down, traffic is automatically redistributed to the other member with no traffic loss.

The main and paired units are managed separately and independently. In-band management can be configured so that both units are managed over the link.

Line redundancy is available for certain Layer 1 Link Bonding configurations, as described further in Layer 1 Link Bonding and Line Redundancy.

7.2.2 Layer 1 Link Bonding and Line Redundancy

Line redundancy is available for the following Layer 1 Link Bonding configurations:

- 4+0 Layer 1 Link Bonding with PTP 850C
- Multiband PTP 850E and PTP 850C with Layer 1 Link Bonding

Line Redundancy means the external switch is connected to both the main and the attached units via an optical splitter. The optical splitter routes traffic between the Ethernet port on the external switch and an Ethernet port on both the main and the attached unit.

Optionally, Line Redundancy can include management redundancy for external management, using an additional split cable between the management ports of each unit and an external management station.

Note: Configurations with Line Redundancy should use Enhanced Link Bonding Mode and a single cable for traffic and protocols.

In normal operation, traffic and management pass only between the external switch and the main unit, and the interface between the switch and the attached unit is turned off. In the event of switchover, the link between the external switch and the attached unit is automatically activated by switching off the interface between the external switch and the main unit and switching on the interface between the external switch and the attached unit so that traffic and management are passed between the external switch and the attached unit.

A set of services for traffic and management must be configured on the attached unit in parallel to the services on the main unit. These services are configured in Operational state. The Line Redundancy mechanism deactivates the services in normal operating state based on the Line Redundancy role configurations, and activates them only in the event of switchover to support the flow of traffic and management from the external switch to the attached unit's radio.

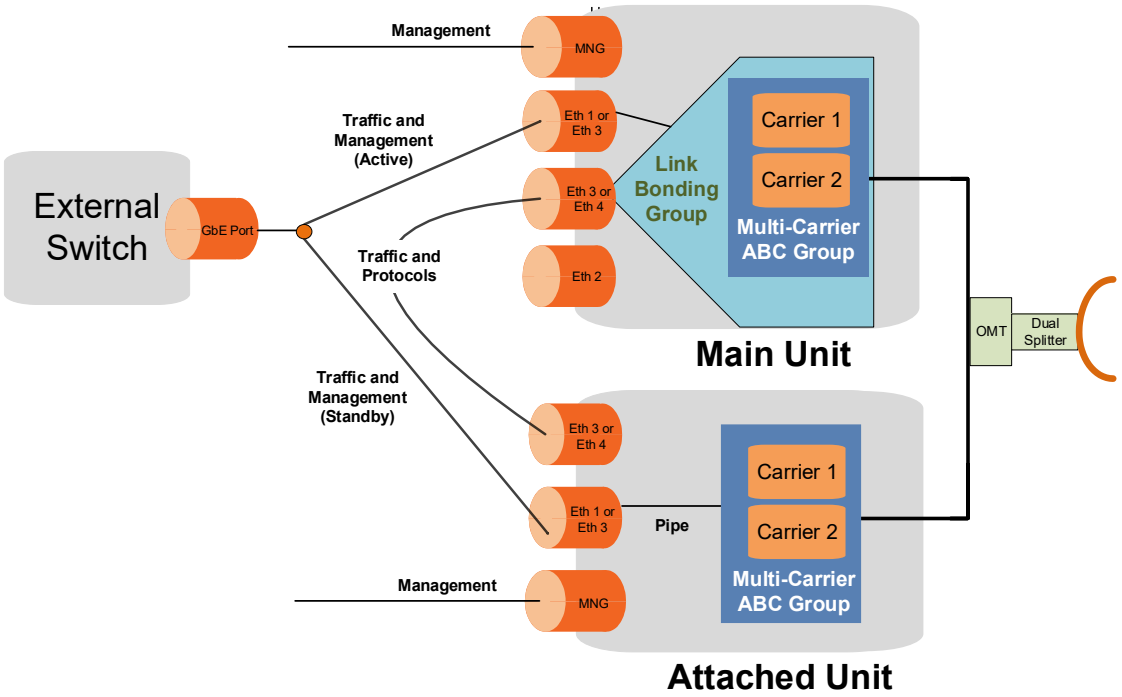


Figure 137: 4+0 PTP 850C with Layer 1 Link Bonding and Line Redundancy

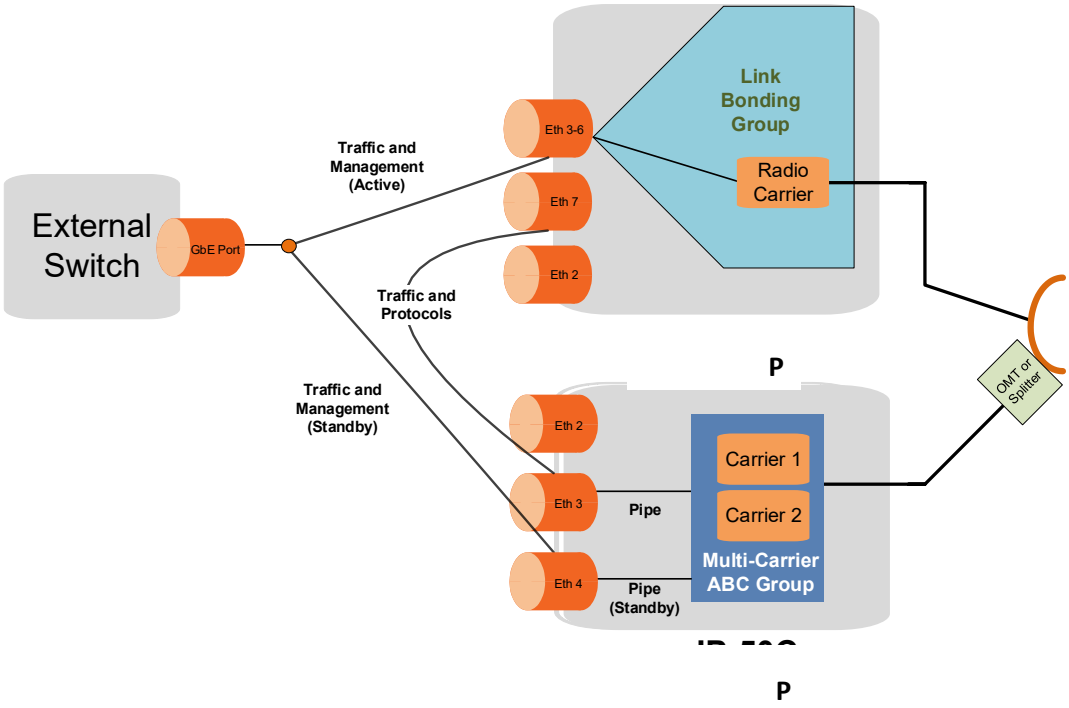


Figure 138: Multiband with Layer 1 Link Bonding and Line Redundancy – Multiband Antenna

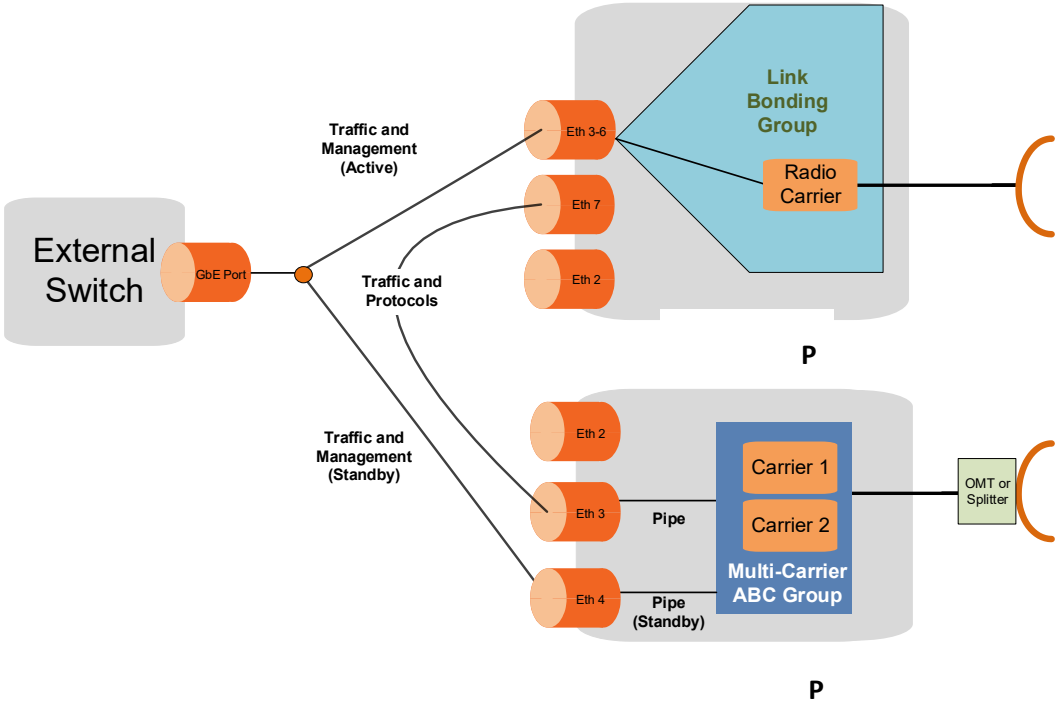


Figure 139: Multiband with Layer 1 Link Bonding and Line Redundancy – Separate Antennas

The following events trigger traffic switchover:

Note: Radio failure on the main unit does not trigger switchover. Since traffic continues to be passed between the main unit and the attached unit, the attached unit's radio link continues to operate.

- Failure of traffic cable between external switch and main unit:

- Traffic interfaces with the external switch on local and remote main units are automatically set to Down.
- Traffic services are automatically disabled on the local and remote main units.
- Traffic interfaces with the external switch on local and remote attached units are automatically set to Up.
- Traffic services are automatically enabled on the local and remote attached units.
- The management service points on the radio of the local and remote attached units are automatically enabled.

- Traffic cable between the main and attached unit fails:
  - The management service points on the radio of the local and remote attached units are automatically enabled.
  - On the remote side of the link, the interfaces connecting the traffic cable between the main and attached unit are automatically set to Down.
- Failure of main unit:
  - Traffic interfaces with the external switch on the remote main unit is automatically set to Down.
  - Traffic services are automatically disabled on the remote main unit.
  - Traffic interfaces with the external switch on local and remote attached units are automatically set to Up.
  - Traffic services are automatically enabled on the local and remote attached units.
  - The management service points on the radio of the local and remote attached units are automatically enabled.
  - On the remote side of the link, the interfaces connecting the traffic cable between the main and attached unit are automatically set to Down.

When the failure is rectified, the configuration automatically reverts to its normal operational configuration after expiration of a Wait to Restore (WTR) timer. Revertive mode cannot be disabled. However, the WTR timer is user-configurable.

Lockout and forced switch are available to manually change the state of the configuration (force-switch) or to manually force the configuration to remain in its current state (lockout). Lockout can be used to override Revertive mode and keep the configuration in switchover mode, should this be necessary.

Redundancy for external management operates independently of Line Redundancy for traffic. Using a split management cable attached to the management ports of each unit and an external management station, you can ensure that external management remains available even if management connectivity to one of the units is lost.

The following table lists the cable recommended for external management redundancy.

Table 16: Cable for External Management Redundancy

Cable	Marketing Model	Description
Management Splitter Cable (P2 to P2 and External	CBL-PTP 820-EXT-PROT+MGMT	CABLE,RJ45F TO 2XRJ45,1.34M,CAT-5E,WITH MALE TO MALE CONNECTION

Cable	Marketing Model	Description
Management Station)		

With external management redundancy, only one management port is up at any one time. External management switching is independent of traffic switchover. The following events trigger external management switchover:

- Management interface failure
- Unit failure
- On main unit, Link Bonding group operational status is Down

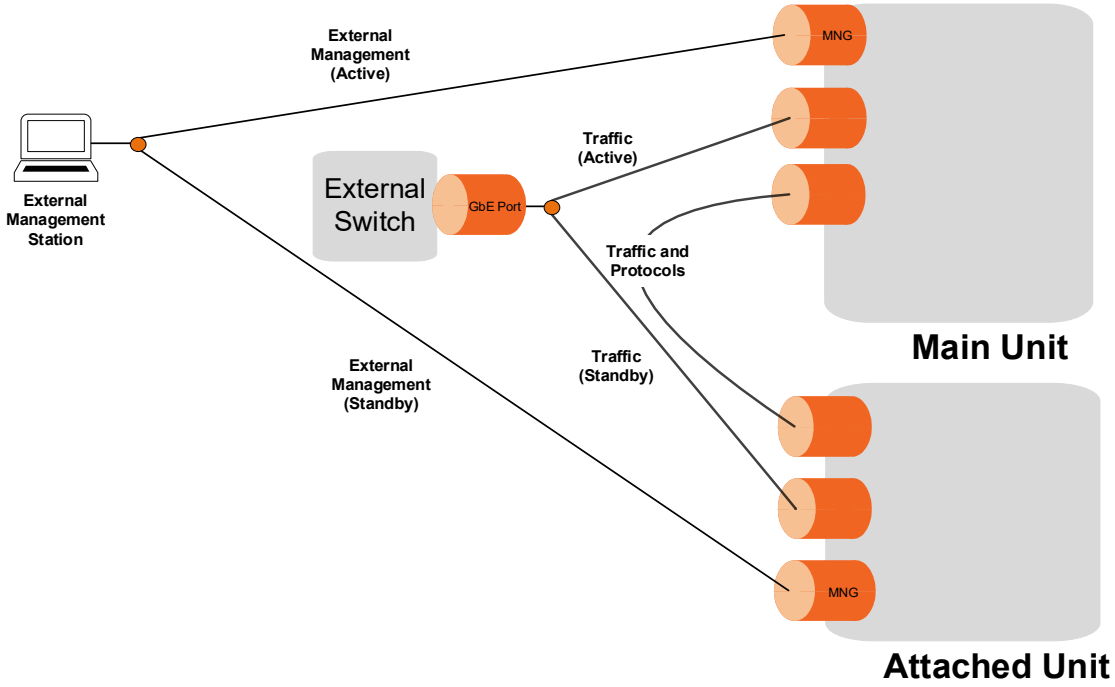


Figure 140: Layer 1 Link Bonding with Line and External Management Redundancy

For instructions on configuring Line Redundancy for configurations with Link Bonding.

7.2.3 Requirements and Limitations for Enhanced Link Bonding Mode

Enhanced Link Bonding mode is required for configurations that use a single cable to carry traffic and L2 protocol data between and main unit and the paired unit. There are several requirements and limitations for Enhanced Link Bonding Mode, as described below.

7.2.3.1 Hardware Requirements for Enhanced Link Bonding Mode

The main unit most support a single-cable configuration. Most PTP 850C and PTP 850E devices support a single-cable configuration. However, some units produced prior to the middle of 2021 may not. It is possible to determine whether or not a particular PTP 850C or PTP 850E device supports this configuration by checking the **Enhanced Mode Supported** field in the General Parameters section

of the Link Bonding page. If the field displays **Yes**, the device supports the single-cable configuration.

If an PTP 850C or PTP 850E device does not support the single-cable configuration, the customer can contact a Cambium representative to discuss alternative solutions.

7.2.3.2 Enhanced Link Bonding Mode Limitations

Users must be aware of the following limitations when using Enhanced Link Bonding mode:

- Link Bonding groups must be configured to the same Link Bonding mode on both sides of the link. In other words, a Link Bonding group configured for Standard mode can only operate with another Link Bonding group configured for Standard mode and a Link Bonding group configured for Enhanced mode can only operate with another Link Bonding group configured for Enhanced mode.
- When a Link Bonding group is configured for Enhanced mode, the interfaces in the group are displayed as Logical Interfaces and services can be configured on these interfaces. This is to enable configuration of protocols on these interfaces. Make sure to avoid configuring traffic services on interfaces that belong to a Link Bonding group; traffic services should only be configured on the Link Bonding group logical interface.

7.2.4 Link Bonding L1 Capacity Calculator

The main unit estimates the L1 capacity of the Link Bonding group and each group member, based on:

- Current radio bandwidth
- Average frame size (user-configurable)

The capacity calculator estimates the potential capacity, not the actual current throughput. Using the capacity calculator has no impact on actual throughput.

7.2.4.1 Displaying Estimated Capacity via the Web EMS

In the Web EMS, the current estimated potential L1 capacity appears in the Capacity column of the Link Bonding page. It also appears in the Link Bonding – Edit page.

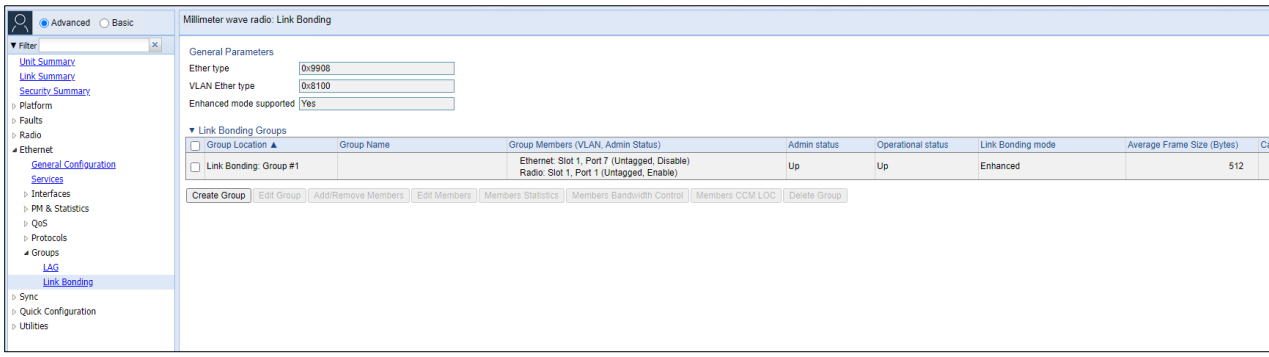


Figure 141: Link Bonding Page (Multiband)

To display the current estimated potential L1 capacity per group member, click **Edit Members** in the Link Bonding page.

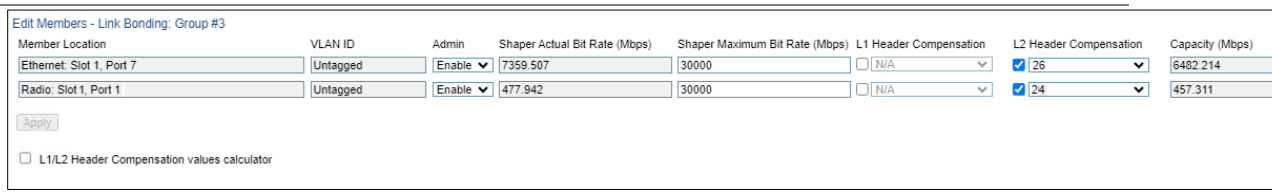


Figure 142: Link Bonding Edit Members Page (Multiband)

The **Average Frame Size** field in the Link Bonding page displays the currently configured average frame size. The default is 512 bytes.

To change the average frame size, select the group and click **Edit** to open the Link Bonding Groups – Edit page. Enter the size you want, in bytes, in the **Average Frame Size** field and click **Apply**. You can enter a value between 64 and 9612.

Note: The **Average Frame Size** does not affect the actual transmitted traffic It is only used to help estimate the current potential capacity.

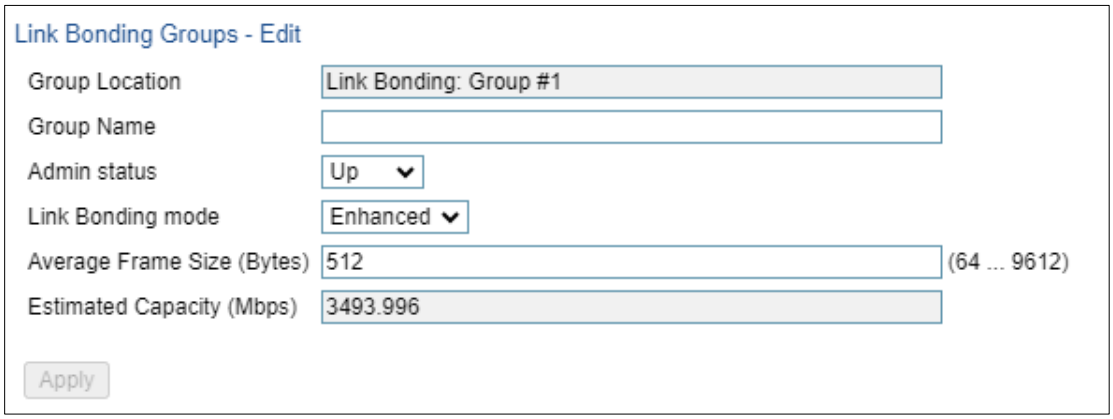


Figure 143: Link Bonding Edit Page

7.2.4.2 Displaying Estimated Capacity via the CLI

To display the current estimated potential L1 capacity for a Link Bonding group, enter the following command in group view:

```
eth group [lbx]>capacity show
```

For example the following commands display the current estimated potential L1 capacity for Link Bonding group

```
root>ethernet interfaces group lb1
eth group [lb1]>capacity show
```

To display the currently configured average frame size, enter the following command in group view:

```
eth group [lbx]>average_packet_size show
```

To change the average frame size, enter the following command in group view:

```
eth group [lbx]> average_packet_size set <64-9612>
```

To display the current estimated potential L1 capacity for a group member, enter the following command in group member view:

```
lbg-member[]> capacity show
```

For example, the following commands display the current estimated potential L1 capacity for Eth 4 that belongs to Link Bonding group 1:

```
root>ethernet interfaces group lb1
eth group [lb1]> ethernet link-bonding-member interface eth slot 1 port 4
eth group [lb1]>capacity show
```

The following commands display the current estimated potential L1 capacity for Multi-Carrier ABC group 1 that belongs to Link Bonding group 1:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]>ethernet link-bonding-member group-on-slot enhanced-abc slot 1
group-id 1
lbg-member[enhanced-abc1/1]> capacity show
```

7.2.5 Configuring Layer 1 Link Bonding



Note

Layer 1 Link Bonding links can also be configured using the Quick Configuration wizard. It is recommended to use the wizard whenever possible. For instructions:

For the main unit, see Configuring a Layer 1 Link Bonding Link Using the Quick Configuration Wizard

For the attached unit, see

Configuring a Paired (Attached) Unit in a Layer 1 Link Bonding GroupConfiguring a Multiband Link with Layer 1 Link Bonding Using the Quick Configuration Wizard

For configurations in which the PTP 850E is connected to a third-party device via the PTP 850E's Management port, make sure to reconfigure management according to the instructions in ***Error! Reference source not found.***. Failure to d o so will lead to loss of management and may lead to RMA at the customer's expense.

To configure a Layer 1 Link Bonding node:

1 Connect the external switch to the Ingress port on the main unit.
2 In the Interface Manager, make sure the port connected to the attached unit for passing traffic between the two units (the Traffic port) is set to **Admin** = **Down**. See Enabling the Interfaces (Interface Manager).
3 On both the main unit and the attached unit, configure the port speed of the Traffic port. The port speed must be the same on both units:

- PTP 850C + PTP 850C: 10 Gbps
- PTP 850C + PTP 850EX: 10 Gbps
- PTP 850C + PTP 820C or PTP 820C-HP: 1 Gbps
- PTP 850E + PTP 850C or PTP 850CX: 10 Gbps
- PTP 850E + PTP 820C or PTP 820C-HP: 1 Gbps.
- PTP 850E + third-party device: Whatever speed is appropriate for the third-party device, making sure the configuration is symmetrical for the main and attached units.
- PTP 850E 2+0 XPIC: 10 Gbps

  If the port speed is 1 Gbps and you are using an SFP port with an electrical SFP transceiver on an PTP 850C or PTP 850E, you must configure the port speed after adding the port to the Link Bonding group. Adding the port to the Link Bonding group automatically configures the port to 10G, which is not supported on SFP ports with electrical SFP transceivers. This is why you must set or reset the port speed to 1G after adding the port to the Link Bonding group.

  4 In the Interface Manager, set the port connected to the attached unit for passing traffic between the two units to **Admin** = **Down**. See Enabling the Interfaces (Interface Manager).
  5 If you are using a separate Protocols cable to carry L2 protocol data between the two units, set the speed of the port connected to the Protocols cable (the Protocols port) as follows:

- PTP 850C + PTP 850C: 2.5 Gbps
- PTP 850C + PTP 850EX: 1 Gbps or 2 Gbps, making sure the configuration is symmetrical for the main and attached units
- PTP 850C + PTP 820C or PTP 820C-HP: 1 Gbps
- PTP 850E + PTP 850C or PTP 850CX: 2.5 Gbps
- PTP 850E + PTP 820C or PTP 820C-HP: 1 Gbps.
- PTP 850E + third-party device: 1 Gbps or 2 Gbps, making sure the configuration is symmetrical for the main and attached units
- PTP 850E 2+0 XPIC: 2.5 Gbps

  6 Configure the script and radio settings for both the main unit and the attached unit, including XPIC.

  Note: If the attached unit is a third-party device, the radio must be configured to fixed mode, not ACM.

  7 In configurations where either the main or the attached unit, or both, are multi-carrier devices, configure Multi-Carrier ABC on the relevant devices. See **Error! Reference source not found.**.
  8 On the main unit only, configure a Link Bonding group that includes the Traffic port and the radio (single-carrier devices) or Multi-Carrier ABC group (multi-carrier devices):

  Note: Before adding a group member, make sure that no shapers or service points are configured on the interface or group.

  i Select **Ethernet** > **Groups** > **Link Bonding**. The Link Bonding page opens.

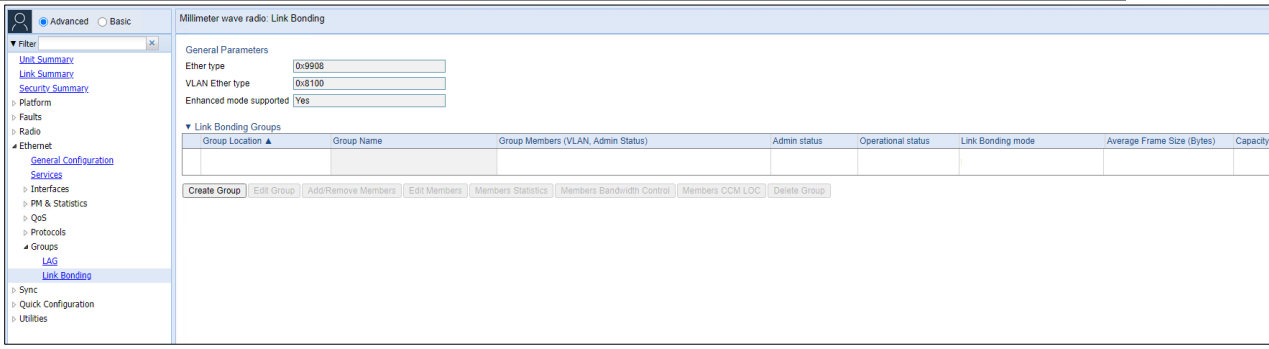


Figure 144: Link Bonding Page (Empty)

ii Click **Create Group**. Page 1 of the Link Bonding Group wizard opens.

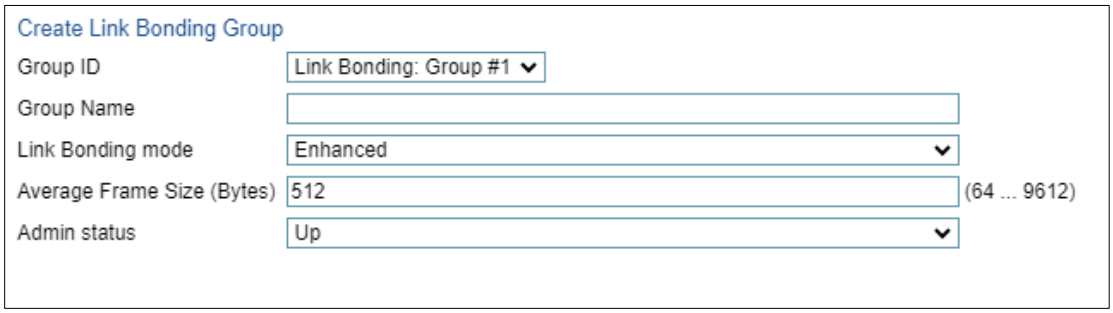


Figure 145: Link Bonding Group Wizard – Page 1

iii In the **Group ID** field, select **Link Bonding: Group #1**.
iv Optionally, in the **Group Name** field, enter a descriptive name for the group.
v In the **Link Bonding Mode** field, select **Standard** or **Enhanced**. You must select **Enhanced** if the configuration uses a single cable for traffic and L2 protocol data. See Requirements and Limitations for Enhanced Link Bonding Mode.
vi In the **Average Frame Size** field, enter a value for calculating the estimated current potential capacity. For an explanation of this field, see Link Bonding L1 Capacity Calculator.

Note: The **Average Frame Size** does not affect the actual transmitted traffic It is only used to help estimate the current potential capacity.

vii In the **Admin status** field, select **Up**.
viii Click **Next**. The Member #1 page opens.

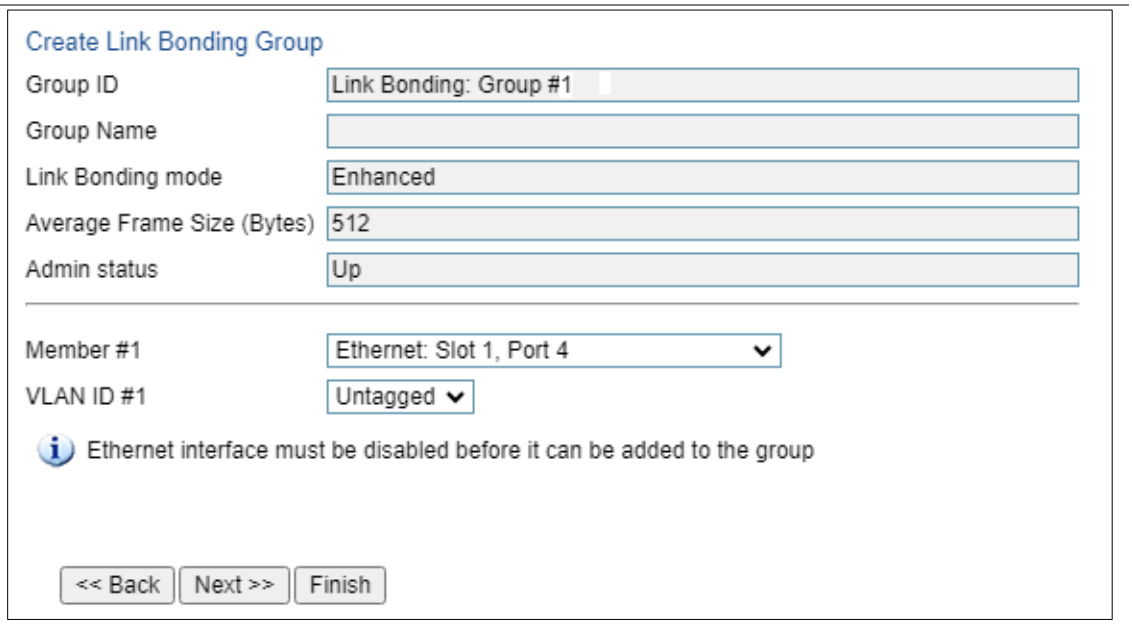


Figure 146: Link Bonding Group Wizard – Member #1 Page (PTP 850C)

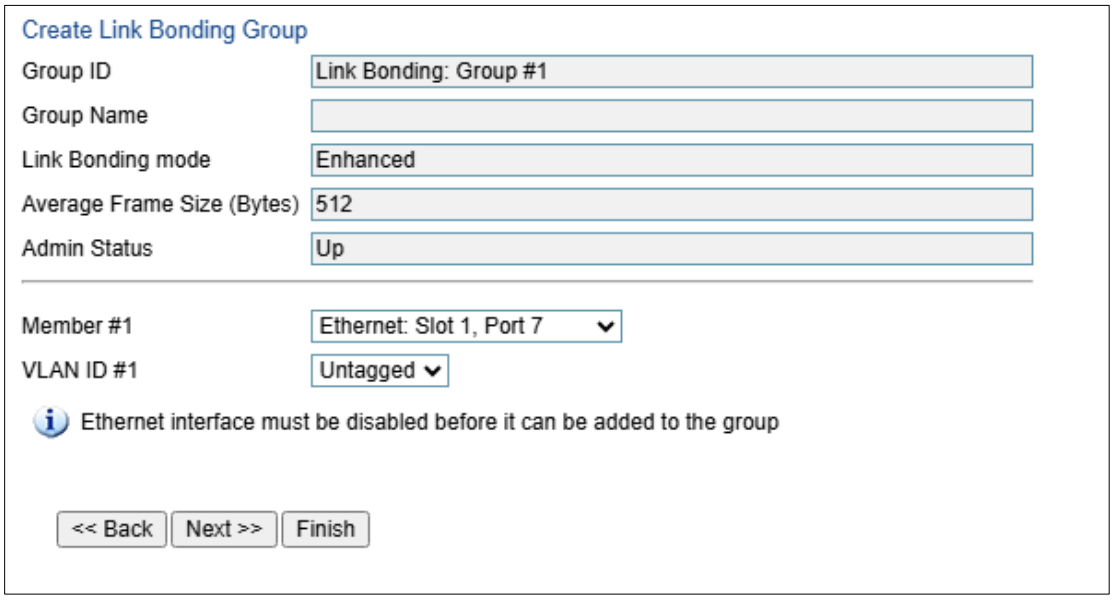


Figure 147: Link Bonding Group Wizard – Member #1 Page (PTP 850E)

ix In the **Member #1** field, select the Traffic port.
x In the **VLAN ID #1** field, select **Untagged**.
xi Click **Next**. The Member #2 page opens.

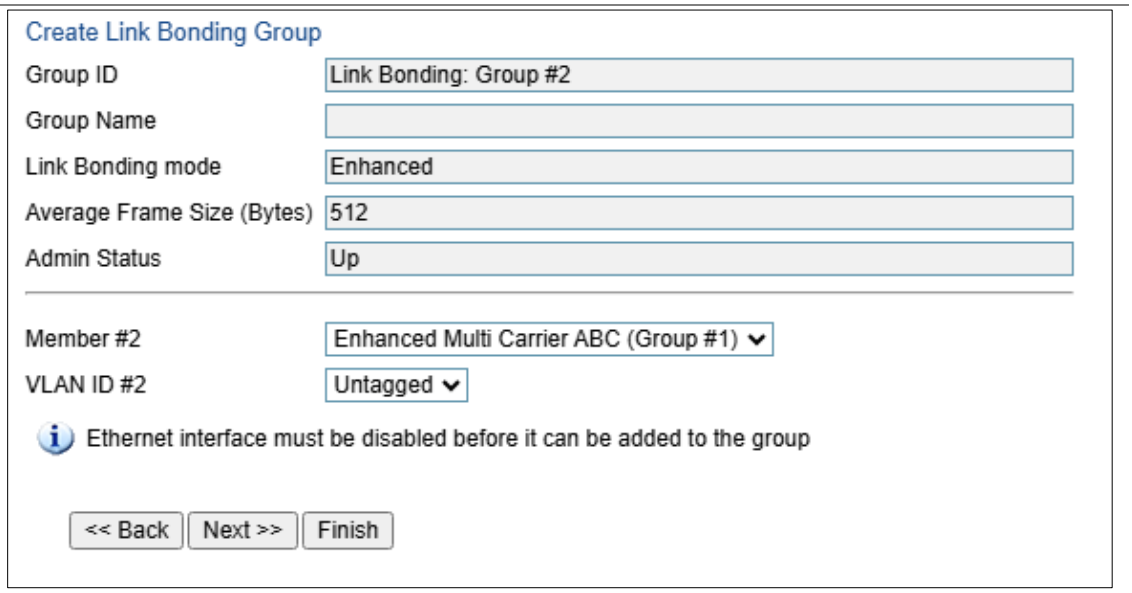


Figure 148: Link Bonding Group Wizard – Member #2 Page (PTP 850C)

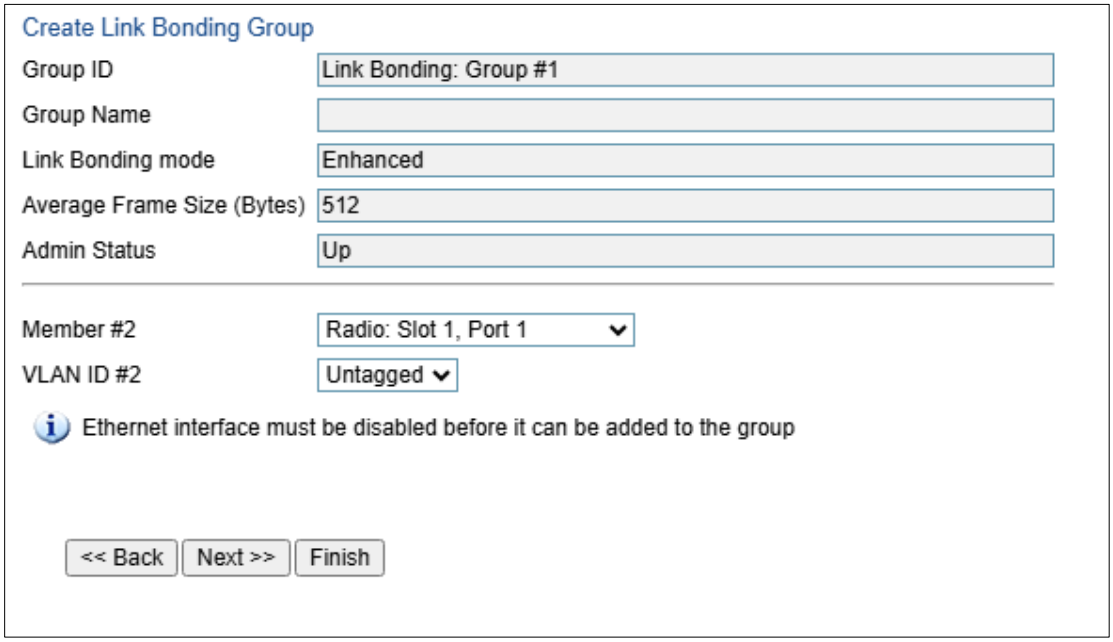


Figure 149: Link Bonding Group Wizard – Member #2 Page (PTP 850E)

xii In the **Member #2** field, select the radio interface (single-carrier device) or Enhanced Multi Carrier ABC group (multi-carrier device).
xiii In the **VLAN ID #2** field, select **Untagged**.
xiv Click **Finish**. The Selection Summary page opens.

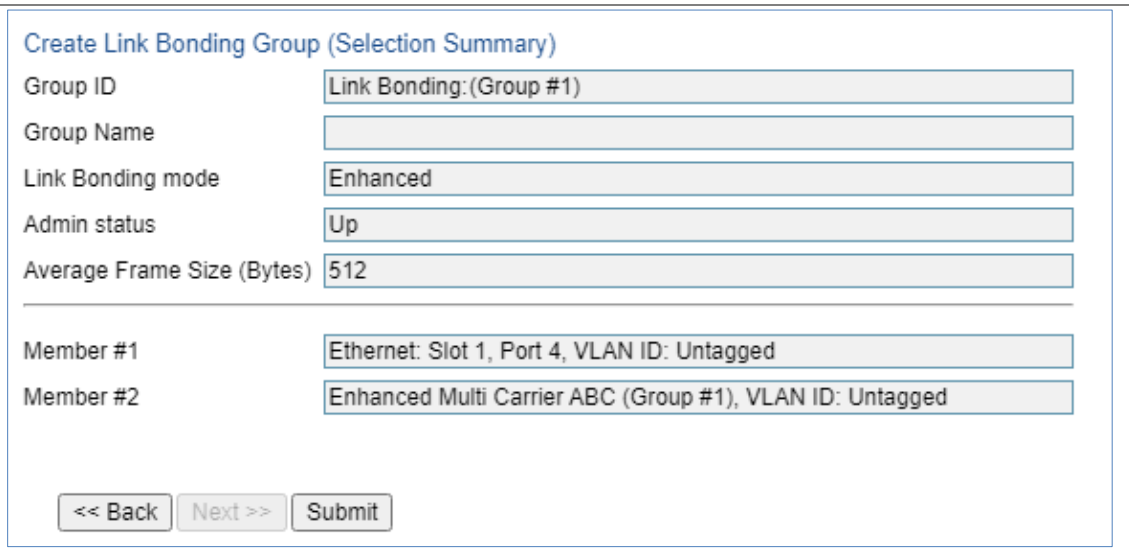


Figure 150: Link Bonding Group Wizard – Selection Summary Page (PTP 850C)

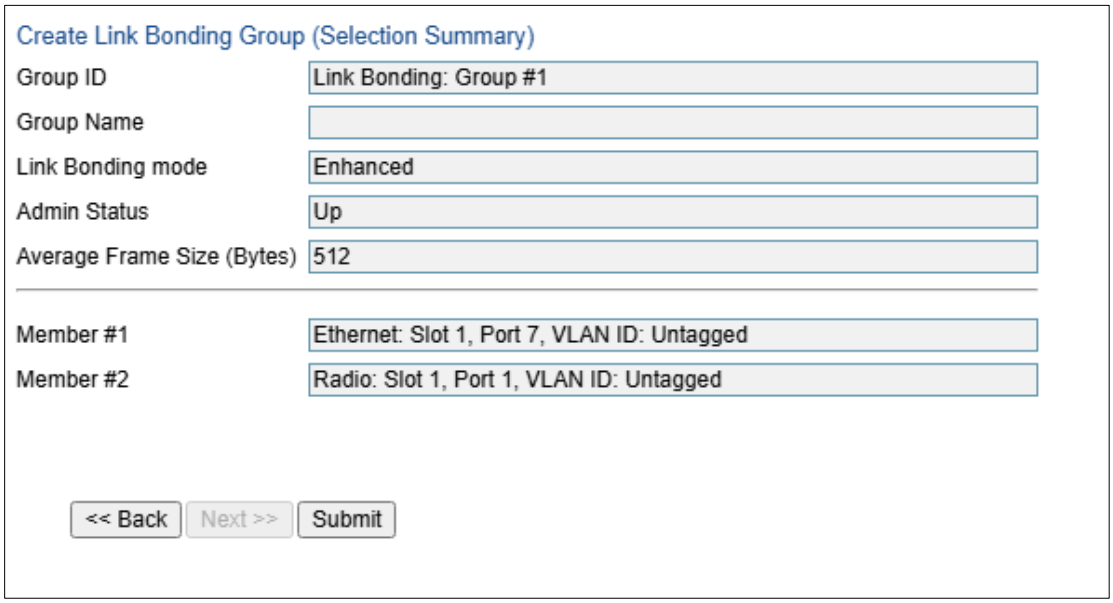


Figure 151: Link Bonding Group Wizard – Selection Summary Page (PTP 850E)

xv Click **Submit**. The group is added to the Link Bonding page.

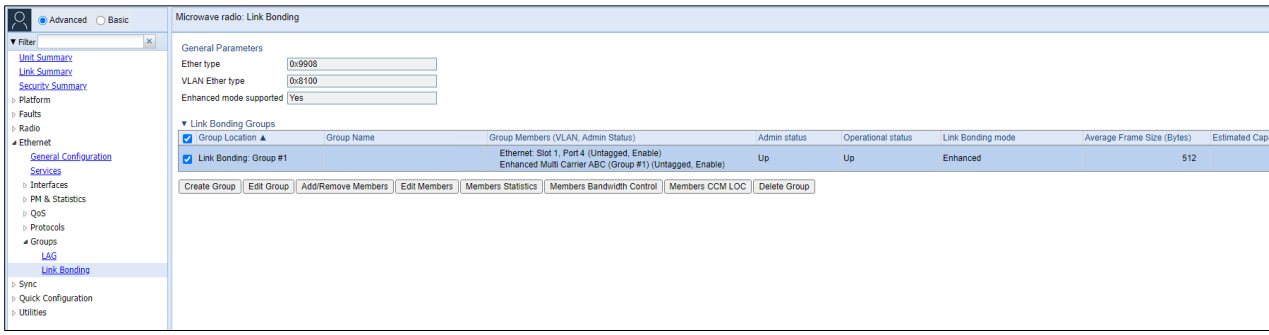


Figure 152: Link Bonding Page (Populated) (PTP 850C)

Note: For an explanation of the **Average Frame Size** and **Capacity** fields, see *Link Bonding L1 Capacity Calculator*.

9 In the Interface Manager, set the Traffic port to **Admin** = **Up**. See Enabling the Interfaces (Interface Manager).
10 Enable PDU encapsulation on the attached unit:

Note: This step is crucial since it ensures that protocols packets are properly tagged and separated from traffic.

i Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 381).
ii Select the port used for L2 protocols data (the Protocols port) and click **Edit**. The Logical Interfaces – Edit page opens (

Figure 382).

Note: In a single-cable configuration, this is the same as the Traffic port. In a two-cable configuration, this is the port to which the Protocols cable is connected.

iii In the field **PDU Encapsulation** field, select **Yes**.
iv Click **Apply**.

Note: The following step is unnecessary if the attached unit is a third-party device. Instead, you must configure OAM CCM to ensure that any traffic flow issues on the attached unit are reported to the main unit. See *Procedure for Configuring Third-Party Devices for Operation in Link Bonding Configurations*.

11 To ensure proper fault handling, configure Automatic State Propagation. For single-cable configurations, you must enable ASP Management Safe mode (CSF mode) to ensure that in-band management is not disrupted in case of a fault on one of the ports connecting the main and attached units. This includes configuring the peer unit to receive CSF PDUs, as described in Step **Error! Reference source not found.** of Error! Reference source not found..

i On the local and remote main units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The Link Bonding group
- Controlled Port: The Ingress port

ii On the local and remote attached units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The Multi-Carrier ABC group or radio interface
- Controlled Port: The Traffic port

See Error! Reference source not found..

12 In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page opens.

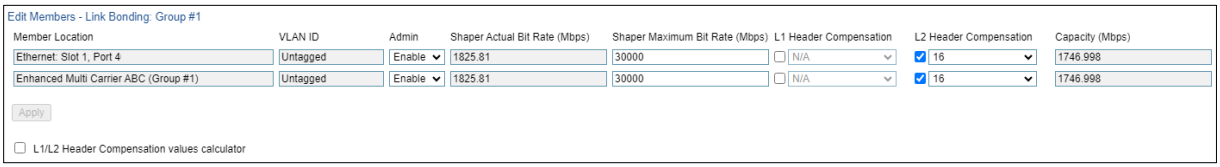


Figure 153: Link Bonding Groups – Edit Members Page (PTP 850C as main unit)

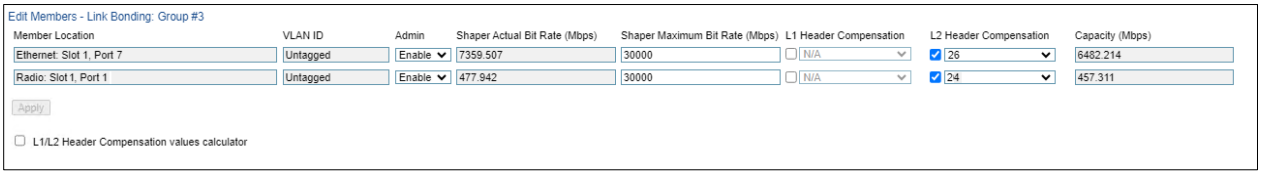


Figure 154: Link Bonding Groups – Edit Members Page (PTP 850E as main unit)

13 In the **Shaper actual bit rate** column, you can adjust the shaper for either or both interfaces in the group. Generally, there is no need to change this parameter from its default value of 30000 Mbps.

Note: The **Shaper actual bit rate** column displays the actual current traffic distribution between the main unit (the radio interface) and the attached unit (the Traffic port). This is displayed in units of Mbps.

14 In the **L1 header compensation** column:

- Do not select the radio member.
- For the Ethernet member, see *L1 and L2 Header Compensation Values*.

Note: The purpose of this setting is to prevent a bottleneck for traffic sent by the Link Bonding group to the main unit's radio.

15 In the **L2 header compensation** column, both interfaces should be selected. For recommended values, see L1 and L2 Header Compensation Values.
16 Click **Apply**.
17 In the **Admin** column, set the Admin status of each group member to **Enable**.

Note: If necessary, you can leave the Admin status of the group members **Disable** until a later time in order to complete the configuration with the group offline, then activate the group members later.

The Admin status must be set to **Disable** whenever you modify the **L1 header compensation** or **L2 header compensation** fields. Otherwise, the modification will have no effect.

18 Click **Apply**.
19 In-band management can be carried between the main unit and the attached unit via the Protocols port.
To configure in-band management, you must define a management service that connects the Protocols port on both units, the Link Bonding groups, and the Ingress port of the main unit:

i On the local main unit, configure a service point on the Ingress port.
ii On the local main unit, configure a service point on the Protocols port.
iii On the local main unit, configure a service point on the Link Bonding group.
iv On the local attached unit, configure a service point on the Protocols port.
v On the remote attached unit, configure a service point on the Protocols port.
vi On the remote main unit, configure a service point on the Protocols port.
vii On the remote main unit, configure a service point on the Link Bonding group.

Note: The following three steps are unnecessary if the attached unit is a third-party device. Instead, you must configure OAM CCM to ensure that any traffic flow issues on the attached unit are reported to the main unit. See *Procedure for Configuring Third-Party Devices for Operation in Link Bonding Configurations*.

20 Configure Radio Bandwidth Notification on the main unit by performing the following steps:

i Select the Link Bonding group in the Link Bonding page and click **Members Bandwidth Control**. The Members Bandwidth Control page opens.

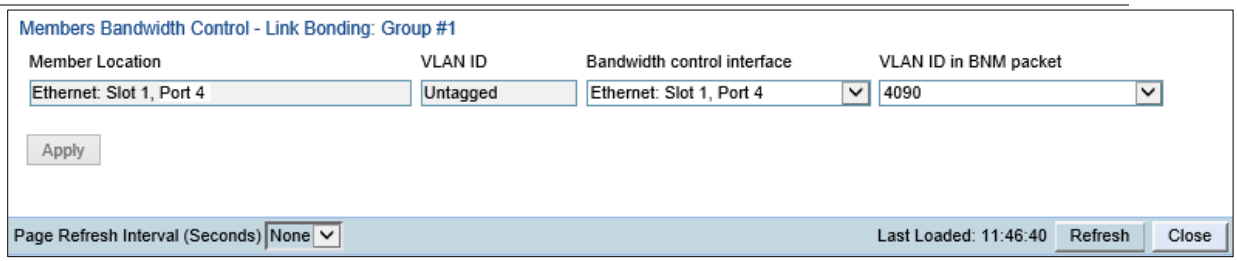


Figure 155: Link Bonding – Members Bandwidth Control Page (Single-Cable Configuration with PTP 850C as main unit and attached unit)

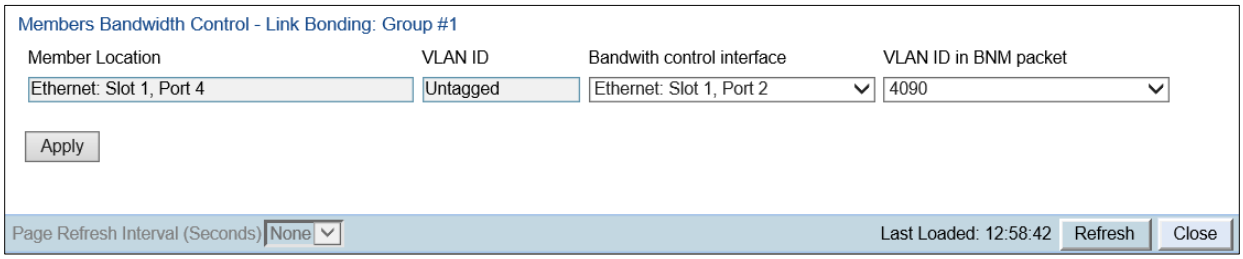


Figure 156: Link Bonding – Members Bandwidth Control Page (Two-Cable Configuration with PTP 850C as main unit and attached unit)

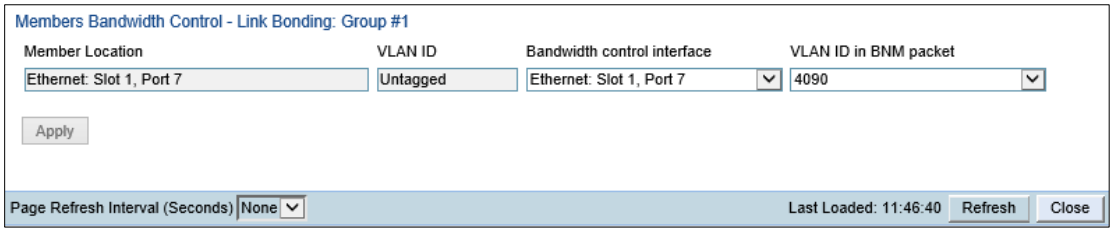


Figure 157: Link Bonding – Members Bandwidth Control Page (Single-Cable Configuration with PTP 850E as main unit)

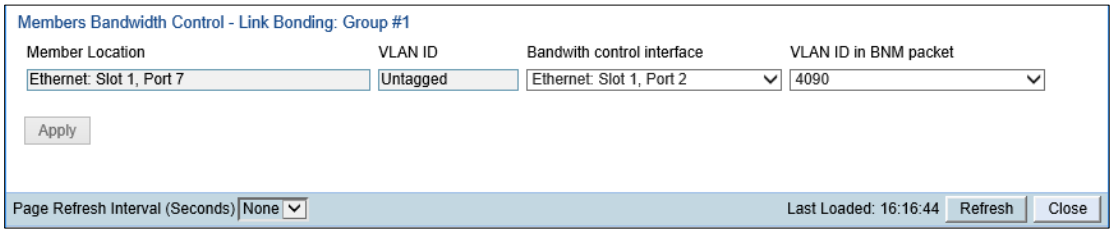


Figure 158: Link Bonding – Members Bandwidth Control Page (Two-Cable Configuration with PTP 850E as main unit)

ii In the **Bandwidth control interface** column:

- For single-cable configurations, select the same port as displayed in the **Member Location** field
- For two-cable configurations, select the Protocols port.

iii In the **VLAN ID in BNM packet** column, select a VLAN ID. You can use any available VLAN ID from 1 to 4090. This is the VLAN use to transfer protocol information between the two units.

iv Click **Apply**.

21 Configure Radio Bandwidth Notification on the attached unit by performing the following steps:

Note: PTP 850EX does not support Radio Bandwidth Notification, and you must use ETH-BN instead. For instructions on configuring ETH-BN, refer

to Section 11.3, Configuring Ethernet Bandwidth Notification (ETH-BN), in the User Guide for PTP 850CX and PTP 850EX, System Release 13.1.

i Select **Ethernet** > **Protocols** > **Bandwidth Notification**. The Bandwidth Notification page opens.

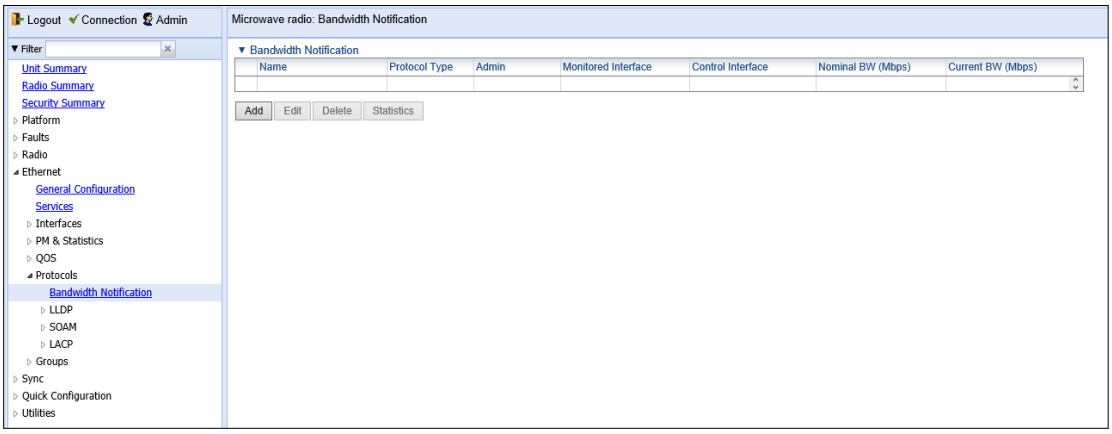


Figure 159: Bandwidth Notification Page (Empty)

ii Click Add. The Bandwidth Notification – Add page opens.

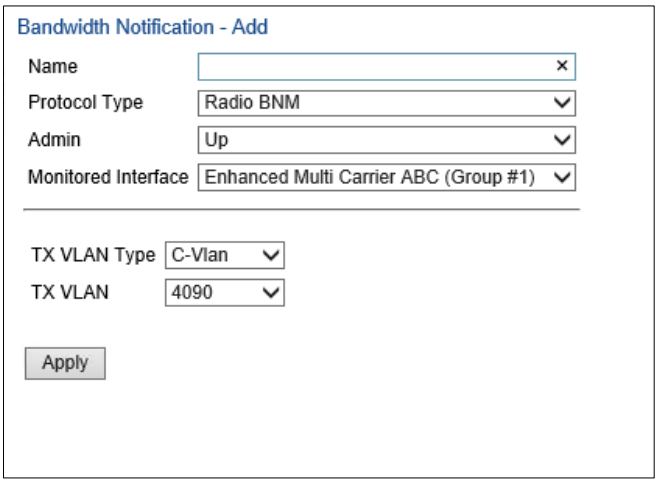


Figure 160: Bandwidth Notification – Add Page (PTP 850C)

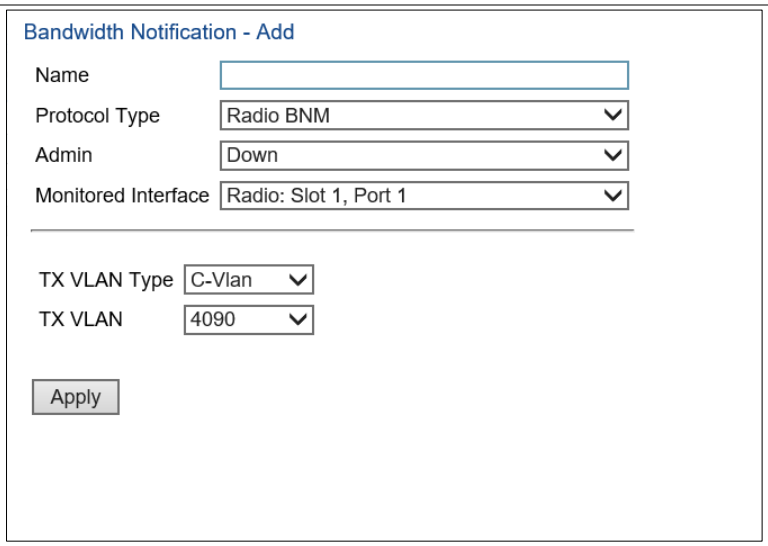


Figure 161: Bandwidth Notification – Add Page (PTP 850E)

iii In the **Name** field, select a descriptive name.

Note: Once you configure the RBN entity, you cannot edit the name later. The only way to change the name is to delete and reconfigure the RBN entity.

iv In the Protocol Type field, select Radio BNM.
v In the Admin field, select Up.
vi In the Monitored Interface field, select the attached unit's radio or Multi-Carrier ABC group.
vii In the TX VLAN Type field, select **C-Vlan**.
viii In the **TX VLAN** field, select **the same VLAN you configured** In the **VLAN ID in BNM packet** column for the main unit.
ix Click **Apply**. The configuration is added to the Bandwidth Notification page with the Protocol Type **Radio BNM**.

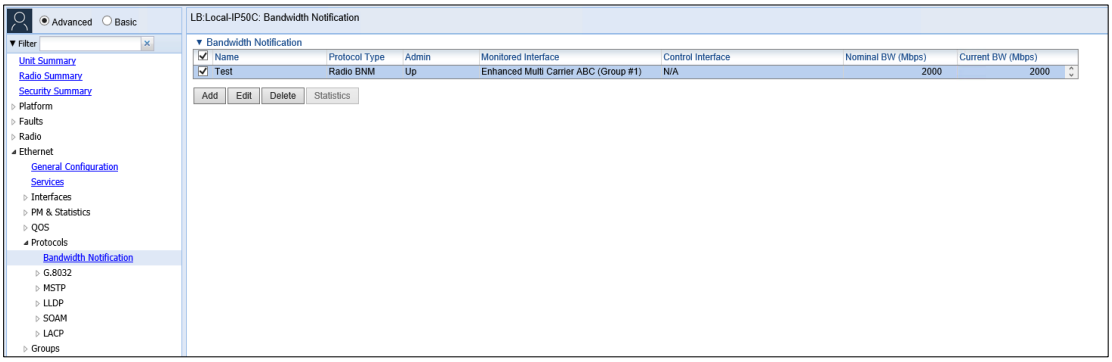


Figure 162: Bandwidth Notification Page (Populated with Radio BNM)

Note: The following step is not necessary is the attached unit is an PTP 850EX using ETH-BN instead of Radio Bandwidth Notification.

22 On the attached unit on both sides of the link, configure a point-to-point service for Radio Bandwidth Notification, with service points on the Multi-Carrier ABC group or radio and on the Protocols port. In single-cable configurations, this is the same as the Traffic. In two-cable configurations, this is the port used for the Protocols cable.

The service points should be configured as follows:

i Create a service point on the Multi-Carrier ABC group with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Use the VLAN you configured in the **VLAN ID in BNM packet** column in Step 14
- Allow Flooding: Allow
- Learning Admin: Disable

ii Create a service point on the Protocols port with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Use the VLAN you configured in the **VLAN ID in BNM packet** column in Step 14
- Allow Flooding: Allow
- Learning Admin: Disable

See Configuring Service Points.

23 On the main unit on both sides of the link, create a point-to-point service for Link Bonding traffic, with service points on the Ingress port and the Link Bonding Group. Both service points should be configured as follows:

- Type: PIPE
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Untagged
- Allow Flooding: Allow
- Learning Admin: Disable

24 On the attached unit on both sides of the link, configure a point-to-point service for Link Bonding traffic, with service points on the radio or Multi-Carrier ABC group and on the Traffic port.

The service points should be configured as follows:

Note: This service is a workaround for SYSTEM RELEASE117-1749, to ensure that customer traffic is separated from Radio Bandwidth Notification protocol traffic.

i Create a service point on the radio or Multi-Carrier ABC group with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation:
  - In configurations without Line Redundancy: Untagged
  - In configurations with Line Redundancy: Any VLAN
- Allow Flooding: Allow
- Learning Admin: Disable

ii Create a service point on the Traffic port with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Untagged
- Allow Flooding: Allow
- Learning Admin: Disable

See Configuring Service Points.

For configurations with line redundancy, proceed to the instructions in Configuring Line Redundancy with Multiband and Link Bonding.

7.2.5.1 CLI Commands

To configure a Link Bonding group on the main unit:

Note: Before adding a group member, make sure that no shapers or service points are configured on the interface or group.

i Create the group by entering the following command in root view:

```
root> ethernet link-bonding create group group_id <1-6> group-name <string>
```

Note: The `name` parameter is optional.

ii Enter the group view by entering the following command in root view:

```
root> ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

```
root> ethernet interfaces group lb1
eth group [lb1]>
```

iii Add the Traffic interface to the Link Bonding Group:

- In most cases, enter the following command in group view:

```
eth group [lbx]> lb-member add interface eth slot 1 port <port> shaper-bit-rate <0-30000> vlan <1-4094|untag> l1-header-compensation-enabled no l1-header-compensation-value <(-63)-63> l2-header-compensation-value <(-63)-63>
```

- In configurations with a third-party device in which the PTP 850E Management port is connected to an electrical port on the third-party device, add the Management port to the Link Bonding Group by entering the following command in group view:

```
eth group [lbx]> lb-member add interface mng slot 1 port 1 shaper-bit-rate <0-30000> vlan untag l1-header-compensation-enabled no l1-header-compensation-value <> l2-header-compensation-enabled yes|no> l2-header-compensation-value <>
```

iv Add the radio interface or Multi-Carrier ABC group to the Link Bonding group:

- If the main unit is an PTP 850C, add the Multi-Carrier ABC group to the Link Bonding Group by entering the following command in group view:

```
eth group [lbx]> lb-member add group-on-slot enhanced-abc slot 1 group-id <1-4> shaper-bit-rate <0-30000> vlan <1-4094|untag>l1-header-compensation-enabled no l1-header-compensation-value <(-63)-63> l2-header-compensation-value <(-63)-63>
```

- If the main unit is an PTP 850E, add radio interface to the Link Bonding Group by entering the following command in group view:

```
eth group [lbx]> lb-member add interface radio slot 1 port 1 shaper-bit-rate <0-30000> vlan untag l1-header-compensation-enabled yes l1-header-compensation-value <> l2-header-compensation-enabled yes|no> l2-header-compensation-value <>
```

- The `shaper-bit-rate` parameter enables you to adjust the shaper for either or both interfaces in the group. This shaper controls the distribution of traffic between the main unit (the radio interface or Multi-Carrier ABC group) and the attached unit (the Ethernet interface). You should set this according to the maximum capacity of the radio interface, or the maximum radio capacity of the attached unit connected to the Ethernet member. The default value is 30000 Mbps.
- The `l1-header-compensation-enabled`_parameter should be set to no for the radio interface. For instructions on setting this parameter for the Ethernet member, see *L1 and L2 Header Compensation Values*.
- The `l2-header-compensation-enabled` parameter should be set to yes for both interfaces.
- The `l2-header-compensation-value` parameter should be set according to the recommended values in *L1 and L2 Header Compensation Values*.

v In Link Bonding group view, enter the following command:

```
eth group [lbx]> edit lbg-mode <enhanced|standard>
```

You must configure the group to *enhanced* mode if the configuration uses a single cable for traffic and L2 protocol data. The default value is *standard*. See Requirements and Limitations for Enhanced Link Bonding Mode.
For example, use the following commands to set Link Bonding group 1 to enhanced mode:

```
root>ethernet interfaces group lb1
eth group [lb1]>edit lbg-mode enhanced
```

To display the currently configured Link Bonding Mode for a specific Link Bonding group, enter the following command in root view:

```
root>ethernet link-bonding show group group_id <1-6>
```

To display the currently configured Link Bonding Mode for all Link Bonding groups configured on the device, enter the following command in root view:

```
root>ethernet link-bonding show all
```

Note: Although most PTP 850C and PTP 850E devices support Enhanced Link Bonding mode, some do not. For details, see Requirements and Limitations for Enhanced Link Bonding Mode.

To enable PDU encapsulation on the attached unit:

Note: This step is crucial since it ensures that protocols packets are properly tagged and separated from traffic.

i Enter interface view for the port carrying L2 protocols data between the two units. In a single-cable configuration, this is the port that carries traffic and L2 protocols data between the two units. In a two-cable configuration, this is the port to which the Protocols cable is connected. To enter interface view, enter the following command in root view:

```
root>ethernet interfaces eth slot 1 port <port>
eth type eth [x/x]
```

If the Protocols port is the PTP 850E Management port, use the following command syntax:

```
root>ethernet interfaces mng slot 1 port 1
eth type mng [1/1]>
```

ii In interface view, enter the following command:

```
eth type eth [x/x]>pdu-encapsulation set yes
```

For example, if the Protocols port is Eth 2, use the following commands to enable PDU encapsulation on Eth 2:

```
root>ethernet interfaces eth slot 1 port 2
eth type eth [1/2]>pdu-encapsulation set yes
```

To display the current PDU encapsulation setting, enter the following command in interface view:

```
eth type eth [x/x]>pdu-encapsulation show
```

Note: The following three steps are unnecessary if the attached unit is a third-party device. Instead, you must configure OAM CCM to ensure that any traffic flow issues on the attached unit are reported to the main unit. See *Procedure for Configuring Third-Party Devices for Operation in Link Bonding Configurations*.

To configure Radio Bandwidth Notification on the main unit via the CLI:

Note: PTP 850EX does not support Radio Bandwidth Notification, and you must use ETH-BN instead. For instructions on configuring ETH-BN, refer to Section 11.3, Configuring Ethernet Bandwidth Notification (ETH-BN), in the User Guide for PTP 850CX and PTP 850EX, System Release 13.1.

i Enter Link Bonding group view by entering the following command in root view:

```
root>ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

ii In group view, enter the following command to enter the view of the main unit's Traffic interface:

```
eth group [lbx]>ethernet link-bonding-member interface eth slot 1 port <port>
vlan <1-4094|untag>
```

If the port is the PTP 850E Management port, use the following command syntax:

```
eth group [lbx]> ethernet link-bonding-member interface mng slot 1 port 1
vlan <1-4094|untag>
```

iii In group member view, enter the following command to create the Radio Bandwidth Control entity.

- For single-cable configurations, the <port> parameter should be the same as the port transmitting traffic to the attached unit.
- For two-cable configurations, the <port> parameter should be the port on the main unit sending Protocols information to the attached unit.

```
lbg-member[ethx/y]>bw-control add bw-ctrl-interface eth bw-ctrl-slot 1
bw-ctrl-port <port> bw-ctrl-vlan <1-4094>bw-ctrl-port-id
```

Note: The bw-ctrl-vlan parameter configures the VLAN used to transfer protocol information between the two units. You can use any available VLAN ID from 1 to 4090.

To configure Radio Bandwidth Notification on the attached unit via the CLI:

i Enter one of the following commands in root view to create a Radio Bandwidth Notification entity:
If the attached unit is using a Multi-Carrier ABC group:

```
root> ethernet abn abn-entity-create protocol-type-rbn abn-name <name>
monitored-group-on-slot enhanced-abc slot 1 group-id 1 vlan untag
```

If the attached unit is using a single radio interface:

```
root> ethernet abn abn-entity-create protocol-type-rbn abn-name <name>
monitored-interface radio monitored-slot 1 monitored-port 1 vlan untag
```

Note: Once you configure the RBN entity, you cannot edit the name later. The only way to change the name is to delete and reconfigure the RBN entity.

To display information about the Radio Bandwidth Notification entity, enter the following command in root view:

```
root> ethernet abn abn-entity-show abn-name <name>
```

ii Enter the following command in root view to set the VLAN type to C-VLAN:

```
root> ethernet abn abn-vlan-type-set abn-name <name> vlan-type c-vlan
```

iii Enter the following command in root view to set the VLAN ID to the same VLAN you configured for the main unit :

```
root> ethernet abn abn-vlan-set abn-name <name> vlan <1-4094>
```

iv Enter the following command in root view to set the Admin status of the Radio Bandwidth Notification entity to Up:

```
root> ethernet abn abn-admin-set abn-name <name> admin up
```

7.2.6 Enabling Link Bonding Throughput Enhancement

Note: Link Bonding Throughput Enhancement is not supported with PTP 850EX.

After configuring a Link Bonding node, it is recommended to enable Link Bonding Throughput Enhancement. Link Bonding Throughput Enhancement is available for both the main unit and the attached unit.

Notes: Link Bonding Throughput Enhancement and Header De-Duplication cannot both be enabled on the same interface.
In configurations with PTP 820N/PTP 820A, Link Bonding Throughput Enhancement can be used for the PTP 850C and PTP 850E as attached unit. For instructions, refer to the User Guide for PTP 820N and PTP 820A, System Release 12.1 and higher.

Link Bonding Throughput Enhancement can be enabled on the Multi-Carrier ABC groups or radio interface on both the main and the attached units.

Link Bonding Throughput Enhancement affects the recommended L2 Header Compensation. Make sure to use the values listed in L1 and L2 Header Compensation Values.

The Link Bonding Throughput Enhancement and L2 Header Compensation settings must be the same for the main units on both sides of the link. Therefore,

the changes should be applied in the following order to ensure that management is not lost:

Note: The settings on attached units do not affect management, and can be changed in any order.

1 Enable Link Bonding Throughput Enhancement on the remote unit (main and/or attached unit):

i Select **Radio > Ethernet Interface > Configuration**. The Radio Ethernet Interface Configuration page opens.

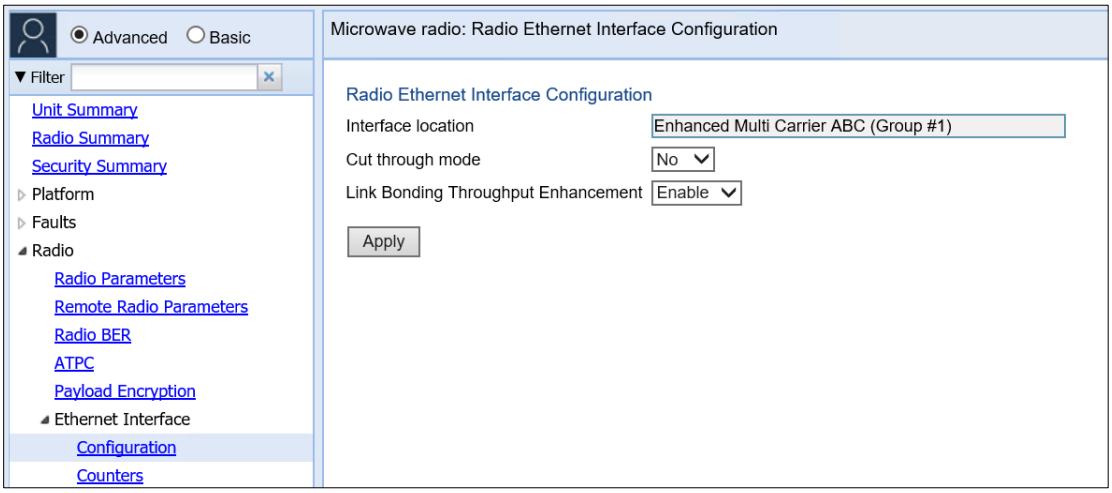


Figure 163: Radio Ethernet Interface Configuration Page (PTP 850C)

ii In the **Link Bonding Throughput Enhancement** field, select **Enable**.
iii Click **Apply**.

2 Enable Link Bonding Throughput Enhancement on the local unit (main and/or attached unit):

i Select **Radio > Ethernet Interface > Configuration**. The Radio Ethernet Interface Configuration page opens (Figure 545).
ii In the **Link Bonding Throughput Enhancement** field, select **Enable**.
iii Click **Apply**.

3 Modify the L2 Header Compensation on the remote unit (main and/or attached unit):

i Select **Ethernet** > **Groups** > **Link Bonding**. The Link Bonding page opens (Figure 178).
ii In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page opens (Figure 181).
iii In the **L2 header compensation** column, adjust the L2 Header Compensation according to the values listed in L1 and L2 Header Compensation Values.
iv Click **Apply**.

4 Modify the L2 Header Compensation on the local unit (main and/or attached unit):

i Select **Ethernet** > **Groups** > **Link Bonding**. The Link Bonding page opens (Figure 178).
ii In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page opens (Figure 181).
iii In the **L2 header compensation** column, adjust the L2 Header Compensation according to the values listed in L1 and L2 Header Compensation Values.
iv Click **Apply**.

7.2.6.1 CLI Commands

Note: For configurations in which the PTP 850E is connected to a third-party device via the PTP 850E's Management port, make sure to reconfigure management according to the instructions in ***Error! Reference source not found.***. Failure to do so will lead to loss of management and may lead to RMA at the customer's expense.

The Link Bonding Throughput Enhancement and L2 Header Compensation settings must be the same for the main units on both sides of the link. Therefore, the changes should be applied in the following order to ensure that management is not lost:

Note: The settings on attached units do not affect management, and can be changed in any order.

1 Enable Link Bonding Throughput Enhancement on the remote unit (main and/or attached unit):

- For a multi-carrier device such as PTP 850C, enter the following command:

```
root> multi-carrier-abc group-id 1 slot 1 type Enhanced
multi-carrier-abc enhanced-group-id [1] slot [1]> lb-throughput-enhancement
set admin enable
```

- For a single-carrier device such as PTP 850E, enter the following command:

```
root> radio slot 1 port 1
radio [1/1]> lb-throughput-enhancement set admin enable
```

2 Enable Link Bonding Throughput Enhancement on the local unit (main and/or attached unit):

- For a multi-carrier device such as PTP 850C, enter the following command:

```
root> multi-carrier-abc group-id 1 slot 1 type Enhanced
multi-carrier-abc enhanced-group-id [1] slot [1]> lb-throughput-enhancement
set admin enable
```

- For a single-carrier device such as PTP 850E, enter the following command:

```
root> radio slot 1 port 1
radio [1/1]> lb-throughput-enhancement set admin enable
```

3 Modify the L2 Header Compensation on the remote unit (main and/or attached unit) by entering the following commands:

- For a multi-carrier device such as PTP 850C, enter the following commands to modify the L2 Header Compensation for the Multi-Carrier ABC group:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]>ethernet link-bonding-member group-on-slot enhanced-abc slot
1 group-id 1
lbg-member[enhanced-abc1/1]>admin set disable
lbg-member[enhanced-abc1/1]> l2-header-compensation edit l1-header-
compensation-enabled <yes|no> l2-header-compensation-value <(-63)-63>
lbg-member[enhanced-abc1/1]>admin set enable
```

To display the current parameter, enter the following command:

```
lbg-member[enhanced-abc1/1]> l2-header-compensation show
```

- For a single-carrier device such as PTP 850E, enter the following commands to modify the L2 Header Compensation for the radio interface:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface radio slot 1 port 1
lbg-member[radio1/1]> admin set disable
lbg-member[radio1/1]> l2-header-compensation edit l1-header-compensation-
enabled <yes|no> l2-header-compensation-value
<(-63)-63>
lbg-member[radio1/1]> admin set enable
```

- Enter the following commands to modify the L2 Header Compensation for the Traffic port:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface eth slot 1 port
<port>
lbg-member[eth4]>admin set disable
lbg-member[eth4]> l2-header-compensation edit l2-header-compensation-enabled
<yes|no> l2-header-compensation-value <(-63)-63>
lbg-member[eth4]>admin set enable
```

To display the current parameter, enter the following command:

```
lbg-member[ethx]> l2-header-compensation show
```

Note: For recommended values, see L1 and L2 Header Compensation Values.

4 Modify the L2 Header Compensation on the local unit (main and/or attached unit) by entering the following commands:

- For the main unit if the main unit is an PTP 850C, enter the following commands to modify the L2 Header Compensation for the Multi-Carrier ABC group:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]>ethernet link-bonding-member group-on-slot enhanced-abc slot
1 group-id 1
lbg-member[enhanced-abc1/1]>admin set disable
lbg-member[enhanced-abc1/1]> l2-header-compensation edit l1-header-
compensation-enabled <yes|no> l2-header-compensation-value <(-63)-63>
lbg-member[enhanced-abc1/1]>admin set enable
```

To display the current parameter, enter the following command:

```
lbg-member[enhanced-abc1/1]> l2-header-compensation show
```

- For the main unit if the main unit is an PTP 850E, enter the following commands to modify the L2 Header Compensation for the radio interface:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface radio slot 1 port 1
lbg-member[radio1/1]> admin set disable
lbg-member[radio1/1]> l2-header-compensation edit l1-header-compensation-
enabled <yes|no> l2-header-compensation-value
<(-63)-63>
lbg-member[radio1/1]> admin set enable
```

- Enter the following commands to modify the L2 Header Compensation for the Traffic port:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface eth slot 1 port 4
lbg-member[eth4]>admin set disable
lbg-member[eth4]> l2-header-compensation edit l2-header-compensation-enabled
<yes|no> l2-header-compensation-value <(-63)-63>
lbg-member[eth4]>admin set enable
```

To display the current parameter, enter the following command:

```
lbg-member[eth4]> l2-header-compensation show
```

Note: For recommended values, see L1 and L2 Header Compensation Values.

7.2.7 Editing a Link Bonding Group or its Members

To change the Group Name or the Admin Status of the Link Bonding group:

1 In the Link Bonding page, select the group and click **Edit Group**. The Edit Group page opens.

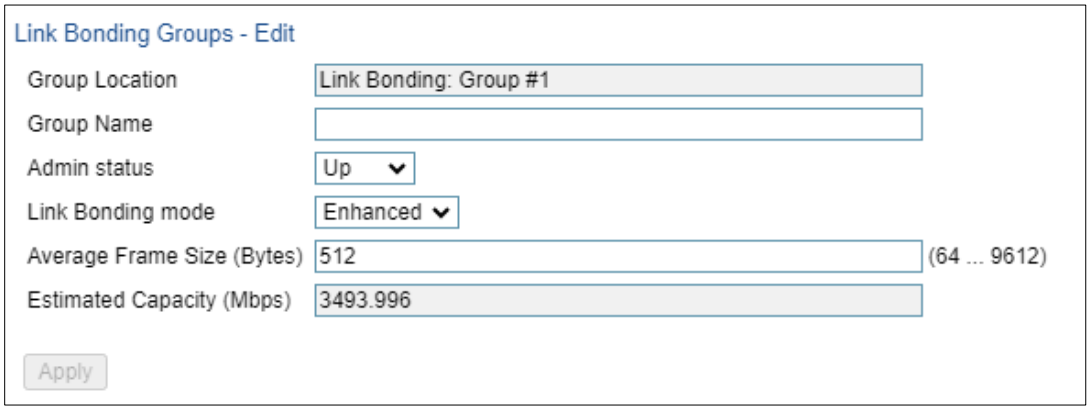


Figure 164: Link Bonding Groups – Edit Page

2 In the Group Name field, enter the new name.
3 In the Admin status field, change the Admin status of the group to Up or Down.
4 Click Apply.

Note: For an explanation of the Link Bonding mode field, see Requirements and Limitations for Enhanced Link Bonding Mode. For an explanation of the Average Frame Size and Capacity fields, see *Link Bonding L1 Capacity Calculator*.

7.2.7.1 CLI Commands

To modify or display the parameters of the Link Bonding group, enter the following command to enter group view:

```
root>ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

To change the name of the Link Bonding group, enter the following command in group view:

```
eth group [lbx]> edit group-name <string>
```

To modify the attributes of a Link Bonding group member, you must first enter one of the following commands to enter the group member's view.

- To enter a Multi-Carrier ABC group member's view, enter the following command in group view:

```
eth group [lb1]>ethernet link-bonding-member group-on-slot enhanced-abc slot 1 group-id <1-4>
```

- To enter a radio interface member's view, enter the following command in group view:

```
eth group [lbx]>ethernet link-bonding-member interface radio slot 1 port 1
```

- To enter the Ethernet member's view, enter the following command in group view:

```
eth group [lbx]>ethernet link-bonding-member interface eth slot 1 port <port>
```

To change the Admin Status of a group member, enter the following command in group member view:

```
lbg-member[radio/ethx/x]>admin set <enable|disable>
```

For example, to disable the radio interface in Link Bonding group 1, enter the following command in group view:

```
lbg-member[enhanced-abc1/1]>admin set disable
```

To display the Admin Status of a group member, enter the following command in group member view:

```
lbg-member[radio/ethx/x]>admin state show
```

You can adjust the maximum shaper for either or both interfaces in the group. You should set this according to the maximum capacity of the link. The default value is 30000 Mbps. To adjust this parameter, enter the following command in group member view:

```
lbg-member[ethx/y]>edit shaper-bit-rate <0-30000>
```

To display configuration of the group member, including its Admin Status and maximum shaper bit rate, enter the following command in group member view:

```
lbg-member[radio/ethx/x]> configuration show
```

The `l1-header-compensation-enabled` parameter should be set to no for both interfaces. If you did not set this parameter properly when configuring the Link Bonding group, or if you need to set them to a different value for any reason, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l1-header-compensation edit l1-header-compensation-enabled <yes|no> l1-header-compensation-value <(-63)-63>
```

The `l2-header-compensation-enabled` parameter should be set to yes for both members of the group. The l2-header-compensation parameter should be set to its default value. If you did not set these parameters properly when configuring the group, or if you need to set them to a different value for any reason, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l2-header-compensation edit l1-header-compensation-enabled <yes|no> l2-header-compensation-value <(-63)-63>
```

Note: Before changing the `l2-header-compensation-enabled` parameter, the Admin status of the group member in the group must be set to `disable`. Otherwise, the change will have no effect. After changing the `l2-header-compensation-enabled` parameter, make sure to set the Admin status of the group member in the group back to `enable`.

For recommended values, see L1 and L2 Header Compensation Values.

To display the L1 Header Compression settings for the group member, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l1-header-compensation show
```

To display the L2 Header Compression settings for the group member, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l2-header-compensation show
```

7.2.8 Displaying Statistics for a Link Bonding Group

You can display the total number of segments and bytes (TX and RX) that have passed through each member of the Link Bonding group.

Note: The ability to clear member statistics is planned for future release.

You can also display and configure thresholds for throughput and utilization on both the group and the member levels. For further information, see ***Error! Reference source not found.***.

To display throughput statistics for the members of the Link Bonding group:

1 In the Link Bonding page, select the group and click **Member Statistics**. The Member Statistics page opens.

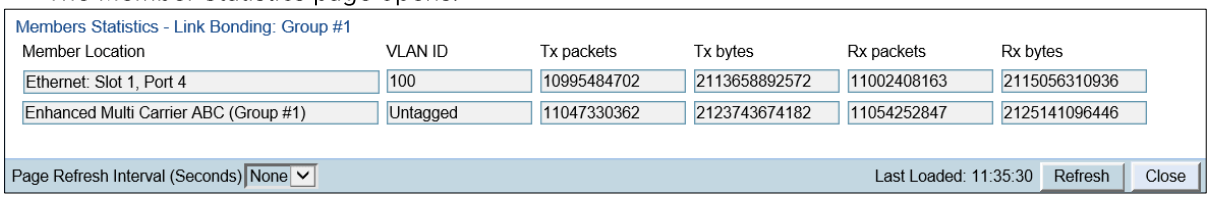


Figure 165: Link Bonding Groups – Member Statistics Page (PTP 850C as main unit)

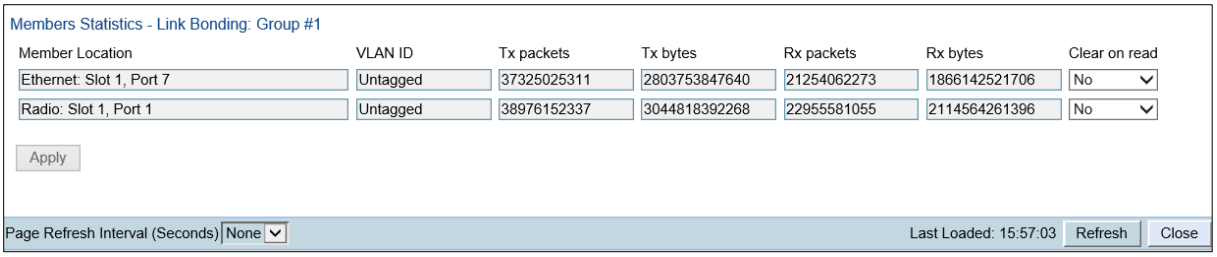


Figure 166: Link Bonding Groups – Member Statistics Page (PTP 850E as main unit)

7.2.8.1 CLI Commands

Enter the group view by entering the following command in root view:

```
root>ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

To display the actual current traffic distribution between the main unit (the Multi-Carrier ABC group) and the attached unit (the Ethernet interface, enter the following command in group member view:

```
eth group [lb1]> lb-member status show all
```

The following example shows the status of a Link Bonding group for which the main unit is an PTP 850C:

```
eth group [lb1]>lb-member status show all
Link Bonding members status Table:

-------------------------------------------------------------------------------
Member Location           VLAN ID    Group Location           Shaper actual bit rate
-------------------------------------------------------------------------------
Ethernet: Slot 1,                Port 4  untagged   Link Bonding: Group #1   1898804
Multi Carrier ABC (Slot 1, Group 1)       untagged   Link Bonding: Group #1   9905046
```

The following example shows the status of a Link Bonding group for which the main unit is an PTP 850E:

```
eth group [lb1]>lb-member status show all
Link Bonding members status Table:

-------------------------------------------------------------------------------
Member Location           VLAN ID    Group Location           Shaper actual bit rate
-------------------------------------------------------------------------------
Ethernet: Slot 1, Port 7  untagged   Link Bonding: Group #1   1898804
Radio: Slot 1, Port 1     untagged   Link Bonding: Group #1   9905046
```

To display statistics for overall traffic passing through the group, enter the following command in group member view:

```
eth group [lb1]> statistics show
```

For example:

```
eth group [lb1]>statistics show
         txPkts                          17304248327
         txOctets                        22885762312
         rxPkts                          0
         rxOctets                        0
         txUnicastPkts                   17304246993
         txMulticastPkts                 0
         txBroadcastPkts                 0
         txPkts64Octets                  0
         txPkts65to127Octets             0
         txPkts128to255Octets            17304248327
         txPkts256to511Octets            0
         txPkts512to1023Octets           0
         txPkts1024to1518Octets          0
         txPkts1519Octets                0
eth group [lb1]>
```

To display the total number of segments and bytes (TX and RX) that have passed through each member of the Link Bonding group, enter the following command in group member view:

```
eth group [lb1]> statistics show
```

For example:

```
eth group [lb1]>statistics show
         txPkts                          17304248327
         txOctets                        22885762312
         rxPkts                          0
         rxOctets                        0
         txUnicastPkts                   17304246993
         txMulticastPkts                 0
         txBroadcastPkts                 0
         txPkts64Octets                  0
         txPkts65to127Octets             0
         txPkts128to255Octets            17304248327
         txPkts256to511Octets            0
         txPkts512to1023Octets           0
         txPkts1024to1518Octets          0
         txPkts1519Octets                0
eth group [lb1]>
```

Note: The ability to clear member statistics is planned for future release.
You can also display and configure thresholds for throughput and utilization on both the group and the member levels. For further information, see *Displaying Link Bonding PMs (CLI).*

7.2.9 Deleting a Link Bonding Group

To delete a Link Bonding group, you must first remove the members from the group:

1 In the Link Bonding page, select the group and click **Add/Remove Members**. The Add/Remove Members page opens.

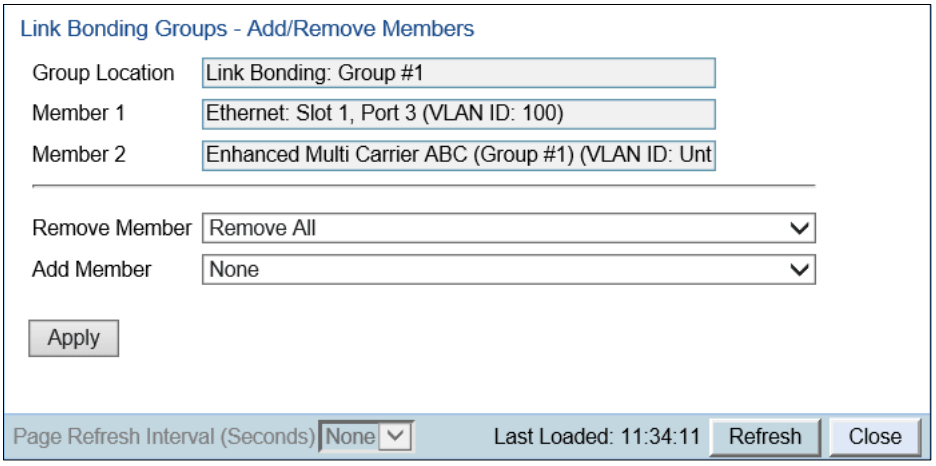


Figure 167: Link Bonding Groups – Member Statistics Page

2 In the **Remove Member** field, select **Remove All**.
3 Click **Apply**.
4 Remove any service points on the Link Bonding group.
5 In the Link Bonding page, select the group and click **Delete Group**.

7.2.9.1 CLI Commands

To delete a Link Bonding group, you must first remove the members from the group:

1 Enter the group view by entering the following command in root view:

```
root>ethernet interfaces group lb<1-6>
```

2 To remove the group members:

- To remove a radio interface member:

```
eth group [lb1]> lb-member delete interface radio slot 1 port 1
```

- To remove a Multi-Carrier ABC group member:

```
eth group [lb1]> lb-member delete group-on-slot enhanced-abc slot 1 group-id
<1-4>
```

- To remove an Ethernet interface member:

```
eth group [lb1]> lb-member delete interface eth slot 1 port <port>
```

3 Exit group view.
4 Remove any service points on the Link Bonding group.
5 In root view, enter the following command to delete the group:

```
root>ethernet link-bonding delete group group_id <1-6>
```

7.2.10 L1 and L2 Header Compensation Values

This section provides the recommended settings for L1 Header Compensation and L2 Header Compensation. The recommended L1 and L2 Header Compensation values are determined by:

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBT Throughput Enhancement Disabled	**Header De-dup/LBT Throughput Enhancement Enabled**	**Header De-dup/LBT Throughput Enhancement Disabled**	**Header De-dup/LBT Throughput Enhancement Enabled**
0 (di	0–80	0–68	0–80	0–69

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
sabl	39	62	76	23

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
ed)				

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
1	8040	6863	8077	6924

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	–81	–69	–81	–70

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	37	60	73	19
2	81	69	81	70

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	38–8	61–7	74–8	20–7

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	2 3 5	0 5 8	2 6 9	1 1 5

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
3	8236	7059	8270	7116

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	–83	–71	–83	–72

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	33	56	65	11
4	83	71	83	72

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	34–8	57–7	66–8	12–7

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	431	254	461	307

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
5	8432	7255	8462	7308

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	–85	–73	–85	–74

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	29	52	57	03
6	85	73	85	74

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	308–8	537–7	588–8	047–7

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	627	450	653	500

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
7	8628	7451	8654	7501

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	–87	–75	–87	–75

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	25	49	50	96
8	87	75	87	75

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	26–8	50–7	51–8	97–7

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	823	647	846	692

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
9	8824	7648	8847	7693

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	–89	–77	–89	–77

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	21	45	42	88
10	89	77	89	77

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	22–9	46–7	43–9	89–7

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	019	843	038	884

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
11	9020	7844	9039	7885

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	–91	–79	–91	–79

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	17	41	34	80
12	91	79	91	79

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	18–9	42–8	35–9	81–8

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	215	039	230	076

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
13	9216	8040	9231	8077

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	–93	–81	–93	–81

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	13	37	26	73
14	93	81	93	81

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	149	388	279	748

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	411	235	423	269

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
15	9412	8236	9424	8270

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	– 95	– 83	– 95	– 83

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	09	33	19	65
16	95	83	95	83

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	10–9	34–8	20–9	66–8

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	607	431	615	461

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
17	9608	8432	9616	8462

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	–97	–85	–97	–85

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	05	29	11	57
18	97	85	97	85

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	06–9	30–8	12–9	58–8

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	803	627	807	653

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
19	9804	8628	9808	8654

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	–99	–87	–99	–87

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	01	25	03	50
20	99	87	99	87

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	02–1	26–8	04–1	51–8

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
	0 0 0 0	8 2 3	0 0 0 0	8 4 6

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
21	n/a	8824	n/a	8847

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		– 89		– 89

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		2 1		4 2

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
22	n/a	8922	n/a	8943

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		–90		–90

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		19		38

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LB Throughput Enhancement Disabled	**Header De-dup/LB Throughput Enhancement Enabled**	**Header De-dup/LB Throughput Enhancement Disabled**	**Header De-dup/LB Throughput Enhancement Enabled**
23	n/a	9020	n/a	9039

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		– 91		– 91

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		17		34

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LB Throughput Enhancement Disabled	**Header De-dup/LB Throughput Enhancement Enabled**	**Header De-dup/LB Throughput Enhancement Disabled**	**Header De-dup/LB Throughput Enhancement Enabled**
24	n/a	9118	n/a	9135

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		–92		–92

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		15		30

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
25	n/a	9216	n/a	9231

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		–93		–93

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		13		26

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
26	n/a	9314	n/a	9327

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		–94		–94

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		11		23

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
27	n/a	9412	n/a	9424

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		–95		–95

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		09		19

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
28	n/a	9510	n/a	9520

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		–96		–96

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		07		15

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
29	n/a	9608	n/a	9616

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		–97		–97

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		05		11

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
30	n/a	9706	n/a	9712

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		–98		–98

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		03		07

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
31	n/a	9804	n/a	9808

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		– 99		– 99

L1HeaderCompensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	HeaderDe-dup/LBThroughputEnhancementDisabled	**HeaderDe-dup/LBThroughputEnhancementEnabled**	**HeaderDe-dup/LBThroughputEnhancementDisabled**	**HeaderDe-dup/LBThroughputEnhancementEnabled**
		01		03

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LB Throughput Enhancement Disabled	**Header De-dup/LB Throughput Enhancement Enabled**	**Header De-dup/LB Throughput Enhancement Disabled**	**Header De-dup/LB Throughput Enhancement Enabled**
32	n/a	9902	n/a	9904

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		–100		–100

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**
		00		00

- For radio interfaces, type of main unit
- For Ethernet interfaces, type of paired unit to which the interface is connected
- Link Bonding Standard or Enhanced mode
- Header De-duplication or Link Bonding Throughput Enhancement Enabled or Disabled on the main unit (for radio interfaces) or the paired unit (for Ethernet interfaces)

Note: For PTP 850E, the values provided in this section are accurate for devices using System Release 12.7. For other System Release versions, refer to the User Guide for the version the device is running.

7.2.10.1 L1 Header Compensation – Recommended Values

L1 Header Compensation should not be enabled for the following interface types:

- Ethernet interface connected to an PTP 850C
- Ethernet interface connected to a third-party device with throughput up to 800 Mbps. For higher throughput.

For other interface types, L1 Header Compensation should be configured according to the tables below.

7.2.10.2 L1 Header Compensation for PTP 850*E* and PTP 850EX

This applies to:

- When PTP 850E is the main unit: the radio interface
- When PTP 850E is the paired unit in an PTP 850E XPIC configuration: the Ethernet interface connected to the paired unit

Note: Link Bonding Throughput Enhancement is not supported with PTP 850EX.

The L1 Header Compensation should be the number shown in the left column for the range that matches the Shaper Actual Bit Rate for the interface in the relevant column. For example, if the Link Bonding group is set to Standard Link Bonding mode, Link Bonding Throughput Enhancement is enabled on the PTP 850E, and the Shaper Actual Bit Rate is 7780, the L1 Header Compensation should be set to 9.

Table 17: L1 Header Compensation for Ethernet Interface Connected to PTP 850E or PTP 850EX

7.2.10.3 L1 Header Compensation for Ethernet Interface Connected to PTP 820C or PTP 820C-HP

Table 18 shows the recommended L1 Header Compensation values for Ethernet members of a Link Bonding group connected to an PTP 820C or PTP 820C-HP paired unit. The L1 Header Compensation should be the number shown in the left column for the range that matches the Shaper Actual Bit Rate for the interface in the relevant column. For example, if the Link Bonding group is set to Standard Link Bonding mode and Header De-Duplication is enabled on the PTP 820C/PTP 820C-HP, and the Shaper Actual Bit Rate is 1000, the L1 Header Compensation should be set to 32.

Table 18: L1Header Compensation for Ethernet Interface Connected to PTP 820C/PTP 820C-HP

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Disabled	**Header De-dup/LBThroughput Enhancement Enabled**	**Header De-dup/LBThroughput Enhancement Disabled**	**Header De-dup/LBThroughput Enhancement Enabled**

0 (disabled)	0–843	0–725	0-846	0-730
1	844-852	726–735	847-855	731-740
2	853–862	736–745	856-865	741-750
3	863–872	746–754	866-875	751-759
4	873–882	755–764	876-884	760-769
5	883–892	765–774	885-894	770-778
6	893	775	895	779

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LB Throughput Enhancement Disabled	**Header De-dup/LB Throughput Enhancement Enabled**	**Header De-dup/LB Throughput Enhancement Disabled**	**Header De-dup/LB Throughput Enhancement Enabled**
	–901	–784	-903	-788

7	902–911	785–794	904-913	789-798
8	912–921	795–803	914–923	799–807
9	922–931	804–813	924–932	808–817
10	932–941	814–823	933–942	818–826
11	942–950	824–833	943–9951	827–836
12	951–960	834–843	952–961	837–846
13	962–9	844–8	962–971	847–8

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LB Throughput Enhancement Disabled	**Header De-dup/LB Throughput Enhancement Enabled**	**Header De-dup/LB Throughput Enhancement Disabled**	**Header De-dup/LB Throughput Enhancement Enabled**
	70	52		55

14	971–980	853–862	972–980	856–865
15	981–990	863–872	981–990	866–875
16	991–1000	873–882	991–1000	876–884
17	1001–1004	883892	1001–1004	885–894
18	1005–1008	893–901	1005–1008	895–903
19	1009–1012	902–911	1009–1012	904–913

20	1013–1017	912–921	1013–1016	914–923
21	1018–1021	922–931	1017–1021	924–932
22	1022–1025	932–941	1022–1025	933–942
23	1026–1029	942–950	1026–1029	943–9951
24	1030–1034	951–960	1030–1033	952–961
25	1035–	962–9	1034–	962–

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LB Throughput Enhancement Disabled	**Header De-dup/LB Throughput Enhancement Enabled**	**Header De-dup/LB Throughput Enhancement Disabled**	**Header De-dup/LB Throughput Enhancement Enabled**
	1038	70	1038	971

26	1039–1042	971–980	1039–1042	972–980
27	1043–1047	981–990	1043–1046	981–990
28	1048–1051	991–1000	1047–1050	991–1000
29	n/a	963–1004	n/a	1001–1004
30	n/a	1005–1008	n/a	1005–1008
31	n/a	1009–	n/a	1009–

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LB Throughput Enhancement Disabled	**Header De-dup/LB Throughput Enhancement Enabled**	**Header De-dup/LB Throughput Enhancement Disabled**	**Header De-dup/LB Throughput Enhancement Enabled**
		1012		1012

32	n/a	1013–1017	n/a	1013–1016
33	n/a	1018–1021	n/a	1017–1021
34	n/a	1022–1025	n/a	1022–1025
35	n/a	1026–1029	n/a	1026–1029
36	n/a	1030–1034	n/a	1030–1033
37	n/a	1035–	n/a	1034–

L1 Header Compensation	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LB Throughput Enhancement Disabled	**Header De-dup/LB Throughput Enhancement Enabled**	**Header De-dup/LB Throughput Enhancement Disabled**	**Header De-dup/LB Throughput Enhancement Enabled**
		1038		1038

38	n/a	1039–1042	n/a	1039–1042
39	n/a	1043–1047	n/a	1043–1046
40	n/a	1048–1051	n/a	1047–1050

7.2.10.4 L1 Header Compensation for Ethernet Interface Connected to Third-Party Devices

Table 19 shows the recommended L1 Header Compensation values for Ethernet members of a Link Bonding group connected to a third-party paired unit. The L1 Header Compensation should be the number shown in the left column for the range that matches the Shaper Actual Bit Rate for the interface in the relevant column. For example, if the Link Bonding group is set to Standard Link Bonding mode and the Shaper Actual Bit Rate is 900, the L1 Header Compensation should be set to 6.

Table 19: L1Header Compensation for Ethernet Interface Connected to Third-Party Devices

L1 Header Compensation	**Link Bonding Standard Mode**	**Link Bonding Enhanced Mode**
0 (disabled)	0 – 843	0-846
1	844 - 852	847- 855
2	853 – 862	856- 865
3	863 – 872	866- 875
4	873- 882	876- 884
5	883- 892	885- 894
6	893- 901	895- 903
7	902- 911	904- 913
8	912- 921	914- 923
9	922- 931	924- 932

L1 Header Compensation	Link Bonding Standard Mode	Link Bonding Enhanced Mode
10	932-941	933-942
11	942-950	943-951
12	951-960	952-961
13	961-970	962-971
14	971-980	972-980
15	981-990	981-990
16	991-1000	991-1000

7.2.10.5 L2 Header Compensation – Recommended Values

The following are the recommended values per interface type. If AES-256 Payload Encryption is enabled on the radio, these numbers should be increased by 2. For example, if AES-256 Payload Encryption and Throughput Enhancement are enabled on an PTP 850C paired unit, the L2 Header Compensation for the Ethernet interface connected to the PTP 850C should be 16 (Standard Mode) or 18 (Enhanced Mode).

Table 20: L2 Header Compensation for Link Bonding Group Members

Interface Type	Link Bonding Standard Mode		Link Bonding Enhanced Mode	
	Header De-dup/LBThroughput Enhancement Dis	Header De-dup/LBThroughput Enhancement Ena	Header De-dup/LBThroughput Enhancement Dis	Header De-dup/LBThroughput Enhancement Ena

	a b l e d	b l e d	a b l e d	b l e d
Ethernet interface connected to PTP850E	24	12	26	14
Ethernet interface connected	26	n/a	28	n/a

to PTP850EX				
Ethernet interface connected to PTP850C	26	14	28	16
Ethernet interface con n	26	14	28	16

ected to PTP820C/PTP820C-HP				
Ethernet interface connected to Third-Party Devi	26		28	

c e		

Note: For third-party devices, the numbers listed above assume that a 4-byte GFP header added to packets. Without such a header, it may be necessary to reduce these numbers for optimal results.

7.2.11 Configuring Synchronization in a Link Bonding Node

SyncE and 1588 PTP can be used with Layer 1 Link Bonding. SyncE and 1588 PTP can be configured for both the main unit and the paired unit. Synchronization messages are passed between the units via the cable carrying L2 protocols data between the units. This can be the traffic cable or a separate Protocols cable.

7.2.11.1 Configuring SyncE in a Link Bonding Node

To configure SyncE on a Link Bonding node:

- On the local main unit, configure the following:
  - Configure the port connected to the external switch as a sync source with priority 1.
  - Configure radio interface 1 as a sync source with priority 2.
  - Configure radio interface 2 (if applicable) as a sync source with priority 3.
  - Configure the Protocols port as a sync source with priority 4 (or 3 for devices with one radio interface).
- On the local paired unit, configure the following:
  - Configure the Protocols port as a sync source with priority 1.
  - Configure radio interface 1 as a sync source with priority 2.
  - Configure radio interface 2 (if applicable) as a sync source with priority 3.
- On the remote paired unit, configure the following:
  - Configure radio interface 1 as a sync source with priority 1.
  - Configure radio interface 2 (if applicable) as a sync source with priority 2.
  - Configure the Protocols port as a sync source with priority 3 (or 2 for devices with one radio interface).
- On the remote main unit, configure the following:
  - Configure the Protocols port as a sync source with priority 1.
  - Configure radio interface 1 as a sync source with priority 2.
  - Configure radio interface 2 (if applicable) as a sync source with priority 3.
  - Configure the port connected to the external switch (Eth 1 or Eth 3) as a sync source with priority 4 (or 3 for devices with one radio interface).

All sync sources should be configured with Sync Interface Quality ”Automatic”.
For instructions on configuring SyncE.

7.2.11.2 Configuring 1588 PTP in a Link Bonding Node

Configuring 1588 PTP via the Main Units

1588 PTP can be passed directly between the main units. This requires that the Link Bonding group be configured for Enhanced Link Bonding mode. Most but not all PTP 850C and PTP 850E devices support Link Bonding Enhanced mode. For details.

If the Link Bonding group is configured for Enhanced Link Bonding mode, you can configure PTP for the Link Bonding Group by configuring 1588 Boundary Clock on the radio interface or Multi-Carrier ABC group that belongs to the Link Bonding group on both sides of the link.

To configure 1588 PTP via the main units:

1 Configure SyncE following the instructions in Configuring the Sync Source.
2 Enable 1588 PTP on each main unit on both sides of the link:

   i Select **Sync > 1588 > General Configuration**. The 1588 – General Configuration page opens.
   ii In the **1588 PTP** field, select **Enable**.
   iii Click **Apply**.

3 On the main unit on both sides of the link, enable Boundary clock on:

   - The port connected to the external switch.
   - The radio interface or Multi-Carrier ABC group.

4 In the Boundary Clock > Port Parameters page, you must enter a VLAN ID in the **VLAN ID** field for the radio or Multi-Carrier ABC group member of the Link Bonding group. Make sure to enter the same VLAN ID on both sides of the link.

Configuring 1588 PTP via the Paired Units

You can configure 1588 PTP via the paired units. This can be used for devices that do not support Link Bonding Enhanced mode. It can also be used as a backup for 1588 PTP via the main units, to ensure that 1588 PTP synchronization survives any down time on the link between the main units.

To configure 1588 PTP via the paired units, you must configure Boundary Clock on the main unit and Transparent Clock on all of the units, as described below. 1588 messages are generated by the Boundary Clock mechanism on the main unit and sent untagged to the paired unit via the cable carrying L2 protocols data between the units. This can be the traffic cable or a separate Protocols cable. They receive VLAN tagging on the paired unit in order to separate them from user traffic.

Note: If the paired unit goes down, 1588 packets will not be transmitted to the other side of the link.

To configure 1588 PTP for the Link Bonding node:

1 Configure SyncE following the instructions in Configuring the Sync Source.
2 Enable 1588 PTP on each unit, including the main unit and the paired unit on both sides of the link:

   i Select **Sync > 1588 > General Configuration**. The 1588 – General Configuration page opens.
   ii In the **1588 PTP** field, select **Enable**.
   iii Click **Apply**.

3 On the main unit on both sides of the link, enable Boundary clock on:

   - The port connected to the external switch.
   - The Protocols port.

4 On the paired unit on both sides of the link, enable Transparent Clock on the radio interface or Multi-Carrier ABC group.
5 On the paired unit on both sides of the link, configure a point-to-point service with service points on the radio interface or Multi-Carrier ABC group and on the Protocols port. The service points should be configured as follows:

- Service point on the Multi-Carrier ABC group:
  - Service Point Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation: Per customer’s choice
  - Allowing Flooding: Allow
  - Learning Admin: Disable
- Service point on the Protocols port:
  - Service Point Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation: Untagged
  - Allowing Flooding: Allow
  - Learning Admin: Disable

7.2.12 Procedure for Upgrading an Existing Link Bonding Group from Standard Mode to Enhanced Mode

The procedure for upgrading an existing Link Bonding group from Standard mode to Enhanced mode depends on whether or not the configuration uses in-band management. If it does, the management services must be carefully re-routed from the Protocols cable to the single cable for traffic and protocols, according to the instructions below.

Use one of the following procedures, according to whether the configuration uses in-band management:

- Upgrading to Enhanced Mode for Groups with In-Band Management
- Upgrading to Enhanced Mode for Groups without In-Band Management

7.2.12.1 Upgrading to Enhanced Mode for Groups with In-Band Management

To upgrade a Link Bonding group from Standard to Enhanced mode for configurations with in-band management:

1. Disable synchronization for the members of the Link Bonding group, i.e., make sure the members are not being used as Synchronization sources.
2. Remove the Ethernet interface connected to the paired unit for traffic from the Link Bonding group on both the local and the remote main units (the order does not matter).
3. On the remote paired unit, add a management service point to the radio or Multi-Carrier ABC group.
4. On the remote main unit, remove the management service point from the Link Bonding group. At this point, in-band management to the remote side of the link will be lost.
5. On the local main unit, remove the management service point from the Link Bonding group.
6. On the local paired unit, add a management service point to the radio or Multi-Carrier ABC group. At this point, in-band management to the remote side of the link will be restored.
7. Remove all the remaining members from the Link Bonding group on both the local and the remote main units (the order does not matter).
8. On the local and the remote main units, change the Link Bonding mode of the Link Bonding group from **Standard** to **Enhanced**.
9. On the local and the remote main units, add back all members of the Link Bonding group except the Ethernet interfaces connected to the Attached Units for traffic.
10. On the remote main unit, add a management service point to the Link Bonding group.
11. On the remote paired unit, remove the management service point from the radio. At this point, in-band management to the remote side of the link will be lost.
12. On the local paired unit, remove the management service point from the radio.
13. On the local main unit, add a management service point to the Link Bonding group. At this point, in-band management to the remote side of the link will be restored.
14. On the local and the remote paired unit, add a management service point to the single Ethernet interface connected to the main unit.
15. On the local and the remote paired units, remove the management service point from the Ethernet interface formerly connected to the main unit for Protocols. At this point, in-band management to the paired units will be lost.

Note: You can remove the Protocols cable now or at any subsequent point.

16 On the local and the remote main units, remove the management service point from the interface formerly connected to the paired unit for Protocols.
17 On the local and the remote main units, add the Ethernet interfaces connected to the paired units for traffic back to the Link Bonding group.
18 On the local and the remote main units, add a management service point to the single Ethernet interface connected to the paired units. At this point, in-band management to the Attached Units will be restored.
19 Reconfigure Radio Bandwidth Notification on both the main units and the paired units.
20 On the local and the remote main units, update the L2 Header Compensation values for the Ethernet interfaces connected to the paired units according to the values listed in L1 and L2 Header Compensation Values.
21 Enable PDU encapsulation on the paired units on the interfaces connected to the main units.
22 Adjust the Automatic State Propagation (ASP) configuration. In most respects, the ASP configuration should be the same as it was in Link Bonding Standard mode. However, in Enhanced mode, you must make sure to enable ASP Management Safe mode (CSF mode). This includes configuring the peer unit to receive CSF PDUs.
23 In the Link Bonding page (Figure 173), select the group and click **Edit Members**. The Edit Members page opens.
24 In the **Admin** column, set the Admin status of each group member to **Enable**.

Note: This parameter determines whether the group member is enabled in the group, not the Admin status of the interface or Multi-Carrier ABC group itself.

The Admin status must be set to **Disable** whenever you modify the **L1 header compensation** or **L2 header compensation** fields. Otherwise, an error message will appear.

25 Click **Apply**.
26 Reconfigure synchronization.

7.2.12.2 Upgrading to Enhanced Mode for Groups without In-Band Management

To upgrade a Link Bonding group from Standard to Enhanced mode for configurations without in-band management:

1 Disable synchronization for the members of the Link Bonding group, i.e., make sure the members are not being used as Synchronization sources.
2 Remove all members from the Link Bonding group on both the local and the remote main units (the order does not matter).
3 On the local and the remote main units, change the Link Bonding mode of the Link Bonding group from **Standard** to **Enhanced**.

Note: You can remove the Protocols cable now or at any subsequent point.

4 On the local and the remote main units, add back all members of the Link Bonding group.
5 On the local and the remote main units, change the L2 Header Compensation values for the Ethernet interfaces connected to the Attached Units according to the values listed in L1 and L2 Header Compensation Values.
6 Enable PDU encapsulation on the paired units on the interfaces connected to the main units.

7 Adjust the Automatic State Propagation (ASP) configuration. In most respects, the ASP configuration should be the same as it was in Link Bonding Standard mode. However, in Enhanced mode, you must make sure to enable ASP Management Safe mode (CSF mode). This includes configuring the peer unit to receive CSF PDUs, of Configuring Automatic State Propagation and Link Loss Forwarding.
8 Reconfigure Radio Bandwidth Notification on both the main units and the paired units.
9 On the paired units on both sides of the link, configure a point-to-point service for Link Bonding traffic, with service points on the radio interface or Multi-Carrier ABC group and on the interface connected to the main unit.
10 In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page opens.
11 In the **Admin** column, set the Admin status of each group member to **Enable**.

Note: This parameter determines whether the group member is enabled in the group, not the Admin status of the interface or Multi-Carrier ABC group itself.

The Admin status must be set to **Disable** whenever you modify the **L1 header compensation** or **L2 header compensation** fields. Otherwise, an error message will appear.

12 Click **Apply**.
13 Reconfigure synchronization.

7.2.13 Procedure for Configuring Third-Party Devices for Operation in Link Bonding Configurations

For Layer 1 Link Bonding configurations in which the paired unit is a third-party device rather than an PTP 850 or PTP 820 device, you must perform a special OAM CCM configuration to ensure that any traffic flow issues on the paired unit are reported to the main unit. This OAM CCM configuration replaces the functionality that is implemented by means of Automatic State Propagation (ASP) and Radio Bandwidth Notification (RBN) for configurations in which the paired unit is an PTP 850 or PTP 820 device.

The OAM CCM mechanism consists of:

- A SOAM MEP which is configured on the main unit interface connected to the paired unit for L2 protocols data (the Protocols port). In single-cable configurations, this is the port used for the single traffic and protocols cable. In two-cable configurations, this is the port used for the Protocols cable.
- A point-to-point service which is configured on the paired unit connected the radio and the port on the paired unit connected to the main unit for L2 protocols data (the Protocols port). In single-cable configurations, this is the port used for the single traffic and protocols cable. In two-cable configurations, this is the port used for the Protocols cable.

  If a loss-of-connectivity event takes place on the paired unit, the MEP detects the event and sets the shaper to 0 on the Link Bonding member that represents the port connected to the paired unit for traffic (the Traffic port). Once this happens, the main unit stops transmitting traffic to the paired unit.

  When traffic to the paired unit is stopped, a user-configurable Wait-to-Restore (WTR) timer starts. Once CCM messages indicate that the loss of connectivity on the paired unit has been restored for the length of the timer, the shaper is reset to its previous value and normal operation is resumed.

  The following events cause the shaper to be set to 0:

- CCM defects are detected via the main unit's Protocols port.

- The Protocols port is down on the main or paired unit.
- The Traffic port is down on the main or paired unit.

To configure OAM CCM for Link Bonding configurations in which the paired unit is a third-party device:

1 On the main unit, create a point-to-point service with a service point on the Protocols port:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Any VLAN from 1 to 4090.
- Allow Flooding: Allow
- Learning Admin: Disable

2 Configure a SOAM MD.

- To configure a SOAM MD via the Web EMS:

i On the main unit, select **Ethernet** > **Protocols** > **SOAM** > **MD**. The SOAM MD page opens.
ii Click **Add**. The SOAM MD – Add page opens.
iii In the **MD Name** field, enter an identifier for the MD (up to 43 alphanumeric characters). The MD Name should be unique over the domain. You must use the same MD Name for the main units on the local and remote side of the link.
iv In the **MD Format** field, select **None**.
v In the **MD Level** field, select 7 to ensure that CCM frames for the Link Bonding group are given priority.
vi Click **Apply**, then **Close**.

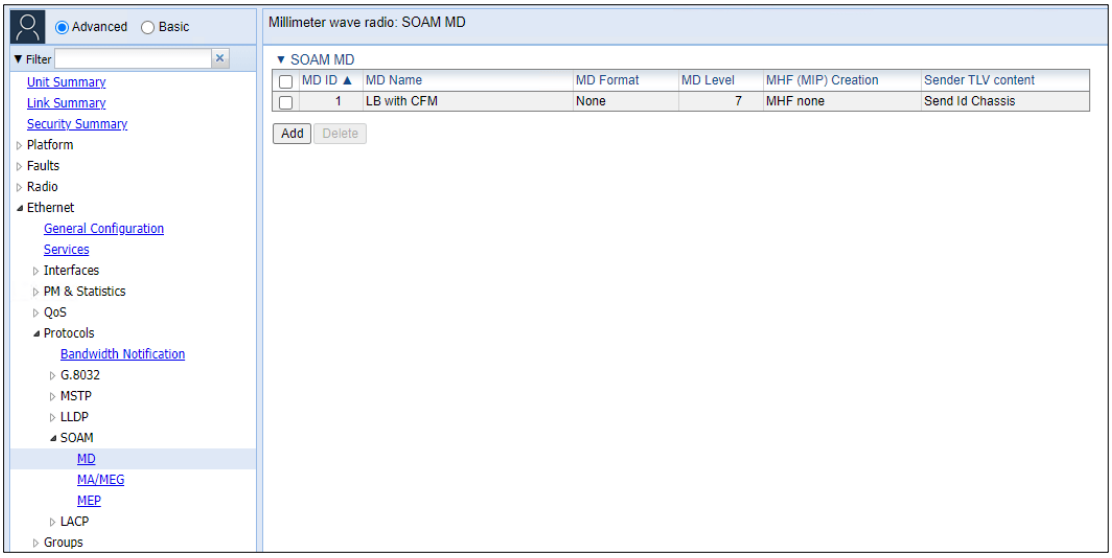


Figure 168: SOAM MD Page – MD for Link Bonding

- To configure a SOAM MD via the CLI:

On the main unit, enter the following command in root view:

```
root> ethernet soam md create md-id <md-id> md-format none md-
name <md-name> md-level <md-level>
```

Use the following parameters:

- md-id – Use any unique number between 1 and 4294967295.
- md-name – Enter an identifier for the MD (up to 43 alphanumeric characters). The MD Name should be unique over the domain. You must use the same MD Name for the main units on the local and remote side of the link.
- md-level – Enter 7 to ensure that CCM frames for the Link Bonding group are given priority.

For example:

```
root> ethernet soam md create 1 md-format none md-name lb1ccm
md-level 7
```

3 Configure a SOAM MEG.

- To configure a SOAM MEG via the Web EMS:

i On the main unit, select **Ethernet** > **Protocols** > **SOAM** > **MA/MEG**. The SOAM MA/MEG page opens (Figure 530).
ii Click **Add MEG**. The SOAM MA/MEG – Add page opens.
iii In the **MD** field, enter the MD you created in Step 2.
iv In the **MA/MEG short name** field, enter a name for the MEG (up to 44 alphanumeric characters). You must use the same MEG name for the main units on the local and remote side of the link.
v In the **MEG Level** field, select **7**.
vi In the **CCM Interval** field, select **100 ms**.
vii In the **Service ID** field, select the service you created in Step 1.
viii In the **MFH (MIP) Creation** field, select **MHF none**.
ix In the **Tx Sender ID TLV content** field, select **Send Id Defer**.
x Click **Apply**, then **Close**.

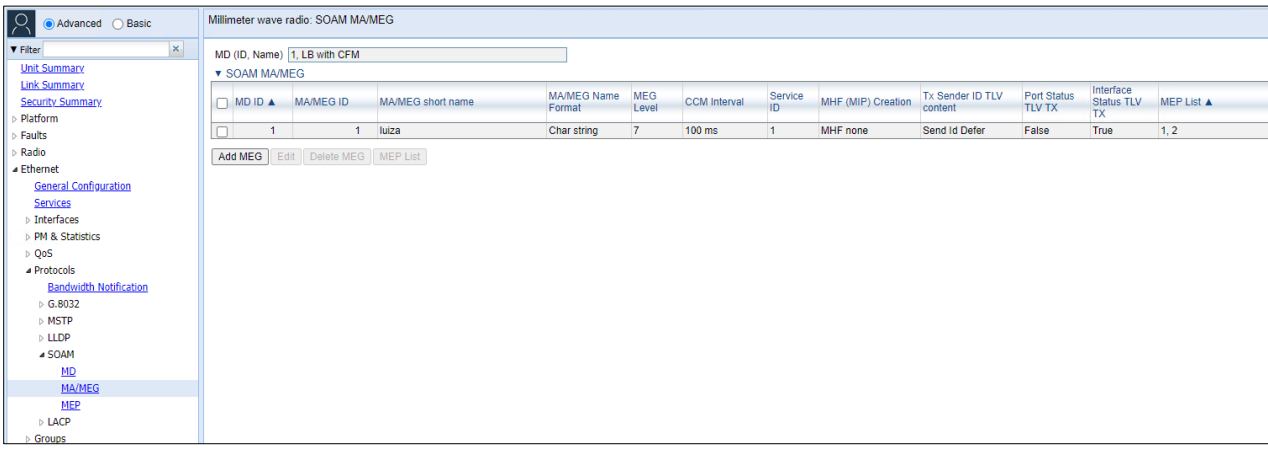


Figure 169: SOAM MA/MEG Page – MEG for Link Bonding

- To configure a SOAM MEG via the CLI:

i On the main unit, enter the following command in root view:

```
root> ethernet soam meg create meg-id <meg-id> meg-fmt
charString meg-name <meg-name> meg-level <meg-level> service-id
<0-4095>
```

Use the following parameters:

- `meg-id` – Use the md-id of the SOAM MD you created in Step 2.
- `meg-name` – Enter a name for the MEG (up to 44 alphanumeric characters). You must use the same MEG name for the main units on the local and remote side of the link.
- `meg-level` – Enter 7.
- `service-id` – Enter the service ID of the service you created in Step 1.

ii On the main unit, set the interval at which CCM messages are sent within the MEG by entering the following command in root view:

```
root> ethernet soam meg ccm-interval set meg-id <meg-id> ccm <ccm>
```

Use the following parameters:

- `meg-id` – Use the meg-id you configured in the previous command.
- `ccm` – enter interval100ms

For example:

```
root> ethernet soam meg create meg-id 1 meg-fmt charString meg-
name lb1ccm meg-level 7 service-id 1
```

```
root> ethernet soam meg ccm-interval set meg-id 1 ccm interval100ms
```

4 Configure two MEPs, one for the local and one for the remote side of the link. The local and remote devices must each use unique MEP IDs.

- To configure a MEP via the Web EMS:

i Select **Ethernet > Protocols > SOAM > MA/MEG**. The SOAM MA/MEG page opens.
ii Select the MEG you created in Step 3.
iii Click **MEP List**. The MEP List page opens.
iv Click **Add**. The Add MEP page opens.
v In the **MEP ID** field, enter a MEP ID (1-8191).
vi Click **Apply**.
vii In the **MEP ID** field, enter an additional MEP ID (1-8191).
viii Click **Apply**, then **Close**.
ix Select **Ethernet > Protocols > SOAM > MEP**. The SOAM MEP page opens.
x In the **MD** field, enter the MD you created in Step 2.
xi Click **Add**. Page 1 of the Add SOAM MEP wizard opens.
xii In the **MA/MEG Name** field, select the MEG you created in Step 3.
xiii Click **Next**. Page 2 of the Add SOAM MEP wizard opens.
xiv In the **Direction** field, select **Down**.
xv In the **MEP ID** field, select the MEP you created in Steps i through viii.
xvi In the **Service Point** field, select the service point you created in Step 1.
xvii Verify that you want to submit the displayed parameters and click **Submit**.

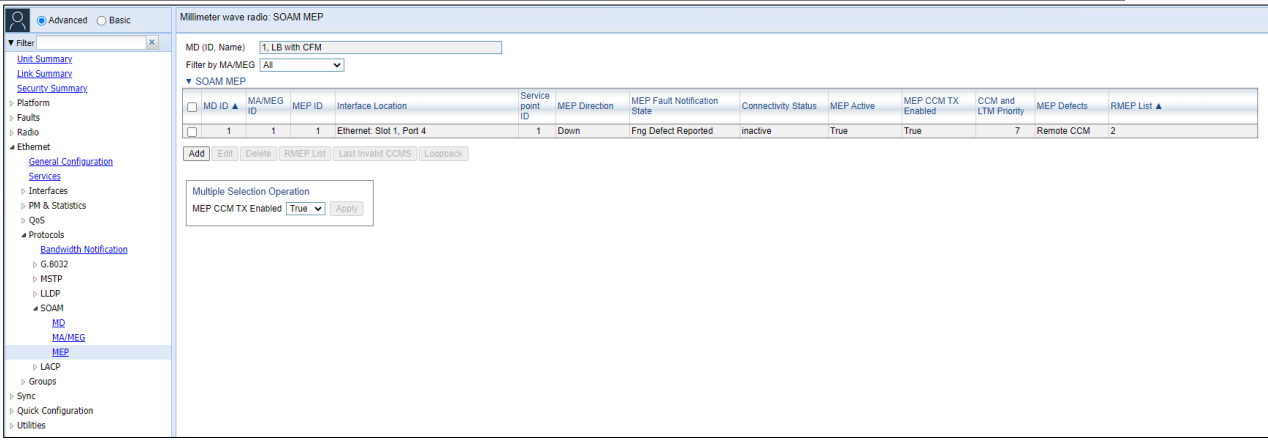


Figure 170: SOAM MEP Page – MEP for Link Bonding

- To configure a MEP via the CLI:

i On the main unit, configure two MEPs, one for the local and one for the remote side of the link. The local and remote devices must each use unique MEP IDs. Use the following command in root view for each MEP:

```
root> ethernet soam meg mep add meg-id <meg-id> mep-id <mep-id>
```

Use the following parameters:

- `meg-id` – Use the meg-id you configured in Step 3.
- `mep-id` – Enter a MEP ID (1-8191). Repeat the command to enter a second MEP ID.

ii On the main unit, assign the MEP to the service point you created in Step 1 by entering the following command in root view:

```
root> ethernet soam mep create meg-id <meg-id> mep-id <mep-id>
sp-id <sp-id> mep-dir <mep-dir>
```

Use the following parameters:

- `meg-id` – Use the meg-id you configured in Step 3.
- `mep-id` – Enter the ID of the MEP you created in the previous step.
- `sp-id` – Enter the ID of the service point you created in Step 3.
- `mep-dir` – Enter `down`.

For example:

```
root> ethernet soam meg mep add meg-id 1 mep-id 3

root> ethernet soam mep create meg-id 1 mep-id 3 sp-id 1 mep-dir
down
```

5 On the main unit, enable the MEP.

- To enable the MEP via the Web EMS:

i In the SOAM MEP page, select the MEP you created in Step 4.
ii Click **Edit**. The SOAM MEP - Edit page opens.
iii In the **MEP Active** field, select **True**.
iv In the **MEP CCM TX Enable** field, select **True**.
v In the **CCM and LTM Priority** field, select the p-bit that will be included in CCMs sent by this MEP (0 to 7). It is recommended to select 7.
vi Click **Apply**, then **Close**.

- To enable the MEP via the CLI:

i Enter the following command in root view to set the MEP to Active:

```
root> ethernet soam mep active set meg-id <meg-id> mep-id <mep-id> mep-active true
```

ii Enter the following command in root view to enable CCM messages for the MEP:

```
root> ethernet soam mep ccm-enable set meg-id <meg-id> mep-id <mep-id> enabled true
```

iii Enter the following command in root view to select the p-bit that will be included in CCMs sent by this MEP (0 to 7). It is recommended to select 7:

```
root> ethernet soam mep ccm-ltm-prio set meg-id <meg-id> mep-id <mep-id> ccm-ltm-priority <0-7>
```

For example:

```
root> ethernet soam mep active set meg-id 1 mep-id 3 mep-active true
```

```
root> ethernet soam mep ccm-enable set meg-id 1 mep-id 3 enabled true
```

```
root> ethernet soam mep ccm-ltm-prio set meg-id 1 mep-id 3 ccm-ltm-priority 7
```

6 On the paired third-party unit, create a point-to-point service between the radio and the port on the paired unit connected to the main unit for L2 protocols data (the Protocols port). This service should be Untagged.

7 On the main unit, configure the SOAM CCM parameters for the Link Bonding group.

- To configure the SOAM CCM parameters for the Link Bonding group via the Web EMS:

i Select the Link Bonding group in the Link Bonding page and click **Members CCM LOC**. The Members CCM LOC page opens.

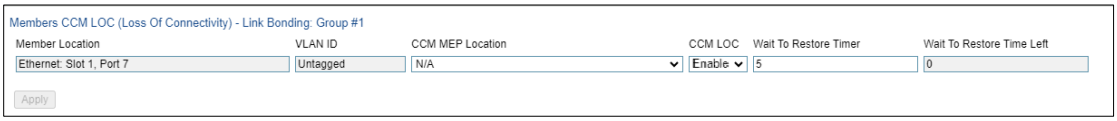


Figure 171: Link Bonding – Members CCM LOC Page

ii In the **CCM MEP Location** field, select the local MEP you created in Step 4.

iii In the **CCM LOC** field, select **Enable**.

iv In the **Wait to Restore Time** field, enter a number (in seconds) for the WTR timer (0-84600).

- To configure the SOAM CCM parameters for the Link Bonding group via the CLI:

i Use the following commands to enter Link Bonding group member view for the Ethernet interface group member:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface eth slot 1 port <port>
```

If the Protocols port is the PTP 850E Management port, use the following command syntax:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface mng
slot 1 port 1
```

ii Use the following command to connect the Link Bonding group to the MEP:

```
lbg-member[eth1/X]>ccm-loc add ccm-loc-service-id <Service id>
ccm-loc-sp-id <SP ID> ccm-loc-meg-level 7 ccm-loc-admin enable
```

The Service ID and SP ID parameters should be the service and service points you created in Step 1. For example, if the Traffic port is port 4, the service ID is 1, and the service point ID is 1, enter the following command:

```
lbg-member[eth1/4]>ccm-loc add ccm-loc-service-id 1 ccm-loc-sp-
id 1 ccm-loc-meg-level 7 ccm-loc-admin enable
```

If the Traffic port is the PTP 850E Management port, the service ID is 2, and the service point ID is 3, enter the following command:

```
lbg-member[mng1/1]>ccm-loc add ccm-loc-service-id 2 ccm-loc-sp-
id 3 ccm-loc-meg-level 7 ccm-loc-admin enable
```

iii Use the following command to configure the WTR timer:

```
lbg-member[eth1/|mng1/X]> wait-to-restore set wtr <0-84600>
```

The wtr parameter is configured in seconds. The default value is 5. For example, the following command sets the WTR timer to 20 seconds:

```
lbg-member[eth1/|mng1/X]> wait-to-restore set wtr 20
```

The following commands are also available:

- To enable or disable the CCM mechanism, enter the following command:

```
lbg-member[eth1/X]> ccm-loc admin set ccm-loc-admin
<enable|disable>
```

- To remove the CCM, enter the following command:

```
lbg-member[eth1/X]> ccm-loc remove
```

- To display the CCM configuration, enter the following command:

```
lbg-member[eth1/X]> ccm-loc show
```

For example:

```
lbg-member[eth1/4]>ccm-loc show
CCM LOC MEP location: SOAM Service 1, Service Point 1, Level 7
CCM LOC ADMIN:   enable
WTR timer:       5
WTR status:      0
lbg-member[eth1/4]>
```

- To display the WTR timer, enter the following command:

```
lbg-member[eth1/X]> wait-to-restore show
```

7.2.13.1 Alarms for CCM LOC Configuration

The following alarms can be used to identify and troubleshoot issues that arise via the CCM LOC mechanism:

- Alarm ID 5033 – MEP RDI received. This indicates that a Remote Defect Indication has been received from the remote MEP.

- Alarm ID 5034 – Remote MEP CCMs are not received. This alarm is raised if the MEP is not receiving CCMs from at least one of the remote MEPs.

  All of these alarms are cleared and the shaper is set back to its original value once the WTR timer has expired. For more details about these and all the other alarms, refer to the MIB Reference Guide for PTP 850 Products.

7.3 Configuring 4+0 Layer 1 Link Bonding

Note: This section is only relevant for PTP 850C.

4+0 Layer 1 Link Bonding links can also be configured using the Quick Configuration wizard. It is recommended to use the wizard whenever possible. See *Configuring a Layer 1 Link Bonding Link Using the Quick Configuration Wizard*.

This section includes:

- 4+0 Layer 1 Link Bonding Overview
- Configuring 4+0 Layer 1 Link Bonding
- Enabling Link Bonding Throughput Enhancement for 4+0 Layer 1 Link Bonding
- Editing a Link Bonding Group or its Members
- Displaying Statistics for a Link Bonding Group
- Deleting a Link Bonding Group

7.3.1 4+0 Layer 1 Link Bonding Overview

Layer 1 Link Bonding aggregates an Ethernet link and four radio carriers into a single link with a single-cable connection to the switch. 4+0 Link Bonding enables you to double the capacity of a 2+0 link. When utilizing XPIC and high-modulation ACM profiles, 4+0 Link Bonding can provide capacity of up to 4 Gbps over 112 MHz channels or 8 Gbps over 224 MHz channels.

In a 4+0 Link Bonding configuration, each PTP 850C unit can use a different frequency, providing operators with more flexibility to utilize the available frequency spectrum in whatever way is most efficient.

For PTP 850C 4+0 Layer 1 Link Bonding links, line redundancy is available. For details, refer to Layer 1 Link Bonding and Line Redundancy and Configuring Line Redundancy for Layer 1 Link Bonding Configurations.

Note: In addition to the configuration described in this section, PTP 850C can be used in Layer 1 Link Bonding configurations with PTP 820N and PTP 820A. For details, refer to Section 6.4, *Configuring Layer 1 Link Bonding*, in the User Guide for PTP 820N and PTP 820A.

7.3.1.1 4+0 Layer 1 Link Bonding Operation

A 4+0 Link Bonding node consists of two PTP 850C units, a main unit and a paired unit. The main unit is attached to the external switch via either Eth 1 (P2, the PoE port) or Eth 3 (P4, the MIMO port).

Note: Although MIMO is not currently supported with PTP 850C, it is planned for future release. Therefore, any customer considering adding MIMO capabilities to the link in the future should use Eth 1 for connection to the external switch in order to leave Eth 3 available for future upgrade to MIMO.

Traffic is passed between the two PTP 850C units via an optical cable that connects Eth 3 (P4, the MIMO port) or Eth 4 (P5) of each unit. This is a 10 Gbps connection with a bidirectional capacity of up to 4 Gbps. The same cable can be used to carry L2 protocol data between the two units.

Alternatively, an optical Protocols cable can be connected between Eth 2 (P3) of each unit to carry L2 protocol data between the two units. These ports must be configured to 2.5 Gbps.

Note: Although MIMO is not currently supported with PTP 850C, it is planned for future release. Therefore, any customer considering adding MIMO capabilities to the link in the future should use Eth 4 for the traffic connection between the two units in order to leave Eth 3 available for future upgrade to MIMO.

It is important to note that special SFP+ modules must be used for both the inter-unit traffic ports (Eth 3/P4 or Eth 4/P5) and (if a separate Protocols cable is used) the Protocols ports (Eth 2, P3). For details and the marketing models of the required SFP+ modules, as well as the optical cables, see the Installation Guide for PTP 850C.

You must configure a Multi-Carrier ABC group on each PTP 850C unit. Each group should include both of the unit's radio carriers.

You must configure a Link Bonding group on the main unit. The Link Bonding group must include the main Unit's Multi-Carrier ABC group and the port carrying traffic between the main unit and the paired unit (Eth 3 or Eth 4).

Each PTP 850C unit is managed separately and independently. In-band management can be configured so that both units are managed over the link.

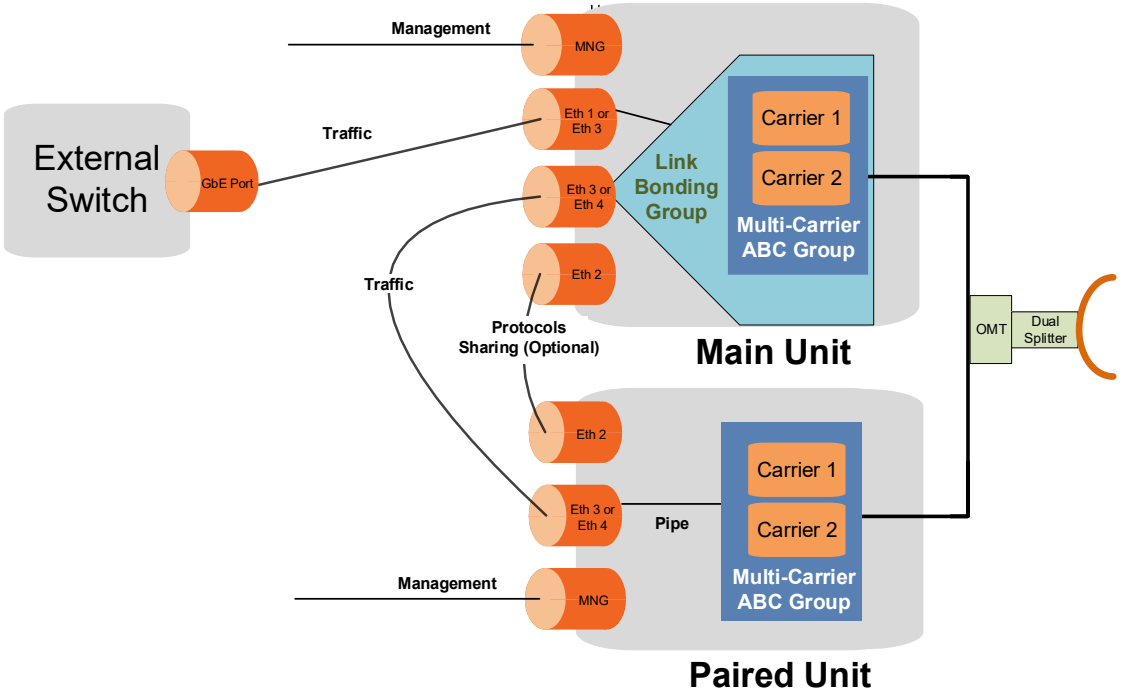


Figure 172: Layer 1 Link Bonding Operation – 4+0 PTP 850C

Note: Line protection with 4+0 Layer 1 Link Bonding is planned for future release.

7.3.1.2 4+0 Layer 1 Link Bonding Hardware Configuration

The two PTP 850C units can be connected to a single antenna using a Dual Splitter and an OMT. Remote-mount configurations are also available. The hardware configuration for 4+0 Link Bonding uses the same mediation devices as PTP 820C.

7.3.2 Configuring 4+0 Layer 1 Link Bonding

To configure a 4+0 Layer 1 Link Bonding node:

1 Connect the external switch to Eth 1 (P2, the PoE port) or Eth 3 (P4, the MIMO port) on the main PTP 850C unit.
2 On both the main unit and the paired unit, configure the port speed of the Traffic port between the two units (Eth 3 or Eth 4) to 10 Gbps.
3 If you are using a separate Protocols cable, on both the main unit and the paired unit, configure the port speed of Eth 2 to 2.5 Gbps.
4 Connect an optical cable between the ports used to transmit traffic and (optionally) L2 protocol data between the two units.
5 In the Interface Manager, set the port connected to the paired unit for passing traffic between the two units to **Admin** = **Down**.
6 Optionally, connect an optical cable between Eth 2 (P3) of each PTP 850C unit. This cable carries L2 protocol data between the two units.

Note: Special SFP+ modules must be used for both the inter-unit traffic ports and the Protocols ports. For details and the marketing models of the required SFP+ modules, as well as the optical cables, see the Installation Guide for PTP 850C.

7 Configure the script and radio settings for both the main unit and the paired unit, including XPIC.
8 On both the main unit and the paired unit, configure a Multi-Carrier ABC group that includes both of the unit's radio carriers.
9 On the main unit only, configure a Link Bonding group that includes the port carrying traffic between the two units (Eth 3 or Eth 4) and the Multi-Carrier ABC group:

Note: Before adding a group member, make sure that no shapers or service points are configured on the interface or group.

i Select **Ethernet** > **Groups** > **Link Bonding**. The Link Bonding page opens.

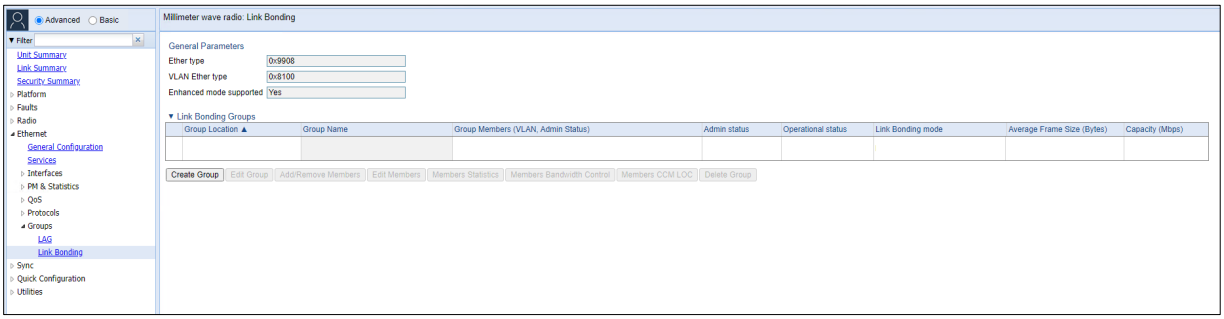


Figure 173: Link Bonding Page (Empty)

ii Click **Create Group**. Page 1 of the Link Bonding Group wizard opens.

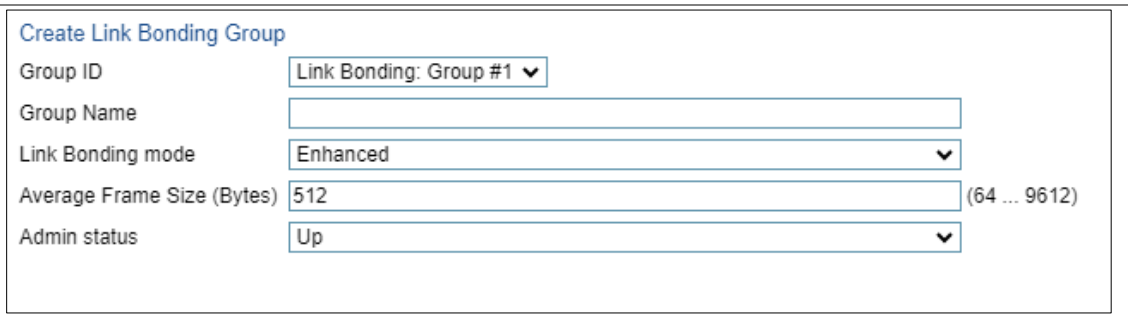


Figure 174: Link Bonding Group Wizard – Page 1

iii In the **Group ID** field, select **Link Bonding: Group #1**.
iv Optionally, in the **Group Name** field, enter a descriptive name for the group.
v In the **Link Bonding Mode** field, select **Standard** or **Enhanced**. You must select **Enhanced** if the configuration uses a single cable for traffic and L2 protocol data.
In the **Average Frame Size** field, enter a value for calculating the estimated current potential capacity. For an explanation of this field, see Link Bonding L1 Capacity Calculator.

Note: The Average Frame Size does not affect the actual transmitted traffic It is only used to help estimate the current potential capacity.

vi In the **Admin status** field, select **Up**.
vii Click **Next**. The Member #1 page opens.

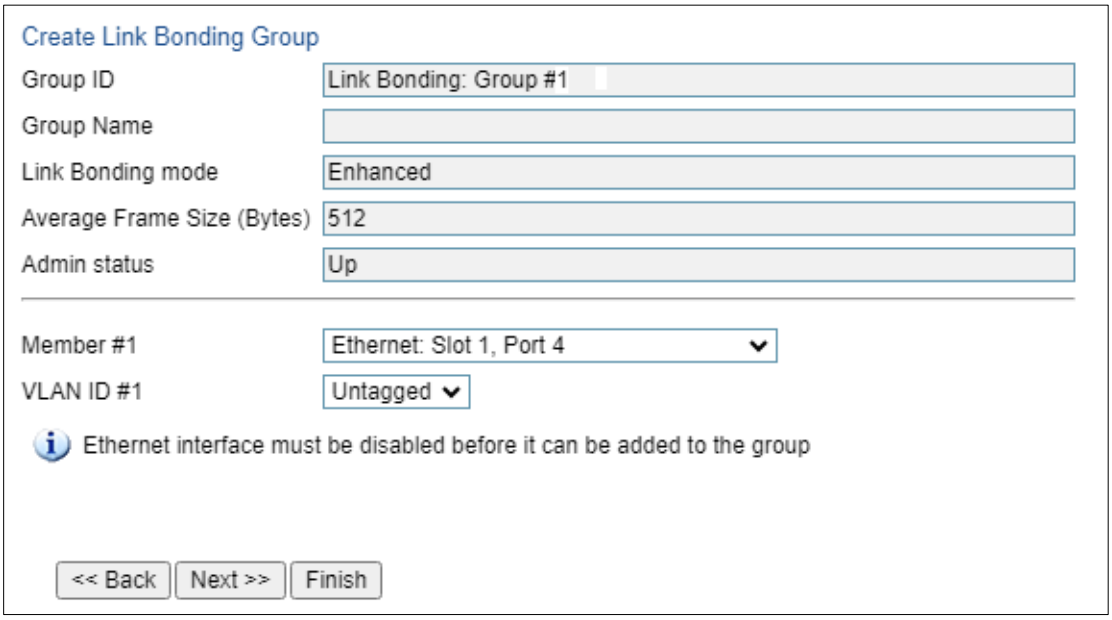


Figure 175: Link Bonding Group Wizard – Member #1 Page

viii In the **Member #1** field, select the Ethernet interface connected to the paired unit for traffic (Eth 3 or Eth 4).
ix In the **VLAN ID #1** field, select **Untagged**.
x Click **Next**. The Member #2 page opens.

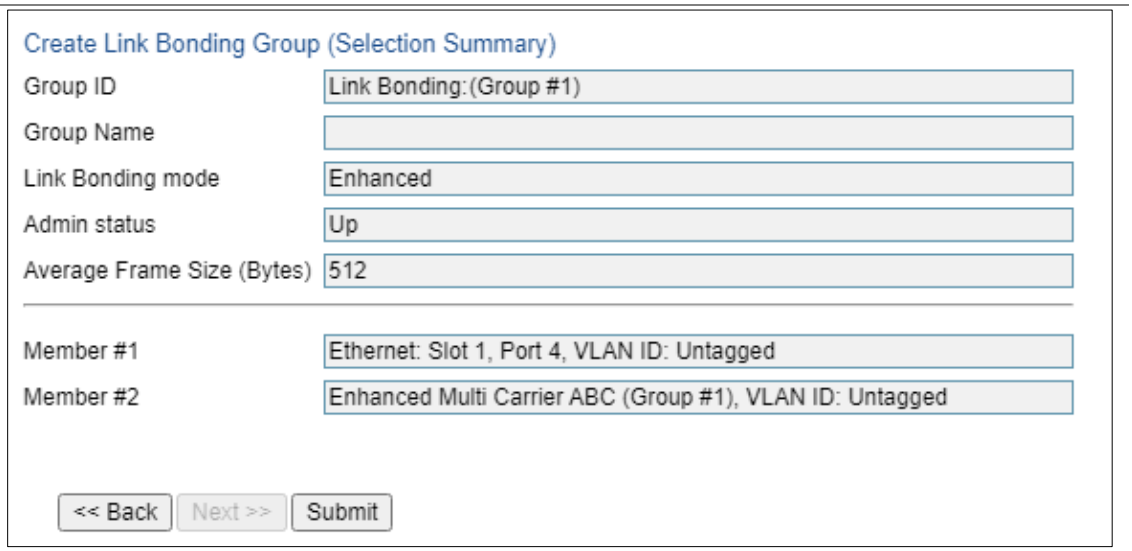


Figure 176: Link Bonding Group Wizard – Member #2 Page

xi In the **Member #2** field, select the Enhanced Multi Carrier ABC group.
xii In the **VLAN ID #2** field, select **Untagged**.
xiii Click **Finish**. The Selection Summary page opens.

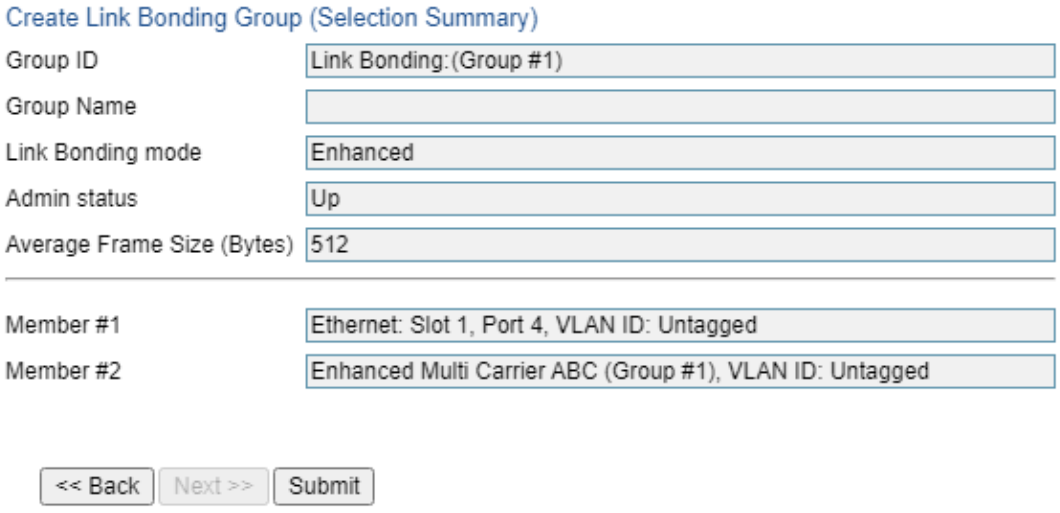


Figure 177: Link Bonding Group Wizard – Selection Summary Page

xiv Click **Submit**. The group is added to the Link Bonding page.

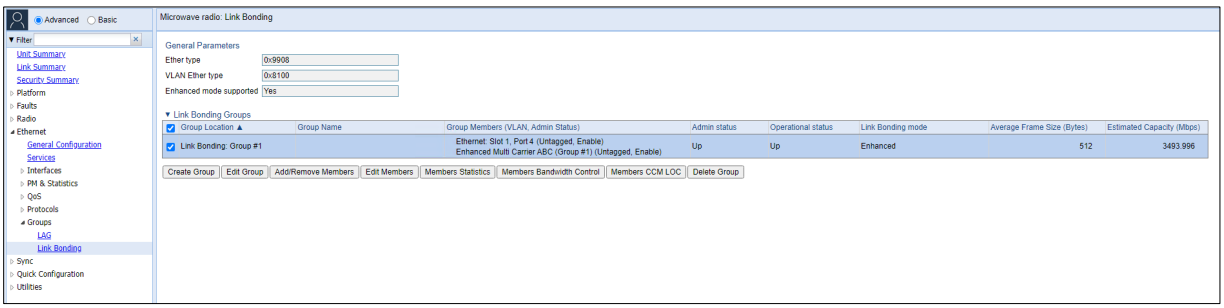


Figure 178: Link Bonding Page (Populated)

Note: For an explanation of the Average Frame Size and Capacity fields, see Link Bonding L1 Capacity Calculator.

10 In the Interface Manager, set the port connected to the paired unit for passing traffic between the two units (Eth 3 or Eth 4) to **Admin** = **Up**.

11 Enable PDU encapsulation on the paired unit:

Note: This step is crucial since it ensures that protocols packets are properly tagged and separated from traffic.

i Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens.

ii Select the port used for L2 protocols data (the Protocols port) and click **Edit**. The Logical Interfaces – Edit page opens.

Note: In a single-cable configuration, this is the port that carries traffic and L2 protocols data between the two units. In a two-cable configuration, this is the port to which the Protocols cable is connected.

iii In the field **PDU Encapsulation** field, select **Yes**.

iv Click **Apply**.

12 To ensure proper fault handling, configure Automatic State Propagation. For single-cable configurations, you must enable ASP Management Safe mode (CSF mode) to ensure that in-band management is not disrupted in case of a fault on one of the ports connecting the main and paired units. This includes configuring the peer unit to receive CSF PDUs.

v On the local and remote main units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The Link Bonding group
- Controlled Port: The port connected to the external switch (Eth 1 or Eth 3)

vi On the local and remote paired units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The Multi-Carrier ABC group
- Controlled Port: The port carrying traffic between the two units (Eth 3 or Eth 4)

13 In-band management can be carried between the main unit and the paired unit via the cable carrying L2 protocols data between the units. This can be the traffic cable (Eth 3 or Eth 4) or a separate Protocols cable (Eth 2). To configure in-band management, you must define a management service that connects the port used for L2 protocols data (the Protocols port) on both units, the Link Bonding groups, and the ingress port of the main unit:

i On the local main unit, configure a service point on the port connected to the external switch (Eth 1 or Eth 3).

ii On the local main unit, configure a service point on the Protocols port.

iii On the local main unit, configure a service point on the Link Bonding group.

iv On the local paired unit, configure a service point on the Protocols port.

v On the remote paired unit, configure a service point on the Protocols port.

vi On the remote main unit, configure a service point on the Protocols port.

vii On the remote main unit, configure a service point on the Link Bonding group.

14 Configure Radio Bandwidth Notification on the main unit by performing the following steps:

i Select the Link Bonding group in the Link Bonding page and click **Members Bandwidth Control**. The Members Bandwidth Control page opens.

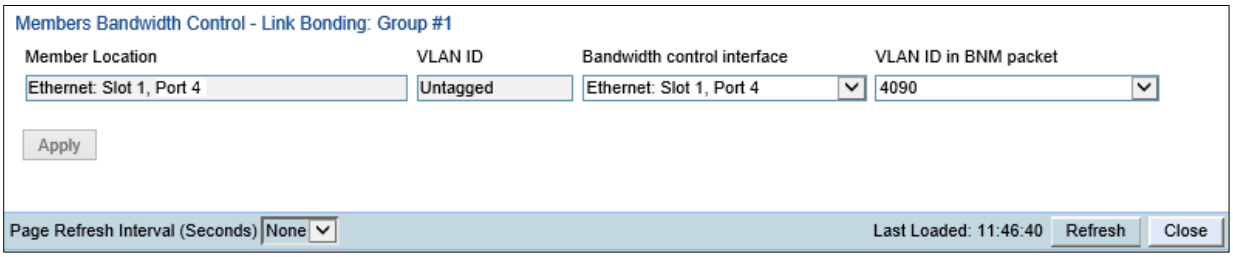


Figure 179: Link Bonding – Members Bandwidth Control Page (Single-Cable Configuration)

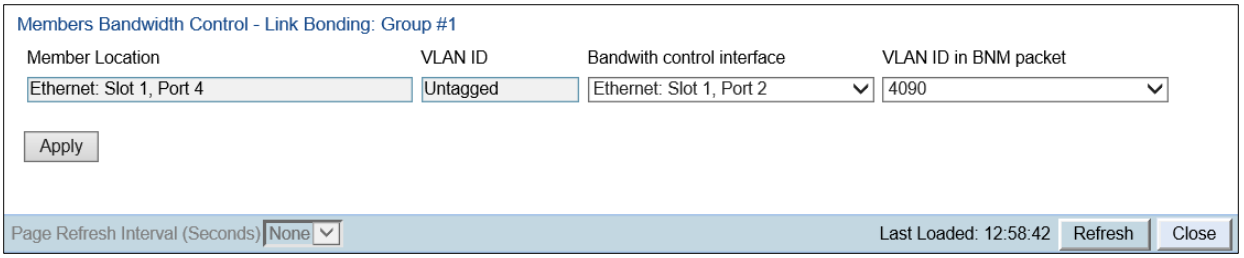


Figure 180: Link Bonding – Members Bandwidth Control Page (Two-Cable Configuration)

ii In the **Bandwidth control interface** column:

- For single-cable configurations, select the same port as displayed in the **Member Location** field (**Ethernet: Slot 1, Port 3** or **Ethernet: Slot 1, Port 4**)
- For two-cable configurations, select the port to which the Protocols cable is connected (**Ethernet: Slot 1, Port 2**).

iii In the **VLAN ID in BNM packet** column, select a VLAN ID. You can use any available VLAN ID from 1 to 4090. This is the VLAN use to transfer protocol information between the two units.

iv Click **Apply**.

15 In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page opens.

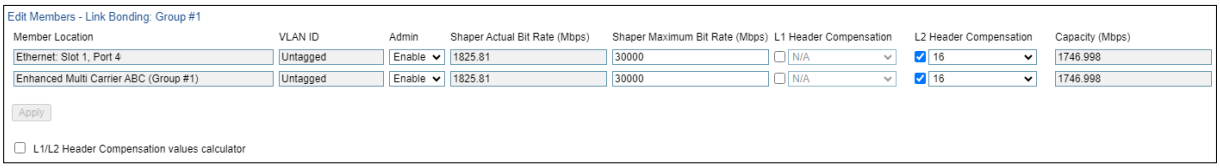


Figure 181: Link Bonding Groups – Edit Members Page

16 In the **Shaper actual bit rate** column, you can adjust the shaper for either or both interfaces in the group. Generally, there is no need to change this parameter from its default value of 30000 Mbps. The **Shaper actual bit rate** column displays the actual current traffic distribution between the main Unit (the radio interface) and the paired unit (the Ethernet interface, through which traffic is sent to the paired unit). This is displayed in units of Mbps**.**

17 In the **L1 header compensation** column, neither interface should be selected.

18 In the **L2 header compensation** column, both interfaces should be selected. For recommended values, see L1 and L2 Header Compensation Values.

19 Click **Apply**.

20 In the **Admin** column, set the Admin status of each group member to **Enable**.

Note: If necessary, you can leave the Admin status of the group members **Disable** until a later time in order to complete the configuration with the group offline, then activate the group members later.

The Admin status must be set to **Disable** whenever you modify the **L1 header compensation** or **L2 header compensation** fields. Otherwise, the modification will have no effect.

21 Click **Apply**.

22 Configure Radio Bandwidth Notification on the paired unit by performing the following steps:

i Select **Ethernet** > **Protocols** > **Bandwidth Notification**. The Bandwidth Notification page opens.

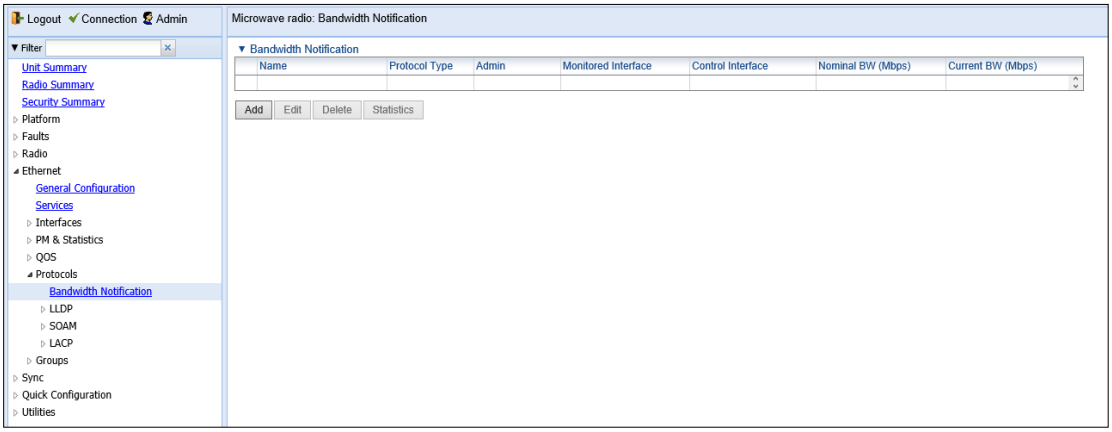


Figure 182: Bandwidth Notification Page (Empty)

ii Click **Add**. The Bandwidth Notification – Add page opens.

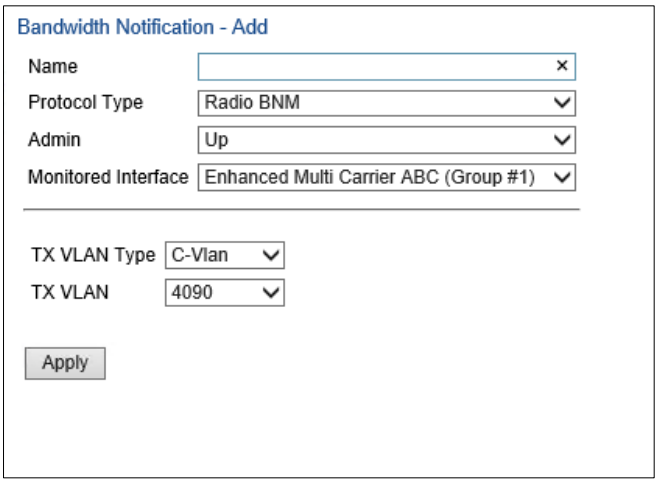


Figure 183: Bandwidth Notification – Add Page

iii In the **Name** field, select a descriptive name.

iv In the **Protocol Type** field, select **Radio BNM**.

v In the **Admin** field, select **Up**.

vi In the **Monitored Interface** field, select the paired unit's Multi-Carrier ABC group.

vii In the **TX VLAN Type** field, select **C-Vlan**.

viii In the **TX VLAN** field, select **the same VLAN you configured** In the **VLAN ID in BNM packet** column for the main unit.

ix Click **Apply**. The configuration is added to the Bandwidth Notification page with the Protocol Type **Radio BNM**.

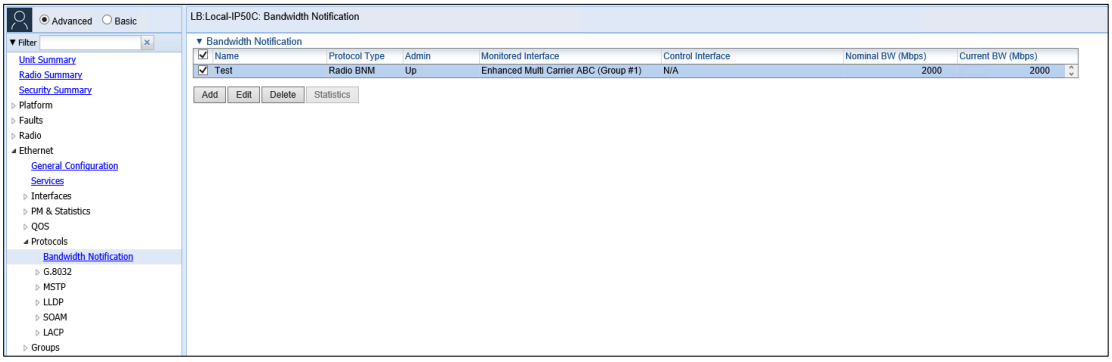


Figure 184: Bandwidth Notification Page (Populated with Radio BNM)

23 On the paired unit on both sides of the link, configure a point-to-point service for Radio Bandwidth Notification, with service points on the Multi-Carrier ABC group and on the interface connected to the main unit for L2 protocols data (the Protocols port). In single-cable configurations, this is the port used for the single traffic and protocols cable. In two-cable configurations, this is the port used for the Protocols cable.

The service points should be configured as follows:

i Create a service point on the Multi-Carrier ABC group with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Use the VLAN you configured in the **VLAN ID in BNM packet** column in Step 14
- Allow Flooding: Allow
- Learning Admin: Disable

ii Create a service point on the Protocols port with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Use the VLAN you configured in the **VLAN ID in BNM packet** column in Step 14
- Allow Flooding: Allow
- Learning Admin: Disable

See Configuring Service Points.

24 On the main unit on both sides of the link, create a point-to-point service for Link Bonding traffic, with service points on the port attached to the external switch and the Link Bonding Group. Both service points should be configured as follows:

- Type: PIPE
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Untagged
- Allow Flooding: Allow
- Learning Admin: Disable

25 On the paired unit on both sides of the link, configure a point-to-point service for Link Bonding traffic, with service points on the Multi-Carrier ABC group and on the interface connected to the main unit for traffic (the Traffic port).

The service points should be configured as follows:

Note: This service is a workaround for SYSTEM RELEASE117-1749, to ensure that customer traffic is separated from Radio Bandwidth Notification protocol traffic.

i Create a service point on the Multi-Carrier ABC group with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Untagged
- Allow Flooding: Allow
- Learning Admin: Disable

ii Create a service point on the Traffic port with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Untagged
- Allow Flooding: Allow
- Learning Admin: Disable

7.3.3 Configuring Line Redundancy with Multiband and Link Bonding

For an overview of Line Redundancy with Multiband and Link Bonding, see Multiband with Layer 1 Link Bonding and Line Redundancy.

Before proceeding with the instructions below, perform the basic Link Bonding configurations described in Configuring Multiband with Layer 1 Link Bonding.

To configure Line Redundancy in a Multiband configuration with Link Bonding:

1 Verify that the port on the paired unit connected to the external switch is set to the same port speed as the port on the main unit connected to the external switch.
2 Make sure that QoS is configured on the paired unit the same as on the main unit.
3 Enable and configure line protection on the main units on both sides of the link:

i Select **Platform > Shelf Management > Line Redundancy**. The Line Redundancy page opens.

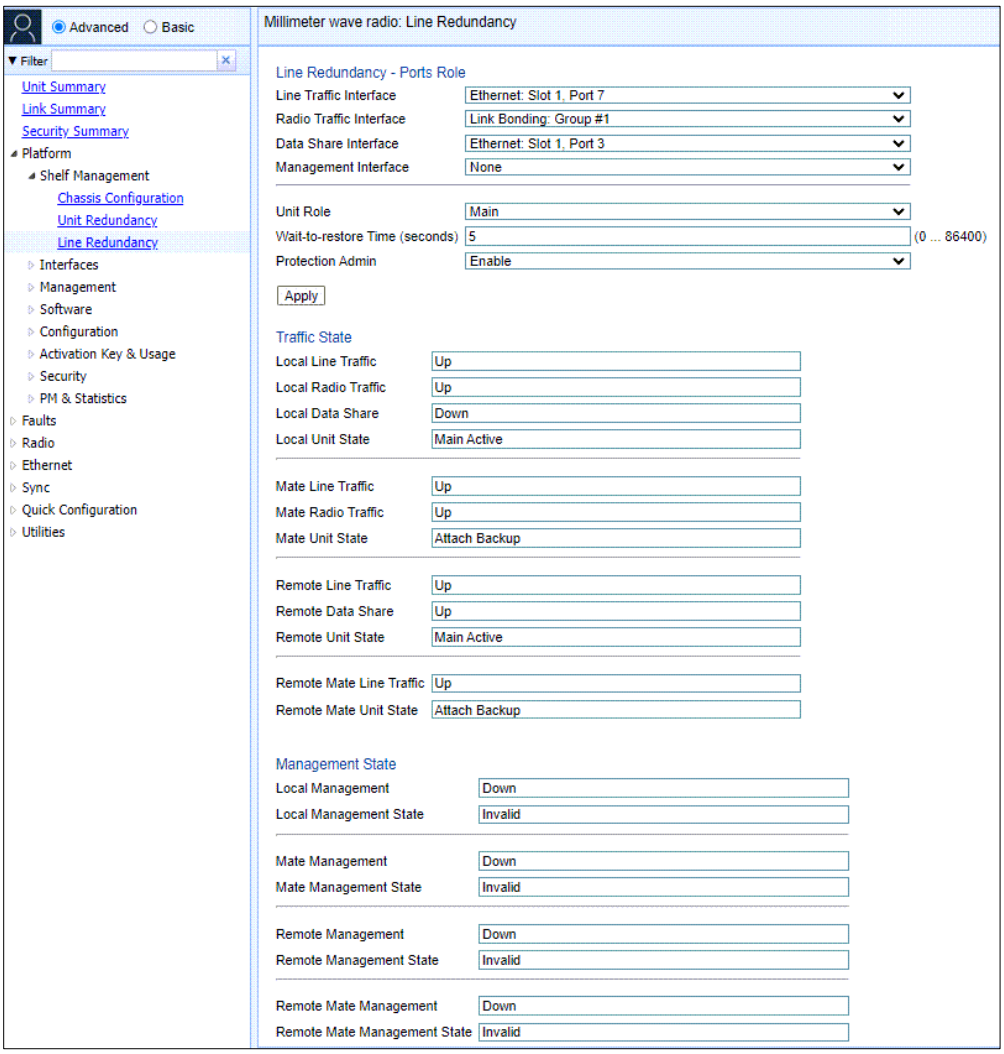


Figure 185: Line Redundancy Page (Main Unit)

ii In the **Line Traffic Interface** field, select the interface connected to the external switch.
iii In the **Radio Traffic Interface** field, select the Link Bonding group.
iv In the **Data Share Interface** field, select the interface connected to the paired unit.

v In the **Management Interface** field, leave the default value of **None**. This field is not operational in System Release 12.7.
vi In the **Unit Role** field, select **Main**.
vii In the **Wait-to-restore time** field, enter the number of seconds to set the Revertive timer's WTR timer. When a failure condition is resolved after a switchover has taken place, the WTR timer is the time the system waits before restoring the system to its normal operational configuration. The value range is 0-84600 seconds. The default is 5 seconds.
viii In the **Protection Admin** field, select **Enable**.
ix Click **Apply**.

4 Enable and configure line protection on the paired units on both sides of the link:

i Select **Platform > Shelf Management > Line Redundancy**. The Line Redundancy page opens.

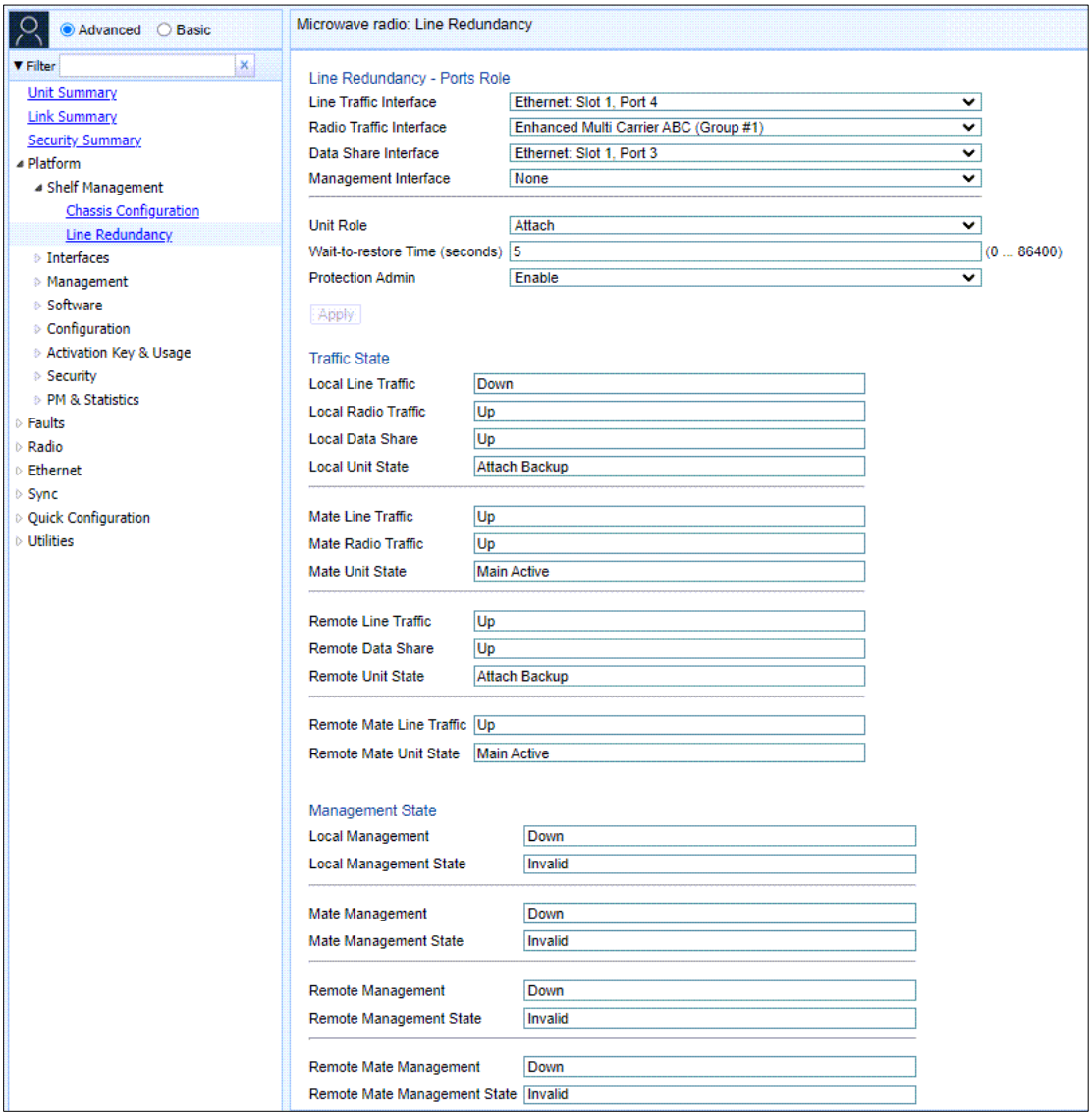


Figure 186: Line Redundancy Page (Paired Unit)

ii In the **Line Traffic Interface** field, select the interface connected to the external switch.
iii In the **Radio Traffic Interface** field, select the Multi-Carrier ABC group. If a single radio interface is being used, select the interface.

iv In the **Data Share Interface** field, select the interface connected to the main unit.
v In the **Management Interface** field, leave the default value of **None**. This field is not operational in System Release 12.7.
vi In the **Unit Role** field, select **Attach**.
vii In the **Wait-to-restore time** field, enter the number of seconds to set the Revertive timer's WTR timer. When a failure condition is resolved after a switchover has taken place, the WTR timer is the time the system waits before restoring the system to its normal operational configuration. The value range is 0-84600 seconds. The default is 5 seconds.
viii In the **Protection Admin** field, select **Enable**.
ix Click **Apply**.

5 On the paired unit on both sides of the link, create a point-to-point service for protection traffic, with service points on the port attached to the external switch and the Multi-Carrier ABC group or radio. Set the **Admin** state of the service to **Operational**.

Note: The Line Redundancy mechanism activates and deactivates these services based on the Line Redundancy operating state and role configurations, so they are not active during normal operation even though they are configured as **Operational**. They are automatically activated in case of Line Redundancy switchover.

Both service points should be configured as follows:

- Type: PIPE
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Untagged
- Allow Flooding: Allow
- Learning Admin: Disable

6 For management, add service points on the management service on the following interfaces on the paired unit:

- The interface connected to the external switch.
- The Multi-Carrier ABC group.

7 If SyncE is configured on the link, add the interface on the paired unit connected to the external switch as a Sync Source, with priority 3.

7.3.3.1 Line Redundancy with Multiband and Link Bonding – Status Parameters

The status indications for Traffic State are available for the following interfaces:

- Local Line Traffic
- Local Radio Traffic
- Local Data Share
- Mate Line Traffic
- Mate Radio Traffic
- Remote Line Traffic
- Remote Data Share
- Remote Mate Line Traffic

Possible statuses are:

- Down
- Unknown
- Invalid
- Up

The following unit status indications are available:

- Local Unit State
- Mate Unit State
- Remote Unit State
- Remote Mate Unit State

Possible statuses are:

- Main Active
- Main Fault
- Attach Backup
- Attach Active
- Main Forced Active
- Main Forced Fault
- Attach Forced Backup
- Attach Forced Active

Note: In System Release 12.7, the Management State fields are not operational.

Table 21: Link Bonding Line Redundancy Status Parameters

Parameter	Definition
Local Line Traffic	Indicates if there is traffic on the interface that connects the external switch to the local main unit.
Local Radio Traffic	Indicates if there is radio traffic on the local main unit.

Parameter	Definition
Local Data Share	Indicates if data is passing between the local main and paired units.
Local Unit State	Indicates the protection state on the local side of the link: • **Attach Backup** – The local main unit is functioning properly and the local paired unit is in backup state • **Attach Active** – Switchover has taken place due to a fault on the main unit and the local paired unit is functioning properly. • **Attach Forced Backup** – The local paired unit was active, but was manually placed in backup state by a forced switch command. • **Attach Forced Active** – The local paired unit is active as the result of a forced switch command.
Mate Line Traffic	Indicates if there is traffic on the interface that connects the external switch to the local paired unit.
Mate Radio Traffic	Indicates if there is radio traffic on the local paired unit.
Mate Unit State	Indicates the protection state on the local side of the link: • **Main Active**– The local main unit is functioning properly and the local paired unit is in backup state. • **Main Fault** – The local main unit is down and the local paired unit is acting as the main unit. • **Main Forced Backup** – The local main unit was manually placed in backup state by a forced switch command. • **Main Forced Active** – The local main unit was in backup state but was manually placed in active state as the result of a forced switch command.
Remote Line Traffic	Indicates if there is traffic on the interface that connects the external switch to the remote main unit.
Remote Data Share	Indicates if data is passing between the remote main and paired units.

Parameter	Definition
Remote Unit State	• Indicates the protection state on the remote side of the link: • **Attach Backup** – The remote main unit is functioning properly and the remote paired unit is in backup state • **Attach Active** – Switchover has taken place due to a fault on the remote main unit and the remote paired unit is functioning properly. • **Attach Forced Backup** – The remote paired unit was active, but was manually placed in backup state by a forced switch command. • **Attach Forced Active** – The remote paired unit is active as the result of a forced switch command.
Remote Mate Line Traffic	Indicates if there is traffic on the interface that connects the external switch to the remote paired unit.
Remote Mate Unit State	Indicates the protection state on the remote side of the link: • **Main Active**– The remote main unit is functioning properly and the remote paired unit is in backup state. • **Main Fault** – The remote main unit is down and the remote paired unit is acting as the main unit. • **Main Forced Backup** – The remote main unit was manually placed in backup state by a forced switch command. • **Main Forced Active** – The remote main unit was in backup state but was manually placed in active state as the result of a forced switch command.

7.3.4 Enabling Link Bonding Throughput Enhancement for 4+0 Layer 1 Link Bonding

After configuring a Link Bonding node, it is recommended to enable Link Bonding Throughput Enhancement. Link Bonding Throughput Enhancement is available for both the main unit and the paired unit.

Link Bonding Throughput Enhancement can be enabled on the Multi-Carrier ABC groups on both the main and the paired units. When it is enabled on the main unit, the L2 Header Compensation for the group must be reduced by 12. When it is enabled on the paired unit, the L2 Header Compensation for the Ethernet interface connected to the paired unit must be reduced by 12.

The Link Bonding Throughput Enhancement and L2 Header Compensation settings must be the same for the main units on both sides of the link. Therefore,

the changes should be applied in the following order to ensure that management is not lost:

Note: The settings on paired units do not affect management, and can be changed in any order.

1 Enable Link Bonding Throughput Enhancement on the remote unit (main and/or paired unit):

i Select **Radio > Ethernet Interface > Configuration**. The Radio Ethernet Interface Configuration page opens.

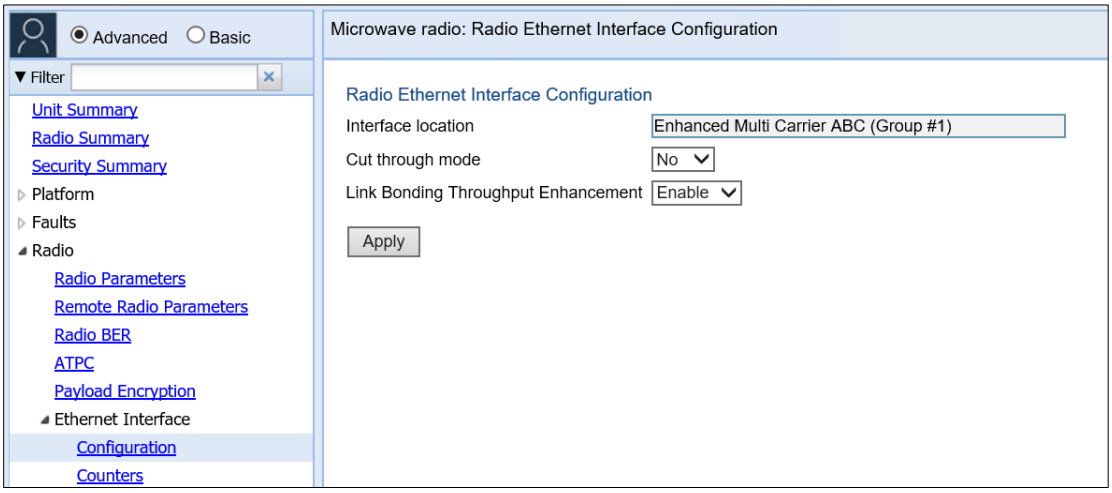


Figure 187: Radio Ethernet Interface Configuration Page (PTP 850C)

ii In the **Link Bonding Throughput Enhancement** field, select **Enable**.
iii Click **Apply**.

2 Enable Link Bonding Throughput Enhancement on the local unit (main and/or paired unit):

i Select **Radio > Ethernet Interface > Configuration**. The Radio Ethernet Interface Configuration page opens.
ii In the **Link Bonding Throughput Enhancement** field, select **Enable**.
iii Click **Apply**.

3 Modify the L2 Header Compensation (decrease by 12) on the remote unit (main and/or paired unit):

i Select **Ethernet** > **Groups** > **Link Bonding**. The Link Bonding page opens.
ii In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page opens.
In the L2 header compensation column, adjust the L2 Header Compensation according to the values listed in L1 and L2 Header Compensation Values.
iii Click **Apply**.

4 Modify the L2 Header Compensation (decrease by 12) on the local unit (main and/or paired unit):

i Select **Ethernet** > **Groups** > **Link Bonding**. The Link Bonding page opens.
ii In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page opens.
iii In the **L2 header compensation** column, adjust the L2 Header Compensation according to the values listed in L1 and L2 Header Compensation Values.
iv Click **Apply**.

7.3.5 Editing a Link Bonding Group or its Members

To change the Group Name or the Admin Status of the Link Bonding group:

1 In the Link Bonding page, select the group and click **Edit Group**. The Edit Group page opens.

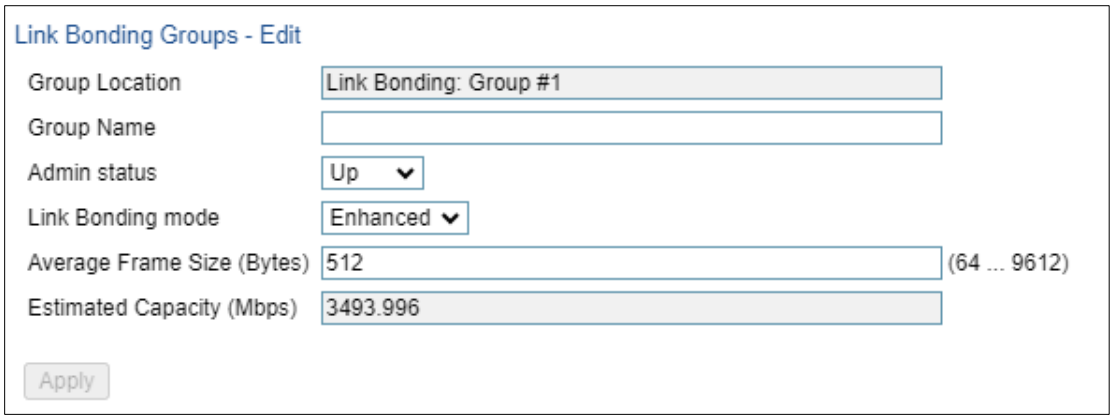


Figure 188: Link Bonding Groups – Edit Page

2 In the **Group Name** field, enter the new name.
3 In the **Admin status** field, change the Admin status of the group to **Up** or **Down**.
4 Click **Apply**.

Note: For an explanation of the Link Bonding mode field, see Requirements and Limitations for Enhanced Link Bonding Mode. For an explanation of the Average Frame Size and Capacity fields, see Link Bonding L1 Capacity Calculator.

7.3.6 Displaying Statistics for a Link Bonding Group

You can display the total number of segments and bytes (TX and RX) that have passed through each member of the Link Bonding group.

	Note:

Note: The ability to clear member statistics is planned for future release.

You can also display and configure thresholds for throughput and utilization on both the group and the member levels. For further information, see Link Bonding PMs.

You can also display and configure thresholds for throughput and utilization on both the group and the member levels. For further information.

To display throughput statistics for the members of the Link Bonding group:

1 In the Link Bonding page, select the group and click **Member Statistics**. The Member Statistics page opens.

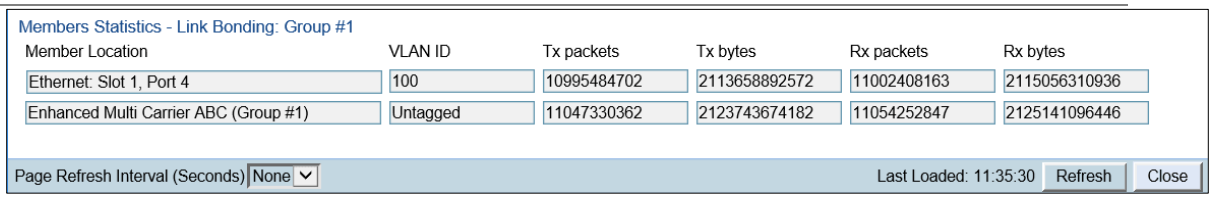


Figure 189: Link Bonding Groups – Member Statistics Page

7.3.7 Deleting a Link Bonding Group

To delete a Link Bonding group, you must first remove the members from the group:

1 In the Link Bonding page, select the group and click **Add/Remove Members**. The Add/Remove Members page opens.

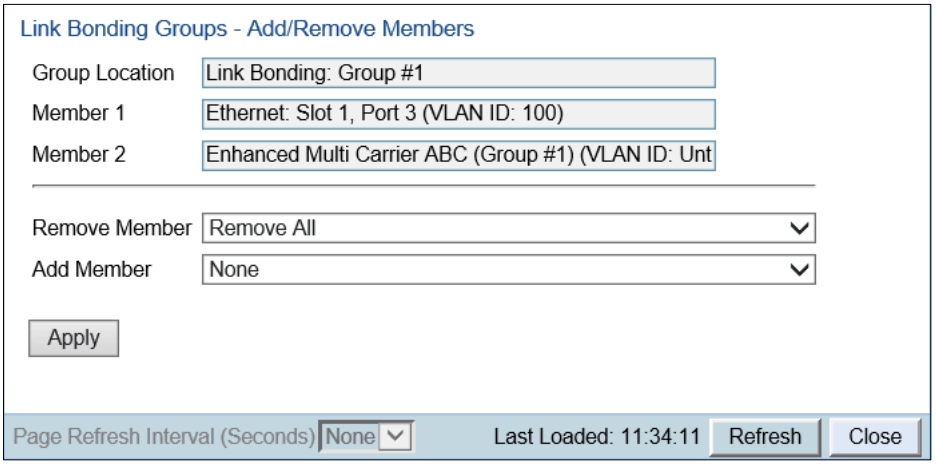


Figure 190: Link Bonding Groups – Member Statistics Page

2 In the **Remove Member** field, select **Remove All**.
3 Click **Apply**.
4 Remove any service points on the Link Bonding group.
5 In the Link Bonding page, select the group and click **Delete Group**.

7.4 Configuring Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP

Note:

Layer 1 Link Bonding links can also be configured using the Quick Configuration wizard. It is recommended to use the wizard whenever possible.

This section includes:

- Overview of Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C HP
- Configuring a Layer 1 Link Bonding Node with PTP 850C and PTP 820C or PTP 820C HP
- Enabling Link Bonding Throughput Enhancement for Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP
- Editing a Link Bonding Group or its Members
- Displaying Statistics for a Link Bonding Group

- Deleting a Link Bonding Group

7.4.1 Overview of Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP

Layer 1 Link Bonding can be used to pair an PTP 850C with an PTP 820C or PTP 820C-HP. This enables operators to add an PTP 850C to existing PTP 820C or PTP 820C-HP deployments in order to add significantly to node capacity utilizing the same physical footprint, adding to rather than replacing the existing PTP 820C or PTP 820C-HP and its capacity. A node using PTP 850C and PTP 820C or PTP 820C-HP with Link Bonding can provide capacity of up to 5 Gbps when both units are utilizing both of their carriers, XPIC, and their widest supported channels and highest modulations.

Note: Only PTP 820C ESS and ESX hardware versions are supported with this configuration.

In addition to the configuration described in this section, PTP 850C can be used in Layer 1 Link Bonding configurations with PTP 820N and PTP 820A.

7.4.1.1 Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP – Operation

In a Layer 1 Link Bonding configuration with an PTP 850C and an PTP 820C or PTP 820C-HP, the PTP 850C serves as the main unit. The PTP 820C or PTP 820C-HP is the paired unit. The main unit is attached to the external switch via either Eth 1 (P2, the PoE port), Eth 3 (P4), or Eth 4 (P5).

Note: If you are using a separate Protocols cable, Eth 1 cannot be used if the paired unit is an PTP 820C ESX, because Eth 1 must be used for the Protocols cable, as described below.

Traffic is passed between the two units via an optical cable that connects each unit. This is a 1 Gbps connection. The same cable can be used to carry L2 protocol data between the two units.

Alternatively, an optical Protocols cable can be used to carry L2 protocol data between the two units. The Protocols cable must be connected between the following ports:

- PTP 850C with PTP 820C (ESS hardware version) or PTP 820C-HP – Eth 3 (P4) or Eth 4 (P5)
- PTP 850C with PTP 820C (ESX hardware version) – Eth 1 (P2)
- PTP 820C (ESS hardware version) or PTP 820C-HP – Eth 3
- PTP 820C (ESX hardware version) – Eth 1

Note: These connections must all use optical cables, except in the case of an PTP 820C ESX hardware version, for which the Protocols Cable must be an electrical cable connected to RJ-45 ports on each of the two units.

The ports must be configured to 1 Gbps.

A Multi-Carrier ABC group that includes both radio carriers must be configured on the PTP 850C. A Multi-Carrier ABC group that includes both radio carriers should also be configured on the PTP 820C or PTP 820C-HP.

A Link Bonding group must be configured on the PTP 850C. The Link Bonding group must include the PTP 850C's Multi-Carrier ABC group and the port connecting the PTP 850C with the paired unit.

Each PTP 850C unit is managed separately and independently. In-band management can be configured so that both units are managed over the link.

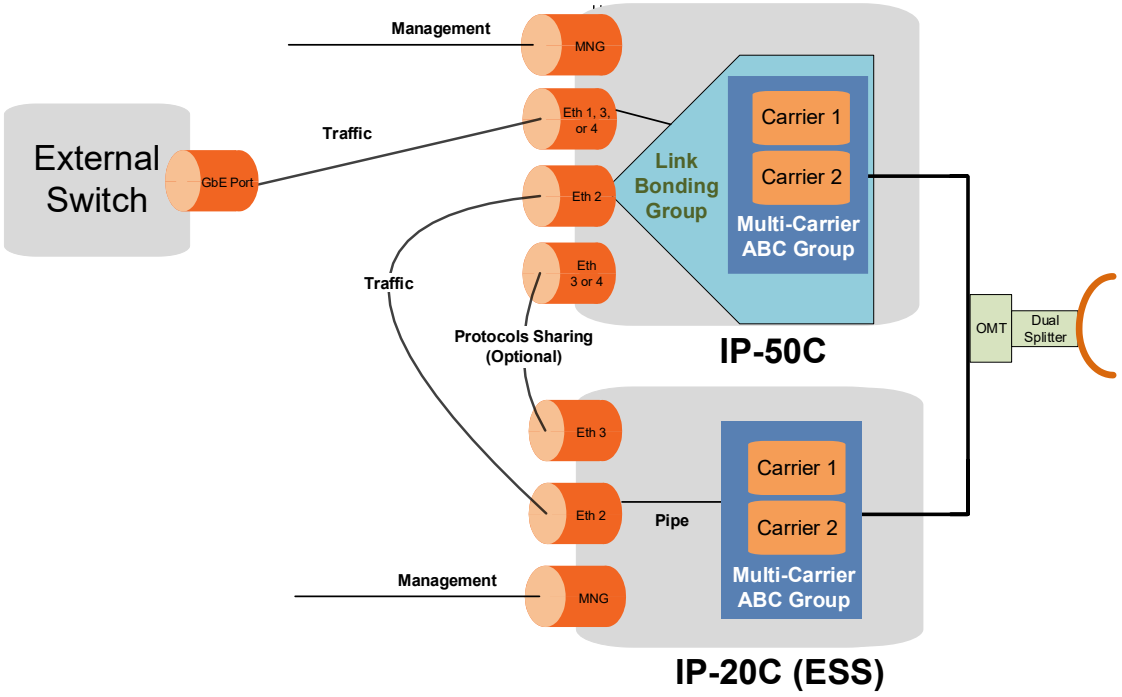


Figure 191: Layer 1 Link Bonding Operation – PTP 850C and PTP 820C (ESS)

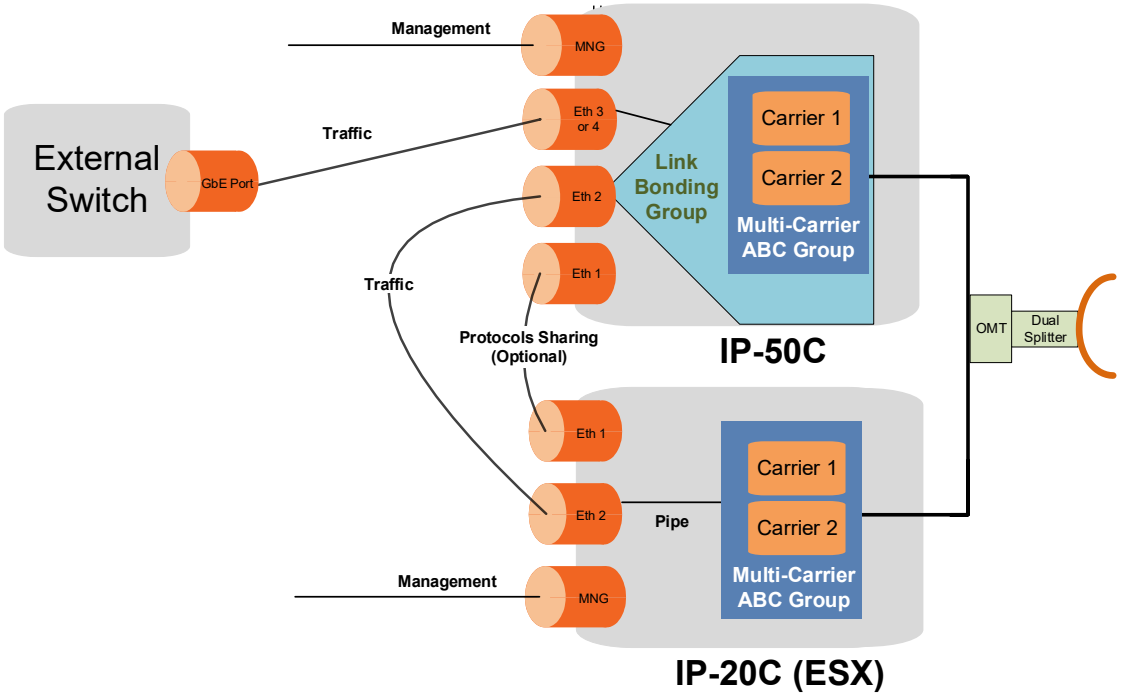


Figure 192: Layer 1 Link Bonding Operation – PTP 850C and PTP 820C (ESX)

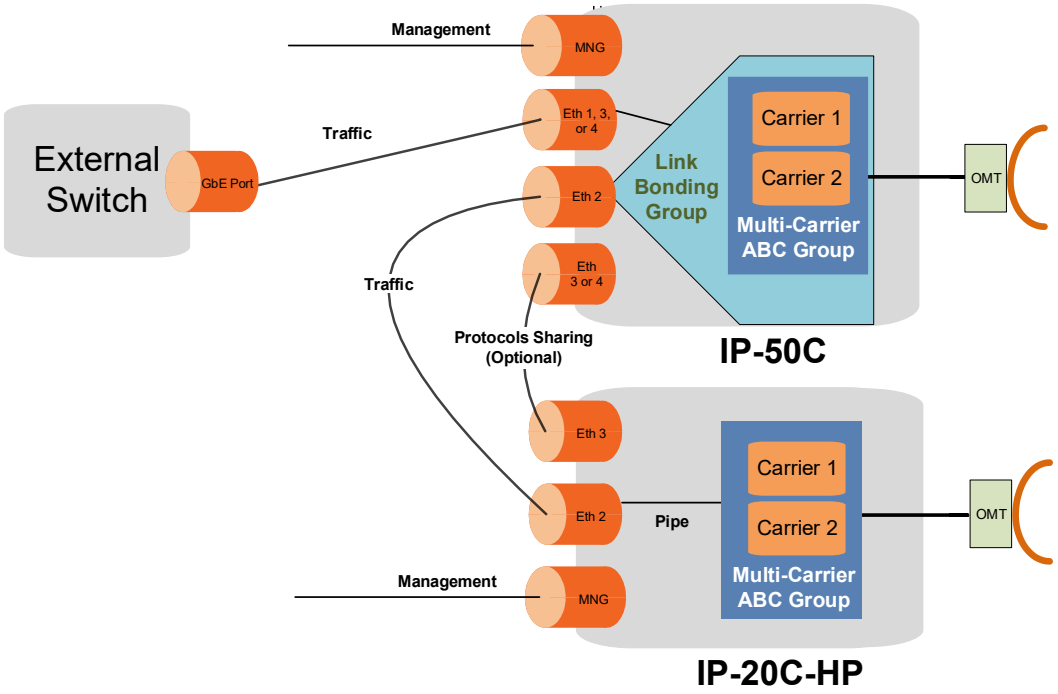


Figure 193: Layer 1 Link Bonding Operation – PTP 850C and PTP 820C-HP

1. ***Note:*** *Line protection with Layer 1 Link Bonding is planned for future release.*

7.4.1.2 Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP – Hardware Configuration

With PTP 820C, the two units can be connected to a single antenna using a Dual Splitter and an OMT. Remote-mount configurations are also available.

With PTP 820C-HP, two separate antennas must be used. Each unit is configured in a 2+0 or 1+0 configuration with its own antenna, and the units are connected only by the Traffic and Protocols cables described above.

7.4.2 Configuring a Layer 1 Link Bonding Node with PTP 850C and PTP 820C or PTP 820C-HP

To configure a Layer 1 Link Bonding node with PTP 850C and PTP 820C or PTP 820C-HP:

1 Connect the external switch to Eth 1 (P2, the PoE port), Eth 3 (P4, the MIMO port), or Eth 4 on the main PTP 850C unit.

Note: Eth 1 cannot be if the paired unit is an PTP 820C ESX, because Eth 1 must be used for the Protocols cable.

2 On both the main unit and the paired unit, configure the port speed of the ports to be used to pass traffic between the two units to 1 Gbps.

Note: If you are using an SFP port on the PTP 850C with an electrical SFP module, you must configure the port speed *after* adding the port to the Link Bonding group. Adding the port to the Link Bonding group automatically configures the port to 10G, which is not supported SFP ports with electrical SFP modules. This is why you must set or reset

the port speed to 1G *after* adding the port to the Link Bonding group.

3 If you are using a separate Protocols cable, on the main unit, select either Eth 3 (P4) or Eth 4 (P5), or (when the paired unit is an PTP 820C ESX, Eth 1/P2) to carry L2 protocol data between the main unit and the paired unit. Configure the port speed of the port you select to 1 Gbps.
4 Optionally, on the PTP 820C or PTP 820C-HP, use Eth 3 or, for PTP 820C ESX, Eth 1, to carry L2 protocol data between the main unit and the paired unit.
5 Connect an optical cable between Eth 2 of each unit. This cable carries traffic between the two units.
6 In the Interface Manager, set the port connected to the paired unit for passing traffic between the two units (Eth 2) to **Admin** = **Down**.
7 Optionally, connect an optical cable or, when the paired unit is an PTP 820C ESX, an electrical cable, between the ports on each unit carrying L2 protocol data between the two units.
8 Configure the script and radio settings for both the main unit and the paired unit, including XPIC.
9 On both the main unit and the paired unit, configure a Multi-Carrier ABC group that includes both of the unit's radio carriers.
10 On the main unit only, configure a Link Bonding group that includes the Multi-Carrier ABC group on the PTP 850C and the interface on the PTP 850C connected to the paired unit for traffic:

Note: Before adding a group member, make sure that no shapers or service points are configured on the interface or group.

v Select **Ethernet** > **Groups** > **Link Bonding**. The Link Bonding page opens.

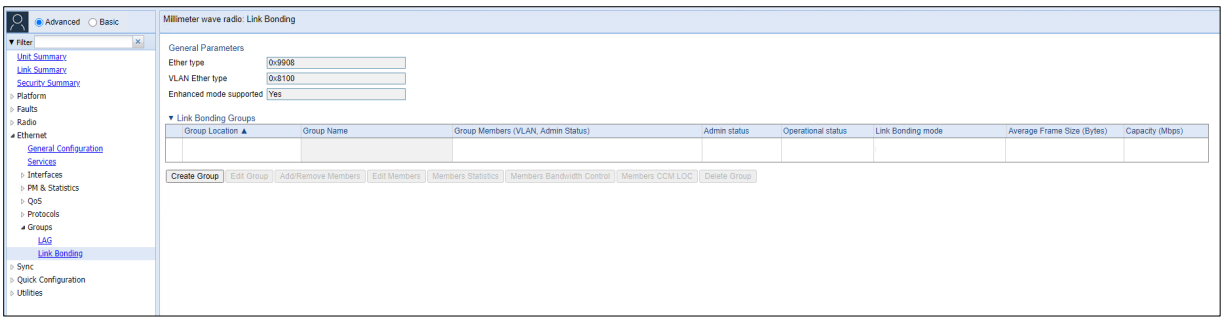


Figure 194: Link Bonding Page (Empty)

vi Click **Create Group**. Page 1 of the Link Bonding Group wizard opens.

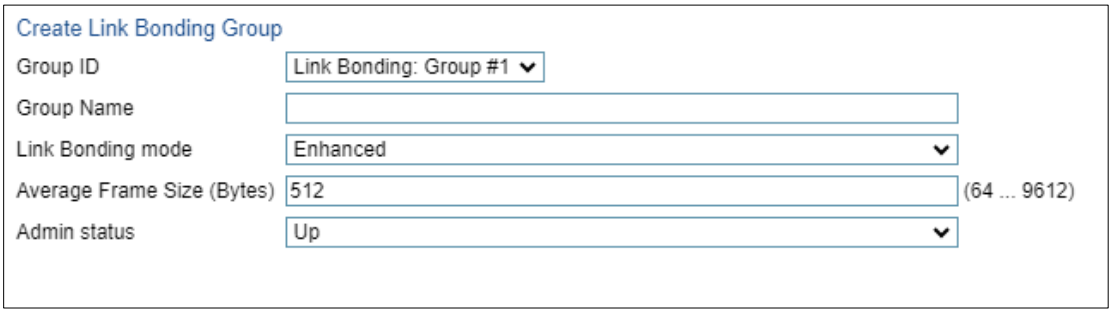


Figure 195: Link Bonding Group Wizard – Page 1

vii In the **Group ID** field, select **Link Bonding: Group #1**.
viii Optionally, in the **Group Name** field, enter a descriptive name for the group.

ix In the **Link Bonding Mode** field, select **Standard** or **Enhanced**. You must select **Enhanced** if the configuration uses a single cable for traffic and L2 protocol data.

Note: Although most PTP 850C and PTP 850E devices support Enhanced Link Bonding mode, some do not. For details.

In the Average Frame Size field, enter a value for calculating the estimated current potential capacity. For an explanation of this field, see Link Bonding L1 Capacity Calculator.

Note: The Average Frame Size does not affect the actual transmitted traffic It is only used to help estimate the current potential capacity.

x In the **Admin status** field, select **Up**.
xi Click **Next**. The Member #1 page opens.

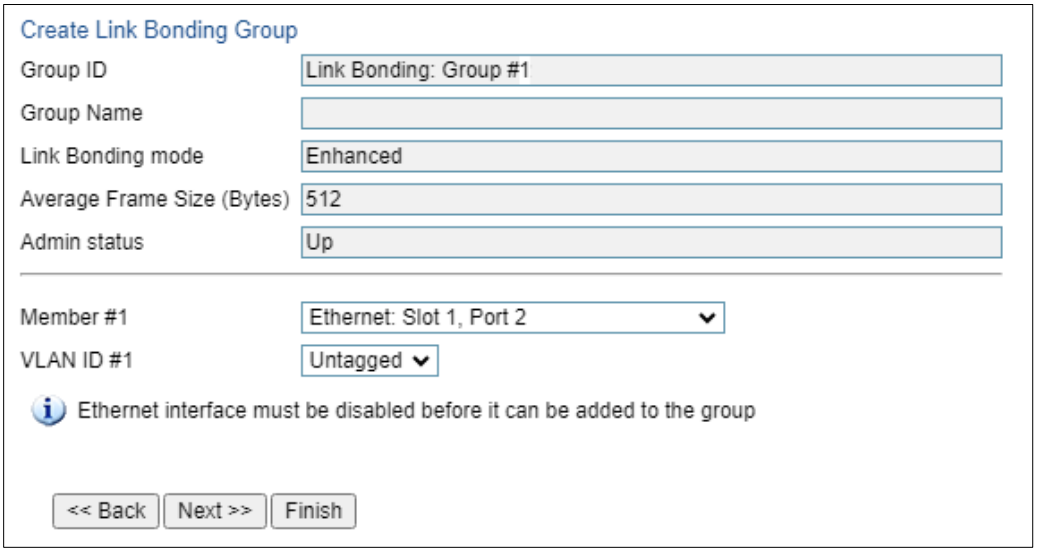


Figure 196: Link Bonding Group Wizard – Member #1 Page

xii In the **Member #1** field, select the Ethernet interface connected to the paired unit for traffic (Eth 2).
xiii In the **VLAN ID #1** field, select **Untagged**.
xiv Click **Next**. The Member #2 page opens.

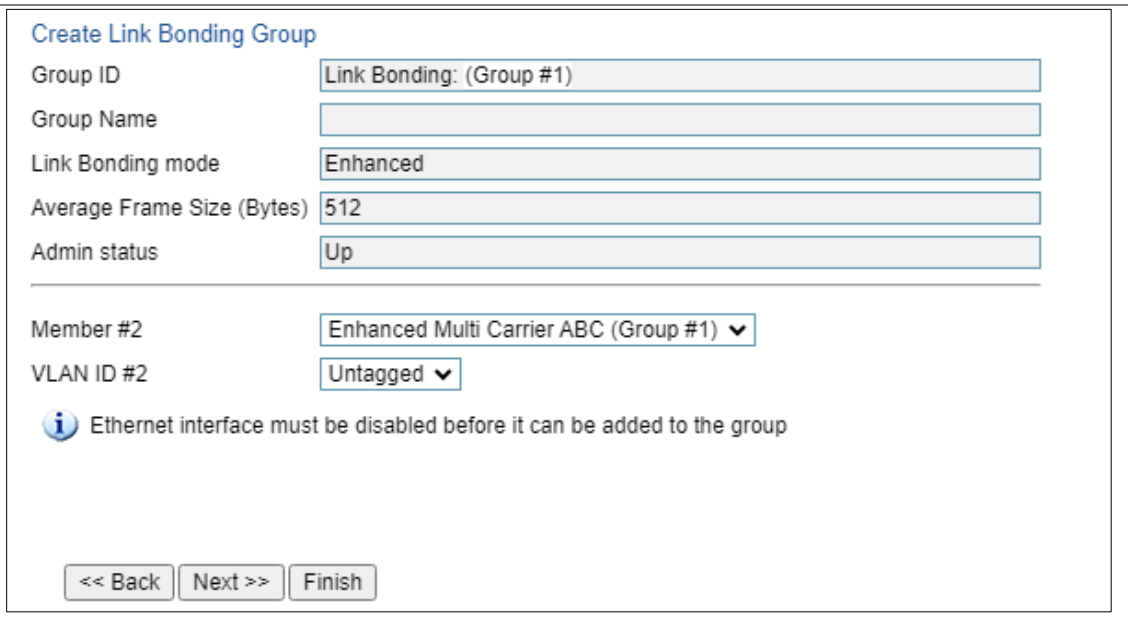


Figure 197: Link Bonding Group Wizard – Member #2 Page

xv In the **Member #2** field, select the Enhanced Multi Carrier ABC group.
xvi In the **VLAN ID #2** field, select **Untagged**.
xvii Click **Finish**. The Selection Summary page opens.

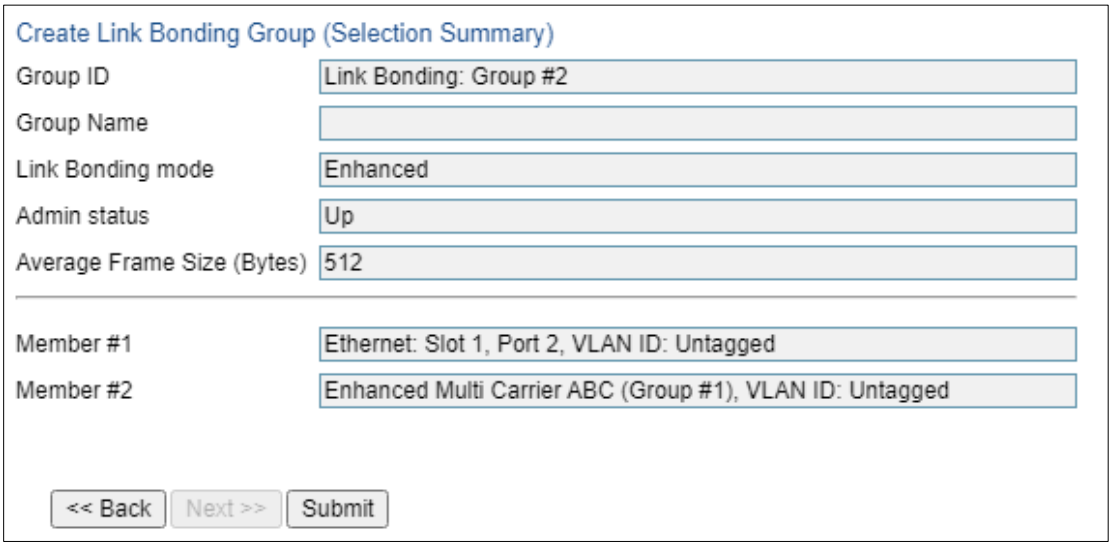


Figure 198: Link Bonding Group Wizard – Selection Summary Page

xviii Click **Submit**. The group is added to the Link Bonding page.

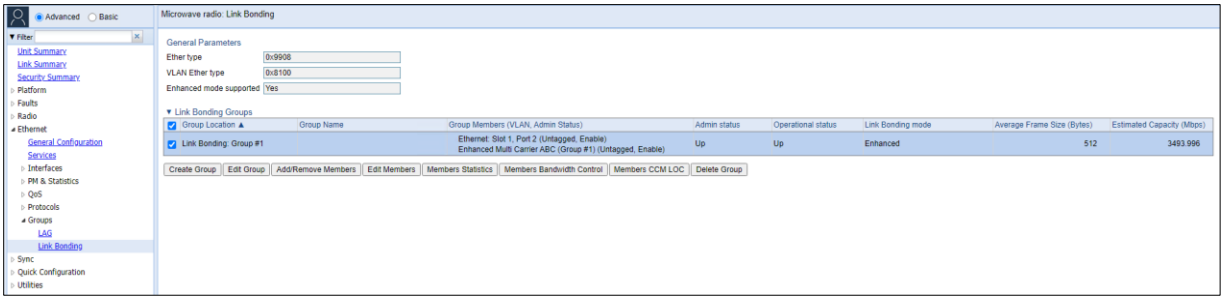


Figure 199: Link Bonding Page (Populated)

11 In the Interface Manager, set the port connected to the paired unit for passing traffic between the two units (Eth 2) to **Admin** = **Up**.
12 Enable PDU encapsulation on the paired unit:

Note: This step is crucial since it ensures that protocols packets are properly tagged and separated from traffic.

i Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens.
ii Select the port used for L2 protocols data (the Protocols port) and click **Edit**. The Logical Interfaces – Edit page opens.
iii In the field **PDU Encapsulation** field, select **Yes**.
iv Click **Apply**.

13 To ensure proper fault handling, configure Automatic State Propagation. For single-cable configurations, you must enable ASP Management Safe mode (CSF mode) to ensure that in-band management is not disrupted in case of a fault on one of the ports connecting the main and paired units. This includes configuring the peer unit to receive CSF PDUs, as described.

v On the local and remote main units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The Link Bonding group
- Controlled Port: The port connected to the external switch (Eth 1, Eth 3, or Eth 4)

vi On the local and remote paired units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The Multi-Carrier ABC group or radio interface
- Controlled Port: The port used to carry traffic between the two units (Eth 2)

14 In-band management can be carried between the main unit and the paired unit via the cable carrying L2 protocols data between the units. This can be the traffic cable or a separate Protocols cable.

To configure in-band management, you must define a management service that connects the port used for L2 protocols data (the Protocols port) on each unit, the Link Bonding groups, and the ingress port of the main unit:

i On the local main unit, configure a service point on the port connected to the external switch.
ii On the local main unit, configure a service point on the Protocols port.
iii On the local main unit, configure a service point on the Link Bonding group.
iv On the local paired unit, configure a service point on the Protocols port.
v On the remote paired unit, configure a service point on the Protocols port.
vi On the remote main unit, configure a service point on the Protocols port.
vii On the remote main unit, configure a service point on the Link Bonding group.

15 Configure Radio Bandwidth Notification on the main unit by performing the following steps:

i Select the Link Bonding group in the Link Bonding page and click **Members Bandwidth Control**. The Members Bandwidth Control page opens.

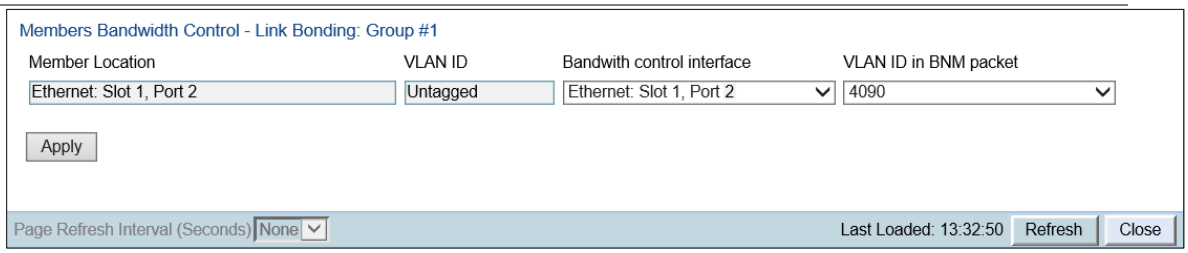


Figure 200: Link Bonding – Members Bandwidth Control Page (Single-Cable Configuration)

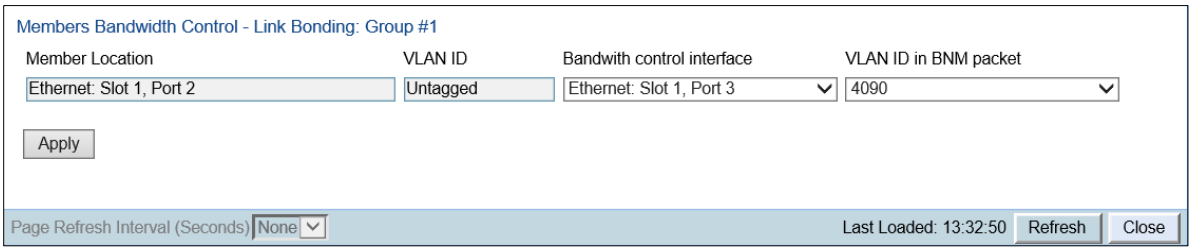


Figure 201: Link Bonding – Members Bandwidth Control Page (Two-Cable Configuration)

ii In the **Bandwidth control interface** column:

- For single-cable configurations, select the same port as displayed in the **Member Location** field.
- For two-cable configurations, select the port to which the Protocols cable is connected.

iii In the **VLAN ID in BNM packet** column, select a VLAN ID. You can use any available VLAN ID from 1 to 4090. This is the VLAN use to transfer protocol information between the two units.

16 In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page opens.

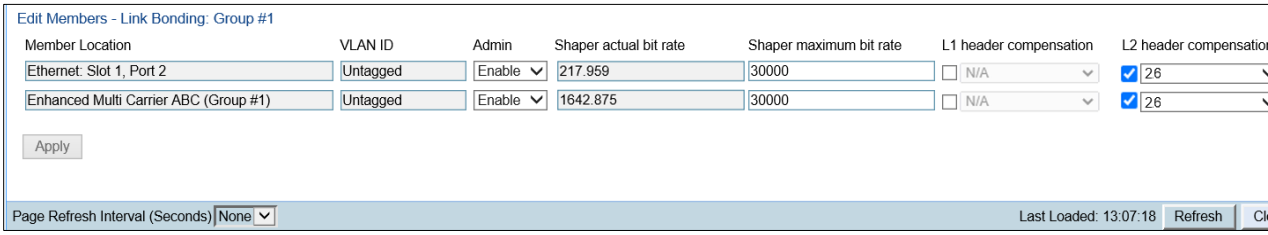


Figure 202: Link Bonding Groups – Edit Members Page (PTP 850C with PTP 820C)

17 In the **Shaper maximum bit rate** column, you can adjust the shaper for either or both interfaces in the group. You should set this according to the maximum capacity of the radio interface, or the maximum radio capacity of the paired unit connected to the Ethernet member. The default value is 30000 Mbps.

Note: The **Shaper actual bit rate** column displays the actual current traffic distribution between the main Unit (the radio interface) and the paired unit (the Ethernet interface, through which traffic is sent to the paired unit). This is displayed in units of Mbps**.**

18 In the **L1 header compensation** column:

- Do not select the radio member.
- For the Ethernet member, see L1 and L2 Header Compensation Values.

Note: The purpose of this setting is to prevent a bottleneck for traffic sent by the Link Bonding group to the paired unit over the Ethernet interface.

19 In the **L2 header compensation** column, both interfaces should be selected. For recommended values, see L1 and L2 Header Compensation Values.
20 Click **Apply**.
21 In the **Admin** column, set the Admin status of each group member to **Enable**.

Note: If necessary, you can leave the Admin status of the group members **Disable** until a later time in order to complete the configuration with the group offline, then activate the group members later.

The Admin status must be set to **Disable** whenever you modify the **L1 header compensation** or **L2 header compensation** fields. Otherwise, the modification will have no effect.

22 Click **Apply**.
23 Configure Radio Bandwidth Notification on the PTP 820C or PTP 820C-HP by performing the following steps:

i Select **Ethernet** > **Protocols** > **Bandwidth Notification**. The Bandwidth Notification page opens.

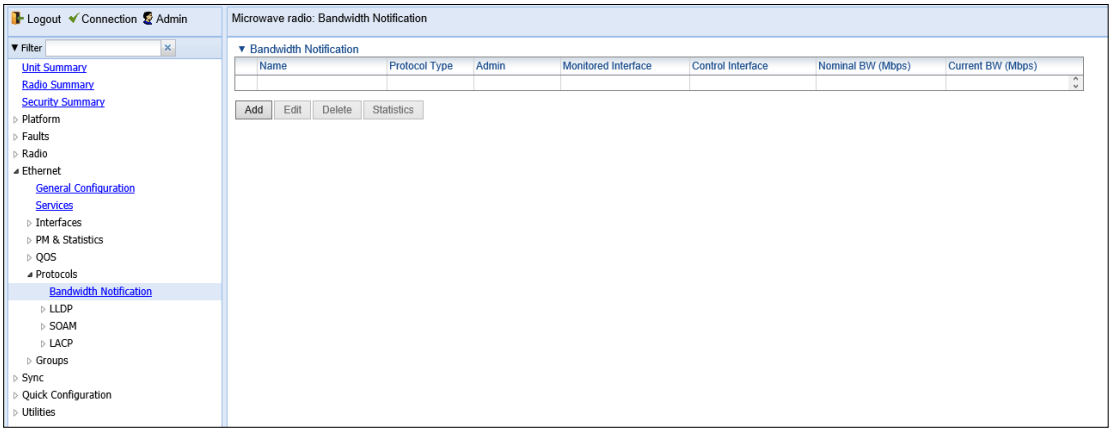


Figure 203: Bandwidth Notification Page (Empty)

ii Click **Add**. The Bandwidth Notification – Add page opens.

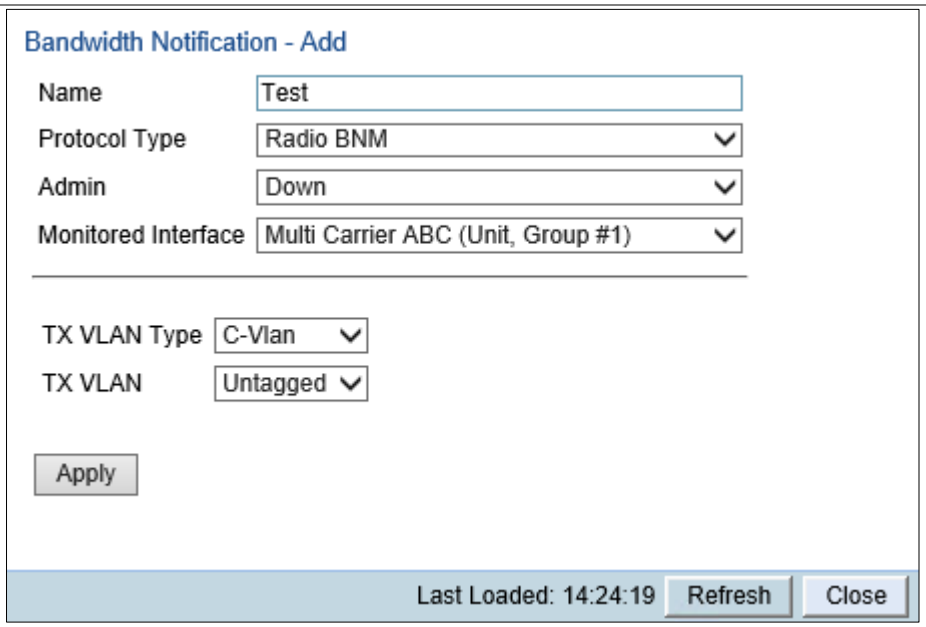


Figure 204: Bandwidth Notification – Add Page

iii In the **Name** field, select a descriptive name.

Note: Once you configure the RBN entity, you cannot edit the name later. The only way to change the name is to delete and reconfigure the RBN entity.

iv In the **Protocol Type** field, select **Radio BNM**.
v In the **Admin** field, select **Up**.
vi In the **Monitored Interface** field, select the paired unit's Multi-Carrier ABC group.
vii In the **TX VLAN Type** field, select **C-Vlan**.
viii In the **TX VLAN** field, select **the same VLAN you configured** In the **VLAN ID in BNM packet** column for the main unit.
ix Click **Apply**. The configuration is added to the Bandwidth Notification page with the Protocol Type **Radio BNM**.

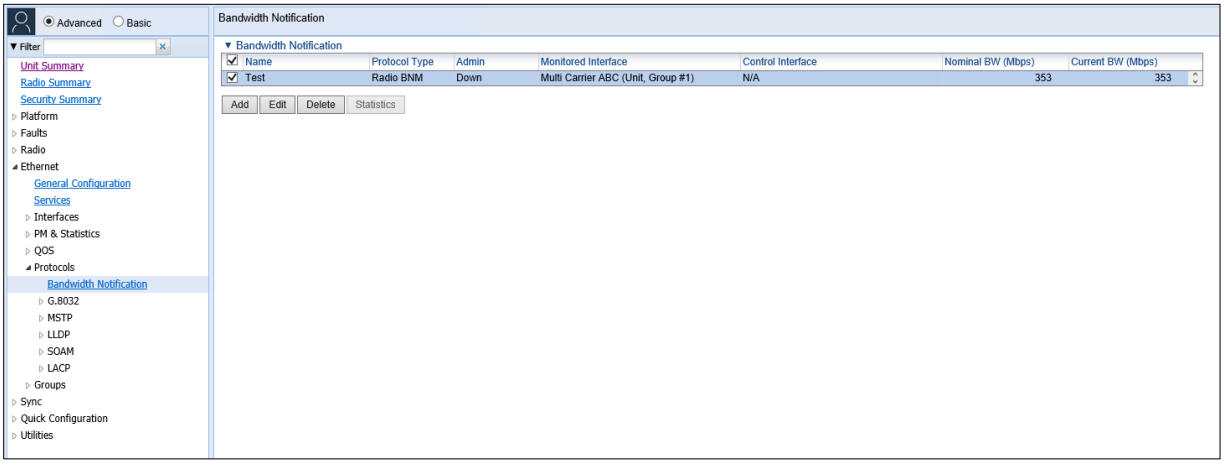


Figure 205: Bandwidth Notification Page (Populated with Radio BNM)

24 On the paired unit on both sides of the link, configure a point-to-point service for Radio Bandwidth Notification, with service points on the Multi-Carrier ABC group and on the interface connected to the main unit for L2 protocols data (the Protocols port). In single-cable configurations, this is the port used for the single traffic and protocols cable. In two-cable configurations, this is the port used for the Protocols cable.

The service points should be configured as follows:

i Create a service point on the Multi-Carrier ABC group with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Use the same VLAN you configured in the VLAN ID in BNM packet column of the Members Bandwidth Control Page.
- Allow Flooding: Allow
- Learning Admin: Disable

ii Create a service point on the Protocols port with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Use the same VLAN you configured in the **VLAN ID in BNM packet** column of the Members Bandwidth Control Page, in Step 15
- Allow Flooding: Allow
- Learning Admin: Disable

25 On the main unit on both sides of the link, create a point-to-point service for Link Bonding traffic, with service points on the port attached to the external switch and the Link Bonding Group. Both service points should be configured as follows:

- Type: PIPE
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Untagged
- Allow Flooding: Allow
- Learning Admin: Disable

26 On the paired unit on both sides of the link, configure a point-to-point service for Link Bonding traffic, with service points on the Multi-Carrier ABC group and Eth 2. The service points should be configured as follows:

Note: This service is a workaround for SYSTEM RELEASE117-1749, to ensure that customer traffic is separated from Radio Bandwidth Notification protocol traffic.

i Create a service point on the Multi-Carrier ABC group with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Untagged.
- Allow Flooding: Allow
- Learning Admin: Disable

ii Create a service point on the port or ports connected to the main unit for traffic, with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Untagged
- Allow Flooding: Allow
- Learning Admin: Disable

7.4.3 Enabling Link Bonding Throughput Enhancement for Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP

After configuring a Link Bonding node, it is recommended to enable Link Bonding Throughput Enhancement. Link Bonding Throughput Enhancement is available for both the main unit and the paired unit.

Note: Link Bonding Throughput Enhancement and Header De-Duplication cannot both be enabled on the same interface.

Link Bonding Throughput Enhancement can be enabled on the Multi-Carrier ABC groups on both the main and the paired units.

Link Bonding Throughput Enhancement affects the recommended L2 Header Compensation. Make sure to use the values listed in L1 and L2 Header Compensation Values.

The Link Bonding Throughput Enhancement and L2 Header Compensation settings must be the same for the main units on both sides of the link. Therefore, the changes should be applied in the following order to ensure that management is not lost:

Note: The settings on paired units do not affect management, and can be changed in any order.

1 Enable Link Bonding Throughput Enhancement on the remote unit (main and/or paired unit):

i Select **Radio** > **Ethernet Interface** > **Configuration**. The Radio Ethernet Interface Configuration page opens.
ii In the **Link Bonding Throughput Enhancement** field, select **Enable**.
iii Click **Apply**.

2 Enable Link Bonding Throughput Enhancement on the local unit (main and/or paired unit):

i Select **Radio** > **Ethernet Interface** > **Configuration**. The Radio Ethernet Interface Configuration page opens.
ii In the **Link Bonding Throughput Enhancement** field, select **Enable**.
iii Click **Apply**.

3 Modify the L2 Header Compensation (decrease by 12) on the remote unit (main and/or paired unit):

i Select **Ethernet** > **Groups** > **Link Bonding**. The Link Bonding page opens.
ii In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page opens.
iii In the **L2 header compensation** column:

- If you enabled Link Bonding Throughput Enhancement on the main unit, reduce the value for the Enhanced Multi Carrier ABC group by 12.
- If you enabled Link Bonding Throughput Enhancement on the paired unit, reduce the value for the Ethernet interface connected to the paired unit for traffic by 16.

iv Click **Apply**.

4 Modify the L2 Header Compensation (decrease by 12) on the local unit (main and/or paired unit):

i Select **Ethernet** > **Groups** > **Link Bonding**. The Link Bonding page opens.
ii In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page opens.
iii In the **L2 header compensation** column:

- If you enabled Link Bonding Throughput Enhancement on the main unit, reduce the value for the Enhanced Multi Carrier ABC group by 12.
- If you enabled Link Bonding Throughput Enhancement on the paired unit, reduce the value for the Ethernet interface connected to the paired unit for traffic by 16.

Note: For recommended values.

iv Click **Apply**.

7.4.4 Editing a Link Bonding Group or its Members

To change the Group Name or the Admin Status of the Link Bonding group:

1 In the Link Bonding page, select the group and click **Edit Group**. The Edit Group page opens.

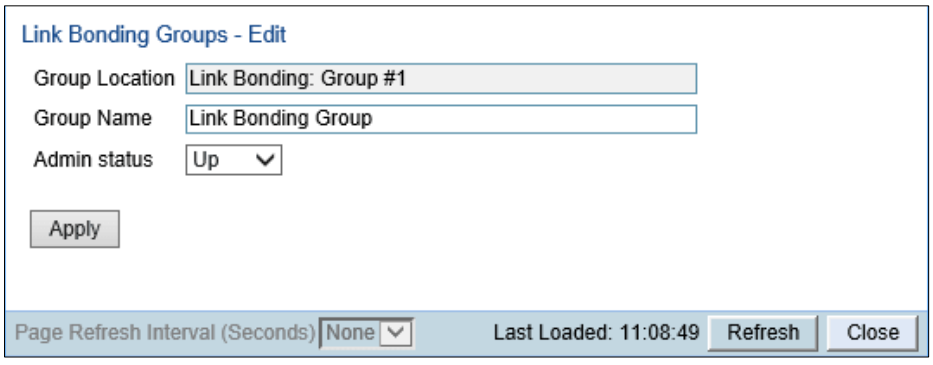


Figure 206: Link Bonding Groups – Edit Page

2 In the **Group Name** field, enter the new name.
3 In the **Admin status** field, change the Admin status of the group to **Up** or **Down**.
4 Click **Apply**.

7.4.5 Displaying Statistics for a Link Bonding Group

You can display the total number of segments and bytes (TX and RX) that have passed through each member of the Link Bonding group.

Note: The ability to clear member statistics is planned for future release.

You can also display and configure thresholds for throughput and utilization on both the group and the member levels. For further information.

To display throughput statistics for the members of the Link Bonding group:

1 In the Link Bonding page, select the group and click **Member Statistics**. The Member Statistics page opens.

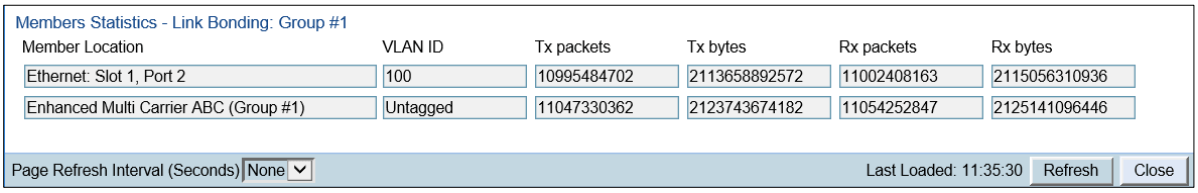


Figure 207: Link Bonding Groups – Member Statistics Page

7.4.6 Deleting a Link Bonding Group

To delete a Link Bonding group, you must first remove the members from the group:

1 In the Link Bonding page, select the group and click **Add/Remove Members**. The Add/Remove Members page opens.

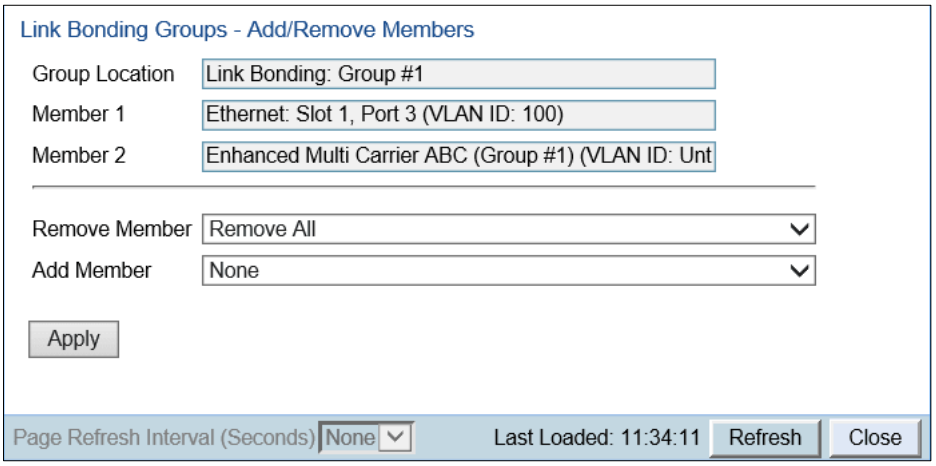


Figure 208: Link Bonding Groups – Member Statistics Page

2 In the **Remove Member** field, select **Remove All**.
3 Click **Apply**.
4 Remove any service points on the Link Bonding group.
5 In the Link Bonding page, select the group and click **Delete Group**.

7.5 Configuring Multiband

This section is only relevant for links that combine PTP 850E withPTP 820C, PTP 820C-HP, PTP 820S, PTP 820N, or PTP 820A unit or a third-party microwave radio, without using Layer 1 Link Bonding.

For Multiband configurations with Layer 1 Link Bonding, see Layer 1 Link BondingConfiguring Multiband with Layer 1 Link Bonding.

7.5.1 Multiband Overview

Multiband bundles E-Band and microwave radios in a single group that is shared with an Ethernet interface. This provides an Ethernet link over the radio with capacity of up to 10 Gbps. A Multiband link is highly resilient because the microwave link acts, in effect, as a backup for the E-Band link.

In the event of radio failure in one device, the other device continues to operate to the extent of its available capacity. Thus, operators benefit from both the high capacity of E-Band and the high reliability of microwave.

7.5.2 Multiband Operation

A Multiband node consists of an PTP 850E unit and an PTP 820C, PTP 820C-HP, or PTP 820S unit or a third-party microwave radio.

In a Multiband configuration, all traffic enters the node via the SFP/SFP+ traffic port (P5, Eth7) or the QSFP port (P4, Eth3 – Eth6). Traffic is passed to a Multiband group that includes the Multiband port (P3, Eth2) and the radio carrier. The Traffic port is the port on the IP-50E connected to the attached unit for passing traffic to the attached unit.

The unit paired with the PTP 850E acts as a pipe. When traffic is passed from the PTP 850E to the paired unit, it is transmitted to either a single radio carrier or 2+0 Multi-Carrier ABC group.

In most circumstances, traffic is passed to the paired unit only when the PTP 850E radio has reached full capacity, or if the ACM profile drops to a point where the PTP 850E's capacity is temporarily less than the traffic load. If the PTP 850E reaches its minimum configured profile, all traffic is passed to the paired unit until the profile rises to a level above the minimum.

To ensure a smooth traffic flow, certain configurations must be performed on the paired unit.

When the PTP 850E is paired with an PTP 820C, PTP 820C-HP, or PTP 820S, the following must be configured on the PTP 820C, PTP 820C-HP, or PTP 820S:

- A Pipe service must be configured between Eth2 and the radio or Multi-Carrier ABC group.
- Automatic State Propagation must be configured, with ASP trigger by remote fault enabled.
- Radio Bandwidth Notification must be enabled.

When the PTP 850E is paired with a third-party unit, the following must be configured on the third-party unit:

- The unit's switching mechanism must be set to Pipe mode.
- Automatic State Propagation must be configured, with ASP trigger by remote fault enabled.
- 802.3X Flow Control must be enabled.

- Ethernet Bandwidth Notification must be enabled

Note

Fixed ACM mode is not supported for Multiband groups.

A Pipe service must be configured between the Ethernet port connected to the PTP 850E and the paired unit's radio or radio group.

Note

If the paired unit is an PTP 820C, PTP 820C-HP, PTP 820S, or third-party microwave radio, the service must be a Pipe service. However, this service must be given higher priority than any other service attached to the interfaces used for Multiband.

The latency differential between the PTP 850E and the paired unit cannot be more than 1.6 ms. That means that under all foreseeable conditions, such as a high ACM profile on one unit and a low ACM profile on the other unit, there should be no more than a 1.6 ms difference between the latency of the two radio carriers in the Multiband link.

For configurations running System Release 13.1 or higher in which the attached unit is an PTP 820C or PTP 820C-HP, a single cable can be used to pass traffic, management, and synchronization between Eth 2 on the PTP 850E and the microwave radio. If the PTP 850E is running an older System Release version or the attached unit is not an PTP 820C or PTP 820C-HP, a separate cable must be used for management and synchronization.

Note

InSystem Release 13.1, 1588 PTP to the attached unit via the main unit requires a separate cable

Figure 210 illustrates ***Error! Reference source not found.*** illustrates Multiband operation with an PTP 50E and PTP 820C, using a single cable for traffic, management, and synchronization. Figure **210** illustrates a configuration that uses a separate cable for synchronization and management of the PTP 820C via the PTP 850E.

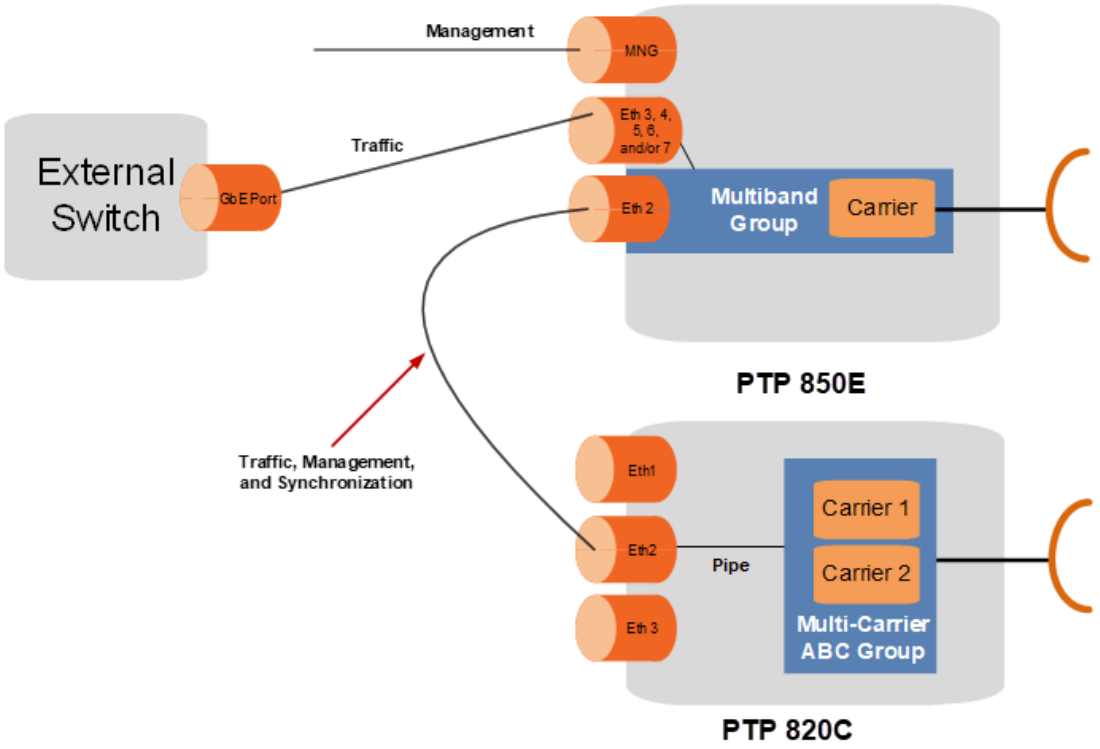


Figure 209: Multiband Operation – PTP 850E and PTP 820C (Single Cable for Traffic, Management, and Synchronization)

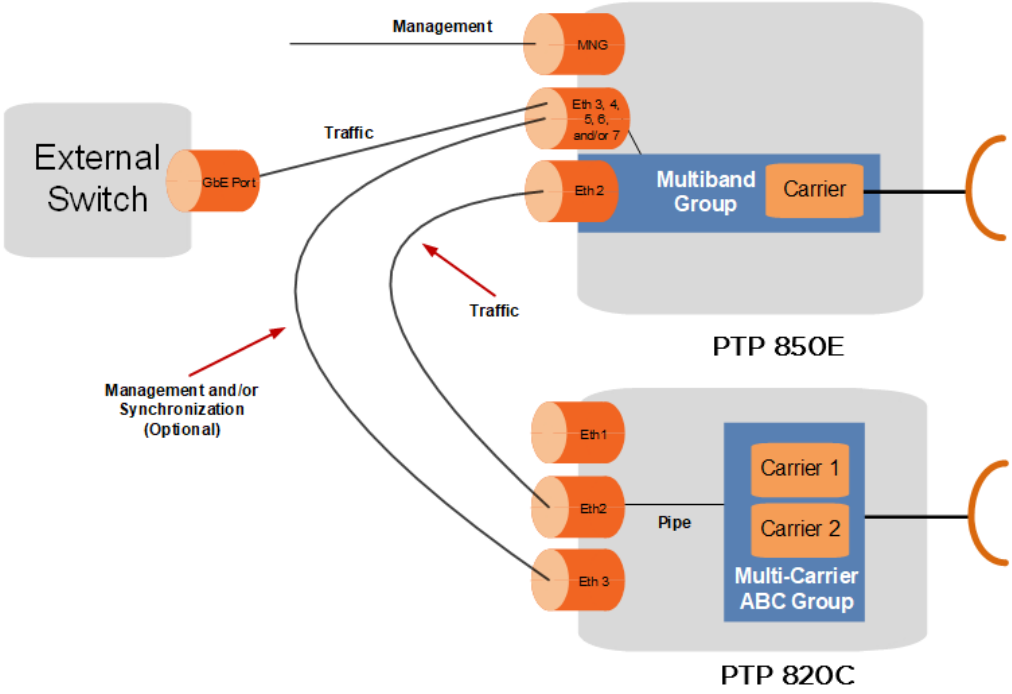


Figure 210: Multiband Operation – PTP 850E and PTP 820C

Figure 211 illustrates Multiband operation with an PTP 850E and a third-party unit. *Figure 211* illustrates a configuration that includes synchronization and management of the third-party unit via the PTP 850E. Synchronization via the PTP 850E requires an optical cable between an Ethernet port on the third-party unit and any free 1G Ethernet port on the PTP 850E, as described in the following sections.

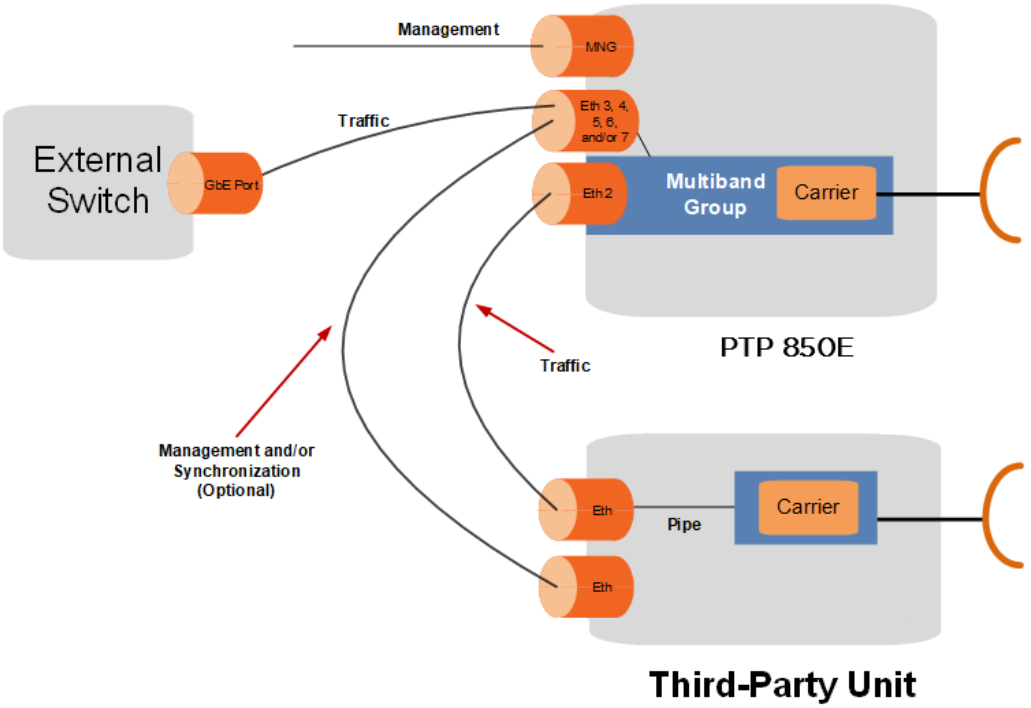


Figure 211: Multiband Operation – PTP 850E and Third-Party Unit

7.5.3 Multiband Configuration

To configure a Multiband node:

1. Connect the external switch to any operational traffic port on the PTP 850E.
2. Connect the Traffic port on the PTP 850E (Port 3, Eth2) to the paired unit. When the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, use the Eth2 port on the PTP 820C, PTP 820C-HP, or PTP 820S.
3. Verify that the **Admin** status of Eth2 on the PTP 850E is **Down**. See Enabling the Interfaces (Interface Manager).
4. Verify that no service points are configured on Eth2 of the PTP 850E. If there are service points on Eth2, remove them. See Deleting a Service Point.
5. Configure the script and radio settings for the PTP 850E and the paired unit. Note that Fixed ACM mode is not supported for an PTP 850E in a Multiband node.
6. On the PTP 850E, configure a Multiband group that includes Eth2 and the radio:

    i Select **Radio** > **Groups** > **Multi Carrier ABC**. The Multi Carrier ABC Groups page opens.

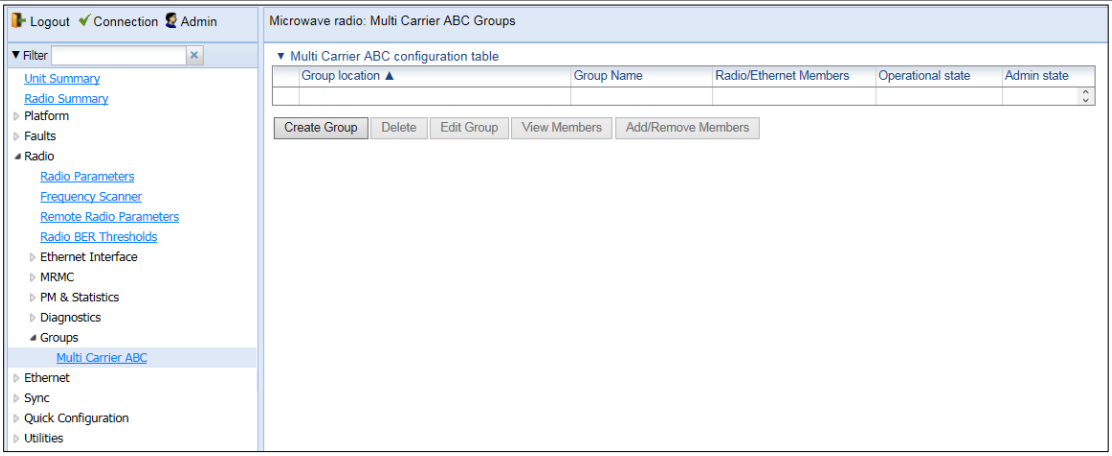


Figure 212: Multi Carrier ABC Groups Page (Empty)

ii Click **Create Group**. Page 1 of the Create ABC Group wizard opens.

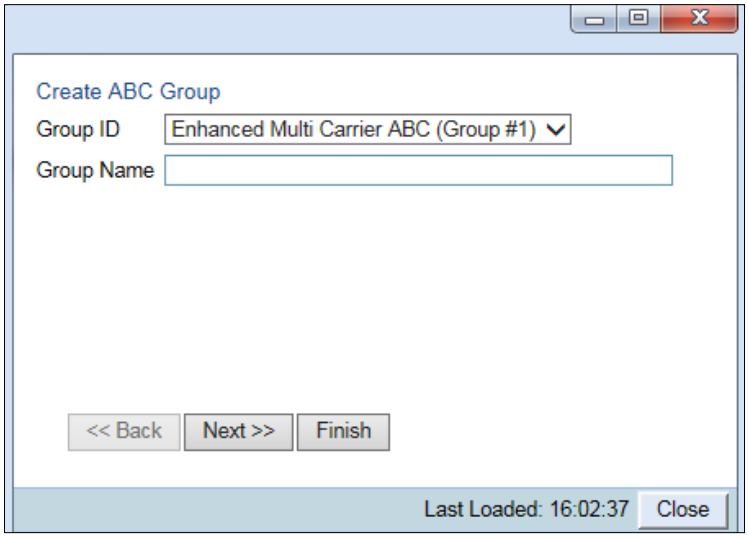


Figure 213: Create ABC Group Wizard – Page 1

iii In the **Group ID** field, select **Enhanced Multi Carrier ABC (Group #1)**.
iv Optionally, in the **Group Name** field, enter a descriptive name for the group.
v Click **Next**. Page 2 of the Create ABC Group wizard opens.

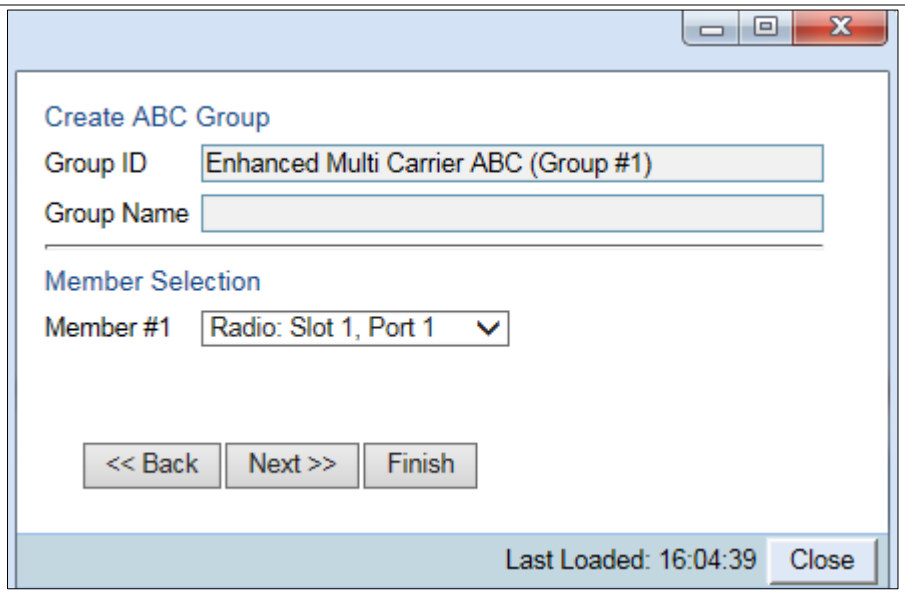


Figure 214: Create ABC Group Wizard – Page 2

vi In the **Member #1** field, select **Radio: Slot 1, Port 1**.
vii Click **Next**. Page 3 of the Create ABC Group wizard opens.

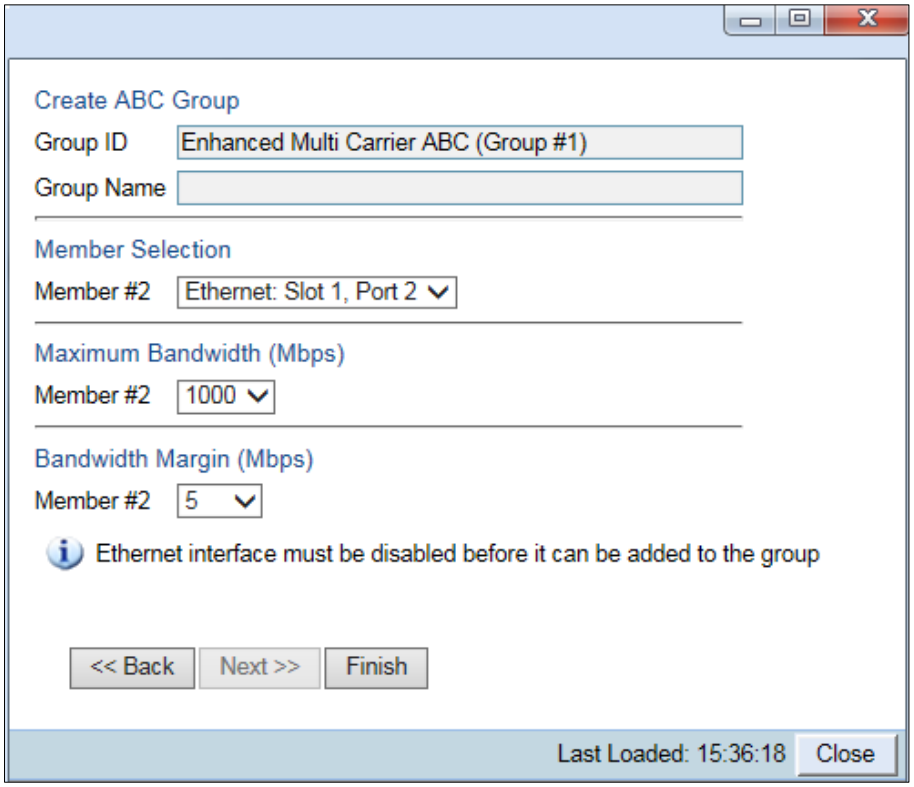


Figure 215: Create ABC Group Wizard – Page 3

viii In the **Member #2** field under **Member Selection**, select **Ethernet: Slot 1, Port 2**.
ix In the **Member #2** field under **Maximum Bandwidth (Mbps)**, select the maximum traffic that the PTP 850E will pass to the paired unit. This parameters should be set to the maximum of the paired unit's capacity. The default value is 1000 Mbps.

Note

The Maximum Bandwidth represents the L1 capacity of the radio link connected to the Ethernet member. The actual bandwidth that will be available for traffic is less due to overhead.

When using a third-party radio as the paired unit, it is particularly important to set this parameter properly in order to ensure optimal performance. Failure to properly set this parameter may lead to frequent pauses as the queue fills up during low capacity periods, such as when weather conditions cause the ACM profile to drop.

When using a third-party radio as the paired unit, it is particularly important to set this parameter properly in order to ensure optimal performance. Failure to properly set this parameter may lead to frequent pauses as the queue fills up during low capacity periods, such as when weather conditions cause the ACM profile to drop.

x In the **Member #2** field under **Bandwidth Margin (Mbps)**, select the bandwidth margin, in Mbps. This parameter deducts the specified throughput from the throughput the PTP 850E would otherwise pass to the paired unit. The purpose of this parameter is to provide a margin of safety that will avoid loss of traffic in the event that the ACM profile is reduced on the paired unit. It is recommended to configure this parameter as follows:

- If the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, or a third-party device with a bandwidth notification mechanism that will inform the PTP 850E of an impending reduction of the ACM profile before the reduction takes place, it is recommended to leave this parameter at its default value of 5 Mbps.
- If the paired unit is a third-party device without a bandwidth notification mechanism that will inform the PTP 850E of an impending reduction of the ACM profile before the reduction takes place, it is recommended to set this parameter to an amount equal to or greater than the largest throughput differential between any two adjacent profiles for the script configured on the paired unit.

The range of values is 5 to 100 Mbps.

xi Click Finish. The Selection Summary page of the Create ABC Group wizard opens.

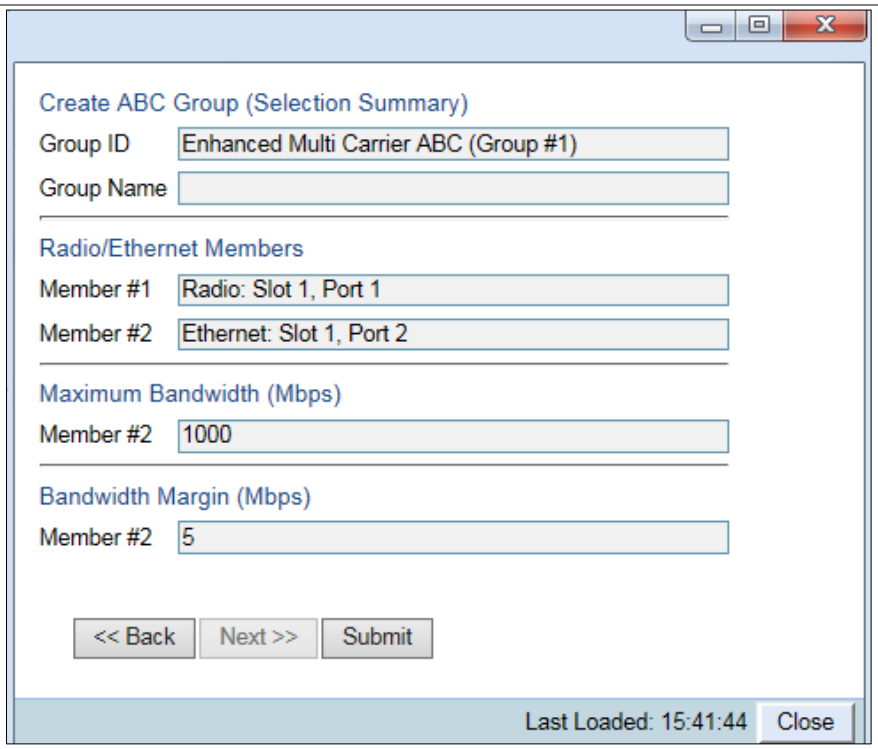


Figure 216: Create ABC Group Wizard – Selection Summary

xii Click **Submit**. The group is added to the Multi Carrier ABC page.

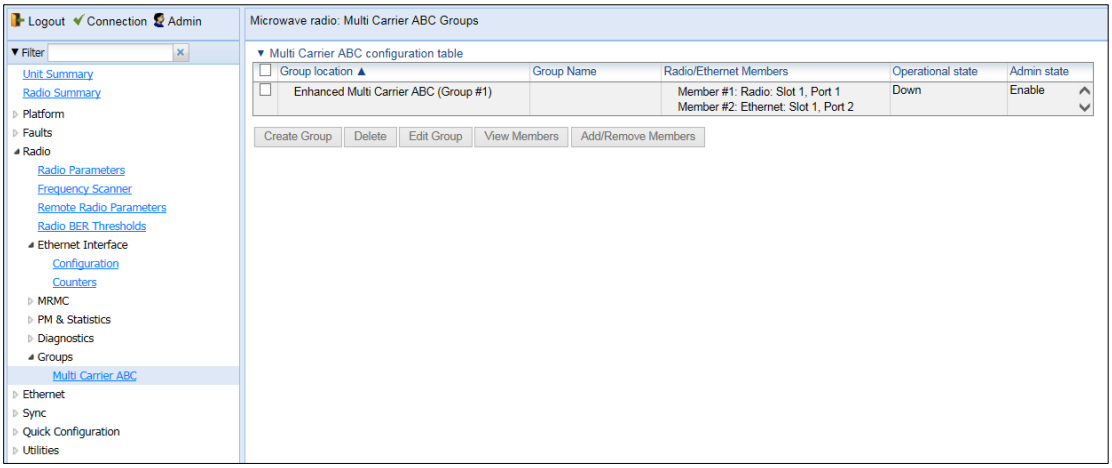


Figure 217: Multi Carrier ABC Groups Page (Populated with Multiband Group)

7 Enable the Eth2 interface. See Enabling the Interfaces (Interface Manager).
8 If the paired unit is an PTP 820C or PTP 820C-HP, verify that XPIC is disabled on the PTP 820C or PTP 820C-HP.
9 On the paired unit, configure a Pipe service between the port receiving traffic from the PTP 850E and the radio or Multi-Carrier ABC group.
10 On the paired unit, configure Automatic State Propagation with **ASP trigger by remote fault** enabled.
11 If the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, configure Radio BNM. For instructions, refer to the *User Guide for PTP 820 All-Outdoor Products*. Make sure to define a Name for the Radio BNM group.

Note
If the paired unit is a third-party radio, enable 802.3X Flow Control.

7.5.4 Editing a Multiband Group or its Members

To change the Group Name of the Multiband group:

1 In the Multi Carrier ABC Groups page, select the group and click **Edit Group**. The Edit Group page opens.

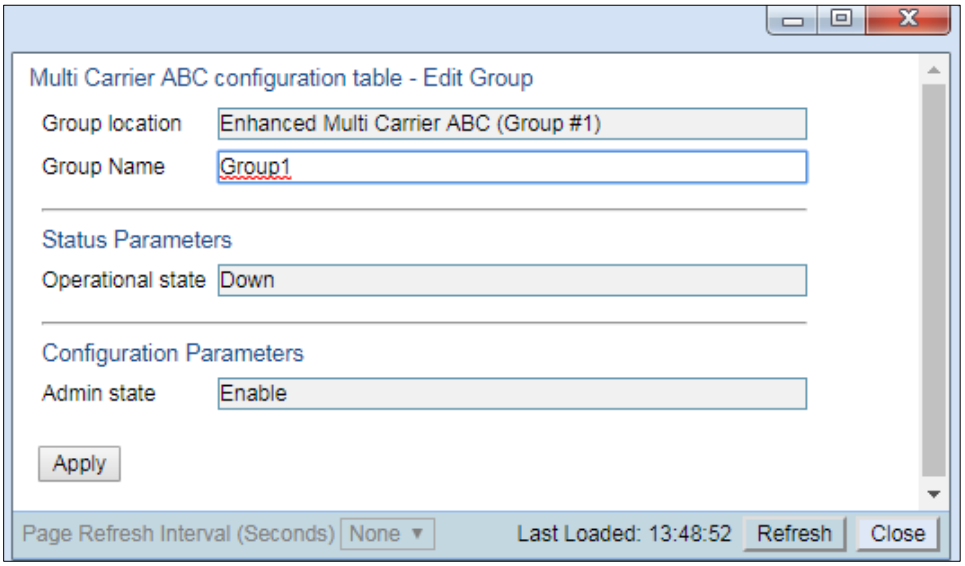


Figure 218: Multi Carrier ABC Groups – Edit Group Page

2 In the **Group Name** field, enter the new name.
3 Click **Apply**.

To change the **Maximum Bandwidth** and the **Bandwidth Margin** parameters:

1 In the Multi Carrier ABC Groups page, select the group and click **Edit Members**. The Edit Members page opens.

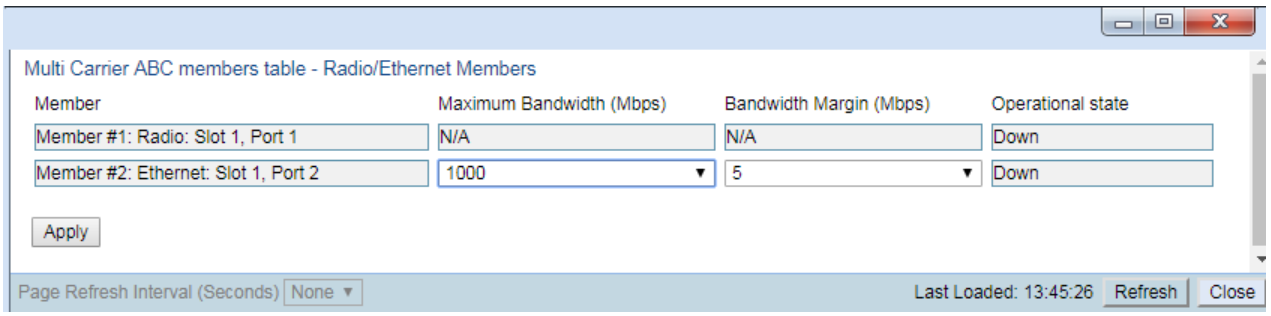


Figure 219: Multi Carrier ABC Groups – Edit Members Page

2 Edit the **Maximum Bandwidth** and/or **Bandwidth Margin** fields in the row of the Ethernet interface.
3 Click **Apply**.

To add or remove members to or from the group:

1 In the Multi Carrier ABC Groups page, select the group and click **Add/Remove Members**. The Add/Remove Members page opens.

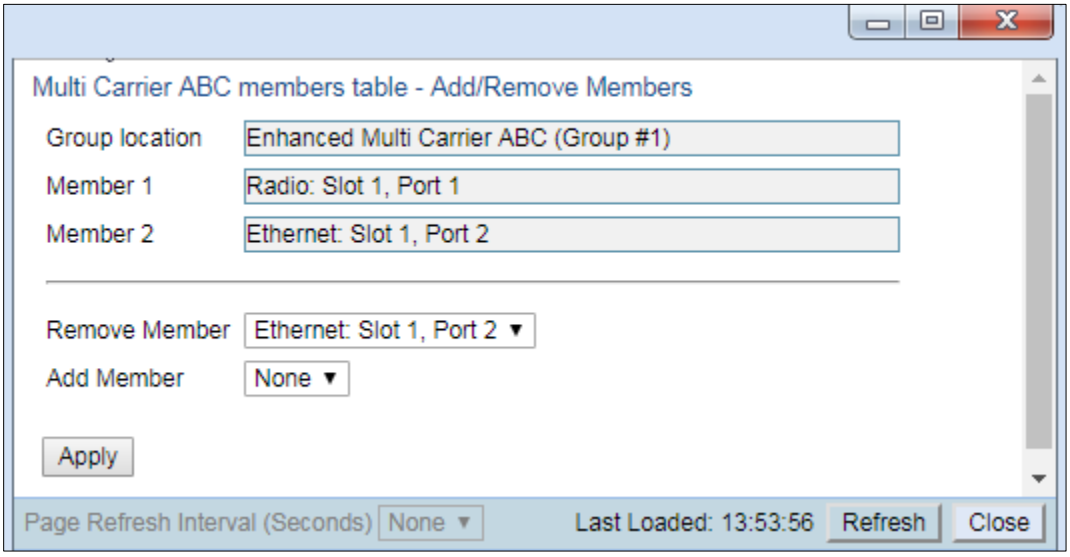


Figure 220: Multi Carrier ABC Groups – Add/Remove Members Page

2 In the **Remove Member** field, select a member or select **Remove All**.
3 In the Add **Member field**, select a member.
4 Click **Apply**.

7.5.5 Multiband Management

The PTP 850E unit in a Multiband configuration can be managed normally, as in any other configuration. For in-band management of the PTP 850E, configure the management service on the PTP 850E Multiband group.

The following options are available for managing the paired unit in a Multiband configuration:

- Inband management via the PTP 850E
- Inband management directly from the external switch
- Out-of-Band management

7.5.5.1 Inband Management via the PTP 850E

The paired unit can managed via the PTP 850E. When the attached unit is an PTP 820C or PTP 820C-HP, the attached unit can be managed via the same cable used for traffic. For other types of devices, In-band management via the PTP 850E requires that the paired unit must have at least two free SFP ports. When the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, this requires an ESS hardware version for the PTP 820C, PTP 820C-HP, or PTP 820S or, for PTP 820C, a 2E2SX hardware version. To manage the paired unit via the PTP 850E, an optical cable must be connected between any free 1G Ethernet port on the PTP 850E and Eth3 on the PTP 820C, PTP 820C-HP, or PTP 820S or the Ethernet port receiving management data on the third-party unit.

A management service must be defined between the management port of the PTP 850E and the port on the PTP 850E that is connected to the paired unit for management. This transmits management to the paired unit.

The paired unit's management service should only have a service point for the Ethernet port connected to the PTP 850E for management. No service point should be defined on the radio or Multi-Carrier ABC group.

Note

To avoid loops, do not configure management between the paired unit and third-party equipment.

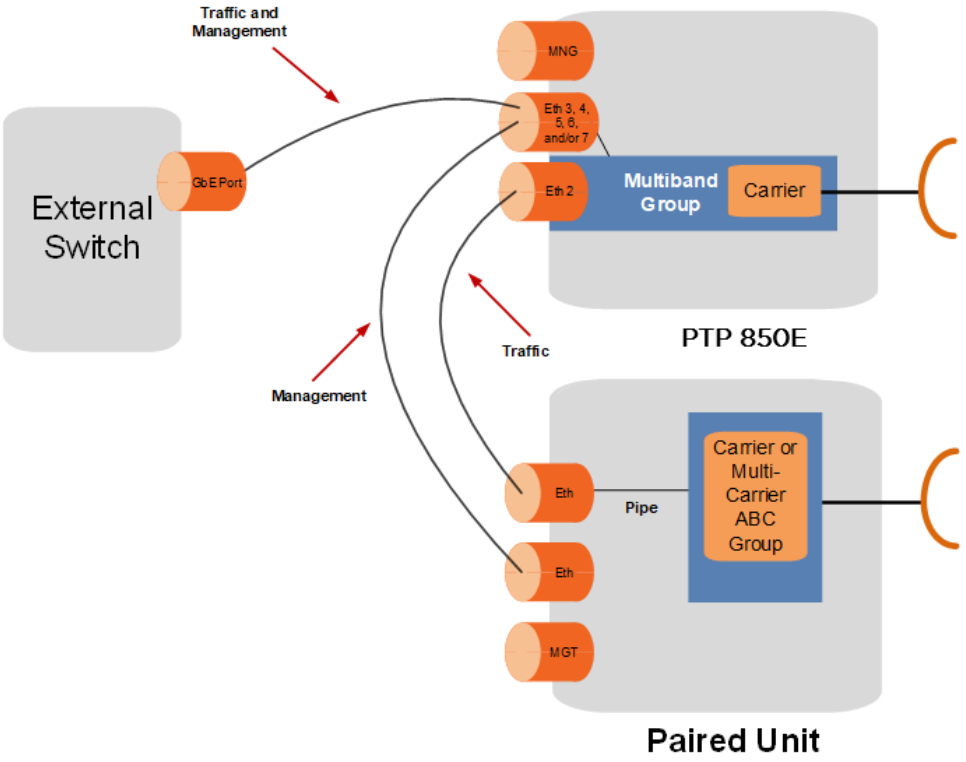


Figure 221: Multiband Configuration with Direct Inband Management to the Attached Unit via a Separate Optical Cable

7.5.5.2 Inband Management Directly via the External Switch

The unit paired with the PTP 850E can be managed by means of a TP cable connected to the MGT port on the paired unit and to the LAN port on a PC or laptop. If the paired unit is a third-party radio, it can also be managed via out-of-band management.

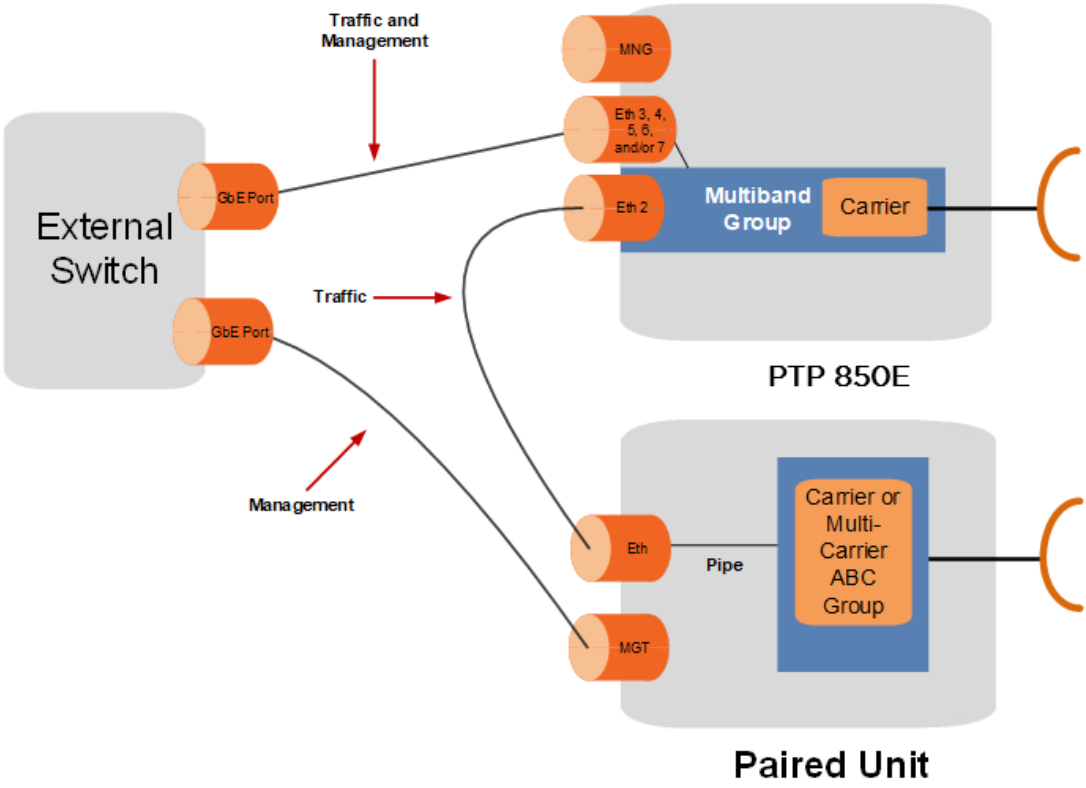


Figure 222: Multiband Configuration with Direct Inband Management to the Paired Unit

7.5.5.3 Out-of-Band Management

The paired unit can be managed by means of a TP cable connected to the MGT port on the paired unit and to the LAN port on a PC or laptop.

In this scenario, the PTP 850E is managed by connecting the PC or laptop used for management to the PoE Injector, which provides transfers power and management to the MGT/PoE port of the PTP 850E.

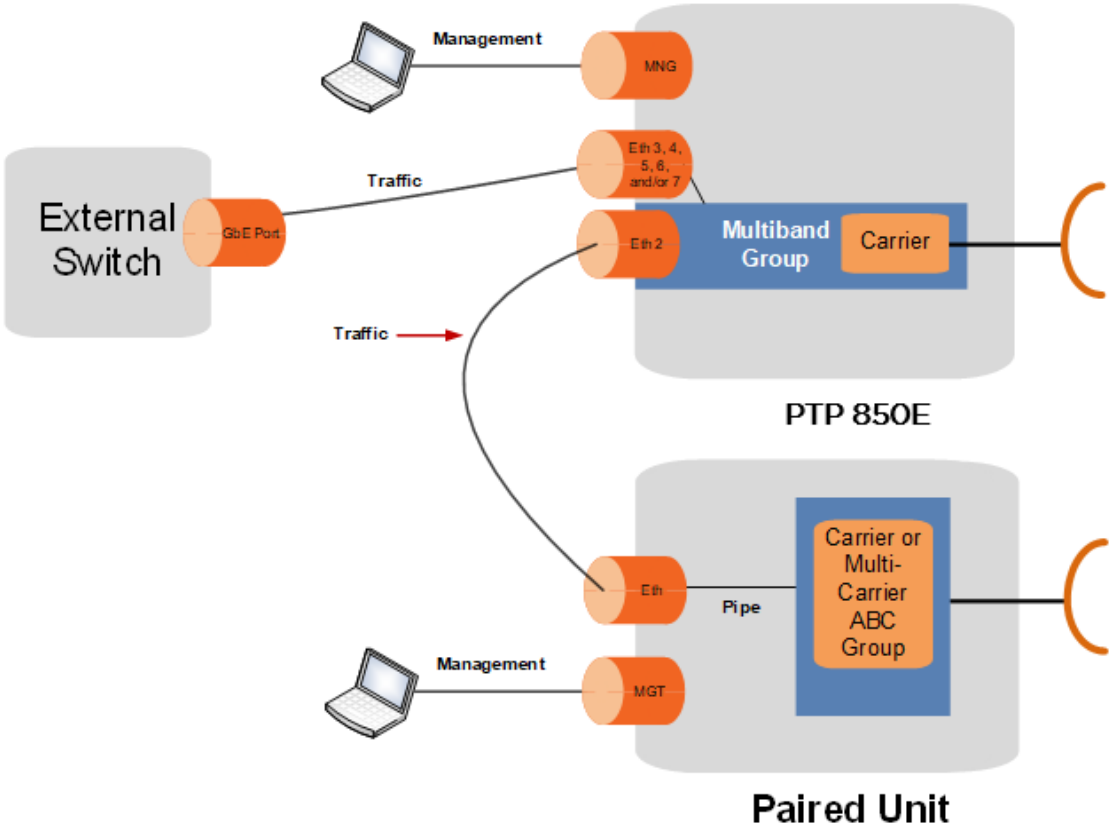


Figure 223: Multiband Configuration with Out-of-Band Management to Both Units

7.5.6 Configuring Synchronization in a Multiband Node

SyncE and 1588 PTP can be used in Multiband nodes. SyncE and 1588 PTP can be configured for both the PTP 850E and the Microwave unit paired with the PTP 850E. For SyncE via the PTP 850E, the paired unit must have at least two free SFP ports. When the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, this requires an ESS hardware version for the PTP 820C, PTP 820C-HP, or PTP 820S or, for PTP 820C, a 2E2SX hardware version. SyncE for the paired unit requires an optical cable between any free 1G Ethernet port on the PTP 850E and Eth3 on the PTP 820C, PTP 820C-HP, or PTP 820S or the Ethernet port receiving management data on the third-party unit. The same cable can be used for both SyncE and in-band management.

Note

When a third-party unit is paired with the PTP 850E, it is a prerequisite that the third-party radio unit support SyncE in order to provide synchronization for the Multiband node.

When a third-party unit is paired with the PTP 850E, it is a prerequisite that the third-party radio unit support SyncE

and, if required, 1588 PTP in order to provide synchronization for the Multiband node.

To configure SyncE on a Multiband node:

1 On the PTP 850E, configure the following synchronization sources:

- The Ethernet port attached to the external switch must be configured as the outgoing clock to the downstream interface
- The PTP 850E radio interface must be configured with SSM enabled and first priority
- The Ethernet port on the PTP 850E transmitting synchronization to the paired unit must be configured with SSM enabled and second priority

Do not configure Eth2 as a synchronization source.

2 On the paired unit, configure two synchronization sources: the Ethernet port receiving synchronization from the PTP 850E, and the radio. When using Multi-Carrier ABC, configure both radios as synchronization sources.

In ring configurations, configure priority order in the direction of traffic on the ring.

For instructions on configuring SyncE, see Configuring the Sync Source.

7.5.6.1 Configuring SyncE in a Multiband Node

For configurations in which the attached unit is an PTP 820C or an PTP 820C-HP, SyncE data can carried via the cable used for traffic between the PTP 850E and the attached unit.

Note

In System Release 13.1, 1588 PTP to the attached unit via the main unit requires a separate cable.

For other configurations, SyncE for a Multiband node requires an optical cable between the PTP 850E and the paired unit, in addition to the cable carrying traffic between the two units. Therefore, the paired unit must have at least two free SFP ports. The same connection can be used for both SyncE and in-band management.

- On the PTP 850E, use any free SFP port for the SyncE connection with the paired unit.
- When the attached unit is an PTP 820S, an ESS hardware version is required. Use Eth 3 for the SyncE connection.
- When the attached unit is an PTP 820N, PTP 820A, or third-party unit, use any free SFP port for the SyncE connection.

To configure SyncE on a Multiband node:

- On the PTP 850E connected to the upstream sync source, configure the following:
  - Configure the port connected to the external switch as a sync source.
  - Configure the radio interface as outgoing clock, with SSM enabled.
  - Configure the port transmitting SyncE to the paired unit as outgoing clock, with SSM enabled.
- On the local paired unit, configure the following:
  - Configure the port receiving SyncE from the PTP 850E as a sync source.

- Configure the radio interface or Multi-Carrier ABC group as outgoing clock, with SSM enabled.

- On the PTP 850E connected to the downstream interface, configure the following:
  - Configure the port connected to the external switch as outgoing clock, with SSM enabled.
  - Configure the radio interface as a sync source with priority 1.
  - Configure the port receiving SyncE from the paired unit as a sync source with priority 2.
- On the remote paired unit, configure the following:
  - Configure the port transmitting SyncE to the PTP 850E as outgoing clock, with SSM enabled.
  - Configure the radio interface or Multi-Carrier ABC group as a sync source.

Figure 224 Multiband Configuration with SyncE – Single Cable for SyncE

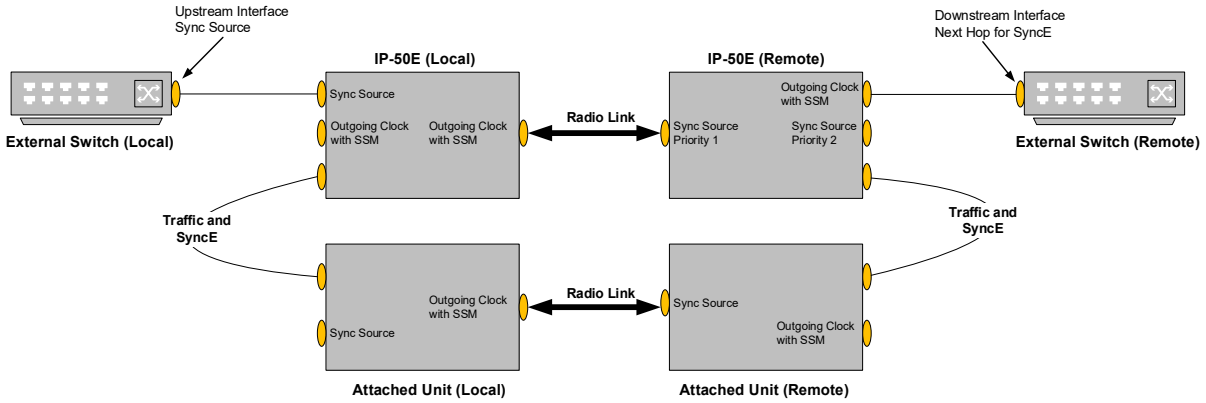
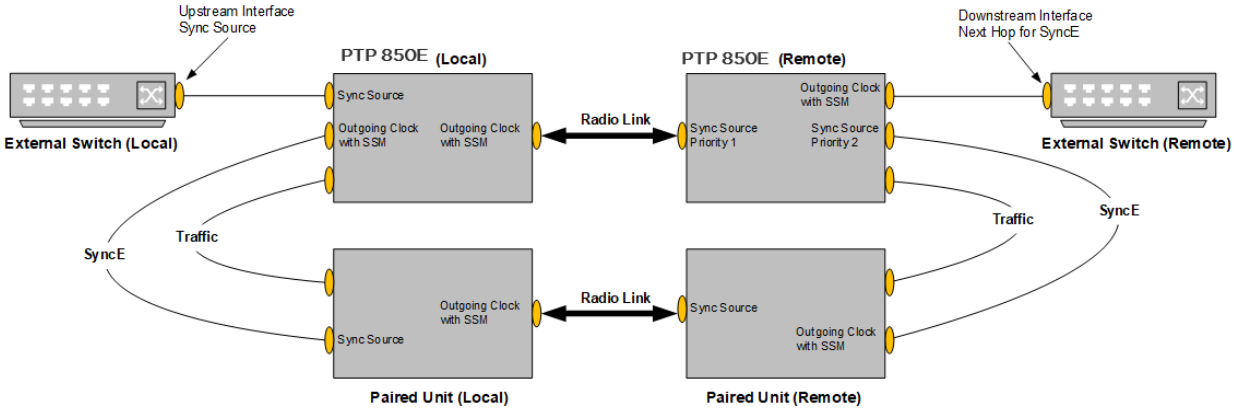


Figure 225 Multiband Configuration with SyncE – Separate Cable for SyncE



In ring configurations, configure priority order in the direction of traffic on the ring.

For instructions on configuring SyncE, see Configuring the Sync Source.

7.5.6.2 Configuring 1588 PTP in a Multiband Node

To use 1588 PTP on an PTP 850E Multiband node, you must configure Boundary Clock on the PTP 850E units and Transparent Clock on all of the units, as described below.



Note

If the Microwave link goes down, 1588 packets will not be transmitted to the other side of the Multiband link.

To configure 1588 PTP for the PTP 850E Multiband node:

1. Configure SyncE following the instructions in Configuring SyncE in a Multiband Node.
2. Enable 1588 PTP on each unit, including the PTP 850E and the paired unit on both sides of the link:
   a. Select **Sync > 1588 > General Configuration**. The 1588 – General Configuration page.
   b. In the **1588 PTP** field, select **Enable**.
   c. Click **Apply**.
3. On each PTP 850E unit, enable Boundary clock on:
   - The port connected to the external switch.
   - The port used for synchronization with the paired unit.
4. Configure a point-to-point service between the following ports on the paired unit:
   - The port used for synchronization with the PTP 850E.
   - The radio interface or group.

7.5.6.3 Configuring Multiband with Layer 1 Link Bonding

Note: This section is relevant for Multiband configurations using Layer 1 Link Bonding. These configurations utilize PTP 850E for E-band and PTP 850C for Microwave.

Multiband with Layer 1 Link Bonding links can also be configured using the Quick Configuration wizard. It is recommended to use the wizard whenever possible.

This section includes:

- Overview of Multiband with Layer 1 Link Bonding
- Configuring Multiband with Layer 1 Link Bonding
- Configuring Synchronization in a Multiband Node with Layer 1 Link Bonding
- Editing a Multiband Link Bonding Group or its Members
- Displaying Statistics for a Multiband Link Bonding Group
- Deleting a Multiband Link Bonding Group

7.5.6.4 Overview of Multiband with Layer 1 Link Bonding

Multiband bundles E-Band and microwave radios in a single group that is shared with an Ethernet interface. Layer 1 Link Bonding enables operators to optimize the capacity of a Multiband link by combining the capacity of the E-Band and Multiband links into a single link of up to 14 Gbps. This is achieved when the PTP

850E is used in 2000 MHz channels, providing 10 Gbps, while the PTP 850C is operating in XPIC mode over 224 MHz channels, providing 4 Gbps at high profiles.

As with other Multiband links, a Multiband link with Layer 1 Link Bonding is highly resilient because it combines the high capacity of E-Band with the high resiliency of Microwave. The advantage of Link Bonding is that it enables the E-Band and Microwave links to aggregate their capacity, rather than utilizing the Microwave link as more of a backup to the E-Band link. In the event of radio failure in one device, the other device continues to operate to the extent of its available capacity. Thus, operators benefit from both the high capacity of E-Band and the high reliability of microwave.

7.5.6.5 Operation of Multiband with Layer 1 Link Bonding

A Multiband node with Link Bonding consists of an PTP 850E and an PTP 850C (the “paired” unit). The PTP 850E is attached to the external switch via Port 4, the QSFP port. This port can be used in QSFP mode (40 Gbps, Eth 3) or in SFP+ mode (10 Gbps, any of Eth 3, Eth 4, Eth 5, or Eth 6).

The PTP 850E unit performs traffic separation, based on the Link Bonding technology embedded in PTP 850E’s Broadcom modem. Traffic separation is performed using Broadcom’s proprietary load balancing method, which is implemented by segmenting and re-assembling the data stream. Each segment is a valid Ethernet packet with a proprietary header added.

Traffic is distributed symmetrically until a member of the Link Bonding group reaches its individual capacity, after which remaining traffic is passed via the remaining group member. If a member of a Link Bonding group goes down, traffic is automatically redistributed to the other member with no traffic loss.

Traffic is passed between the two units via an optical cable that connects Eth 7 (P5) of the PTP 850E to Eth 4 (P5) of the PTP 850C. This is a 10 Gbps connection with a bidirectional capacity of up to 4 Gbps.

In addition to the traffic connection between the two units, an optical Protocols cable must be connected between Eth 2 (P3) of the PTP 850E (P3) of the PTP 850E to Eth 2 (P3) of the PTP 850C. This connection carries L2 protocol data between the two units. The ports must be configured to 2.5 Gbps.

It is important to note that special SFP+ modules must be used for both the inter-unit traffic ports and the Protocols ports. For details and the marketing models of the required SFP+ modules, as well as the optical cables, see the Installation Guide for PTP 850E.

Alternatively, for configurations in which the paired unit is a third-party device, traffic can be passed between the two units via a CAT-5 cable between the PTP 850E Management port (P2) and an electrical port on the third-party device. In this configuration, you must configure in-band management, using one of the other PTP 850E ports, not the Management port.

You should configure a Multi-Carrier ABC group that includes both of the unit’s radio carriers on the PTP 850C unit.

You must configure a Link Bonding group on the PTP 850E unit. The Link Bonding group must include the PTP 850E unit’s radio interface and the PTP 850E Ethernet port (Eth 7) connecting the PTP 850E to the PTP 850C.

Each unit in the Multiband node is managed separately and independently. Inband management can be configured so that both units are managed over the link.

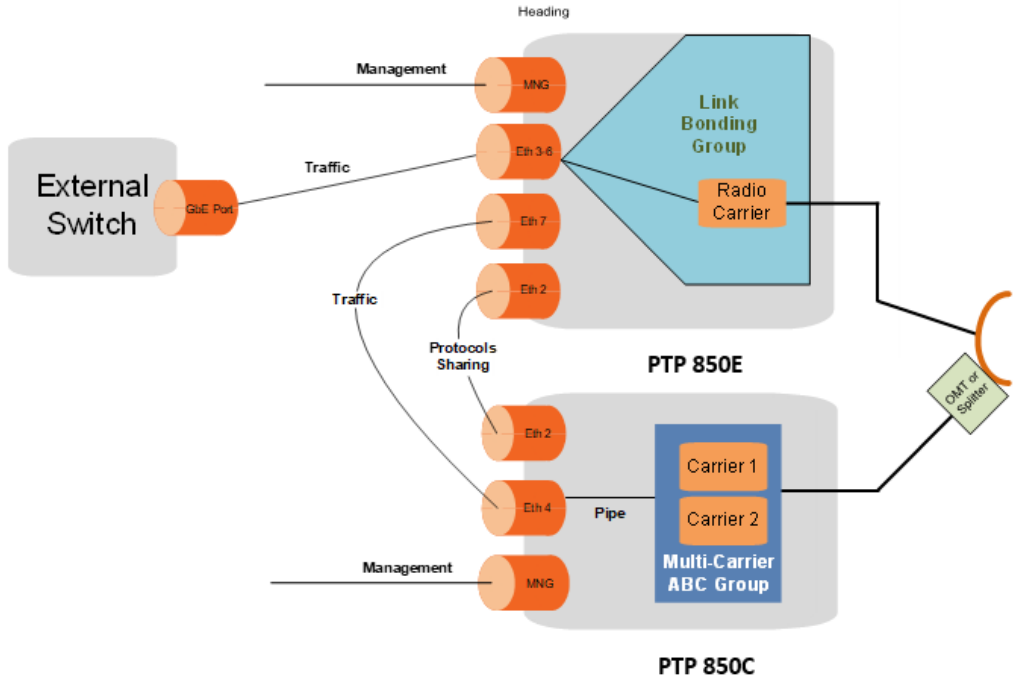


Figure 226: Multiband with Layer 1 Link Bonding – Multiband Antenna

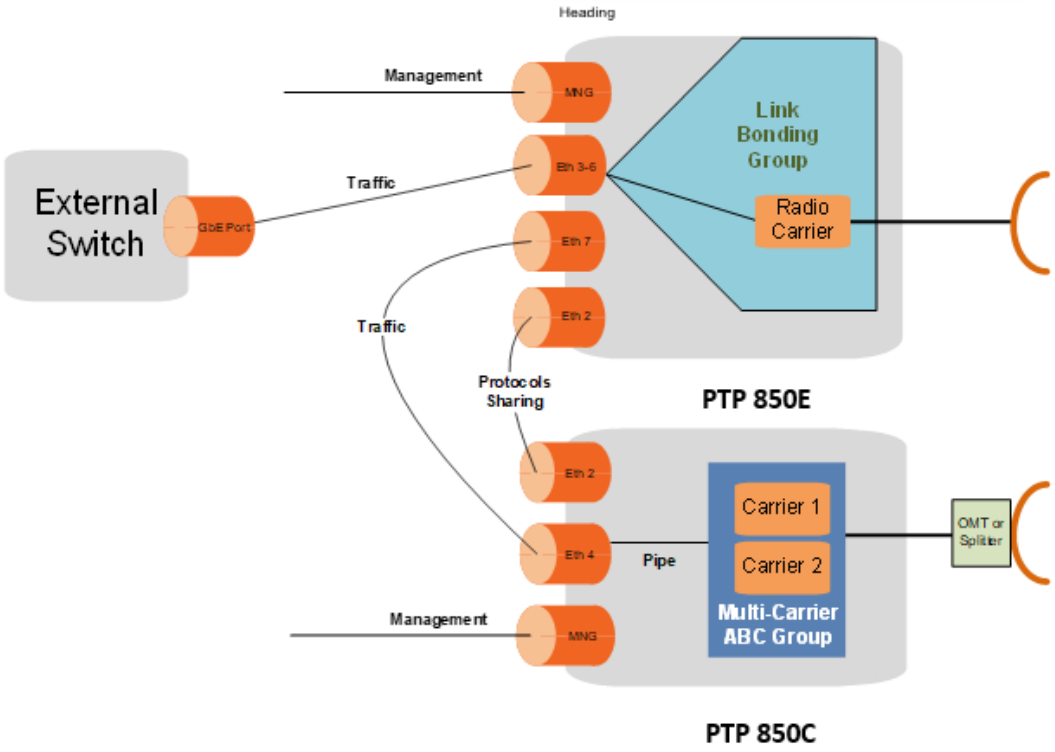


Figure 227: Multiband with Layer 1 Link Bonding – Separate Antenna

7.5.7 Multiband with Layer 1 Link Bonding – Hardware Configuration

A Multiband node with PTP 850E and PTP 850C can be configured with a single, Multiband Antenna. Alternatively, each unit can be configured with separate

antennas, making sure that the distance between the units does not exceed the length of either the Traffic or the Protocols cable.

In either case, the PTP 850C is connected to the antenna via an OMT (for dual polarization) or a Splitter (for single polarization).

For details, including the marketing models of the cables and SFP modules that must be used for the inter-unit connections, refer to the Installation Guide for PTP 850E.

7.5.8 Multiband with Layer 1 Link Bonding and Line Redundancy

A Multiband node with PTP 850E and PTP 850C can be configured with line redundancy. Line redundancy means the external switch is connected to both the main (PTP 850E) and the paired (PTP 850C) units via an optical splitter. The optical splitter routes traffic between the Ethernet port on the external switch and an Ethernet port on both the main and the paired unit.

Note: This configuration should use Enhanced Link Bonding Mode and a single cable for traffic and protocols.

In normal operation, traffic and management pass only between the external switch and the main unit, and the interface between the switch and the paired unit is turned off. In the event of switchover, the link between the external switch and the paired unit is automatically activated by switching off the interface between the external switch and the main unit and switching on the interface between the externall switch and the paired unit so that traffic and management are passed between the external switch and the paired unit.

A set of services for traffic and management must be configured on the paired unit in parallel to the services on the main unit. These services are configured in Operational state. The Line Redundancy mechanism deactivates the services in normal operating state based on the Line Redundancy role configurations, and activates them only in the event of switchover to support the flow of traffic and management from the external switch to the paired unit’s radio.

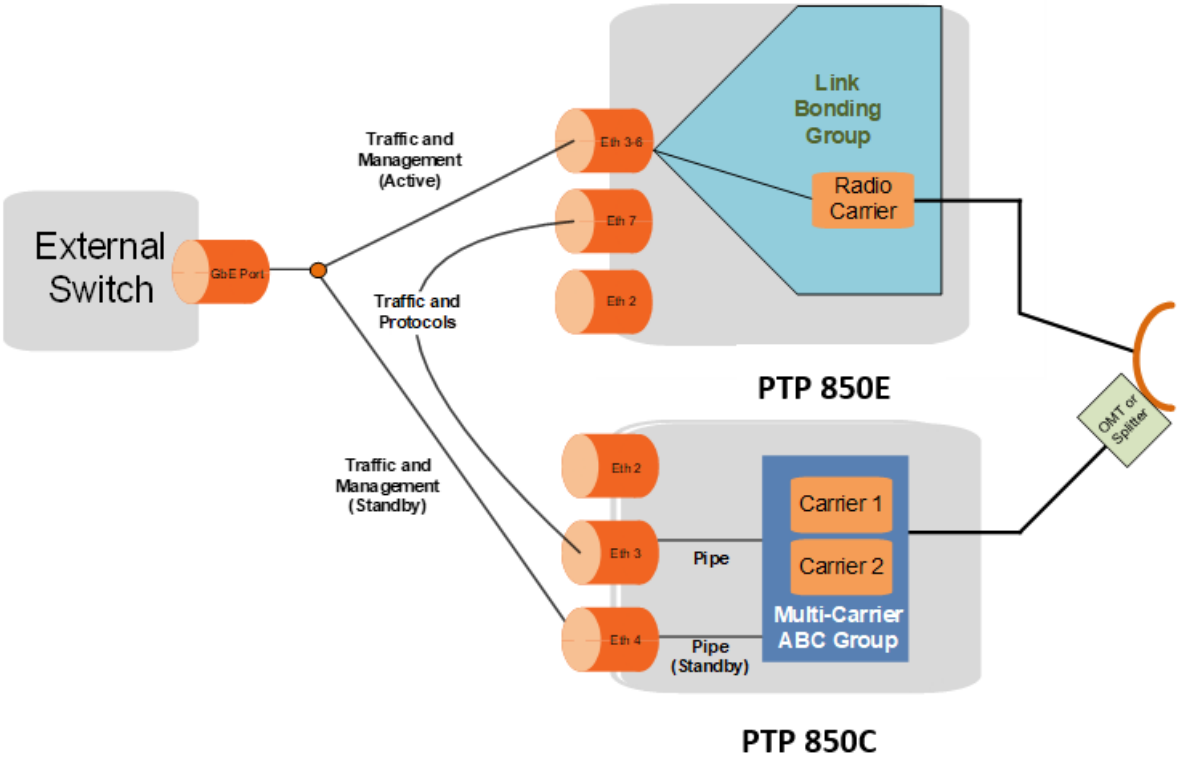


Figure 228: Multiband with Layer 1 Link Bonding and Line Redundancy – Multiband Antenna

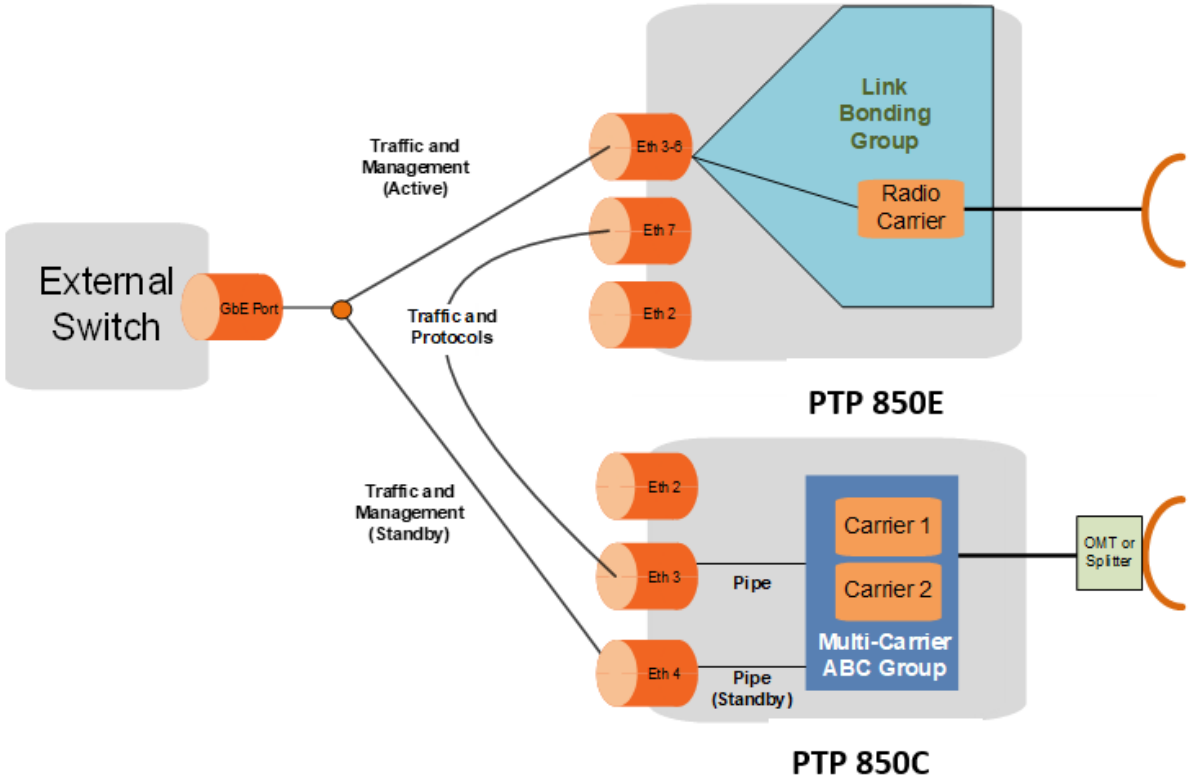


Figure 229: Multiband with Layer 1 Link Bonding and Line Redundancy – Separate Antennas

The following events trigger switchover:

Note: Radio failure on the main unit does not trigger switchover. Since traffic continues to be passed between the main unit and the paired unit, the paired unit's radio link continues to operate.

- Failure of traffic cable between external switch and main unit:
  - Traffic interfaces with the external switch on local and remote main units are automatically set to Down.
  - Traffic services are automatically disabled on the local and remote main units.
  - Traffic interfaces with the external switch on local and remote paired units are automatically set to Up.
  - Traffic services are automatically enabled on the local and remote paired units.
  - The management service points on the radio of the local and remote paired units are automatically enabled.
- Traffic cable between the main and paired unit fails:
  - The management service points on the radio of the local and remote paired units are automatically enabled.
  - On the remote side of the link, the interfaces connecting the traffic cable between the main and paired unit are automatically set to Down.
- Failure of main unit:
  - Traffic interfaces with the external switch on the remote main unit is automatically set to Down.
  - Traffic services are automatically disabled on the remote main unit.
  - Traffic interfaces with the external switch on local and remote paired units are automatically set to Up.
  - Traffic services are automatically enabled on the local and remote paired units.
  - The management service points on the radio of the local and remote paired units are automatically enabled.
  - On the remote side of the link, the interfaces connecting the traffic cable between the main and paired unit are automatically set to Down.

When the failure is rectified, the configuration automatically reverts to its normal operational configuration after expiration of a Wait to Restore (WTR) timer. Revertive mode cannot be disabled. However, the WTR timer is user-configurable.

Lockout and forced switch are available to manually change the state of the configuration (force-switch) or to manually force the configuration to remain in its current state (lockout). Lockout can be used to override Revertive mode and keep the configuration in switchover mode, should this be necessary. In System Release 12.7, lockout and forced switch must be applied via CLI.

7.5.9 Configuring Multiband with Layer 1 Link Bonding

To configure a Multiband node with Layer 1 Link Bonding:

1. Connect the external switch to the QSFP port (P4, Eth3 – Eth6) on the PTP 850E. This port can be configured to operate in QSFP mode (40 Gbps) or SFP+ mode (10 Gbps).
2. In the Interface Manager, make sure the port connected to the PTP 850C for passing traffic between the two units is set to **Admin** = **Down**.
3. Configure the speed of Eth 7 on the PTP 850E and Eth 4 on the PTP 850C to 10 Gbps.
4. On both the PTP 850E and the PTP 850C, configure the port speed of Eth 2 to 2.5 Gbps.

5 Connect an optical cable between Eth 7 (P5) on the PTP 850E and Eth 4 (P5) on the PTP 850C. This cable carries traffic between the two units.
6 Connect an optical cable between Eth 2 (P3) of each unit. This cable carries L2 protocol data between the two units.

Note: Special SFP+ modules must be used for both the inter-unit traffic ports (Eth 7/P5 on the PTP 850E, Eth 4/P5 on the PTP 850C) and the Protocols ports (Eth 2/P3 on both units). For details and the marketing models of the required SFP+ modules, as well as the optical cables, see the Installation Guide for PTP 850E.

7 Configure the scripts and radio settings for both units, including XPIC on the PTP 850C if so desired.
8 On the PTP 850C, configure a Multi-Carrier ABC group that includes both of the unit's radio carriers.
9 On the PTP 850E only, configure a Link Bonding group that includes the radio interface and the Ethernet interface (Eth 7) connected to the PTP 850C:

Note: Before adding a group member, make sure that no shapers or service points are configured on the interface.

i Select **Ethernet** > **Groups** > **Link Bonding**. The Link Bonding page opens.

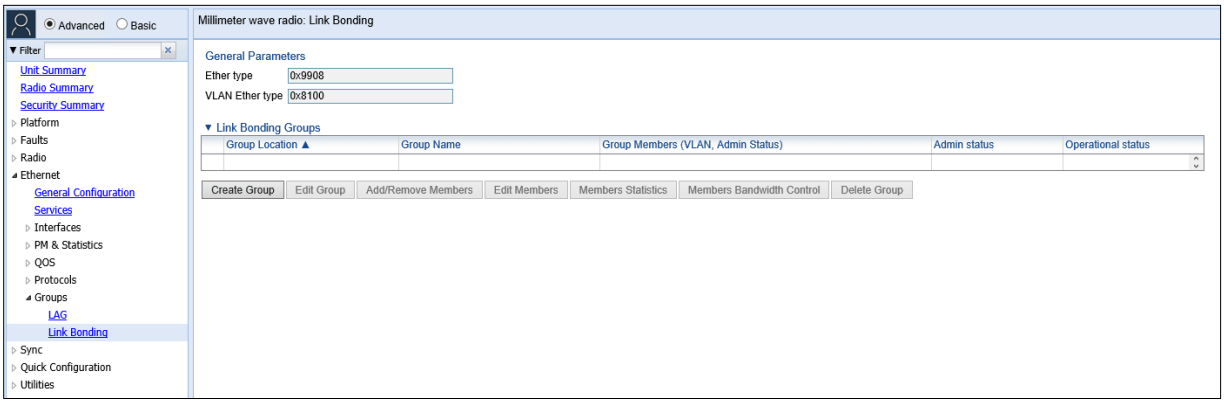


Figure 230: Link Bonding Page (Empty)

ii Click **Create Group**. Page 1 of the Link Bonding Group wizard opens.

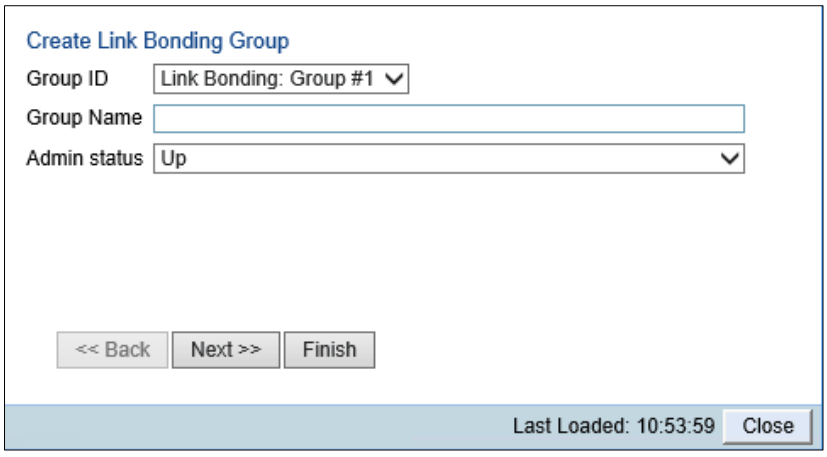


Figure 231: Link Bonding Group Wizard – Page 1

iii In the **Group ID** field, select **Link Bonding: Group #1**.
iv Optionally, in the **Group Name** field, enter a descriptive name for the group.

v In the **Admin status** field, select **Up**.
vi Click **Next**. Page 2 of the Link Bonding Group wizard opens.

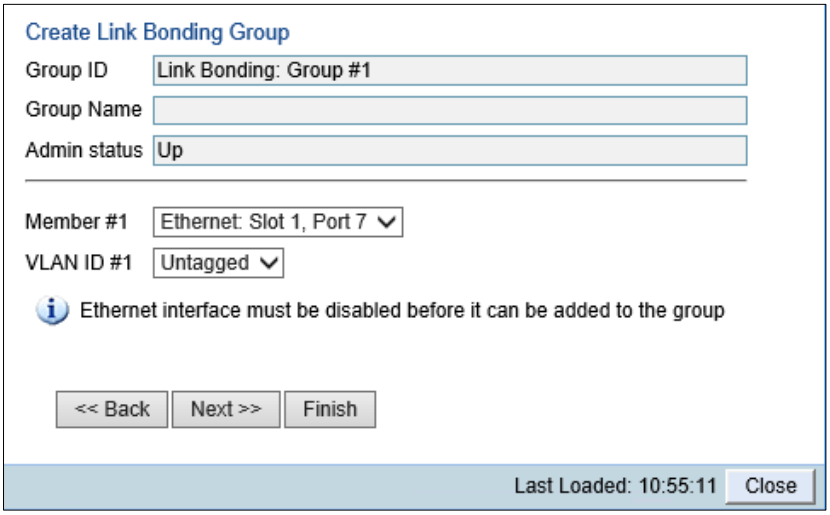


Figure 232: Link Bonding Group Wizard – Radio Member

vii n the **Member #1** field, select **Radio: Slot 1, Port 1**.
In the **VLAN ID #1** field, leave the default value of **Untagged**.
viii Click **Next**. Page 3 of the Link Bonding Group wizard opens.

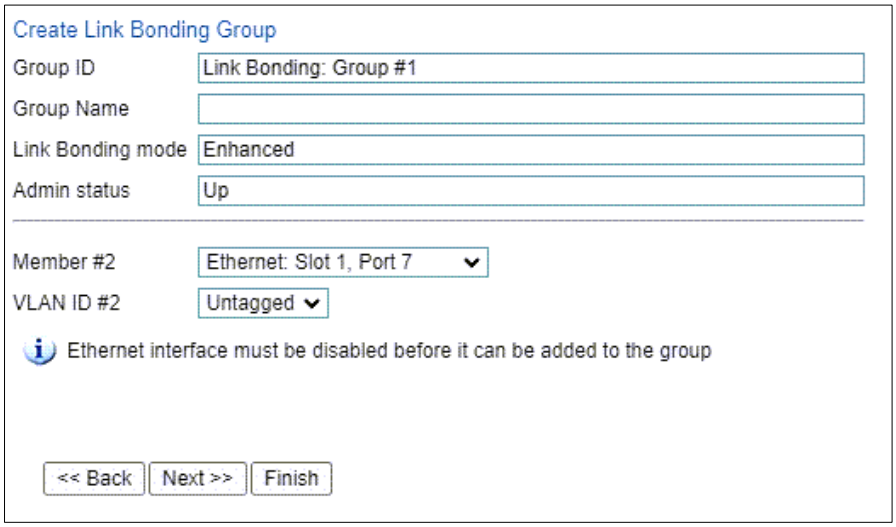


Figure 233: Link Bonding Group Wizard – Ethernet Member

ix In the **Member #2** field, select the port connected to the paired unit for passing traffic between the two units. In most configurations, this is **Ethernet: Slot 1, Port 7**. In configurations with a third-party device in which the PTP 850E Management port is connected to an electrical port on the third-party device, select **Management: Slot 1, Port 1**
x In the **VLAN ID #2** field, leave the default value of **Untagged**.
xi Click **Finish**. The Selection Summary page opens.

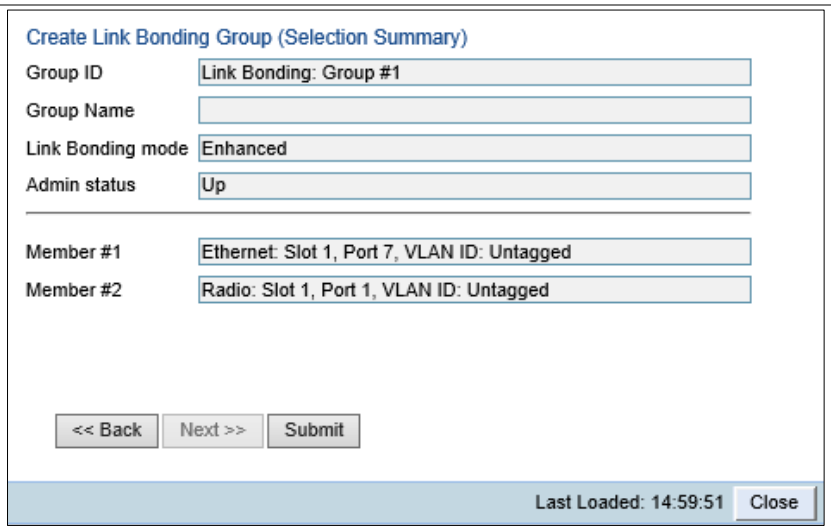


Figure 234: Link Bonding Group Wizard – Selection Summary Page

xii Click **Submit**. The group is added to the Link Bonding page.

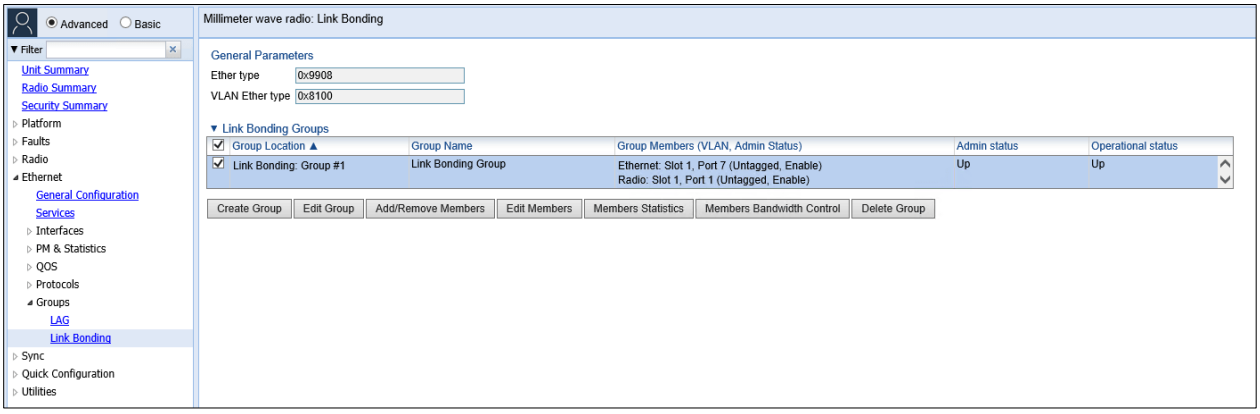


Figure 235: Link Bonding Page (Populated)

10 In the Interface Manager, set the port connected to the PTP 850C for passing traffic between the two units to **Admin** = **Up**. See Enabling the Interfaces (Interface Manager).

11 In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page opens.

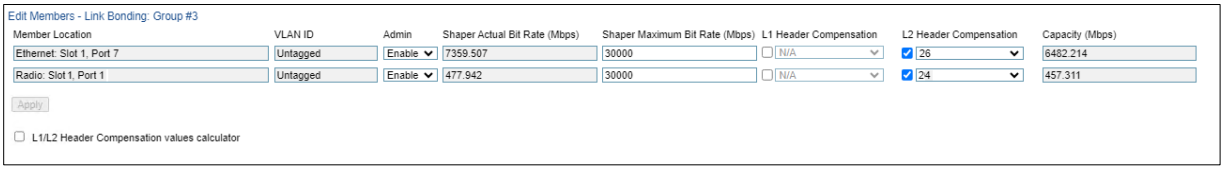


Figure 236: Link Bonding Groups – Edit Members Page

12 In the **Shaper actual bit rate** column, you can adjust the shaper for either or both interfaces in the group. Generally, there is no need to change this parameter from its default value of 30000 Mbps. The **Shaper actual bit rate** column displays the actual current traffic distribution between the PTP 850E radio (the radio interface) and the PTP 850C (the Ethernet interface, through which traffic is sent to the PTP 850C). This is displayed in Mbps.

Note: In order to change any of the values in the **Shaper actual bit rate** column, you must first verify that Inband Management is enabled. Otherwise, the change will have no effect.

13 In the **L1 header compensation** column:

- Do not select the Ethernet member.
- If the **Shaper actual bit rate** for the radio member is less than 8076, do not select the Ethernet member. If the **Shaper actual bit rate** for the radio member is 8076 or higher, set the **L1 header compensation** according to the **Shaper actual bit rate** for the radio member.

Note: The purpose of this setting is to prevent a bottleneck for traffic sent by the Link Bonding group to the PTP 850E's radio.

Table 22: L1 Header Compensation for Radio Interface (PTP 850E-PTP 850C Multiband Configuration)

Shaper Actual Bit Rate for Radio Member	L1 Header Compensation for Radio Member
Shaper actual bit rate is less than 8076	Do not select L1 Header Compensation
Shaper actual bit rate is 8076 to 8172	1
Shaper actual bit rate is 8173 to 8268	2
Shaper actual bit rate is 8269 to 8364	3
Shaper actual bit rate is 8266 to 8460	4
Shaper actual bit rate is 8461 to 8556	5
Shaper actual bit rate is 8557 to 8652	6
Shaper actual bit rate is 8653 to 8749	7
Shaper actual bit rate is 8750 to 8845	8
Shaper actual bit rate is 8846 to 8941	9
Shaper actual bit rate is 8942 to 9037	10
Shaper actual bit rate is 9038 to 9133	11
Shaper actual bit rate is 9134 to 9229	12
Shaper actual bit rate is 9230 to 9325	13
Shaper actual bit rate is 9326 to 9422	14

Shaper Actual Bit Rate for Radio Member	L1 Header Compensation for Radio Member
Shaper actual bit rate is 9423 to 9518	15
Shaper actual bit rate is 9519 to 9614	16
Shaper actual bit rate is 9615 to 9710	17
Shaper actual bit rate is 9711 to9806	18
Shaper actual bit rate is 9807 to 9902	19
Shaper actual bit rate is 9903 to 10000	20

14 In the **L2 header compensation** column, both interfaces should be selected. Generally, there is no need to change this parameter from its default value of 26 for the Ethernet interface and 24 for the radio interface.
15 Click **Apply**.
16 In the **Admin** column, set the Admin status of each group member to **Enable**.

Note: This parameter determines whether the group member is enabled in the group, not the Admin status of the interface itself. In order to enable a group member, you must first verify that Inband Management is enabled. Otherwise, the change will have no effect.

The Admin status must be set to **Disable** whenever you modify the **L2 header compensation** field. Otherwise, the modification will have no effect.

17 Click **Apply**.
18 To ensure proper fault handling, configure Automatic State Propagation (ASP as follows:

i On the local and remote PTP 850E units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The Link Bonding group
- Controlled Port: The port connected to the external switch (Eth 3, Eth 4, Eth 5, or Eth 6).

ii On the local and remote PTP 850C units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The Multi-Carrier ABC group
- Controlled Port: Eth 4

19 Inband management can be carried between the PTP 850E and the PTP 850C via the Protocols cable that connects Eth 2 (P3) of each unit. To configure inband management, you must enable inband management on both units and define a management service that connects Eth 2 of both units, the Link Bonding groups, and the ingress port of the PTP 850E:

i On the local PTP 850E, configure a service point on the port connected to the external switch (Eth 3, Eth 4, Eth 5, or Eth 6).
ii On the local PTP 850E, configure a service point on Eth 2.
iii On the local PTP 850E, configure a service point on the Link Bonding group.
iv On the local PTP 850C, configure a service point on Eth 2.
v On the remote PTP 850C, configure a service point on Eth 2.
vi On the remote PTP 850E, configure a service point on Eth 2.
vii On the remote PTP 850E, configure a service point on the Link Bonding group.

20 Configure Radio Bandwidth Notification on the PTP 850E by performing the following steps:

i Select the Link Bonding group in the Link Bonding page and click **Members Bandwidth Control**. The Members Bandwidth Control page opens.

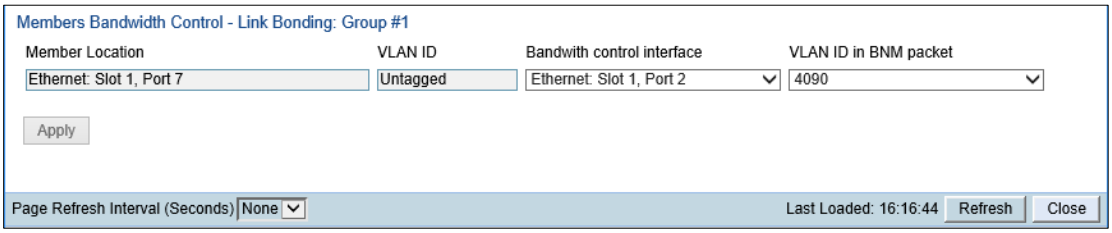


Figure 237: Link Bonding – Members Bandwidth Control Page

ii In the **Bandwidth control interface** column:

- For configurations that use the same cable for traffic and protocols, select the same port as displayed in the **Member Location** field.
- For configurations that use separate cables for traffic and protocols, select the port to which the Protocols cable is connected.

iii In the **VLAN ID in BNM packet** column, select **VLAN ID 4090**. This is the VLAN use to transfer protocol information between the two units.

21 Configure Radio Bandwidth Notification on the PTP 850C by performing the following steps:

i Select **Ethernet** > **Protocols** > **Bandwidth Notification**. The Bandwidth Notification page opens.

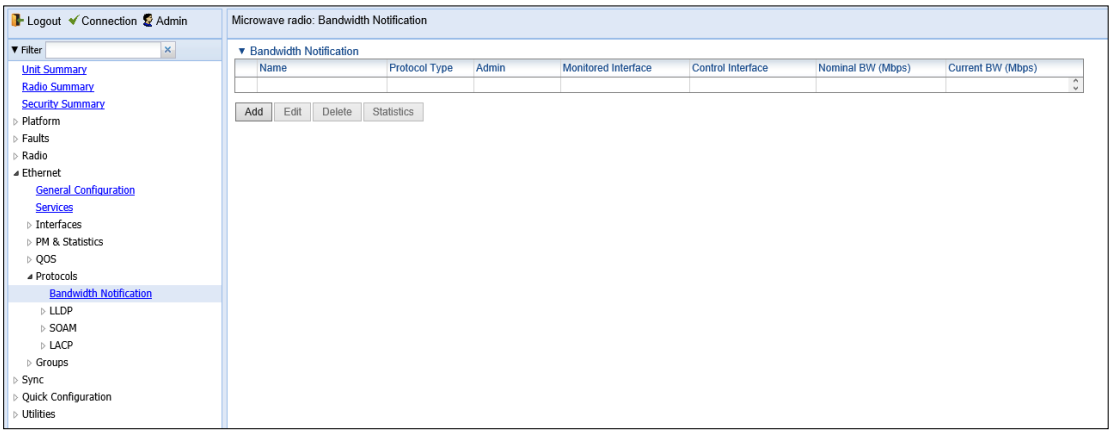


Figure 238: Bandwidth Notification Page (Empty)

ii Click **Add**. The Bandwidth Notification – Add page opens.

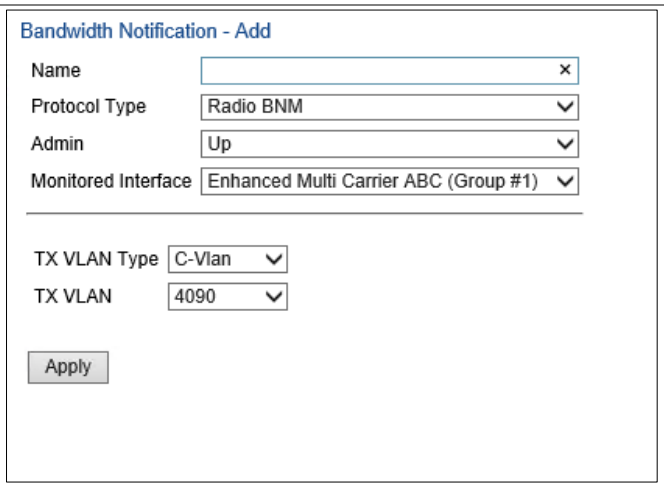


Figure 239: Bandwidth Notification – Add Page

iii In the **Name** field, select a descriptive name.

Note: Once you configure the RBN entity, you cannot edit the name later. The only way to change the name is to delete and reconfigure the RBN entity.

iv In the **Protocol Type** field, select **Radio BNM**.
v In the **Admin** field, select **Up**.
vi In the **Monitored Interface** field, select the PTP 850C's Multi-Carrier ABC group.
vii In the **TX VLAN Type** field, select **C-Vlan**.
viii In the **TX VLAN** field, select **VLAN ID 4090**.
ix Click **Apply**. The configuration is added to the Bandwidth Notification page with the Protocol Type **Radio BNM**.

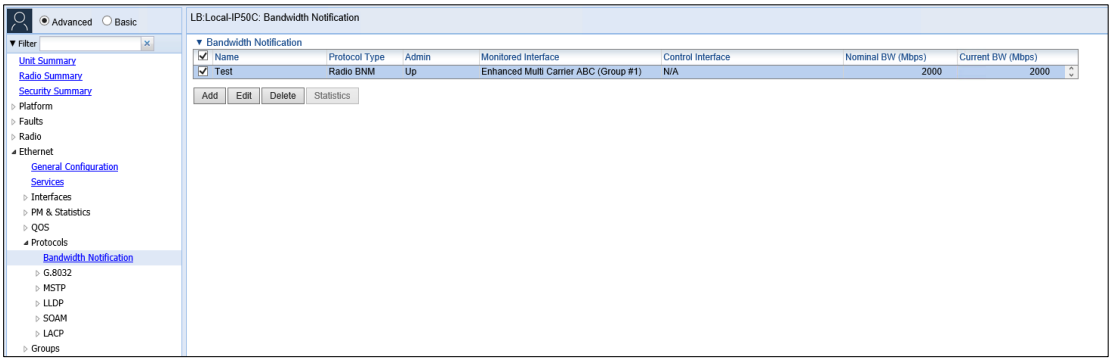


Figure 240: Bandwidth Notification Page (Populated with Radio BNM)

22 On the paired unit on both sides of the link, configure a point-to-point service for Radio Bandwidth Notification, with service points on the Multi-Carrier ABC group and Eth 2. The service points should be configured as follows:

i Create a service point on the Multi-Carrier ABC group with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: 4090
- Allow Flooding: Allow
- Learning Admin: Disable

ii Create a service point on Eth 2 with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: 4090
- Allow Flooding: Allow
- Learning Admin: Disable

See Configuring Service Points.

7.5.10 Configuring Synchronization in a Multiband Node with Layer 1 Link Bonding

SyncE and 1588 PTP can be used in Multiband nodes with Layer 1 Link Bonding. SyncE and 1588 PTP can be configured for both the PTP 850E and the PTP 850C. Synchronization messages are passed between the units via the Protocols cable.

7.5.10.1 Configuring SyncE in a Multiband Node with Layer 1 Link Bonding

To configure SyncE on a Multiband node with Layer 1 Link Bonding:

- **On the local PTP 850E, configure the following:**
  - Configure the port connected to the external switch (Eth 3, Eth 4, Eth 5, or Eth 6) as a sync source with priority 1.
  - Configure the radio interface as a sync source with priority 2.
  - Configure Eth 2 as a sync source with priority 3.
- **On the local PTP 850C, configure the following:**
  - Configure Eth 2 as a sync source with priority 1.
  - Configure radio interface 1 as a sync source with priority 2.
  - Configure radio interface 2 as a sync source with priority 3.
- **On the remote PTP 850C, configure the following:**
  - Configure radio interface 1 as a sync source with priority 1.
  - Configure radio interface 2 as a sync source with priority 2.
  - Configure Eth 2 as a sync source with priority 3.
- **On the remote PTP 850E, configure the following:**
  - Configure Eth 2 as a sync source with priority 1.
  - Configure the radio interface as a sync source with priority 2.
  - Configure the port connected to the external switch (Eth 3, Eth 4, Eth 5, or Eth 6) as a sync source with priority 3.

All sync sources should be configured with Sync Interface Quality G.813/8262. For instructions on configuring SyncE, see Configuring the Sync Source.

7.5.10.2 Configuring 1588 PTP in a Multiband Node with Layer 1 Link Bonding

To use 1588 PTP on a Multiband node with Layer 1 Link Bonding, you must configure Boundary Clock on the PTP 850E and Transparent Clock on all of the units, as described below. 1588 messages are generated by the Boundary Clock mechanism on the PTP 850E and sent untagged to the PTP 850C via the Protocols cable. They receive VLAN tagging on the PTP 850C in order to separate them from user traffic.

Note: If the PTP 850C goes down, 1588 packets will not be transmitted to the other side of the link.

To configure 1588 PTP for the Multiband node with 4+0 Layer 1 Link Bonding:

1 Configure SyncE following the instructions in Configuring the Sync Source.
2 Enable 1588 PTP on each unit, including the PTP 850E and the PTP 850C on both sides of the link:

i Select **Sync > 1588 > General Configuration**. The 1588 – General Configuration page opens.
ii In the **1588 PTP** field, select **Enable**.
iii Click **Apply**.

3 On the PTP 850E unit on both sides of the link, enable Boundary clock on:

- The port connected to the external switch (Eth 1 or Eth 3 Eth 3, Eth 4, Eth 5, or Eth 6).
- Eth 2.

4 On the PTP 850C unit on both sides of the link, enable Transparent Clock on the Multi-Carrier ABC group.
5 On the PTP 850C unit on both sides of the link, configure a point-to-point service with service points on the Multi-Carrier ABC group and Eth 2. The service points should be configured as follows:

- Service point on the Multi-Carrier ABC group:
  - Service Point Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation: Per customer’s choice
  - Allowing Flooding: Allow
  - Learning Admin: Disable
- Service point on Eth 2:
  - Service Point Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation: Untagged
  - Allowing Flooding: Allow
  - Learning Admin: Disable

7.5.11 Enabling Link Bonding Throughput Enhancement for Multiband with Layer 1 Link Bonding

After configuring a Link Bonding node, it is recommended to enable Link Bonding Throughput Enhancement. Link Bonding Throughput Enhancement is available for the main unit only, not for the paired unit.

Link Bonding Throughput Enhancement is enabled on the main unit's radio interface. When it is enabled, the L2 Header Compensation for the radio interface must be reduced by 12.

Link Bonding Throughput Enhancement affects the recommended L2 Header Compensation. Make sure to use the values listed in L1 and L2 Header Compensation Values.

The Link Bonding Throughput Enhancement and L2 Header Compensation settings must be the same for the main units on both sides of the link. Therefore, the changes should be applied in the following order to ensure that management is not lost:

1 Enable Link Bonding Throughput Enhancement on the remote unit:

i Select **Radio > Ethernet Interface > Configuration**. The Radio Ethernet Interface Configuration page opens.

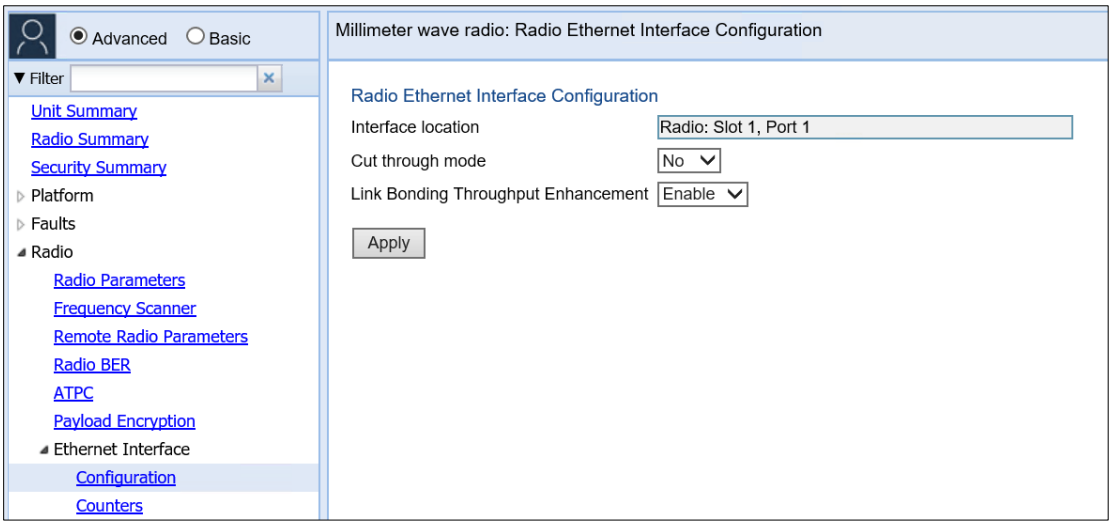


Figure 241: Radio Ethernet Interface Configuration Page (PTP 850E)

ii In the **Link Bonding Throughput Enhancement** field, select **Enable**.
iii Click **Apply**.

2 Enable Link Bonding Throughput Enhancement on the local unit:

i Select **Radio > Ethernet Interface > Configuration**. The Radio Ethernet Interface Configuration page opens (Figure 241).
ii In the **Link Bonding Throughput Enhancement** field, select **Enable**.
iii Click **Apply**.

3 Modify the L2 Header Compensation (decrease by 12) on the remote unit:

i Select **Ethernet** > **Groups** > **Link Bonding**. The Link Bonding page opens .
ii In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page opens.
iii In the **L2 header compensation** column, reduce the value for the radio interface by 12. For example, if the group was set to the default value of 24, change it to 12.
iv Click **Apply**.

4 Modify the L2 Header Compensation (decrease by 12) on the local unit:

i Select **Ethernet** > **Groups** > **Link Bonding**. The Link Bonding page opens.

ii In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page.

iii In the **L2 header compensation** column, reduce the value for the radio interface by 12. For example, if the group was set to the default value of 24, change it to 12.

iv Click **Apply**.

7.5.12 Editing a Multiband Link Bonding Group or its Members

To change the Group Name or the Admin Status of the Link Bonding group:

1 In the Link Bonding page, select the group and click **Edit Group**. The Edit Group page opens.

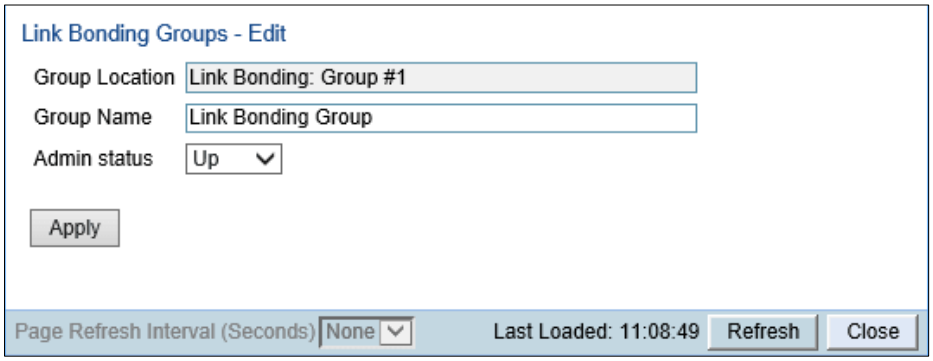


Figure 242: Link Bonding Groups – Edit Page

2 In the **Group Name** field, enter the new name.

3 In the **Admin status** field, change the Admin status of the group to **Up** or **Down**.

4 Click **Apply**.

7.5.13 Displaying Statistics for a Multiband Link Bonding Group

You can display the total number of segments and bytes (TX and RX) that have passed through each member of the Link Bonding group.

Note: The ability to clear these statistics is planned for future release.

To display throughput statistics for the members of the Link Bonding group:

1 In the Link Bonding page, select the group and click **Member Statistics**. The Member Statistics page opens.

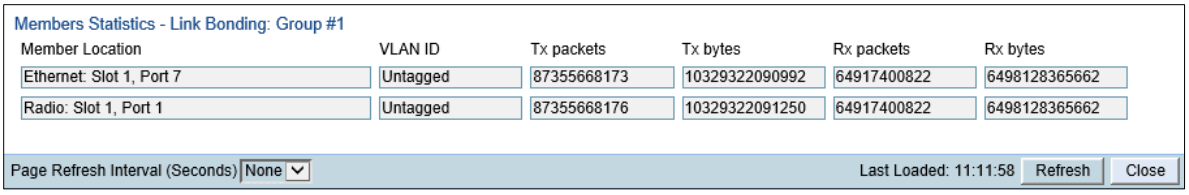


Figure 243: Link Bonding Groups – Member Statistics Page

7.5.14 Deleting a Multiband Link Bonding Group

To delete a Link Bonding group, you must first remove the members from the group:

1 In the Link Bonding page, select the group and click **Add/Remove Members**. The Add/Remove Members page opens.

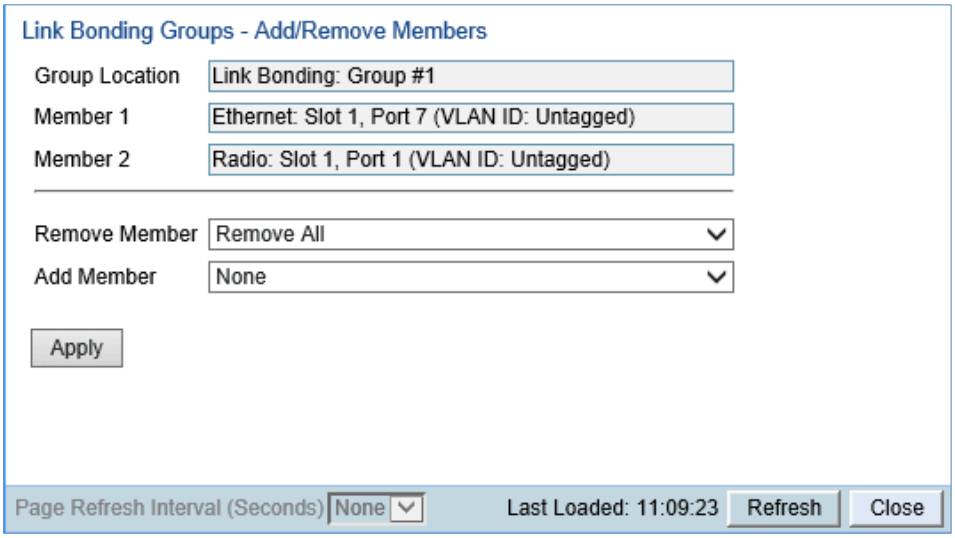


Figure 244: Link Bonding Groups – Member Statistics Page

2 In the **Remove Member** field, select **Remove All**.
3 Click **Apply**.
4 Remove any service points on the Link Bonding group.
5 In the Link Bonding page, select the group and click **Delete Group**.

7.6 Configuring XPIC

This section includes:

- XPIC Overview
- Configuring Layer 1 Link Bonding (Optional – PTP 850E Only)
- Configuring the Radio Carriers
- Deleting an AMCC (XPIC) Group
- Performing Antenna Alignment for XPIC
- XPIC Status and Troubleshooting

7.6.1 XPIC Overview

Cross Polarization Interference Canceller (XPIC) is a feature that enables two radio carriers to use the same frequency with a polarity separation between them. Since they will never be completely orthogonal, some signal cancelation is required.

With PTP 850C, XPIC is configured with the two carriers of a single PTP 850C unit on each side of the link.

With PTP 850C, XPIC uses two PTP 850E units on each side of the link.

XPIC enables PTP 850E links of up to 20 Gbps, consisting of 10 Gbps per each PTP 850E unit.

XPIC with PTP 850C - Overview

XPIC enables PTP 850C links of up to 2 Gbps, consisting of 1 Gbps per carrier.[12] XPIC can be installed in either of the following configurations:

- Direct Mount – The PTP 850C unit is connected to the antenna via an OMT.
- Remote Mount – The PTP 850C unit is connected to the antenna via two flexible waveguides. Some configurations also require an OMT.

To configure and enable XPIC:

- Install the PTP 850C unit in a dual polarization configuration, according to the instructions in the PTP 850C Installation Guide.
    - Configure the carriers – See *Configuring the Radio Carriers*
    - Perform antenna alignment – See *Performing Antenna Alignment for XPIC*

In order for XPIC to be operational, all the following conditions must be met:

- The frequency of both carriers should be equal.
- The same script must be loaded in both carriers.

XPIC with PTP 850E - Overview

XPIC enables PTP 850E links of up to 20 Gbps, consisting of 10 Gbps per each PTP 850E unit.

Optionally, XPIC can be configured with Layer 1 Link Bonding. In this case, a single 40 Gbps traffic connection can be configured with the external switch via the QSFP port on one of the PTP 850E units (the main unit). This provides a link of up to 20 Gbps, with traffic distribution being performed by the main unit.

An PTP 850E 2+0 XPIC configuration requires two PTP 850E units on each side of the link. Two options are available:

An PTP 850E 2+0 XPIC configuration requires two PTP 850E units on each side of the link. Two options are available:

- Direct Mount – The PTP 850E units are connected to the antenna via an OMT. One unit must be installed with horizontal polarization and the other must be installed with vertical polarization.
- Integrated Antenna – One PTP 850E unit and integrated antenna is assembled with a vertical polarization and the other PTP 850E unit and integrated antenna is assembled with a horizontal polarization.

For both options, the following cables must be used to connect the two units:

- An XPIC cable must be connected between the Protection/XPIC ports (P6) of each unit. This cable carries the data necessary for each unit to perform interference cancellation.
- A Clock Sharing cable must be connected between the TNC ports of each unit. This cable transmits clock frequency information between the two units, enabling synchronization.

On each side of the link, the unit with the higher MAC address is automatically assigned the role of clock master unit.

With Layer 1 Link Bonding, an additional two cables are required:

- Traffic Cable – An optical cable that passes traffic between the two units via a 10 Gbps connection between Eth 7 (P5) of each unit.
- Protocols Cable – An optical cable that carries L2 protocol data between the two units via a 2.5 Gbps connection between Eth 2 (P3) of each unit. The ports must be configured to 2.5 Gbps.

With Layer 1 Link Bonding, the main unit receives traffic from the external switch via P4 (Eth 3), which can be configured at 40 Gbps or 10 Gbps. At 40 Gbps, the XPIC link can provide up to 20 Gbps capacity. At 10 Gbps, the link can provide up to 10 Gbps capacity. Traffic distribution is performed by the active PTP 850E, which distributes traffic between its own radio and the paired unit via the Traffic Cable.

The main unit can be either vertical or horizontal. Just make sure that the main units on both side of the link have the same polarization (vertical or horizontal), and that the paired units on both side of the link have the same polarization, which should be the opposite polarization of the main units.

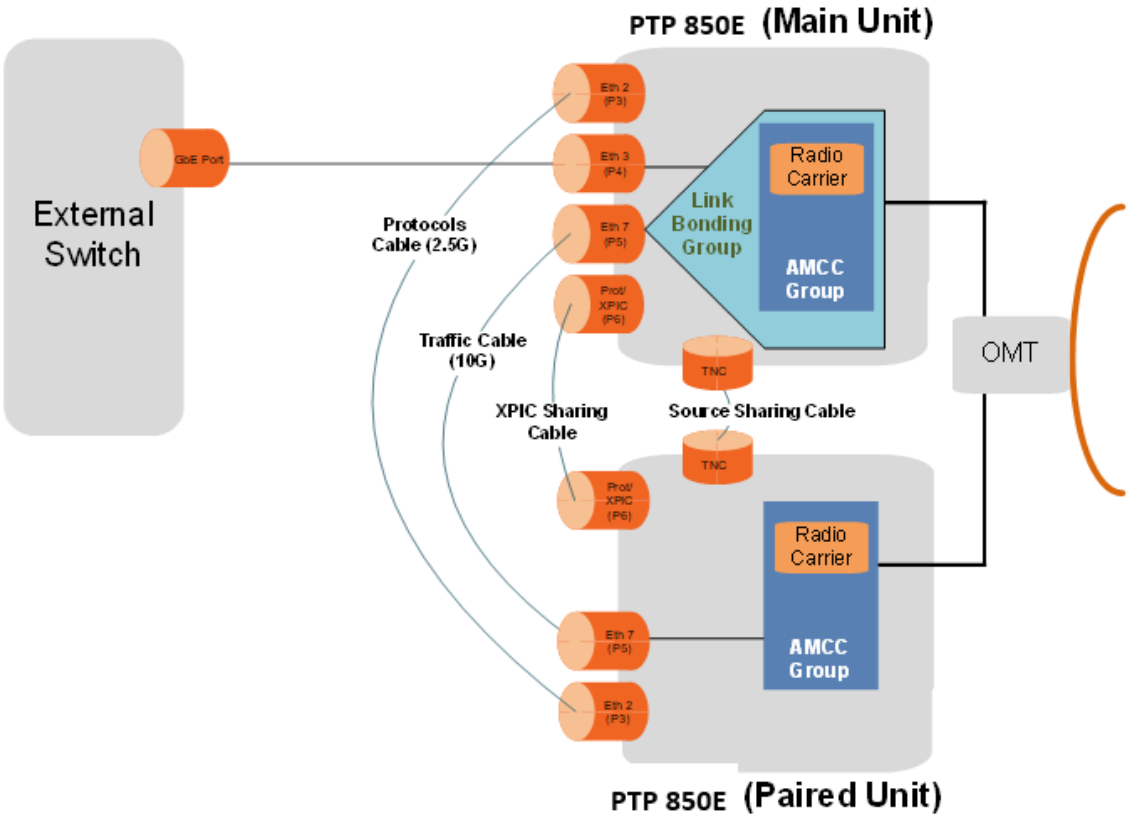


Figure 245: 2+0 XPIC Configuration - Direct Mount (with Link Bonding)

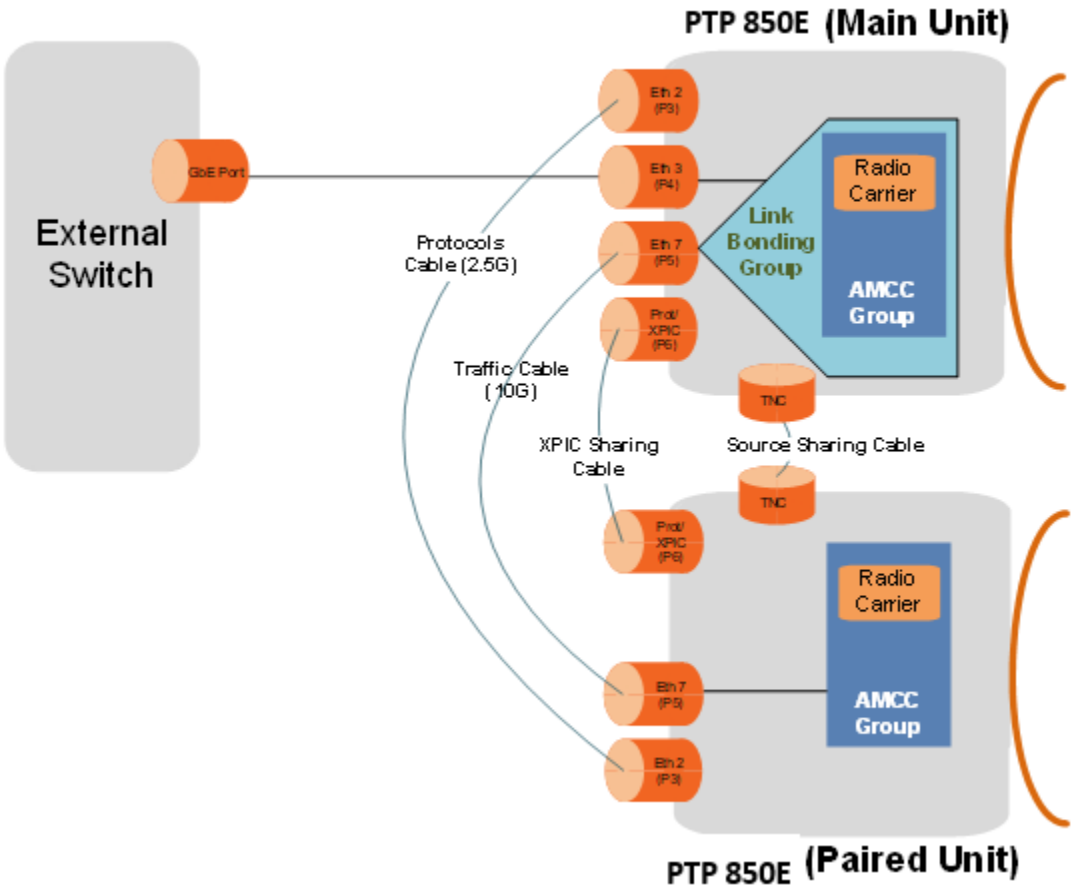


Figure 246: 2+0 XPIC Configuration – Integrated Antenna (with Link Bonding)

Without Layer 1 Link Bonding, each PTP 850E unit receives traffic from the external switch independently of the other unit. The traffic flows are completely independent, with no traffic sharing or load balancing between the units.

Management data is not shared between the two PTP 850E units. Therefore, management must be configured independently for each PTP 850E unit. Inband management can be used as long as LAG is not configured on the external switch. However, if LAG *is* configured on the external switch, inband management cannot be used, since there is no mechanism for sharing management traffic between the PTP 850E units.

Figure 247 2+0 XPIC Configuration – Direct Mount

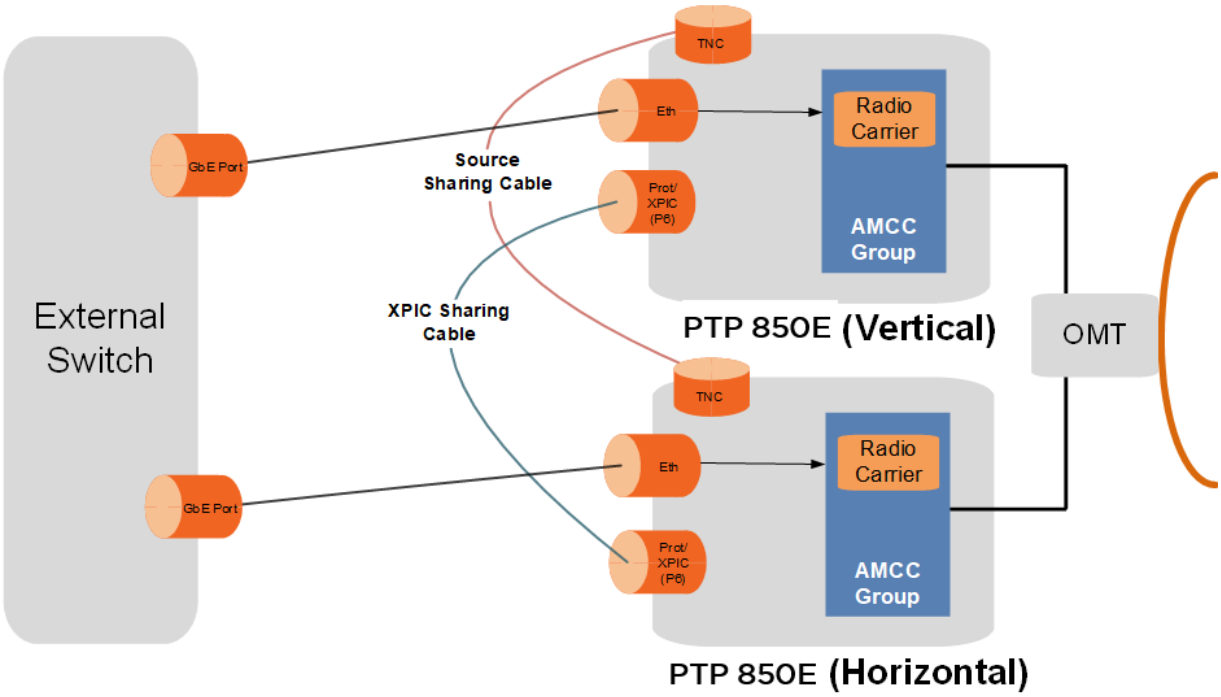
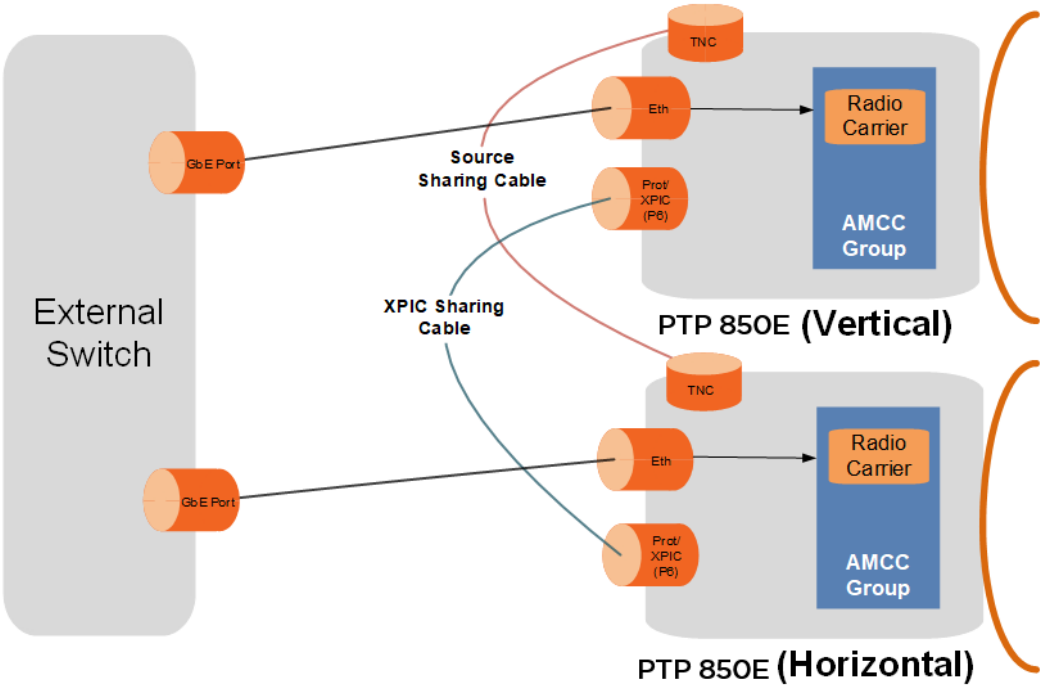


Figure 248 2+0 XPIC Configuration – Integrated Antenna



In order for XPIC to be operational, all the following conditions must be met:

- The frequency of both carriers should be equal.

- The same script must be loaded in both carriers.



Note

Power redundancy and PoE cannot be used with XPIC.

To configure and enable XPIC:

- Install the PTP 850E units and cables – See the PTP 850E Installation Guide, Section 5.5, 2+0 (XPIC) with 43 dBi Flat Antenna and Alignment Device or Section 6.3, 2+0 Direct Mount Dual Polarization (XPIC).
- Configure the carriers – See
- Configuring the Radio Carriers
- Perform antenna alignment

7.6.2 Configuring Layer 1 Link Bonding (Optional – PTP 850E Only)

To configure an XPIC link with Layer 1 Link Bonding:

1 Connect the external switch to the QSFP port (P4, Eth3 – Eth6) on the main unit. This port can be configured to operate in QSFP mode (40 Gbps) or SFP+ mode (10 Gbps). See Configuring Ethernet Interfaces.
2 On the main unit, in the Interface Manager make sure Eth 7 is set to **Admin** = **Down**. See Enabling the Interfaces (Interface Manager).
3 On both the main unit and the paired unit, configure the speed of Eth 7 to 10 Gbps. See Configuring Ethernet Interfaces.
4 Connect an optical cable between Eth 7 (P5) of the main unit and the paired unit. This cable carries traffic between the two units.
5 On both the main unit and the paired unit, configure the port speed of Eth 2 to 2.5 Gbps. See Configuring Ethernet Interfaces.
6 Connect an optical cable between Eth 2 (P3) of the main unit and the paired unit. This cable carries L2 protocol data between the two units.

Note: Special SFP+ modules must be used for both the inter-unit traffic ports (Eth 7/P5) and the Protocols ports (Eth 2/P3). For details and the marketing models of the required SFP+ modules, as well as the optical cables, see the Installation Guide for PTP 850E.

7 On the main unit only, configure a Link Bonding group that includes the radio interface and the Ethernet interface (Eth 7) connected to the paired unit for traffic:

Note: Before adding a group member, make sure that no shapers or service points are configured on the interface.

i Select **Ethernet** > **Groups** > **Link Bonding**. The Link Bonding page opens.

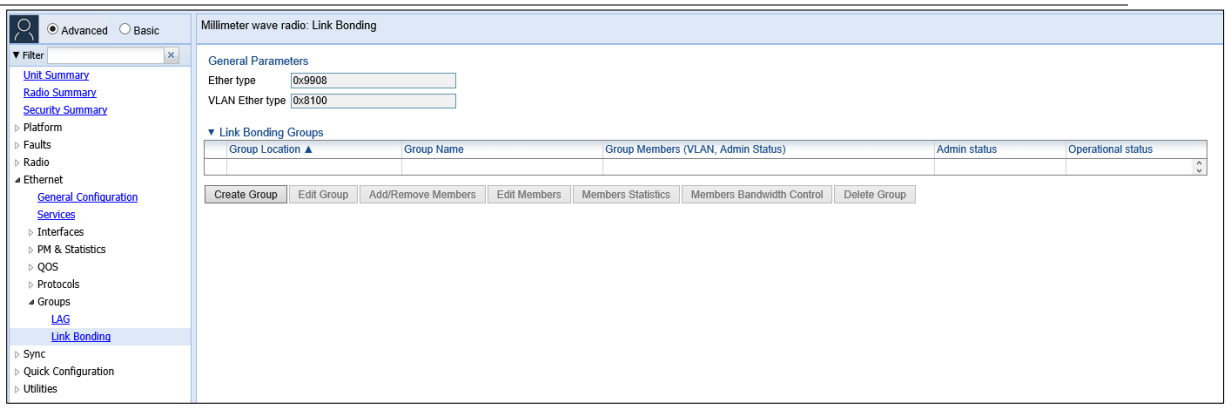


Figure 249: Link Bonding Page (Empty)

ii Click **Create Group**. Page 1 of the Link Bonding Group wizard opens.

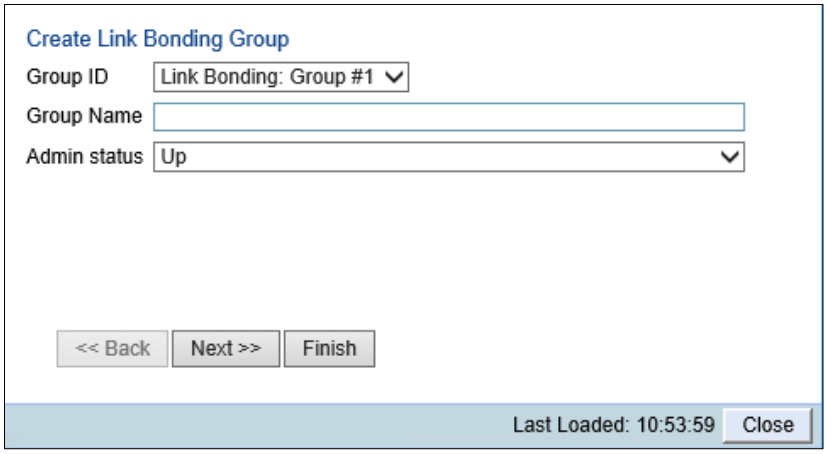


Figure 250: Link Bonding Group Wizard

iii In the **Group ID** field, select **Link Bonding: Group #1**.
iv Optionally, in the **Group Name** field, enter a descriptive name for the group.
v In the **Admin status** field, select **Up**.
vi Click **Next**. Page 2 of the Link Bonding Group wizard opens.

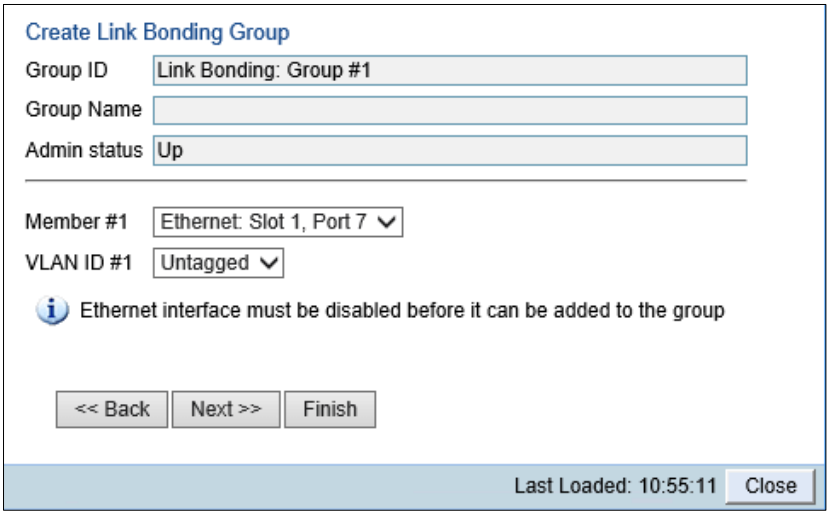


Figure 251: Link Bonding Group Wizard

vii n the **Member #1** field, select Ethernet: Slot 1, Port 7. This is the port connected to the paired unit.
viii In the **VLAN ID #1** field, leave the default value of **Untagged**.
ix Click **Next**. Page 3 of the Link Bonding Group wizard opens.

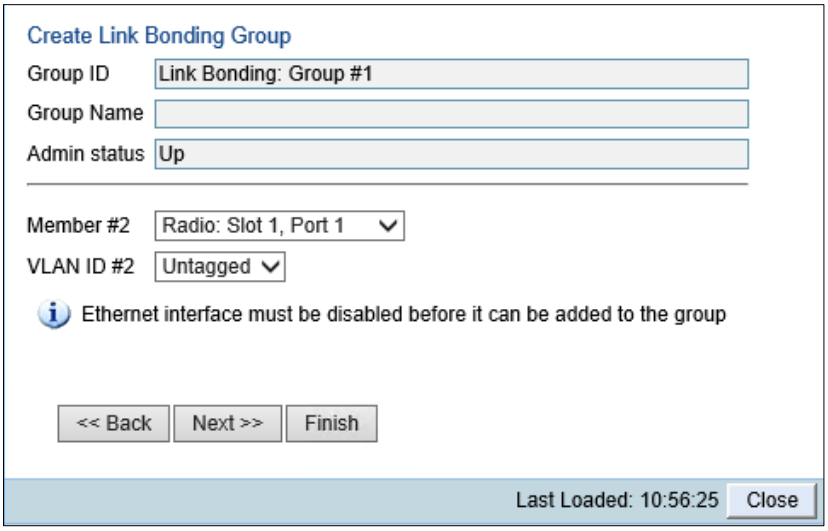


Figure 252: Link Bonding Group Wizard

x In the **Member #2** field, select Radio: Slot 1, Port 1.
xi In the **VLAN ID #2** field, leave the default value of **Untagged**.
xii Click **Next**. The Selection Summary page opens.

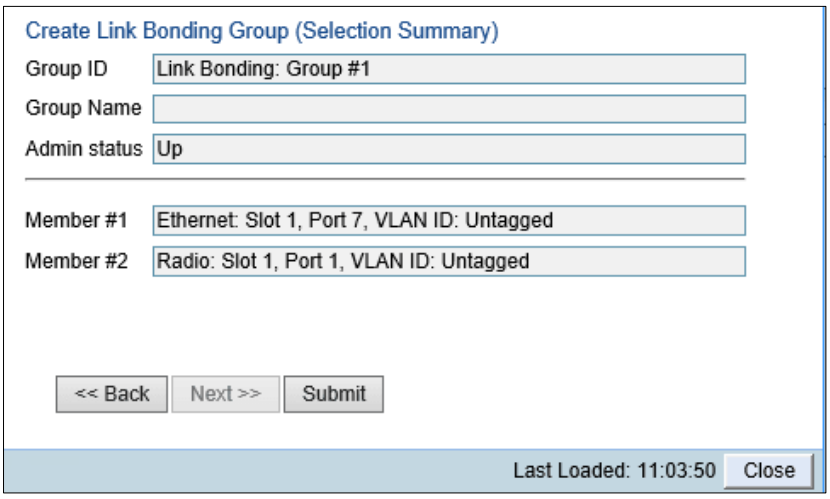


Figure 253: Link Bonding Group Wizard – Selection Summary Page

xiii Click **Submit**. The group is added to the Link Bonding page.

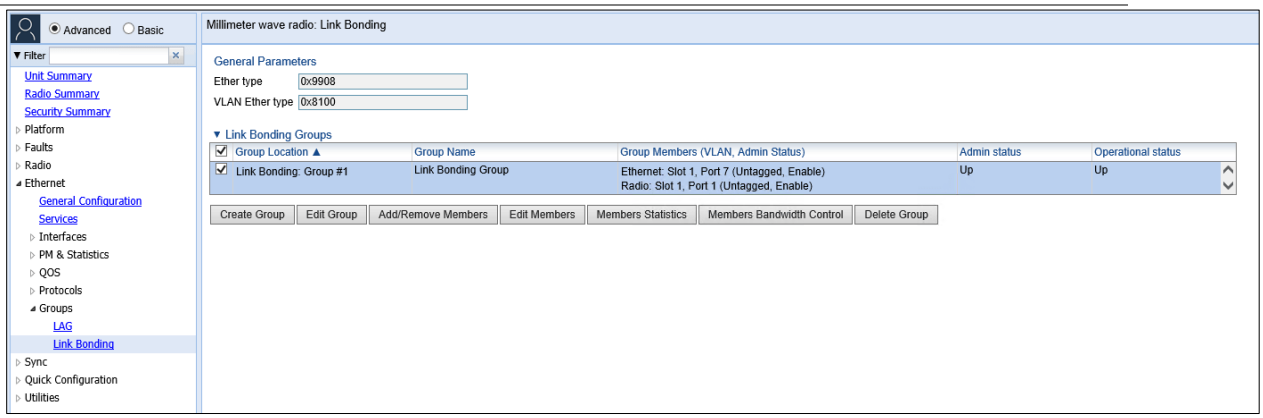


Figure 254: Link Bonding Page (Populated)

8 In the Interface Manager, set the port connected to the paired unit for passing traffic between the two units to **Admin** = **Up**. See Enabling the Interfaces (Interface Manager).

9 In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page opens.

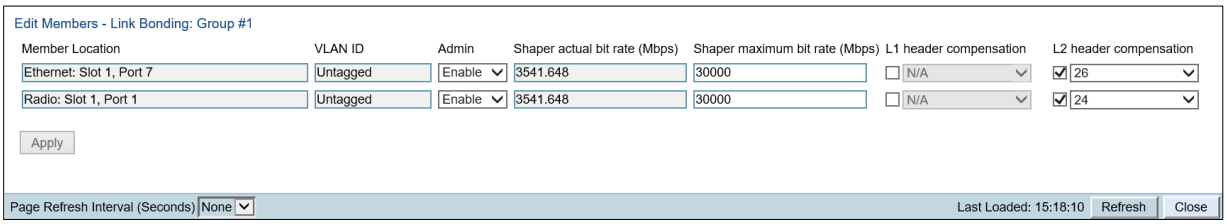


Figure 255: Link Bonding Groups – Edit Members Page

10 In the **Shaper maximum bit rate** column, you can adjust the shaper for either or both interfaces in the group. Generally, there is no need to change this parameter from its default value of 30000 Mbps. The **Shaper actual bit rate** column displays the actual current traffic distribution between the main unit (the radio interface) and the paired unit (the Ethernet interface, through which traffic is sent to the paired unit). This is displayed in Mbps.

11 In the **L1 header compensation** column:

- Do not select the Ethernet member.
- If the **Shaper actual bit rate** for the radio member is less than 8076, do not select the Ethernet member. If the **Shaper actual bit rate** for the radio member is 8076 or higher, set the **L1 header compensation** according to the **Shaper actual bit rate** for the radio member, as listed in Table 23.

Note: The purpose of this setting is to prevent a bottleneck for traffic sent by the Link Bonding group to the main unit's radio.

Table 23: L1 Header Compensation for Radio Interface (PTP 850E XPIC Configuration)

Shaper Actual bit Rate for Radio Member	L1 Header Compensation for Radio Member
Shaper actual bit rate is less than 8076	Do not select L1 Header Compensation
Shaper actual bit rate is 8076 to 8172	1

Shaper Actual bit Rate for Radio Member	L1 Header Compensation for Radio Member
Shaper actual bit rate is 8173 to 8268	2
Shaper actual bit rate is 8269 to 8364	3
Shaper actual bit rate is 8266 to 8460	4
Shaper actual bit rate is 8461 to 8556	5
Shaper actual bit rate is 8557 to 8652	6
Shaper actual bit rate is 8653 to 8749	7
Shaper actual bit rate is 8750 to 8845	8
Shaper actual bit rate is 8846 to 8941	9
Shaper actual bit rate is 8942 to 9037	10
Shaper actual bit rate is 9038 to 9133	11
Shaper actual bit rate is 9134 to 9229	12
Shaper actual bit rate is 9230 to 9325	13
Shaper actual bit rate is 9326 to 9422	14
Shaper actual bit rate is 9423 to 9518	15

Shaper Actual bit Rate for Radio Member	L1 Header Compensation for Radio Member
Shaper actual bit rate is 9519 to 9614	16
Shaper actual bit rate is 9615 to 9710	17
Shaper actual bit rate is 9711 to 9806	18
Shaper actual bit rate is 9807 to 9902	19
Shaper actual bit rate is 9903 to 10000	20

12 In the **L2 header compensation** column, both interfaces should be selected. Generally, there is no need to change this parameter from its default value of 26 for the Ethernet interface and 24 for the radio interface.
13 Click **Apply**.
14 In the **Admin** column, set the Admin status of each group member to **Enable**.

Note: If necessary, you can leave the Admin status of the group members **Disable** until a later time in order to complete the configuration with the group offline, then activate the group members later.

The Admin status must be set to **Disable** whenever you modify the **L1 header compensation** or **L2 header compensation** fields. Otherwise, the modification will have no effect.

15 Click **Apply**.
16 To ensure proper fault handling, configure Automatic State Propagation (ASP) as follows:

i On the local and remote main units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The Link Bonding group
- Controlled Port: The port connected to the external switch (Eth 3).

ii On the local and remote paired units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The radio port
- Controlled Port: The port connected to the main unit (Eth 7)

17 In-band management can be carried between the main unit via the Protocols cable that connects Eth 2 (P3) of each unit. To configure in-band management, you must enable in-band management on both units and define a management service that connects Eth 2 of both units, the Link Bonding groups, and the ingress port of the main unit (Eth 3):

i On the local main unit, configure a service point on the port connected to the external switch (Eth 3).

ii On the local main unit, configure a service point on Eth 2.
iii On the local main unit, configure a service point on the Link Bonding group.
iv On the local paired unit, configure a service point on Eth 2.
v On the remote paired unit, configure a service point on Eth 2.
vi On the remote main unit, configure a service point on Eth 2.
vii On the remote main unit, configure a service point on the Link Bonding group.

18 Configure Radio Bandwidth Notification on the main unit by performing the following steps:

i Select the Link Bonding group in the Link Bonding page and click **Members Bandwidth Control**. The Members Bandwidth Control page opens.

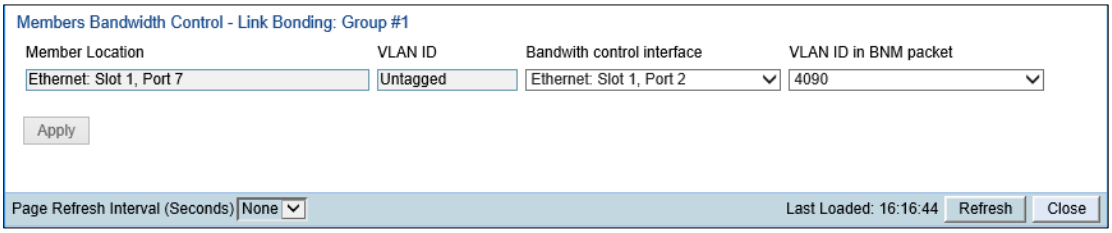


Figure 256: Link Bonding – Members Bandwidth Control Page

ii In the **Bandwidth control interface** column, make sure **Ethernet: Slot 1, Port 2** is selected.
iii In the **VLAN ID in BNM packet** column, select **VLAN ID 4090**. This is the VLAN use to transfer protocol information between the two units.

19 Configure Radio Bandwidth Notification on the paired unit by performing the following steps:

i Select **Ethernet** > **Protocols** > **Bandwidth Notification**. The Bandwidth Notification page opens.

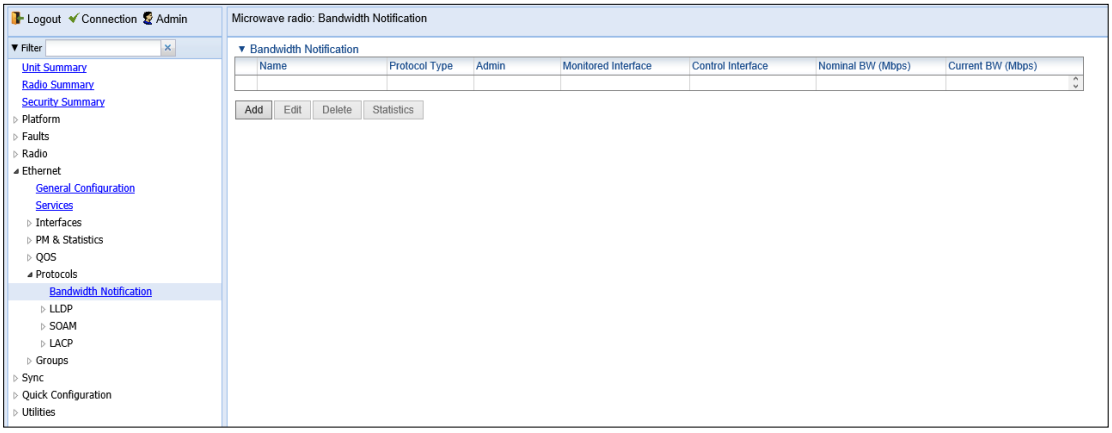


Figure 257: Bandwidth Notification Page (Empty)

ii Click **Add**. The Bandwidth Notification – Add page opens.

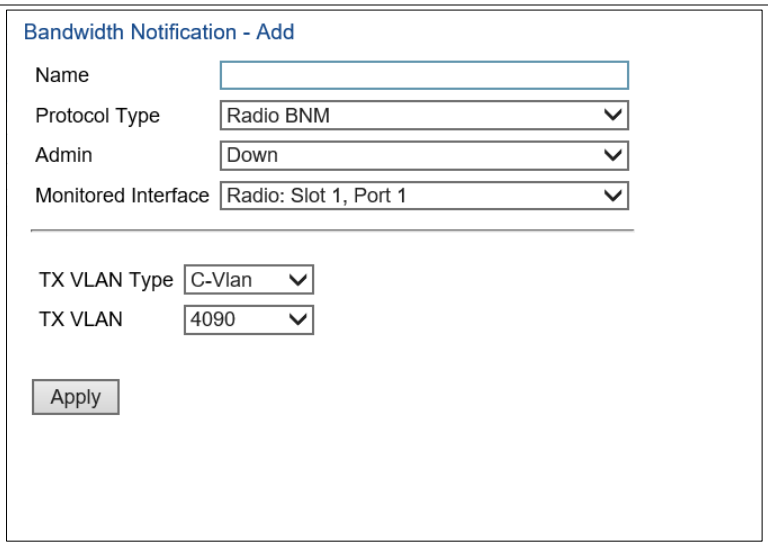


Figure 258: Bandwidth Notification – Add Page

iii In the **Name** field, select a descriptive name.
iv In the **Protocol Type** field, select **Radio BNM**.
v In the **Admin** field, select **Up**.
vi In the **Monitored Interface** field, select the paired unit's radio interface.
vii In the **TX VLAN Type** field, select **C-Vlan**.
viii In the **TX VLAN** field, select **VLAN ID 4090**.
ix Click **Apply**. The configuration is added to the Bandwidth Notification page with the Protocol Type **Radio BNM**.

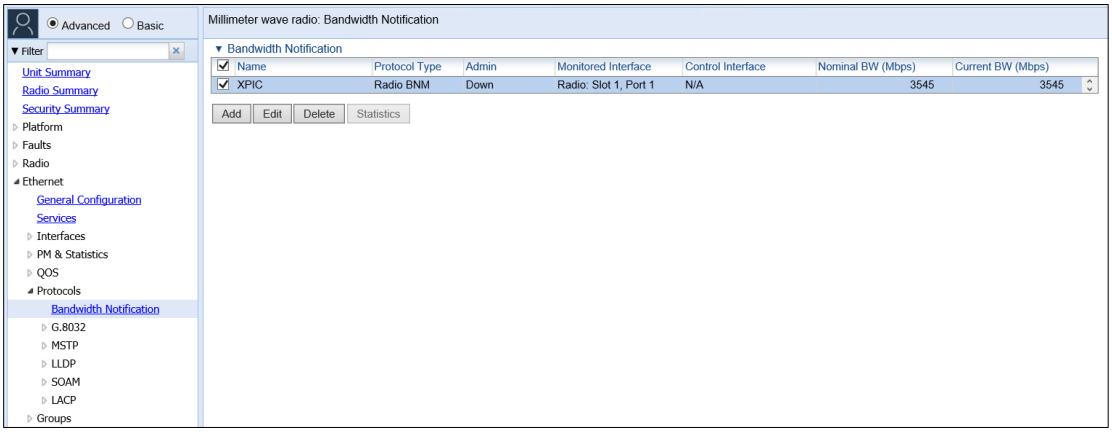


Figure 259: Bandwidth Notification Page (Populated with Radio BNM)

20 On the paired unit on both sides of the link, configure a point-to-point service for Radio Bandwidth Notification, with service points on the radio interface and Eth 2. The service points should be configured as follows:

i Create a service point on the radio interface with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: 4090
- Allow Flooding: Allow
- Learning Admin: Disable

ii Create a service point on Eth 2 with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: 4090
- Allow Flooding: Allow
- Learning Admin: Disable

See Configuring Service Points.

7.6.2.1 Configuring Synchronization in an XPIC Node with Layer 1 Link Bonding

SyncE and 1588 PTP can be used in XPIC nodes with Layer 1 Link Bonding. SyncE and 1588 PTP can be configured for both the main unit and the paired unit. Synchronization messages are passed between the units via the Protocols cable.

Configuring SyncE in an XPIC Node with Layer 1 Link Bonding

To configure SyncE on an XPIC node with Layer 1 Link Bonding:

- On the local main unit, configure the following:
  - Configure the port connected to the external switch (Eth 3) as a sync source with priority 1.
  - Configure the radio interface as a sync source with priority 2.
  - Configure Eth 2 as a sync source with priority 3.
- On the local paired unit, configure the following:
  - Configure Eth 2 as a sync source with priority 1.
  - Configure the radio interface as a sync source with priority 2.
- On the remote paired unit, configure the following:
  - Configure the radio interface as a sync source with priority 1.
  - Configure Eth 2 as a sync source with priority 2.
- On the remote main unit, configure the following:
  - Configure Eth 2 as a sync source with priority 1.
  - Configure the radio interface as a sync source with priority 2.
  - Configure the port connected to the external switch (Eth 3) as a sync source with priority 3.

All sync sources should be configured with Sync Interface Quality ”Automatic”.
For instructions on configuring SyncE,

Configuring 1588 PTP in an XPIC Node with Layer 1 Link Bonding

To use 1588 PTP on an XPIC node with Layer 1 Link Bonding, you must configure Boundary Clock on the main unit and Transparent Clock on all of the units, as described below. 1588 messages are generated by the Boundary Clock mechanism on the main unit and sent untagged to the paired unit via the Protocols cable. They receive VLAN tagging on the paired unit in order to separate them from user traffic.

Note: If the paired unit goes down, 1588 packets will not be transmitted to the other side of the link.

To configure 1588 PTP for the XPIC node with Layer 1 Link Bonding:

1 Configure SyncE following the instructions in Configuring the Sync Source.
2 Enable 1588 PTP on each unit, including the main and paired units on both sides of the link:

i Select **Sync > 1588 > General Configuration**. The 1588 – General Configuration page opens.
ii In the **1588 PTP** field, select **Enable**.
iii Click **Apply**.

3 On the main units on both sides of the link, enable Boundary clock on:

- The port connected to the external switch (Eth 3).
- Eth 2.

4 On the paired unit on both sides of the link, enable Transparent Clock on the radio interface.

5 On the paired units on both sides of the link, configure a point-to-point service with service points on the radio interface and Eth 2. The service points should be configured as follows:

- Service point on the radio interface:
  - Service Point Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation: Per customer's choice
  - Allowing Flooding: Allow
  - Learning Admin: Disable
- Service point on Eth 2:
  - Service Point Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation: Untagged
  - Allowing Flooding: Allow
  - Learning Admin: Disable

7.6.2.2 Enabling Link Bonding Throughput Enhancement for XPIC with Layer 1 Link Bonding (CLI)

After configuring a Link Bonding node, it is recommended to enable Link Bonding Throughput Enhancement. Link Bonding Throughput Enhancement is available for both the main unit and the attached unit.

Note: In configurations with PTP 820N/PTP 820A and PTP 850E, Link Bonding Throughput Enhancement can be used for the PTP 850E as attached unit. For instructions, refer to the User Guide for PTP 820N and PTP 820A, System Release 12.0.5 and higher.

Link Bonding Throughput Enhancement can be enabled on the radio interface of both the main unit and the attached unit.

Link Bonding Throughput Enhancement affects the recommended L2 Header Compensation. Make sure to use the values listed in L1 and L2 Header Compensation Values.

The Link Bonding Throughput Enhancement and L2 Header Compensation settings must be the same for the main units on both sides of the link. Therefore, the changes should be applied in the following order to ensure that management is not lost:

Note: The settings on attached units do not affect management, and can be changed in any order.

1 Enable Link Bonding Throughput Enhancement on the remote unit (main and/or attached unit) by entering the following commands:

```
root> radio slot 1 port 1
radio [1/1]> lb-throughput-enhancement set admin enable
```

2 Enable Link Bonding Throughput Enhancement on the local unit (main and/or attached unit) by entering the following commands:

```
root> radio slot 1 port 1
radio [1/1]> lb-throughput-enhancement set admin enable
```

3 Modify the L2 Header Compensation on the remote unit (main and/or attached unit) by entering the following commands:

- For the main unit, enter the following commands to modify the L2 Header Compensation for the radio interface:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface radio slot 1
port 1
lbg-member[radio1/1]> admin set disable
lbg-member[radio1/1]> l2-header-compensation edit l1-header-
compensation-enabled <yes|no> l2-header-compensation-value
<(-63)-63>
lbg-member[radio1/1]> admin set enable
```

To display the current parameter, enter the following command:

```
lbg-member[radio1/1]> l2-header-compensation show
```

- For the attached unit, enter the following commands to modify the L2 Header Compensation for the interface connected to the attached unit:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface eth slot 1 port
4
lbg-member[eth4]>admin set disable
lbg-member[eth4]> l2-header-compensation edit l1-header-compensation-
enabled <yes|no> l2-header-compensation-value <(-63)-63>
lbg-member[eth4]>admin set enable
```

To display the current parameter, enter the following command:

```
lbg-member[eth4]> l2-header-compensation show
```

Note: For recommended values, see L1 and L2 Header Compensation Values.

4 Modify the L2 Header Compensation on the local unit (main and/or attached unit) by entering the following commands:

- For the main unit, enter the following commands to modify the L2 Header Compensation for the radio interface:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface radio slot 1
port 1
lbg-member[radio1/1]> admin set disable
lbg-member[radio1/1]> l2-header-compensation edit l1-header-
compensation-enabled <yes|no> l2-header-compensation-value
<(-63)-63>
lbg-member[radio1/1]> admin set enable
```

To display the current parameter, enter the following command:

```
lbg-member[radio1/1]> l2-header-compensation show
```

- For the attached unit, enter the following commands to modify the L2 Header Compensation for the interface connected to the attached unit:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface eth slot 1 port 4
lbg-member[eth4]>admin set disable
lbg-member[eth4]> l2-header-compensation edit l1-header-compensation-enabled
<yes|no> l2-header-compensation-value <(-63)-63>
lbg-member[eth4]>admin set enable
```

To display the current parameter, enter the following command:

```
lbg-member[eth4]> l2-header-compensation show
```

Note: For recommended values, see L1 and L2 Header Compensation Values.

7.6.2.3 Editing a Link Bonding Group or its Members

To change the Group Name or the Admin Status of the Link Bonding group:

1 In the Link Bonding page, select the group and click **Edit Group**. The Edit Group page opens.

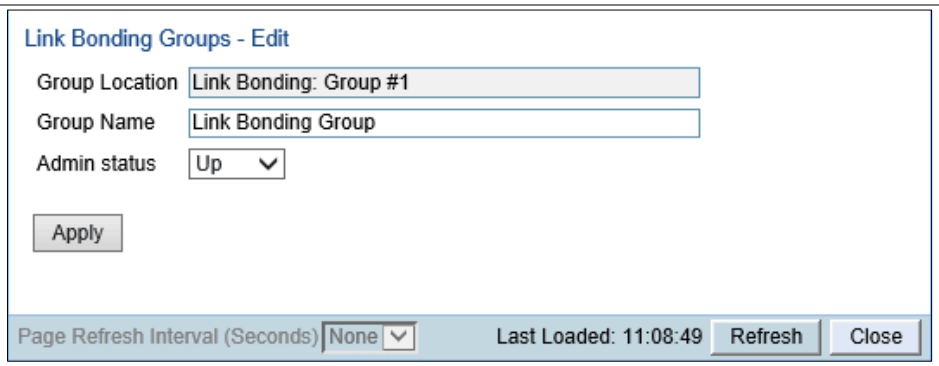


Figure 260: Link Bonding Groups – Edit Page

2 In the **Group Name** field, enter the new name.
3 In the **Admin status** field, change the Admin status of the group to **Up** or **Down**.
4 Click **Apply**.

7.6.2.4 Displaying Statistics for a Link Bonding Group

You can display the total number of segments and bytes (TX and RX) that have passed through each member of the Link Bonding group.

Note: The ability to clear member statistics is planned for future release. You can also display and configure thresholds for throughput and utilization on both the group and the member levels.

To display throughput statistics for the members of the Link Bonding group:

1 In the Link Bonding page, select the group and click **Member Statistics**. The Member Statistics page opens.

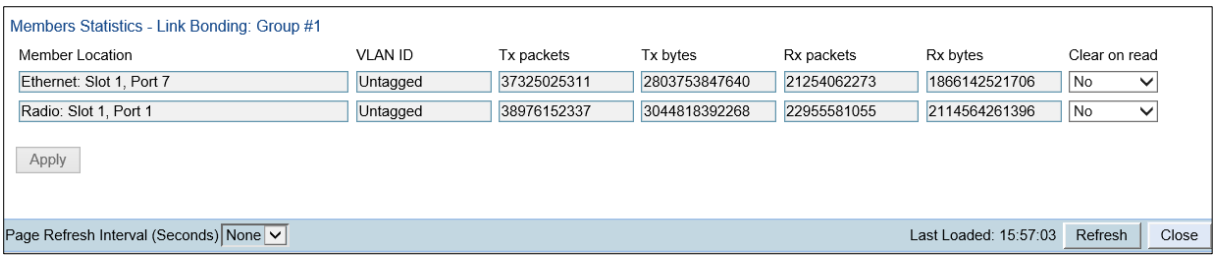


Figure 261: Link Bonding Groups – Member Statistics Page

7.6.2.5 Deleting a Link Bonding Group

To delete a Link Bonding group, you must first remove the members from the group:

1 In the Link Bonding page, select the group and click **Add/Remove Members**. The Add/Remove Members page opens.

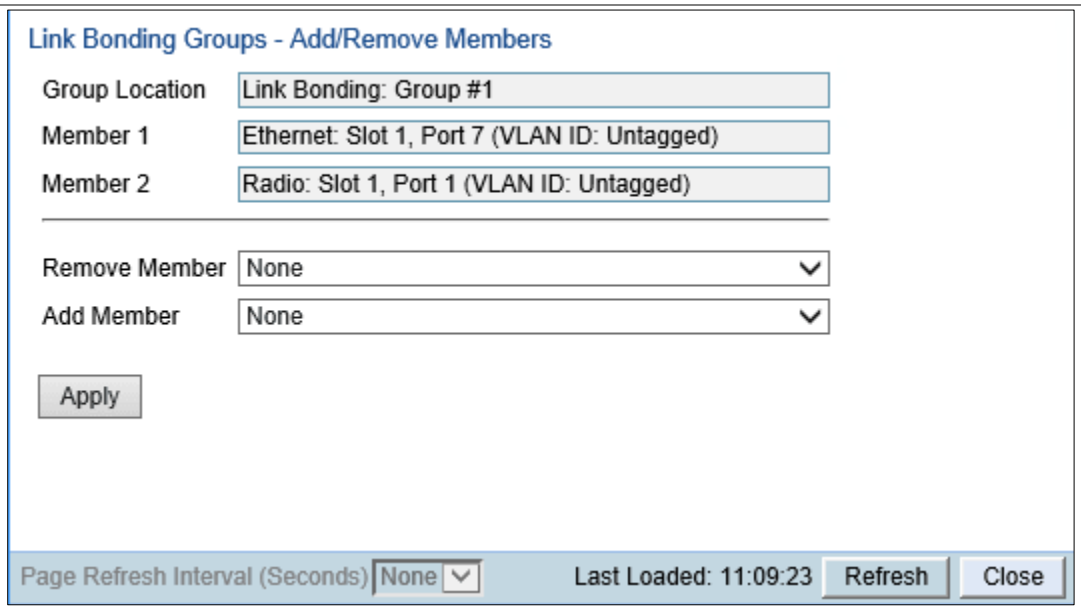


Figure 262: Link Bonding Groups – Member Statistics Page

2 In the **Remove Member** field, select each member individually and click **Apply**.
3 Remove any service points on the Link Bonding group.
4 In the Link Bonding page, select the group and click **Delete Group**.

7.6.3 Configuring the Radio Carriers

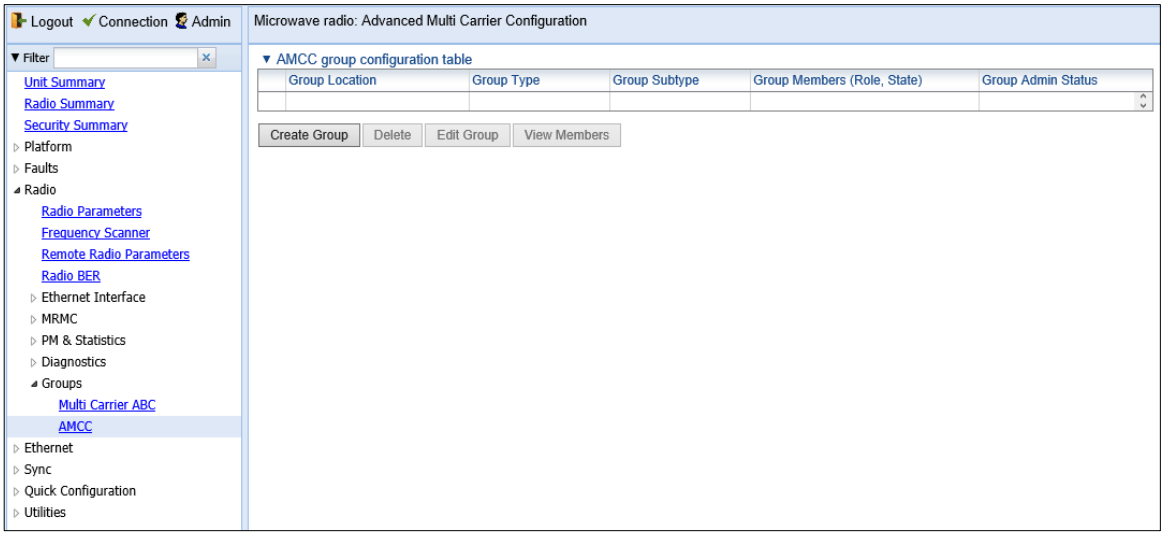
Note

You can perform the entire configuration using the 1+0 Quick Configuration wizard. See Configuring a 1+0 Link Using the Quick Configuration Wizard.

Configuring XPIC on the Radio Carriers – PTP 850C

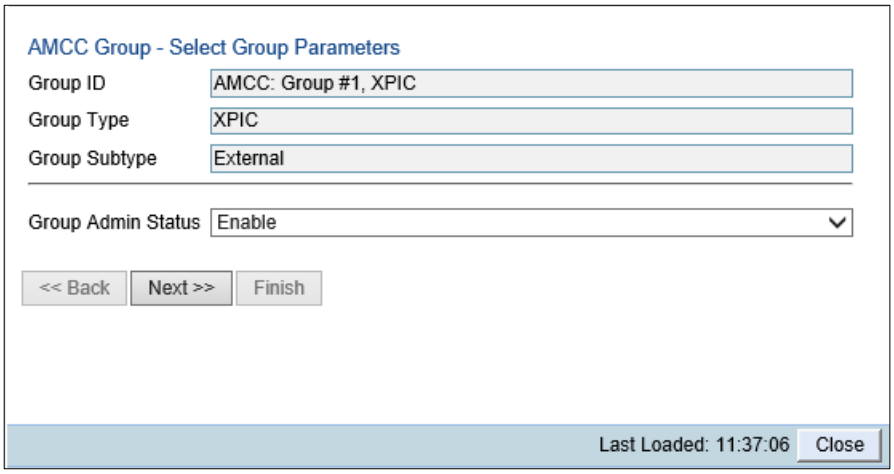
1. Configure each radio carrier unit on both sides of the link to the desired frequency channel. Both carriers must be configured to the same frequency channel.
2. Create an AMCC group .To create an AMCC group:
    a. Select **Radio > Groups > AMCC**. The Advanced Multi Carrier Configuration page opens.

Figure 263 Advanced Multi Carrier Configuration Page



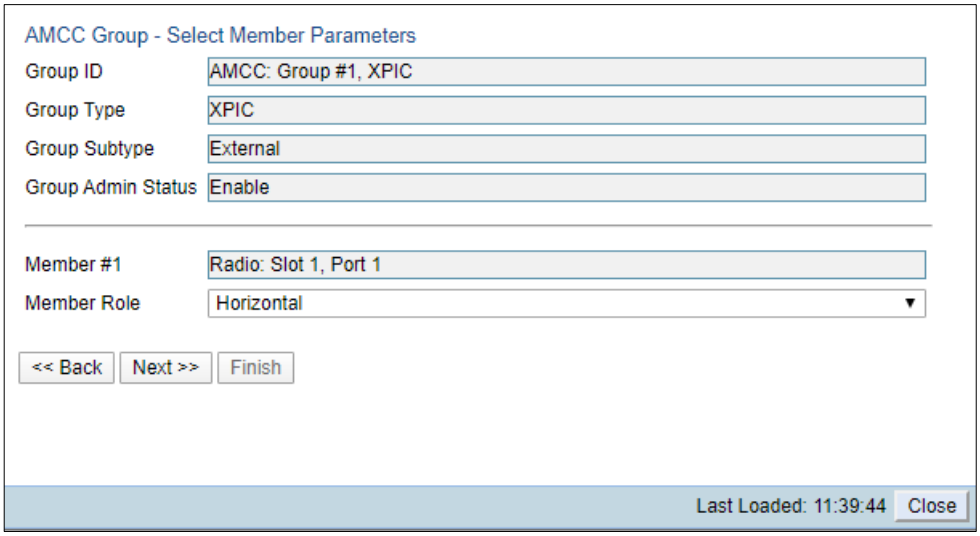
b. Click **Create Group**. The AMCC Group – Select Group Parameters page opens.

Figure 264 AMCC Group – Select Group Parameters Page



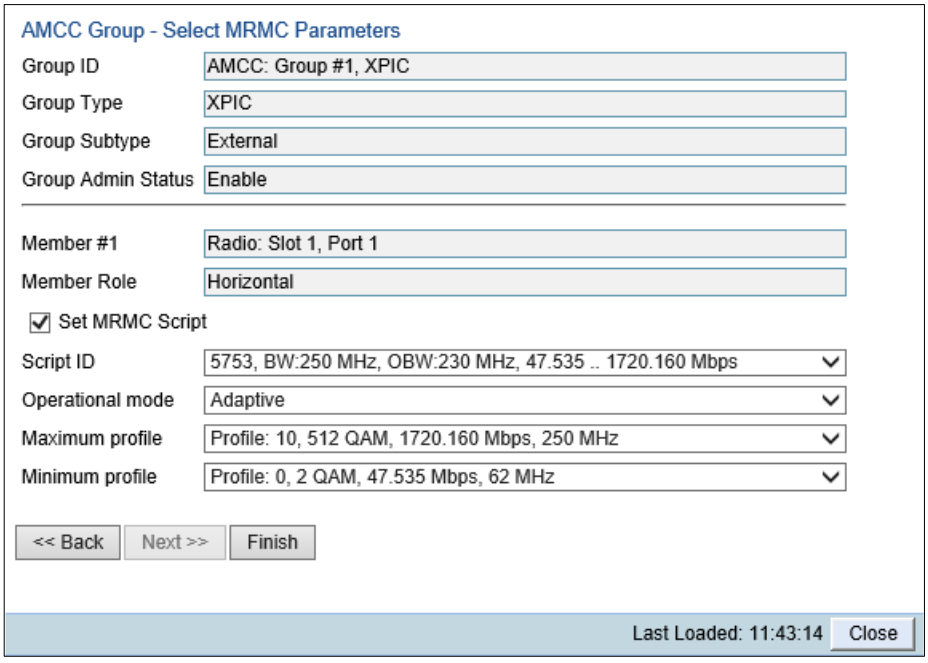
c. In the Group **Admin Status** field, select **Enable**.
d. Click **Next**. The AMCC Group – Select Member Parameters page opens.

Figure 265 AMCC Group – Select Member Parameters Page



e. In the **Member Role** field, select **Horizontal** or **Vertical**. Make sure the Member Role you select matches the actual polarization of the PTP 850E unit, and that the Member Role you configure in the paired unit is not the same as the role you configure here.
f. Click **Next**. The AMCC Group – Select MRMC Parameters page opens.

Figure 266 AMCC Group – Select MRMC Parameters Page



g. Make sure **Set MRMC Script** is selected.
h. In the **Script ID** field, select the MRMC script you want to assign to the radio. Only XPIC scripts will appear in this field. For a full explanation of choosing an MRMC script.
i. In the Operational **Mode** field, select the ACM mode: **Adaptive** or **Fixed**.

- In Adaptive ACM mode, TX and RX rates are dynamic. An ACM-enabled radio system automatically chooses which profile to use according to the channel fading conditions.
- Fixed ACM mode applies constant TX and RX rates. However, unlike regular scripts, with a Fixed ACM script you can specify a maximum profile to inhibit inefficient transmission levels.

j. Do one of the following:

- If you selected Adaptive in the Operational Mode field, the following two fields are displayed:
  - Maximum profile – Enter the maximum profile for the script.
  - Minimum profile – Enter the minimum profile for the script.



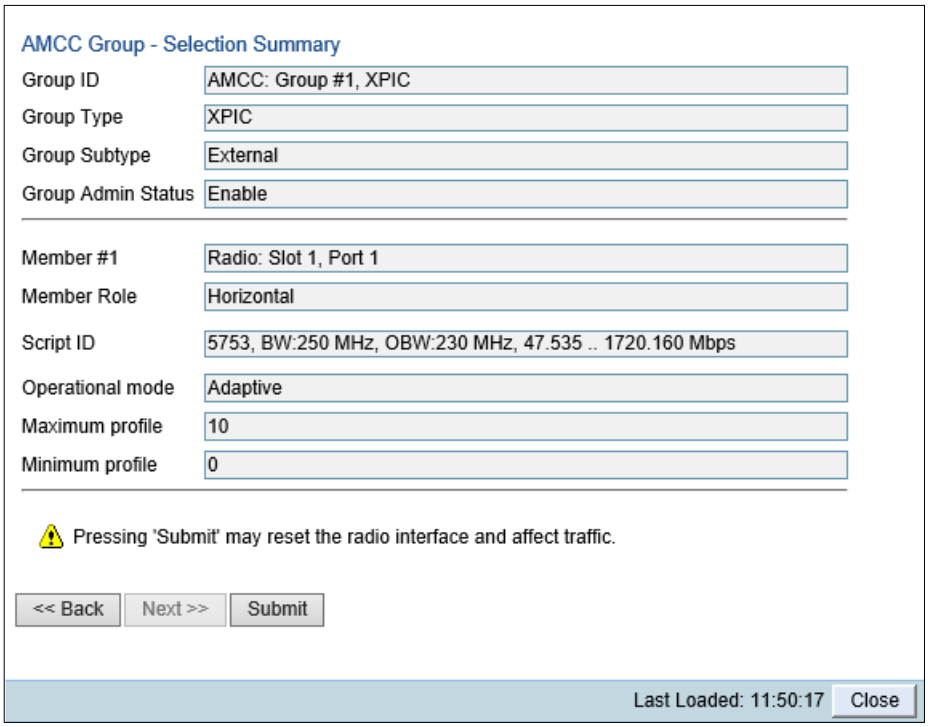
Note

The default minimum profile is 0.

- If you selected **Fixed** in the **Operational Mode** field, the next field is **Profile**. Select the ACM profile for the radio in the **Profile** field.

k. Click **Finish**. The AMCC Group – Selection Summary page opens.

Figure 267 AMCC Group – Selection Summary Page



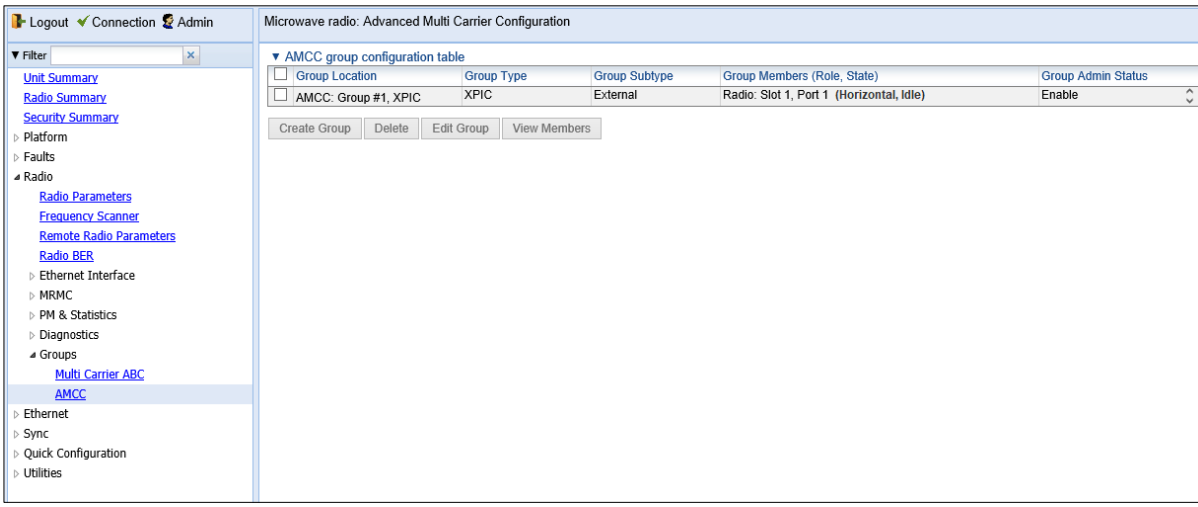
l. Review the parameters you have selected. If they are correct, click **Submit**. If you want to change any of the configurable parameters, click **Back**.

7.6.4 Deleting an AMCC (XPIC) Group

To delete an AMCC (XPIC) group:

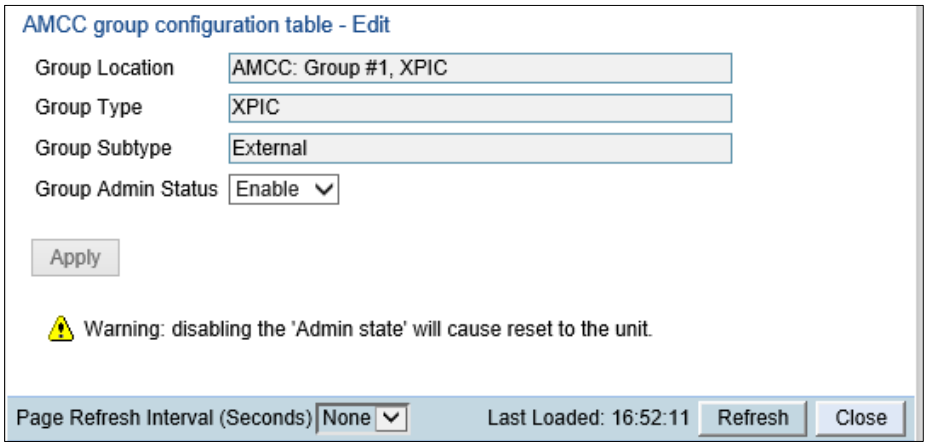
1. Select **Radio > Groups > AMCC**. The Advanced Multi Carrier Configuration page opens.

Figure 268 Advanced Multi Carrier Configuration Page (Populated)



2. Select the group and click **Edit Group**. The AMCC Group – Edit page opens.

Figure 269 AMCC Group – Edit Page



3. In the Group Admin Status field, select Disable.
4. Click Apply, then Close.
5. In the Advanced Multi Carrier Configuration page, select the group and click

Configuring XPIC on the Radio Carriers – PTP 850E

To configure the radio carriers:

1 Configure each PTP 850E unit on both sides of the link to the desired frequency channel. Both carriers must be configured to the same frequency channel. See *Configuring the Radio Parameters*.

2 Create an AMCC group for the radio carrier. You must create a group on each PTP 850E unit, even though each group consists of only one radio carrier. To create an AMCC group:

i Select **Radio > Groups > AMCC**. The Advanced Multi Carrier Configuration page opens.

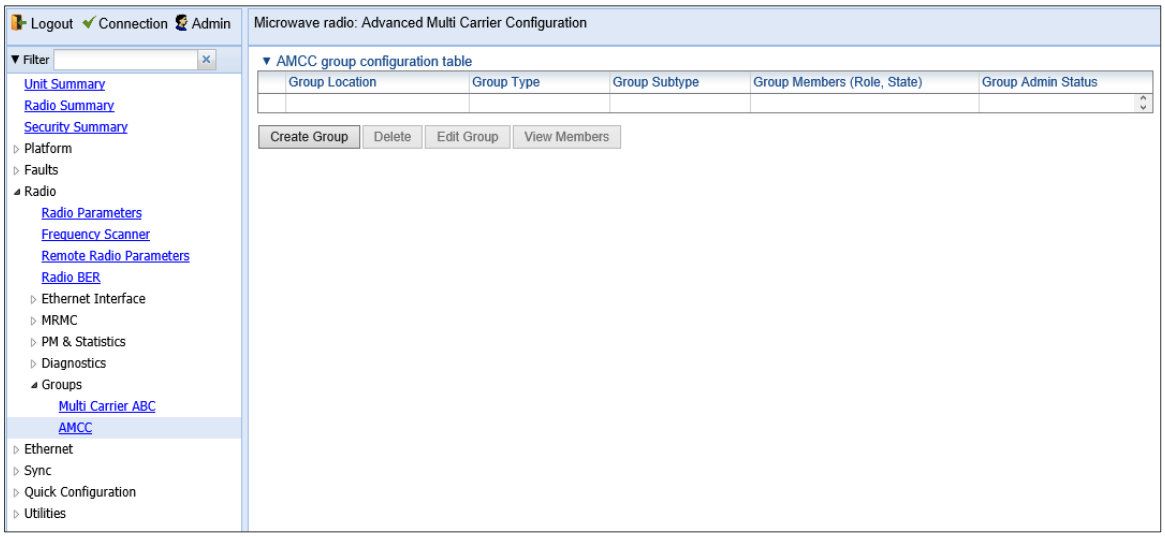


Figure 122: Advanced Multi Carrier Configuration Page

ii Click **Create Group**. The AMCC Group – Select Group Parameters page opens.

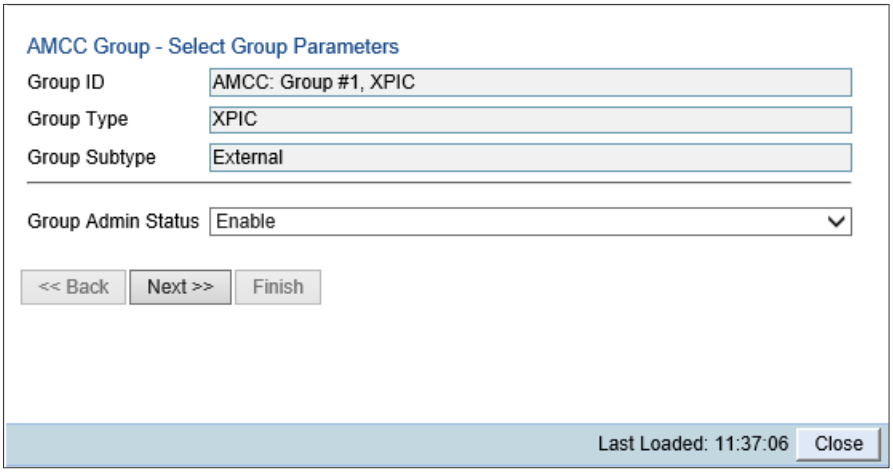


Figure 123: AMCC Group – Select Group Parameters Page

iii In the **Group Admin Status** field, select **Enable**.

iv Click **Next**. The AMCC Group – Select Member Parameters page opens.

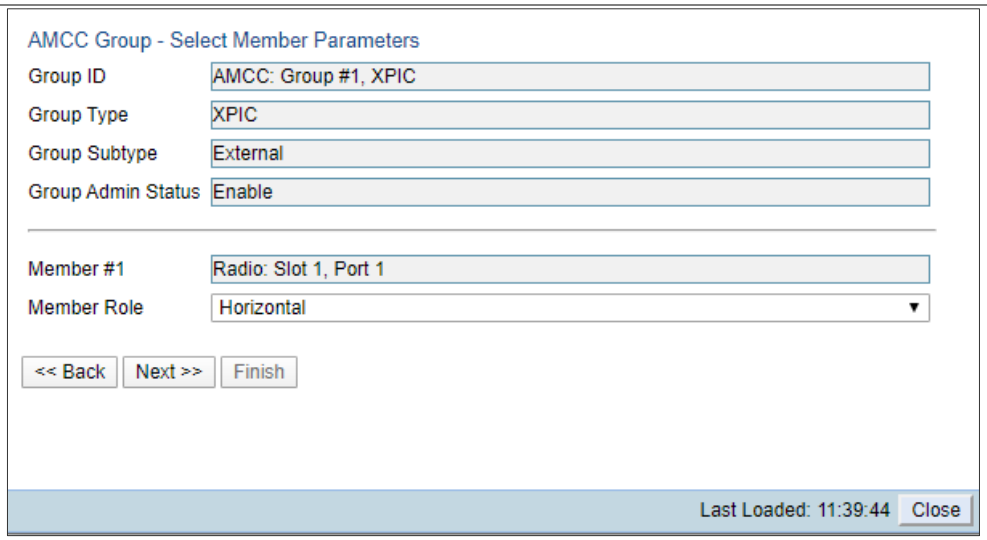


Figure 124: AMCC Group – Select Member Parameters Page

v In the Member Role field, select Horizontal or Vertical. Make sure the Member Role you select matches the actual polarization of the PTP 850E unit, and that the Member Role you configure in the paired unit is not the same as the role you configure here.

vi Click Next. The AMCC Group – Select MRMC Parameters page opens.

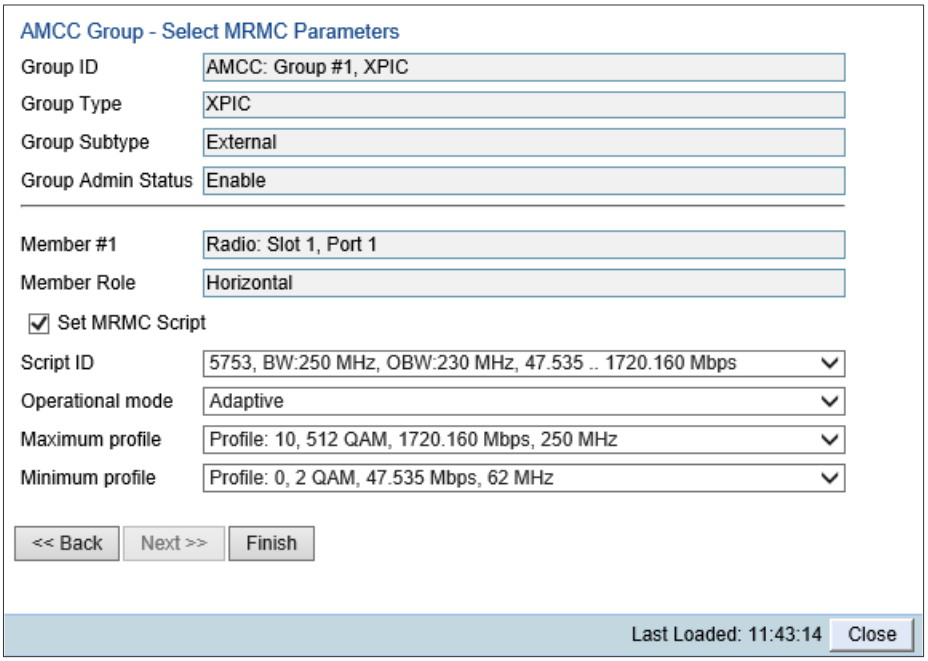


Figure 125: AMCC Group – Select MRMC Parameters Page

vii Make sure Set MRMC Script is selected.

viii In the Script ID field, select the MRMC script you want to assign to the radio. Only XPIC scripts will appear in this field. For a full explanation of choosing an MRMC script, see *Configuring the Radio (MRMC) Script(s)*.

ix In the **Operational** Mode field, select the ACM mode: Adaptive or Fixed.

- In Adaptive ACM mode, TX and RX rates are dynamic. An ACM-enabled radio system automatically chooses which profile to use according to the channel fading conditions.
- Fixed ACM mode applies constant TX and RX rates. However, unlike regular scripts, with a Fixed ACM script you can specify a maximum profile to inhibit inefficient transmission levels.

x Do one of the following:

- If you selected **Adaptive** in the **Operational Mode** field, the following two fields are displayed:
  - **Maximum profile** – Enter the maximum profile for the script. See *Configuring the Radio (MRMC) Script(s)*.
  - **Minimum profile** – Enter the minimum profile for the script. See *Configuring the Radio (MRMC) Script(s)*.
- If you selected Fixed in the Operational Mode field, the next field is Profile. Select the ACM profile for the radio in the Profile field.

xi Click Finish. The AMCC Group – Selection Summary page opens.

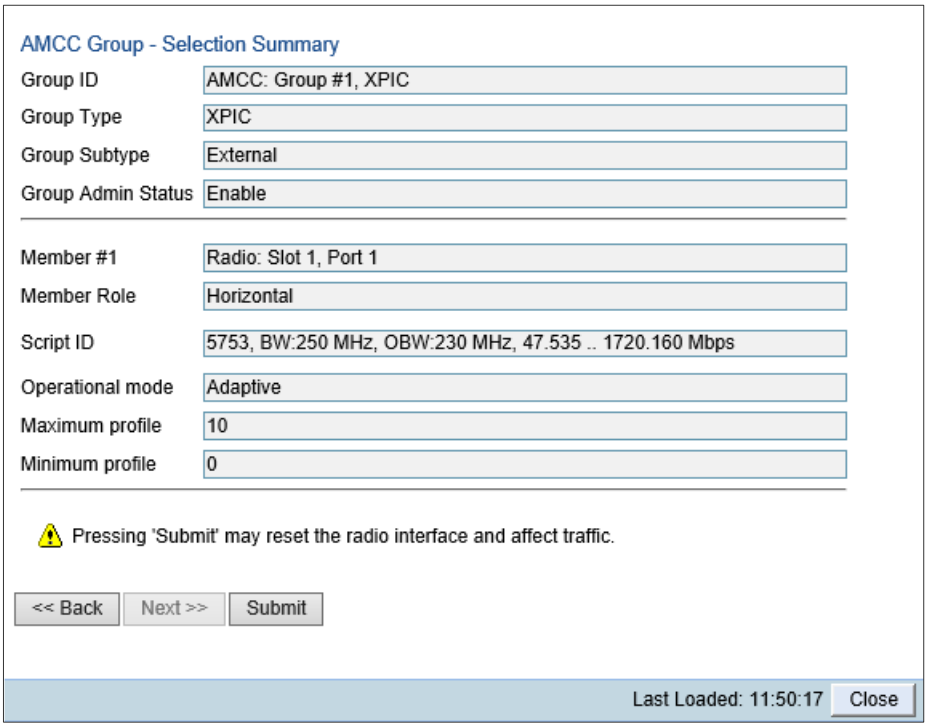


Figure 126: AMCC Group – Selection Summary Page

xii Review the parameters you have selected. If they are correct, click Submit.

If you want to change any of the configurable parameters, click Back.

7.6.5 Performing Antenna Alignment for XPIC

The antenna alignment procedure for XPIC depends on whether you are using a direct mount configuration with a single antenna and OMT or an integrated antenna configuration with two PTP 850E-integrated antenna assemblies.

7.6.5.1 XPIC Alignment for PTP 850C

1 Align the antennas for the first carrier. While you are aligning these antennas, mute the second carrier. See *Configuring the Radio Parameters*.

2 Adjust the antenna alignment until you achieve the maximum RSL for the first- carrier link (the "RSL_{wanted}"). This RSL should be no more than +/-2 dB from the expected level. Record the RSL of the first carrier as the "RSL_{wanted}").

3 Measure the RSL of the second carrier and record it as the "$RSL_{unwanted}$").

4 Determine the XPD by subtracting $RSL_{unwanted}$ from the RSL_{wanted}.

5 The XPD should be at least 25dB. If it is not, you should adjust the OMT assembly on the back of the antenna at one side of the link until you achieve the highest XPD, which should be no less than 25dB. Adjust the OMT very slowly in a right-left direction. OMT adjustment requires very fine movements and it may take several minutes to achieve the best possible XPD.

6 Unmute all the carriers and check the RSL levels of all the carriers on both sides of the link. The RSL of the horizontal carrier of the local unit should match the RSL of the vertical carrier of the remote unit, within ±2dB. The RSL of the vertical carrier of the local unit should match the RSL of the horizontal carrier of the remote unit, within ±2dB.

7 Check the XPI levels of all the carriers on both sides of the link. All the carriers should have approximately the same XPI value. Do not adjust the XPI at the remote side of the link, as this may cause the XPI at the local side of the link to deteriorate.

In some cases, the XPI might not exceed the required 25dB minimum

due to adverse atmospheric conditions. If you believe this to be the case, you can leave the configuration at the lower values, but be sure to monitor the XPI to make sure it subsequently

7.6.5.2 XPIC Alignment for PTP 850E Direct Mount Configurations

1. Make sure the antennas have been properly leveled on both sides of the link. Proper leveling is crucial in order to optimize XPIC performance.
2. Mute the horizontal unit.
3. Adjust the antenna alignment until you achieve the maximum RSL for the vertical unit (the "RSL_{wanted}"). This RSL should be no more than +/-2 dB from the expected level. Record the RSL of the first carrier as the "RSL_{wanted}").
4. Measure the RSL of the horizontal unit and record it as the "$RSL_{unwanted}$").
5. Determine the XPD by subtracting the $RSL_{unwanted}$ from the RSL_{wanted}.
6. The XPD should be at least 25dB on the vertical and horizontal units. If it is not, you should adjust the OMT assembly on the back of the antenna at one side of the link until you achieve the balance and highest XPD, which should be no less than 25dB. Adjust the OMT very slowly in a right-left direction. OMT adjustment requires very fine movements and it may take several minutes to achieve the best possible XPD.
7. Unmute all the carriers and check the RSL levels of all the carriers on both sides of the link. The RSL of the horizontal unit at the local site should match the RSL of the vertical unit at the local site, within ±2dB. The RSL of the vertical unit at the remote site should match the RSL of the horizontal unit at the remote site, within ±2dB.

7.6.5.3 XPIC Alignment for PTP 850E Integrated Antenna Configurations

1. Make sure the horizontal antenna is roughly aligned to the horizontal antenna at the other side of the link and that the vertical antenna is roughly aligned to the vertical antenna at the other side of the link.
2. Mute the horizontal unit.
3. Adjust the antenna alignment of the vertical unit until you achieve the maximum RSL for the vertical unit (the "RSL_{wanted}"). This RSL should be no more than +/-2 dB from the expected level. Record the RSL of the vertical unit as the "RSL_{wanted}"). For instructions on adjusting the antenna alignment, see the PTP 850E Installation Guide, Section 5.4, *Performing Antenna Alignment Using the Enhanced Alignment Kit.*
4. Measure the RSL of the horizontal unit and record it as the "$RSL_{unwanted}$").
5. Determine the XPD by subtracting the $RSL_{unwanted}$ from the RSL_{wanted}.

6. The XPD should be at least 25dB. If it is not, you should adjust the alignment of the horizontal unit until you achieve the highest XPD, which should be no less than 25dB.
7. Unmute all the PTP 850E units and check the RSL levels of all the units on both sides of the link. The RSL of the local horizontal unit should match the RSL of the remote vertical unit, within ±2dB. The RSL of the local vertical unit should match the RSL of the remote horizontal unit, within ±2dB.

7.6.6 XPIC Status and Troubleshooting

The XPIC status for the radio carrier is displayed in the Group Members (Role, State) column of the Advanced Multi Carrier Configuration page.

Figure 270 Advanced Multi Carrier Configuration Page (Populated) – PTP 850C

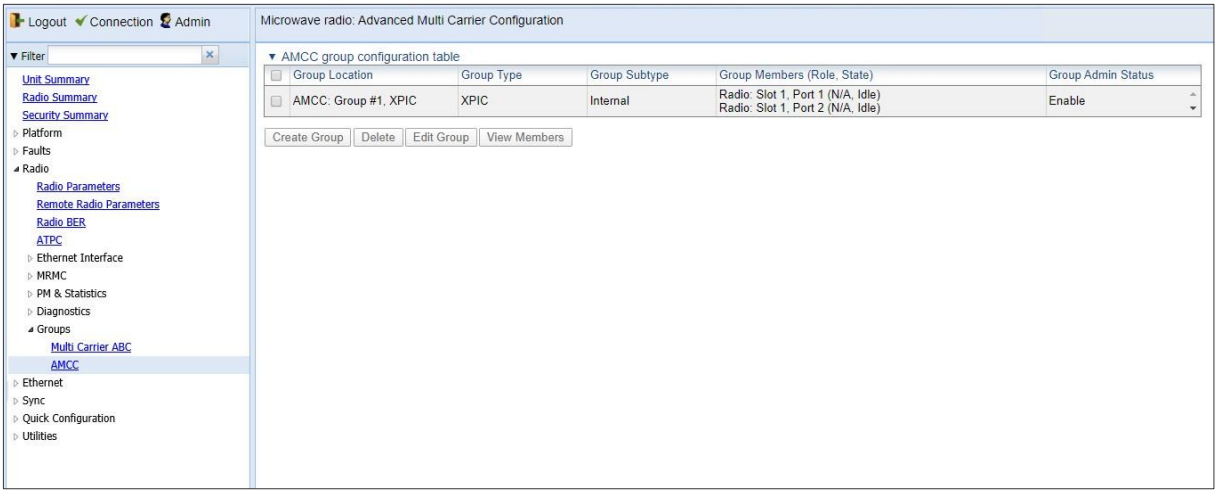
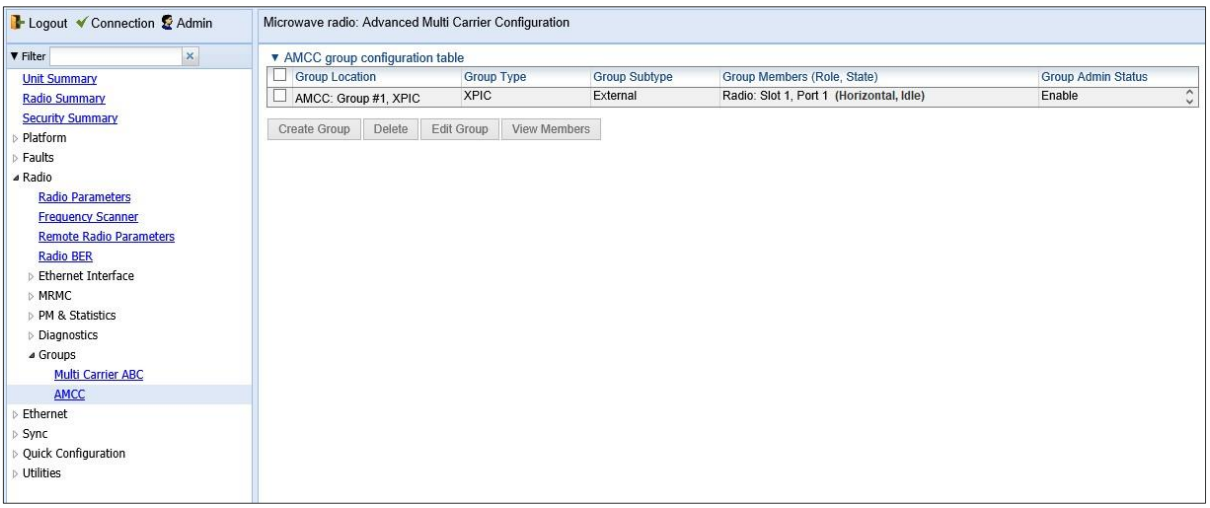


Figure 271 Advanced Multi Carrier Configuration Page (Populated) – PTP 850E



Possible statuses are:

Idle – XPIC is working properly.

INIT – Indicates that the Admin state of the radio interface is Down. Go to the Interface Manager and set the Admin status of the radio interface to Up. See Enabling the Interfaces (Interface Manager).

Configuration not supported – Indicates that the MRMC script configured for the radio carrier does not support XPIC. See Configuring the Radio Carriers.

Single Channel – Indicates one of the following:

The Clock Sharing cable is not connected to one of the units, or is defective.

The XPIC cable is not connected to one of the units, or is defective.

One of the PTP 850E units in the XPIC pair is down.

If this status appears, make sure that both units are up and check that all the cables are properly connected.

7.7 Configuring Line Redundancy for Link Bonding Configurations

For an overview of Line Redundancy with Link Bonding, see Multiband with Layer 1 Link Bonding and Line Redundancy.

Before proceeding with the instructions below, perform the basic Link Bonding configurations.

To configure Line Redundancy in a configuration with Link Bonding:

1. Verify that the port on the attached unit connected to the external switch is set to the same port speed as the port on the main unit connected to the external switch.
2. Make sure that QoS is configured on the attached unit the same as on the main unit.
3. Enable and configure line redundancy on the main units on both sides of the link:
   i. Select **Platform > Shelf Management > Line Redundancy**. The Line Redundancy page opens.

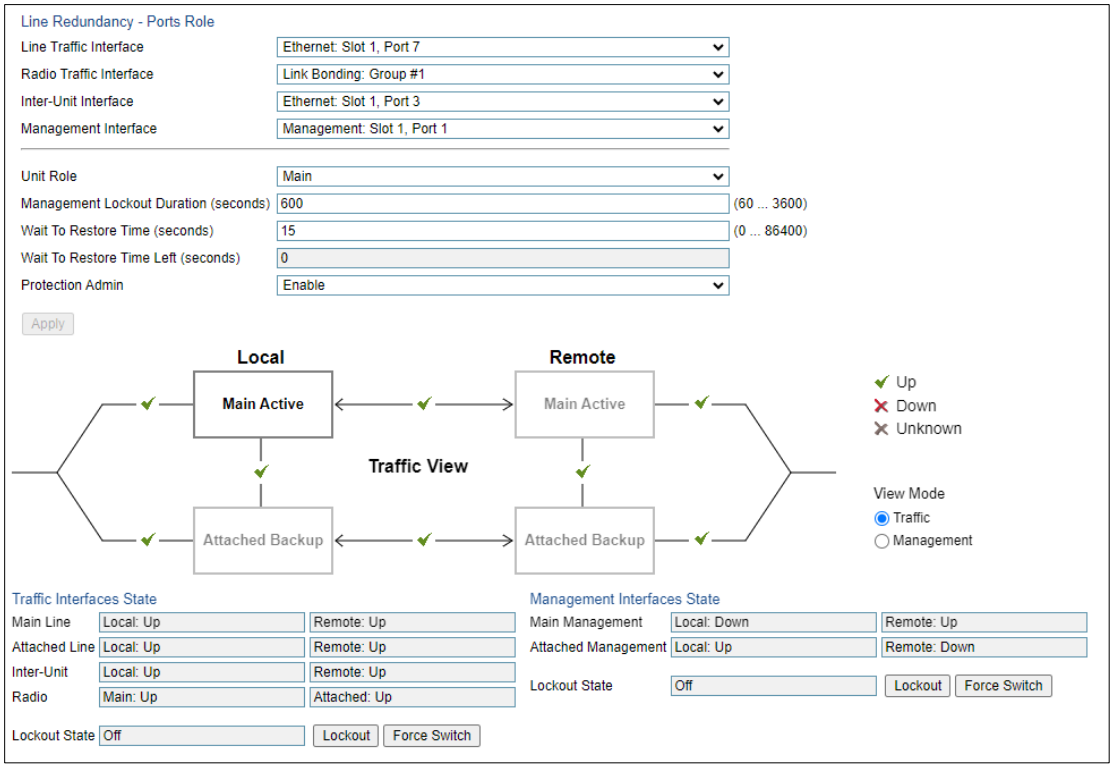


Figure 272: Line Redundancy Page (Main Unit)

ii In the **Line Traffic Interface** field, select the interface connected to the external switch.
iii In the **Radio Traffic Interface** field, select the Link Bonding group.
iv In the **Inter-Unit Interface** field, select the interface connected to the attached unit.
v In the **Management Interface** field:

- For external management redundancy, select the Management interface.
- For other configurations, leave the default value of **None**.

vi In the **Unit Role** field, select **Main**.
vii In the **Management Lockout Duration** field, enter the number of seconds that a lockout of the external management state will remain in effect after the lockout command is executed. The value range is 60-3600 seconds. The default is 600 seconds.
viii In the **Wait-to-restore time** field, enter the number of seconds to set the Revertive timer's WTR timer. When a failure condition is resolved after a switchover has taken place, the WTR timer is the time the system waits before restoring the system to its normal operational configuration. The value range is 0-84600 seconds. The default is 5 seconds.

Note: The Revertive timer only applies to traffic. Line redundancy for external management does not have a revertive timer.

ix In the **Protection Admin** field, select **Enable**.
x Click **Apply**.

Note: For an explanation of the Status parameters, see Line Redundancy with Multiband and Link Bonding – Status Parameters.

4 Enable and configure line redundancy on the attached units on both sides of the link:

i Select **Platform > Shelf Management > Line Redundancy**. The Line Redundancy page opens.

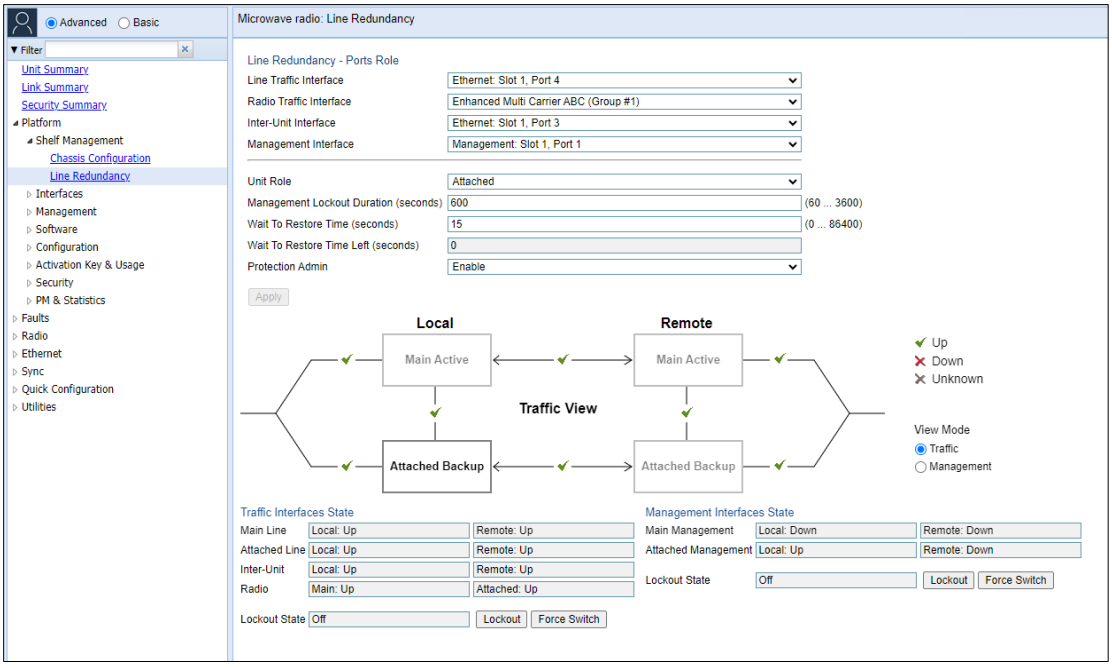


Figure 273: Line Redundancy Page (Attached Unit)

ii In the **Line Traffic Interface** field, select the interface connected to the external switch.

iii In the **Radio Traffic Interface** field, select the Multi-Carrier ABC group. If a single radio interface is being used, select the interface.
iv In the **Inter-Unit Interface** field, select the interface connected to the main unit.
v In the **Management Interface** field:

- For external management redundancy, select the Management interface.
- For other configurations, leave the default value of **None**.

vi In the **Unit Role** field, select **Attach**.
vii In the **Management Lockout Duration** field, enter the number of seconds that a lockout of the external management state will remain in effect after the lockout command is executed. The value range is 60-3600 seconds. The default is 600 seconds.
viii In the **Wait-to-restore time** field, enter the number of seconds to set the Revertive timer's WTR timer. When a failure condition is resolved after a switchover has taken place, the WTR timer is the time the system waits before restoring the system to its normal operational configuration. The value range is 0-84600 seconds. The default is 5 seconds.
ix In the **Protection Admin** field, select **Enable**.
x Click **Apply**.

5 On the attached unit on both sides of the link, create a point-to-point service for protection traffic, with service points on the port attached to the external switch and the Multi-Carrier ABC group or radio. Set the **Admin** state of the service to **Operational**. See The Ethernet Services Page.

Note: The Line Redundancy mechanism activates and deactivates these services based on the Line Redundancy operating state and role configurations, so they are not active during normal operation even though they are configured as **Operational**. They are automatically activated in case of Line Redundancy switchover.

Both service points should be configured as follows:

- Type: PIPE
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Untagged
- Allow Flooding: Allow
- Learning Admin: Disable

6 For management, add service points on the management service on the following interfaces on the attached unit:

- The interface connected to the external switch.
- The Multi-Carrier ABC group.

7 If SyncE is configured on the link, add the interface on the attached unit connected to the external switch as a Sync Source, with priority 3. See Configuring the Sync Source.

7.7.1 Line Redundancy with Link Bonding – Force-Switch and Lockout

You can configure lockout and forced switchover in the bottom of the Line Redundancy page.

To force the line redundancy for traffic to remain in its current state (lockout), click **Lockout** in the **Traffic Interfaces State** section on the lower left of the page. Lockout can be used to override Revertive mode and keep the configuration in switchover mode, should this be necessary.

To clear a Lockout, click **Clear Lockout**, which appears in place of the **Lockout** button when Lockout state has been activated.

The current lockout state is displayed in the **Lockout State** field.

To force a traffic switchover regardless of whether a failure state exists, click **Force Switch** in the **Traffic Interfaces State** section on the lower left of the page.

To prevent Revertive mode from operating to return the configuration to normal configuration, click **Lockout** after implementing the forced switchover.

Note: The Revertive timer only applies to traffic. Line redundancy for external management does not have a revertive timer.

To force line redundancy for external management to remain in its current state (lockout), click **Lockout** in the **Management Interfaces State** section on the lower right of the page. The lockout remains in effect for the time configured in the **Management Lockout Duration** field.

When management lockout is active, the **Lockout State** field displays the time remaining for the lockout. To end the lockout state, click **Clear Lockout**.

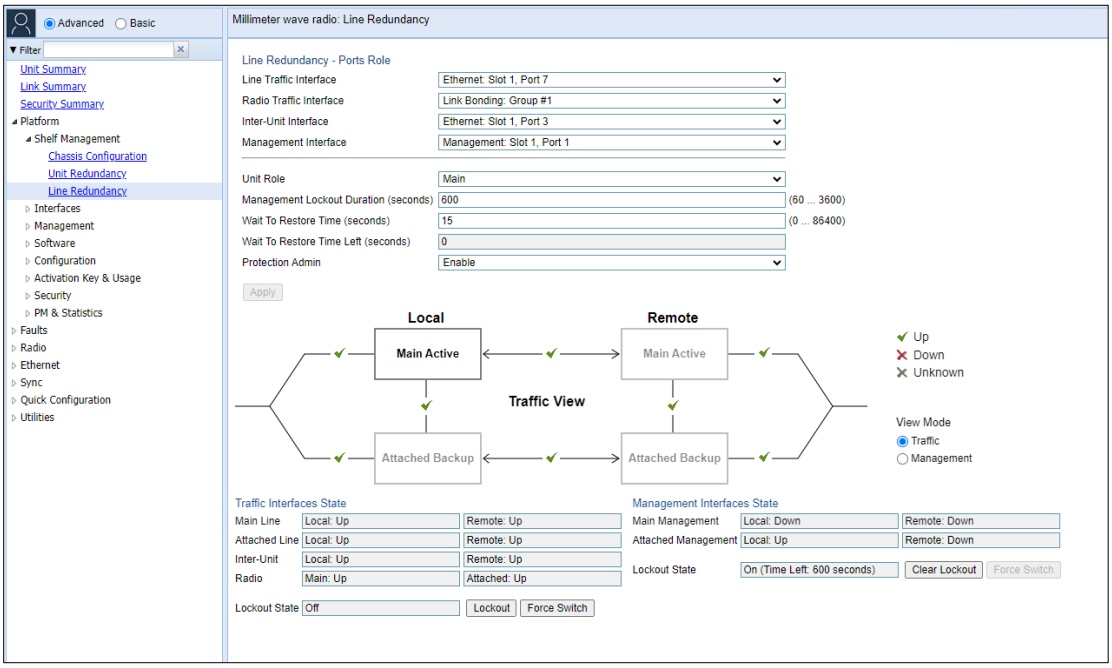


Figure 274: Line Redundancy Page (Attached Unit)

To force an external management switchover regardless of whether a failure state exists, click **Force Switch** in the **Management Interfaces State** section on the lower right of the page.

Line Redundancy with Multiband and Link Bonding –Status ParametersThe Line Redundancy page displays the status of line redundancy for both traffic and external management, in both graphic format and through status fields that display the state of the interfaces.

Status indications for traffic are available for the following interfaces:

- Main Line – The active interface attached to the external switch.
- Attached Line – The inactive (backup) interface attached to the external switch.
- Inter-Unit – The connection between the main and attached units.
- Radio The radio link.

Possible operational statuses are:

- Down – The interface is down.
- Unknown – Communication with the interface is unavailable.
- Invalid – Line redundancy is disabled on at least one of the devices. This indication is only available on the graphical display.
- Up – The specified interface is up.

Note: For management interfaces, **Down** can mean the interface is either down or in standby mode. To avoid loops, the system only allows one management interface to be active at the same time.

To display the status of external management redundancy, select **Management** in the View Mode section to the right of the graphical display.

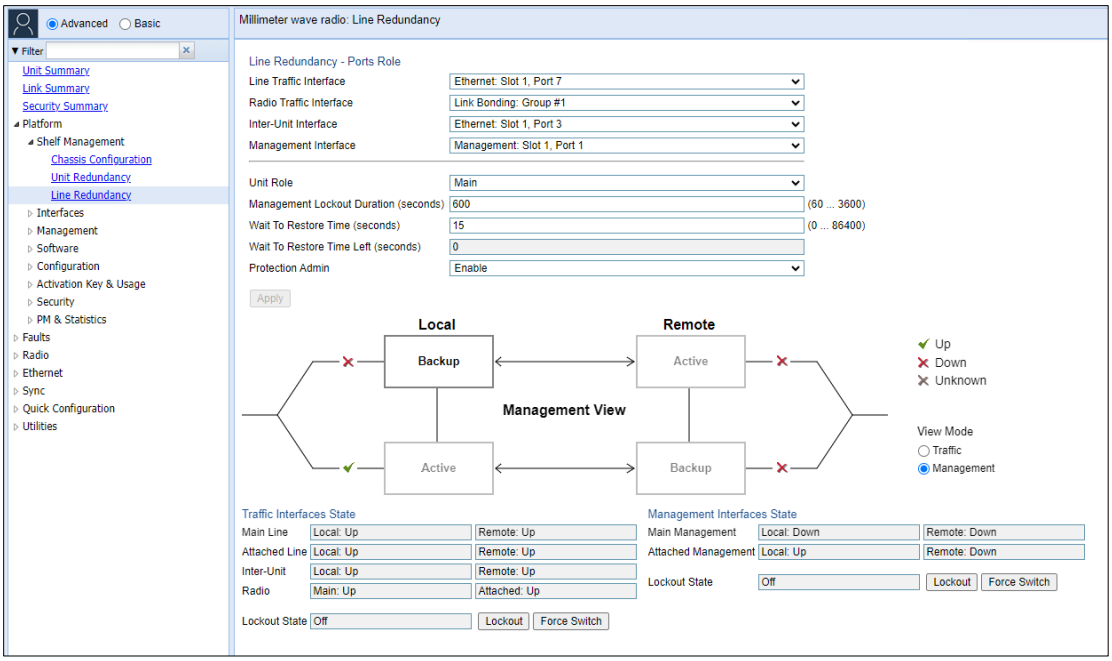


Figure 275: Line Redundancy Page – Management View Mode

7.8 Configuring Unit Redundancy

Note: This section is only relevant for PTP 850E.

This section includes:

- Unit Redundancy Overview
- Encrypting the Protection Link
- Configuring Ethernet Interface Protection
- Configuring Unit Redundancy
- Configuring Revertive Protection
- Viewing the Configuration of the Standby unit
- Editing Standby Unit Settings
- Viewing Link and Protection Status and Activity
- Manually Switching to the Standby Unit
- Disabling Automatic Switchover to the Standby Unit
- Disabling Unit Redundancy

7.8.1 Unit Redundancy Overview

Unit Redundancy utilizes two PTP 850E units connected to a single antenna via a coupler (PTP 820E-CPLR-Kit). to provide hardware redundancy for the radio link and Ethernet traffic.

One PTP 850E operates in active mode and the other operates in standby mode. Each PTP 850E monitors its own radio. If a switchover occurs, the roles are switched. The active unit goes into standby mode and the standby unit goes into active mode.

The standby unit is managed by the active unit. The standby unit's transmitter is muted, but the standby unit's receiver is kept on in order to monitor the link. However, the received signal is terminated at the switch level.

To configure Unit Redundancy, you must perform the following steps:

1 Optionally, encrypt the external protection link using IPSec.
2 Configure Ethernet interface protection.
3 Configure Unit Redundancy and HSB radio protection.

Note: For FIPS configurations, the external protection link must be encrypted using IPsec. This encrypts all IP packets that pass between the management ports of the two PTP 850E units. For instructions.

7.8.1.1 Unit Redundancy Management

PTP 850E units in a redundancy configuration must have their CPUs interconnected in order to synchronize their protection status. The same IP address is used for both PTP 850E units, to ensure that management is not lost in the event of switchover.

Note: If the units are not initially assigned the same IP address, a mismatch alarm is raised when Unit Redundancy is configured. When copy-to-mate is performed, the IP address of the active unit is copied also to the standby unit, and the alarm is cleared.

A protection cable is required to enable this connectivity. This cable connects the two PTP 850E units via their Protection ports (P6). Optionally, you can configure IPSec encryption on the Protection ports.

For local management, a splitter cable is required to connect the management ports (P2) of the two PTP 850E units and an external management station.

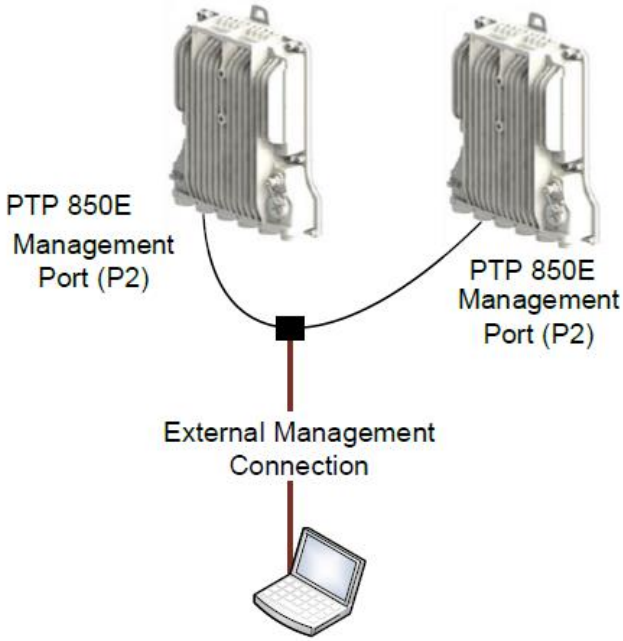


Figure 276: Management Splitter Connection

Note that in order for the splitter cable to work the management port must be set to:

- Auto Negotiation = Off
- Speed = 100 Mbps.

See Configuring Unit Redundancy, Step 2. Until you have changed the configuration of the management port, you should use a regular RJ-45 cable for management of a single unit.

The active and standby units must have the same configuration. The configuration of the active unit can be manually copied to the standby unit. Upon copying, the standby unit is reset and a temporary loss of management connection should be expected. Therefore, it is important to ensure that the units are fully and properly configured when the system is initially brought into service.

Table 24: Management Cables for Unit Redundancy

Cable	Marketing Model	Description
Protection Cable (P6 to P6)	DP2DP_EXT_CBL_XPIC_PROT	CABLE,DP TO DP,0.7M,WITH 2xM28 GLAN RES
Management Splitter Cable (P2 to P2 and External Management Station)	CBL-PTP 820-EXT-PROT+MGMT	CABLE,RJ45F 2XRJ45,1.34M 5E,WITH MAL MALE CONNECTIO

7.8.1.2 Unit Redundancy Revertive Mode

PTP 850E supports revertive HSB protection. In revertive HSB protection mode, the user defines the primary radio on each side of the link. The primary radio should be the radio on the coupler's main path and the secondary radio should be the radio on the coupling path.

The system monitors the availability of the primary path at all times. Whenever the primary path is operational and available, without any alarms, but the secondary path is active, a timer is activated. The timer is user-configurable from ten seconds to ten minutes. The default values is 60 seconds.

If the primary path remains operational and available for the period of the timer, the system initiates a revertive unit switchover. Every revertive unit switchover is recorded as an event in the event log.

Note: Each switchover causes traffic disruption.

7.8.1.3 Unit Switchover

In the event of switchover, the standby unit becomes the active unit and the active unit becomes the standby unit. Switchover takes less than 50 msec.

The following events trigger switchover for Unit Redundancy according to their priority, with the highest priority triggers listed first:

1 Force switch
2 Radio Failures (LOF, Excessive BER)
3 Line Failures
4 Manual switch

In the event that the local active unit is not powered off or its radio transmitter is malfunctioning, the remote unit sends a Change Remote message to the local standby unit, which then becomes the active unit. This is possible because the active remote unit monitors radio failures such as LOF and Excessive BER, for both itself and its mate unit. The Change Remote message is sent when both remote units encounter LOF or Excessive BER at the same time.

7.8.1.4 Unit Redundancy Configuration Overview

To configure Unit Redundancy, you must perform the following steps:

1 Optionally, encrypt the external protection link using IPSec.
2 Configure Ethernet interface protection.
3 Configure Unit Redundancy.
4 Optionally, you can configure revertive protection to ensure that the primary path is used whenever possible.

7.8.2 Configuring Ethernet Interface Protection

The Ethernet interfaces can be protected in either of two ways:

- **Split Protection Mode** – For Port 5 (SFP+, Eth 7), an optical splitter is used to route traffic to Port 5 on each PTP 850E unit. For Port 4 (QSFP, Eth 3-6), an optical splitter is used with MPO-MPO cables to route traffic to the QSFP splitter for each PTP 850E unit.

  Note: For the QSFP port, Split Protection mode can only be used for 4x1/10Gbps configurations, not 1x40Gbps configurations. Support for Split Protection mode with 1x40Gbps is planned for future release.

- **Line Protection Mode** – Traffic is routed from two Ethernet ports on the external switch to a port on the active PTP 850E unit and a port on the standby PTP 850E unit. LACP protocol is used to determine which PTP 850E port is active and which port is standby, and traffic is only forwarded to the active port. Line Protection mode can be used with all PTP 850E Ethernet ports supported for traffic.

  Notes: Line Protection mode is planned for future release.
  For Line Protection mode, the external switch must support LACP.

7.8.2.1 Configuring Split Ethernet Interface Protection Mode (CLI)

To configure split Ethernet interface protection mode:

1. For each Ethernet link, use an optical splitter to route traffic between the Ethernet port on the external switch and an Ethernet port on each PTP 850E unit or each QSFP splitter.
2. Proceed to Configuring Unit Redundancy.

7.8.2.2 Configuring Line Protection Mode

To configure line protection mode:

1. Configure the Ethernet ports on the external switch in LACP mode. The external switch must support LACP.

   Note: PTP 850 supports a special LACP implementation for purposes of line protection only. This LACP implementation is configured on the logical interface level, as described below. Regular LACP is configured as part of the LAG configuration, and is not supported with unit redundancy.

2. For each Ethernet link, connect one port on the external switch to an Ethernet port on the active PTP 850E (or QSFP splitter), and the other port on the external switch to an Ethernet port on the standby PTP 850E (or QSFP splitter).
3. Enable LACP on the Ethernet interface connected to the external switch on the active PTP 850E:

   i Select **Ethernet** > **Interfaces** > **Logical Interfaces**. The Logical Interfaces page opens.
   ii Select the interface and click **Edit**. The Logical Interfaces – Edit page opens.

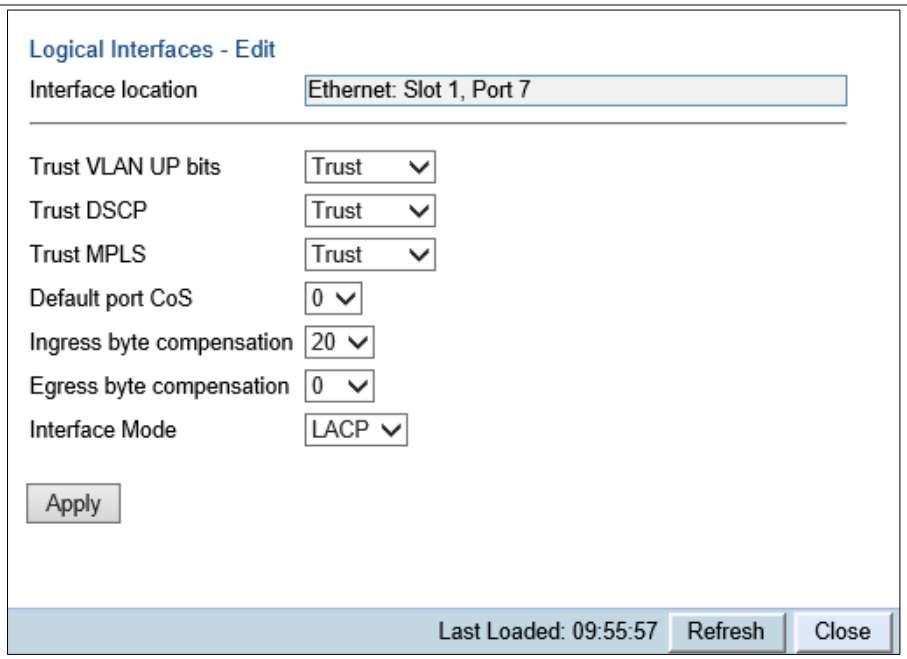


Figure 277: Logical Interfaces – Edit Page

iii In the **Interface Mode** field, select **LACP**.
iv Click **Apply**, then **Close**.

7.8.3 Configuring Unit Redundancy

To configure Unit Redundancy:

1 Before enabling Unit Redundancy, you must:

   i Verify that both units have the same hardware part number and the same software version. If the units do not have the same software version, upgrade each unit to the most recent software release.
   ii Assign an IP address to each unit. For instructions.
   iii Establish a management connection to one of the units. You can select either unit; once you enable Protection Administration, the system will determine which unit becomes the Active unit.

2 Before enabling Unit Redundancy, you must set the Management port to 100 Mbps and Auto Negotiation = Off. This should be done before connecting the management splitter cable (CBL-PTP 820-EXT-PROT+MGMT), since the cable will not work while the management port is set to its default settings of Auto Negotiation = On and Port Speed = 1000 Mbps.
In Advanced mode, select **Platform > Interfaces > Management**. The Management Interface Configuration page opens.

Note: Alternatively, in Basic mode, select **Interfaces > Interface Manager**, select the Management port, and click **Physical Interface**.

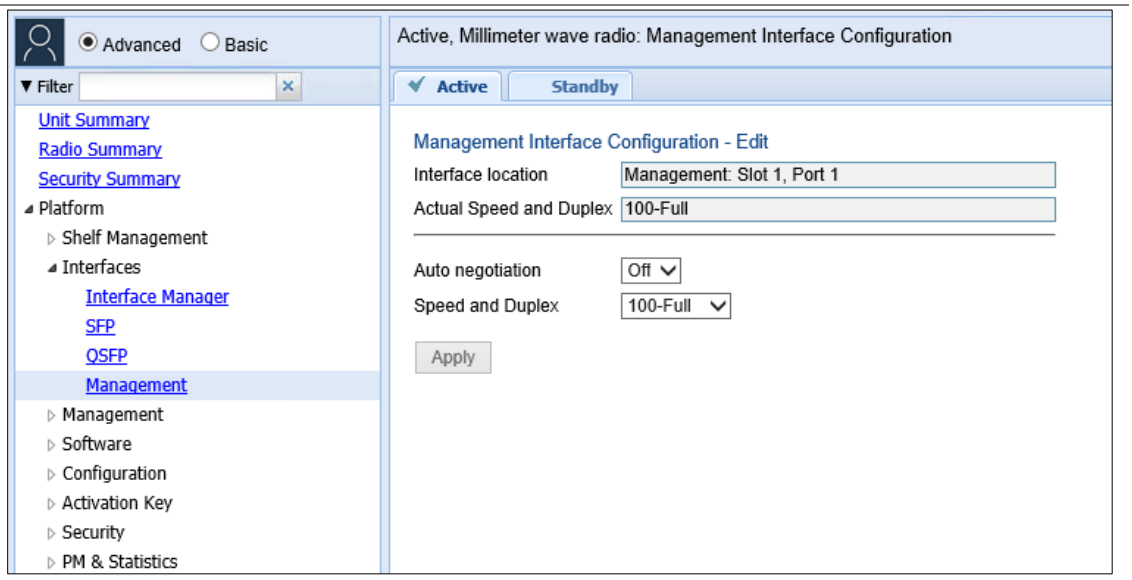


Figure 278: Management Interface Configuration Page

In the **Auto negotiation** field, select **Off**.
In the Speed and Duplex field, select 100-Full.
Click **Apply**.

Note: In Basic mode, you can configure the Management port from the Interface Manager page.

Note that if at any time you disable Unit Redundancy and wish to change the settings of the management port, you should do so only after changing the management cable to a regular RJ-45 cable.

3 Select **Platform > Shelf Management > Unit Redundancy**. The Unit Redundancy page opens.

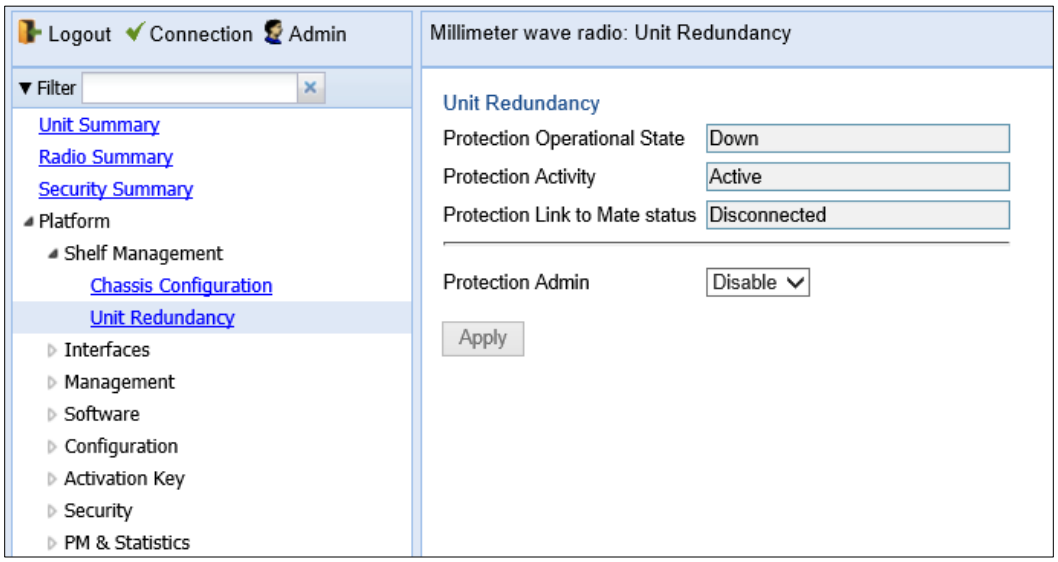


Figure 279: Unit Redundancy Page

4 In the **Protection Admin** field, select **Enable**.
5 Click **Apply**.

The system configures itself for Unit Redundancy:

- The system determines which unit is the Active unit based on a number of pre-defined criteria.
- When the system returns online, all management must be performed via the Active unit using the IP address you defined for that unit.
- The IP address you defined for the unit which is now the Standby unit is no longer valid, and the management port of the Standby unit becomes non-operational.
- Management of the Standby unit is performed via the Active unit, via the cable between the two Protection ports connecting the two units.
- Unit Redundancy is enabled on both units.
- The Unit Redundancy page refreshes to include additional fields.

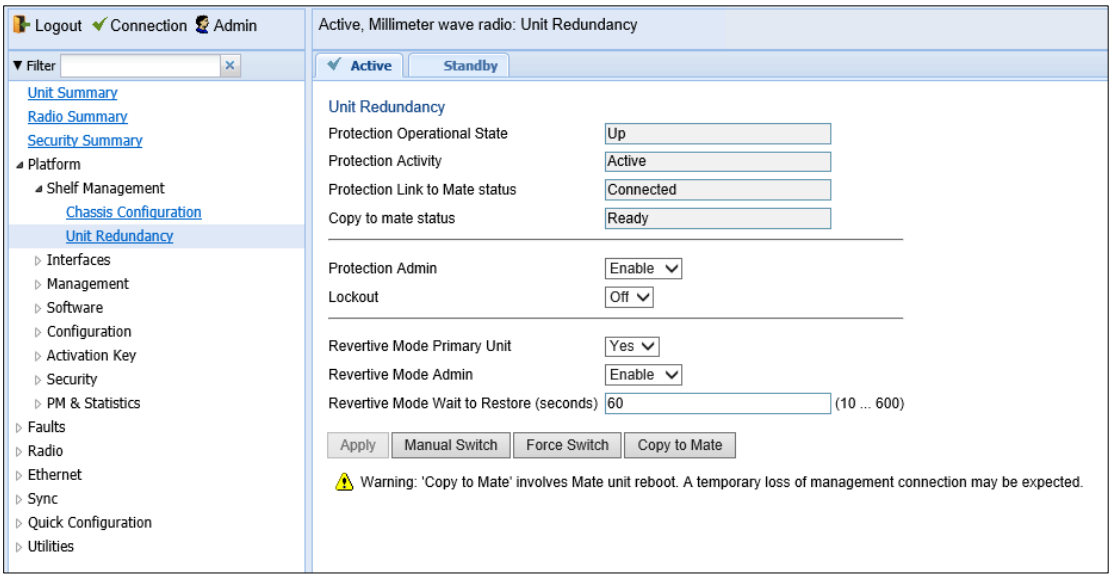


Figure 280: Unit Redundancy Page when Redundancy Enabled

In additional, almost every Web EMS page will now include two tabs on top of the main section of the page:

- **Active** – Enables you to configure the Active unit.
- **Standby** – In most cases, this tab is read-only and enables you to display Standby unit parameters. Even when a switchover occurs, the unit displayed in the Web EMS is always the currently Active unit.

Note: The parameters that are editable on the **Standby** tab are described in Editing Standby Unit Settings.

6 Once you have enabled Unit Redundancy:

i Perform all necessary radio configurations on the Active unit, such as setting the frequency, assigning MRMC scripts, and unmuting the radio.

ii Perform all necessary Ethernet configurations on the Active unit, such as defining Ethernet services.

iii In the Unit Redundancy page, click **Copy to Mate** to copy the configuration of the Active unit to the Standby unit. Confirm the action in the confirmation window that appears.

Note: While the system is performing the copy-to-mate operation, a temporary loss of management connection will occur.

To keep the Standby unit up-to-date, after any change to the configuration of the Active unit click **Copy to Mate** to copy the configuration to the Standby unit.

If you change the configuration of the Active unit but do not perform **Copy to Mate**, a Configuration Mismatch alarm appears in the **Faults** > **Current Alarms** page.

Note: You can use the following CLI command to display a list of mismatched parameters:

```
root> platform management protection show
mismatch details
```

User profiles and user accounts are copied to the Standby unit dynamically, without the need to perform a Copy-to-Mate operation. This includes both new user profiles and user accounts and changes to existing user profiles and user accounts.

Note that it may take up to a minute for new user profile or user account and changes to existing user profiles and accounts to be copied to the Standby unit. Therefore, if an unexpected switchover takes place less than one minute after adding or modifying a user profile or account:

- Check that the user profile or account is configured in the new Active unit. If it is not, reconfigure the user profile or account and make sure at least one minute passes before another switchover occurs.
- If the user profile or account is configured in the new Active unit, check that you can successfully log into the unit with that user. If you cannot, delete the user profile or account and re-configure it in the new Active unit.

7.8.4 Configuring Revertive Protection

To configure revertive mode:

1. Select **Platform** > **Shelf Management** > **Unit Redundancy**. The Unit Redundancy page opens.
2. In the **Revertive Mode Primary Unit** field:
    - To set the Active unit as the primary unit, click **Yes** in the screen for the Active unit and click **Apply**, then click **No** in the screen for the Standby unit and click **Apply**.
    - To set the Standby unit as the primary unit, click **No** in the screen for the Active unit and click **Apply**, then click **Yes** in the screen for the Standby unit and click **Apply**.
3. In the **Revertive Mode Admin** field, select **Enable** to enable revertive protection or **Disable** to disable revertive protection.
4. In the **Revertive Mode Wait to Restore** field, configure the timer (in seconds). The range of values is 10 to 600 seconds. The default values is 60 seconds.
5. Click **Apply**.

7.8.5 Viewing the Configuration of the Standby unit

You can view the settings of the standby unit any time.

To view the settings of the standby unit, click the **Standby** tab of the desired page. The following is an example of the **Standby** tab of the Radio Parameters page after **Protection Admin** has been enabled.

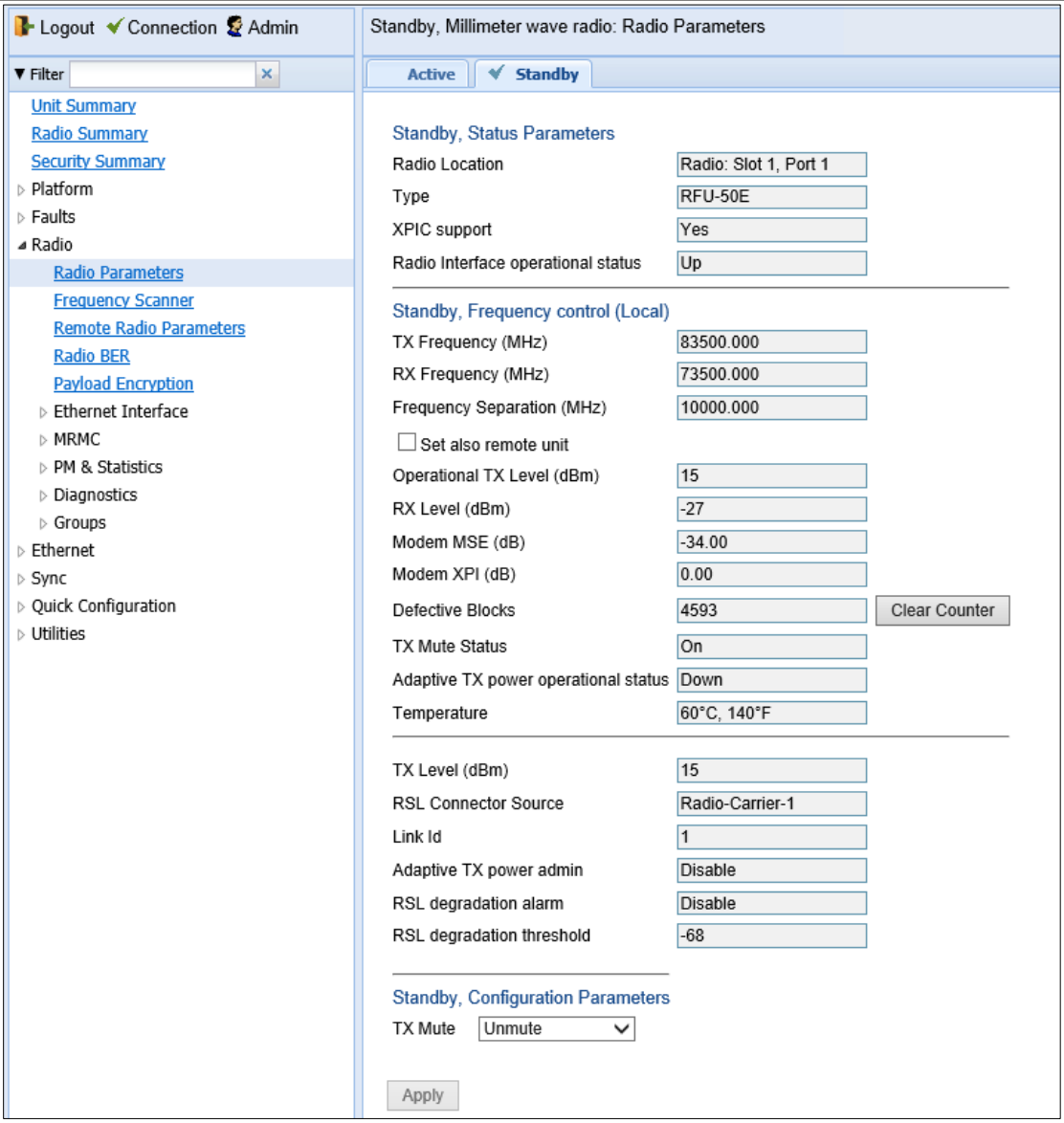


Figure 281: Standby Tab of Radio Parameters Page

7.8.6 Editing Standby Unit Settings

Almost all settings of the standby unit are view-only. However, several settings are editable on the Standby unit. They must be configured separately for the Standby unit, and are not copied via copy-to-mate, nor do they trigger a configuration mismatch in the CLI.

In the Web EMS, failure to synchronize these configuration settings causes a configuration mismatch alarm.

The following settings must be configured separately on the standby unit:

- Revertive Mode – If Revertive Mode is enabled, you must set the **Revertive Mode Primary Unit** field in the standby unit to the opposite setting as the active unit.
- Setting the Unit Name – in the **Name** field of the Unit Parameters page.
- Disabling/enabling Radio TX-mute – in the **TX mute** field of the Edit Radio Parameters page.

- Clearing the Radio and RMON counters – in the **Clear Counter** field of the Counters page.
- Setting the activation key configuration
- Defining user accounts
- Setting synchronization settings

7.8.7 Viewing Link and Protection Status and Activity

You can view link and protection status and activity any time.

To view link and protection status and activity:

1 Select **Platform > Shelf Management > Unit Redundancy**. The Unit Redundancy page opens.

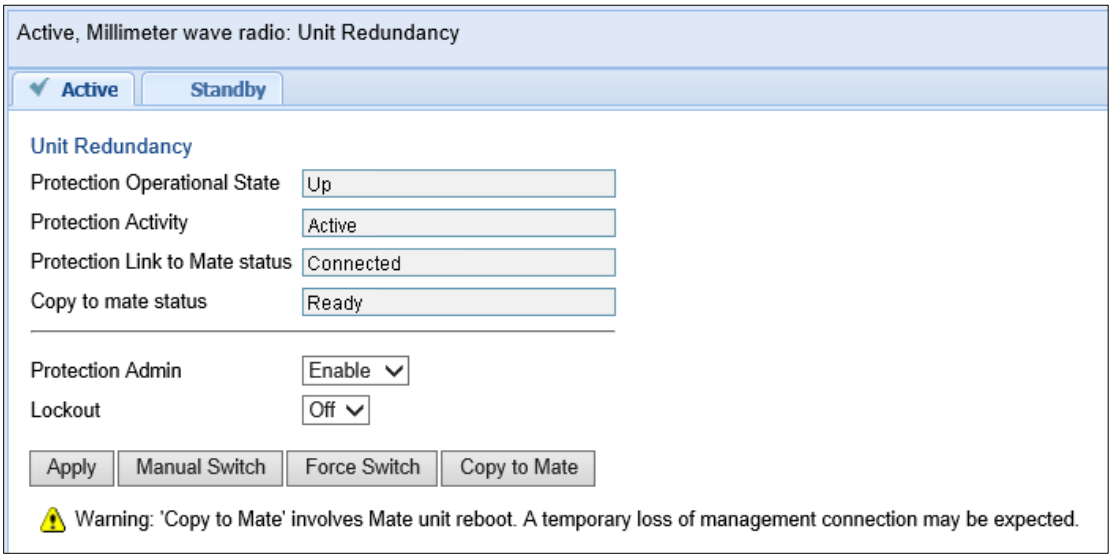


Figure 282: Unit Redundancy Page

The following information is displayed:

- **Protection Operational State** – Indicates whether Unit Redundancy is functional (available in practice). Unit Redundancy is not functional if any of the following occurred:
  - The management connection to the mate is down.
- **Protection Activity** – The activity state of the device: Active or Standby.
- **Protection Link to Mate Status** – Indicates whether the two units (the Active and the Standby) are physically connected.
- **Copy to mate status** – Indicates the status of the last copy-to-mate operation
- **Protection Admin –** Indicates whether Unit Redundancy is enabled or disabled.
- **Lockout –** Indicates whether lockout is enabled (**On**) or disabled (**Off**).

7.8.8 Manually Switching to the Standby Unit

At any point, you can manually switch to the Standby unit, provided that the highest protection fault level in the Standby unit is no higher than the highest protection fault level on the Active unit.

To manually switchover to the Standby unit:

1 Select **Platform > Management > Unit Redundancy**. The Unit Redundancy page opens.
2 Click **Manual Switch**.
3 Confirm the action in the confirmation window that appears.

7.8.9 Disabling Automatic Switchover to the Standby Unit

At any point, you can perform lockout, which disables automatic switchover to the standby unit.

To disable automatic switchover to the Standby unit:

1 Select **Platform > Shelf Management > Unit Redundancy**. The Unit Redundancy page opens.
2 Select **On** in the **Lockout** field.
3 Click **Apply**.

To re-enable automatic switchover, select **Off** in the **Lockout** field and then click **Apply**.

7.8.10 Disabling Unit Redundancy

You can disable Unit Redundancy at any time. If you disable Unit Redundancy, on the active unit, the standby unit retains its IP address and remains in standby mode, with its radio muted. To restore the standby unit to normal operation as a standalone unit, reboot the unit. When the unit comes back up, it will no longer be in standby mode, and the radio will no longer be muted. The unit will retain all its other configuration parameters, including its IP address.

To disable Unit Redundancy:

1 Select **Platform > Shelf Management > Unit Redundancy**. The Unit Redundancy page opens.
2 Select **Disable** in the **Protection Admin** field.
3 Click **Apply**.

Configuring Link Aggregation (LAG) and LACP

Note: This section is only relevant for PTP 850S.

Link aggregation (LAG) enables you to group several physical Ethernet or radio interfaces into a single logical interface bound to a single MAC address. This logical interface is known as a LAG group. Traffic sent to the interfaces in a LAG group is distributed by means of a load balancing mechanism. PTP 850S uses a distribution function of up to Layer 4 in order to generate the most efficient distribution among the LAG physical ports.

This section explains how to configure LAG and includes the following topics:

- LAG Overview
- Configuring a LAG Group
- Enabling and Disabling LAG Group Shutdown in Case of Degradation Event
- Configuring Enhanced LAG Distribution
- Deleting a LAG Group
- Displaying LACP Parameters and Statistics

LAG Overview

LAG can be used to provide redundancy for Ethernet interfaces, both on the same PTP 850S unit (line protection) and on separate units (line protection and equipment protection). LAGs can also be used to provide redundancy for radio links.

LAG can also be used to aggregate several interfaces in order to create a wider (aggregate) link. For example, LAG can be used to create a 4 Gbps channel.

You can create up to four LAG groups. The following restrictions exist with respect to LAG groups:

- Only physical interfaces (including radio interfaces), not logical interfaces, can belong to a LAG group.
- Interfaces can only be added to the LAG group if no services or service points are attached to the interface.
- Any classification rules defined for the interface are overridden by the classification rules defined for the LAG group.
- When removing an interface from a LAG group, the removed interface is assigned the default interface values.

There are no restrictions on the number of interfaces that can be included in a LAG. It is recommended, but not required, that each interface in the LAG have the same parameters (e.g., speed, duplex mode).

The LAG page lists all LAG groups configured on the unit.



Note

To add or remove an Ethernet interface to a LAG group, the interface must be in an administrative state of “down”. This restriction does not apply to radio interfaces. For instructions on setting the administrative state of an interface, see Enabling the Interfaces (Interface Manager).

PTP 850S supports LACP, which expands the capabilities of static LAG and provides interoperability with third-party equipment that uses LACP. LACP improves the communication between LAG members. This improves error detection capabilities in situations such as improper LAG configuration or improper cabling. It also enables the LAG to detect uni-directional failure and remove the link from the LAG, preventing packet loss.

LACP is enabled as part of the LAG configuration process. It should only be used if the LAG is in a link with another LACP-enabled LAG.



Note

LACP is not supported with Unit Redundancy. For Unit Redundancy, a special, limited implementation is configured on the logical interface level. See Configuring Line Protection Mode.

LACP can only be used with Ethernet interfaces.

LACP cannot be used with Enhanced LAG Distribution or with the LAG Group Shutdown in Case of Degradation Event feature.

PTP 850C and PTP 850E also support Multi-Homing for ETH-BN and CSF messages. You can enable Multi-Homing when creating or editing a LAG. When Multi-Homing is enabled:

- If ETH-BN (Ethernet Bandwidth Notification) is enabled on one of the interfaces in the LAG, ETH-BN messages are sent simultaneously on all of the LAG members. See Configuring Ethernet Bandwidth Notification (ETH-BN).
- If ASP Management Safe Mode is enabled on one of the interfaces in the LAG, CSF messages are sent simultaneously on all of the LAG members. See Configuring Automatic State Propagation and Link Loss Forwarding.

Configuring a LAG Group
Adding and Removing Group Members

1. To create a LAG group:
2. Select **Ethernet** > **Groups** > **LAG**. The LAG page opens.
3. Click **Create Group** underneath the Link Aggregation table. The Create LAG Group page opens.



Figure 283 Create LAG Group – Page 1

4. In the Group ID field, select a LAG Group ID. Only LAG IDs that are not already assigned to a LAG group appear in the dropdown list.
5. In the LACP field, select Enable to enable LACP on the LAG or Disable to disable LACP on the LAG. The default value is Disable.
6. In the Member 1 field, select an interface to assign to the LAG group. Only interfaces not already assigned to a LAG group appear in the dropdown list.
7. Click Next. A new Create LAG Group page opens.
8. In the Member 2 field, select an additional interface to assign to the LAG Group.
9. To add additional interfaces to the LAG group, repeat steps 5 and 6.
10. When you have finished adding interfaces to the LAG group, click Finish. A new Create LAG Group page opens displaying all the interfaces you have selected to include in the LAG group.

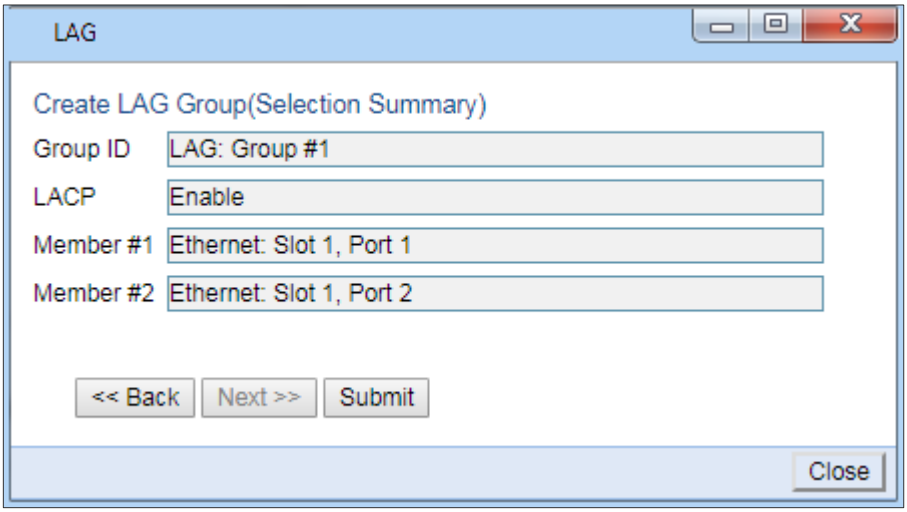


Figure 284 Create LAG Group – Final Page

Click **Submit**. If all the interfaces meet the criteria listed above, a message appears that the LAG group has been successfully created. If not, a message appears indicating that the LAG group was not created and giving the reason.

Editing a LAG Group

1. To edit an existing LAG group:

2. Select **Ethernet** > **Groups** > **LAG**. The LAG page opens.

3. Select the LAG group you want to edit in the Link Aggregation table.

4. Click **Edit** underneath the Link Aggregation table. The Link Aggregation - Edit page opens.

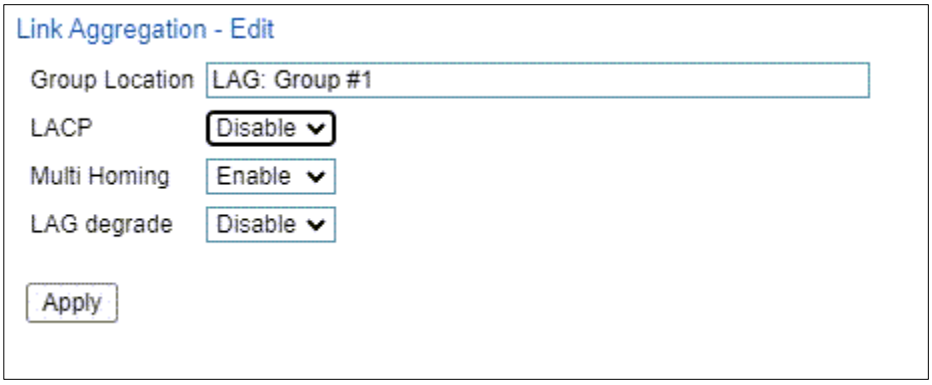


Figure 285 Link Aggregation - Edit Page

Do any of the following:

- To enable or disable LACP, select **Enable** or **Disable** in the **LACP** field.
- To enable or disable Multi-Homing, select **Enable** or **Disable** in the **Multi Homing** field.
- To enable or disable LAG Group Shutdown in case of Degradation Event, select **Enable** or **Disable** in the **LAG degrade** field.

4 Click **Apply**.

To add or remove members from an existing LAG group:

1 Select the LAG group in the Link Aggregation table of the LAG page.
2 Click **Add/Remove Members** underneath the Link Aggregation table. The Link Aggregation - Add/Remove Members page opens.

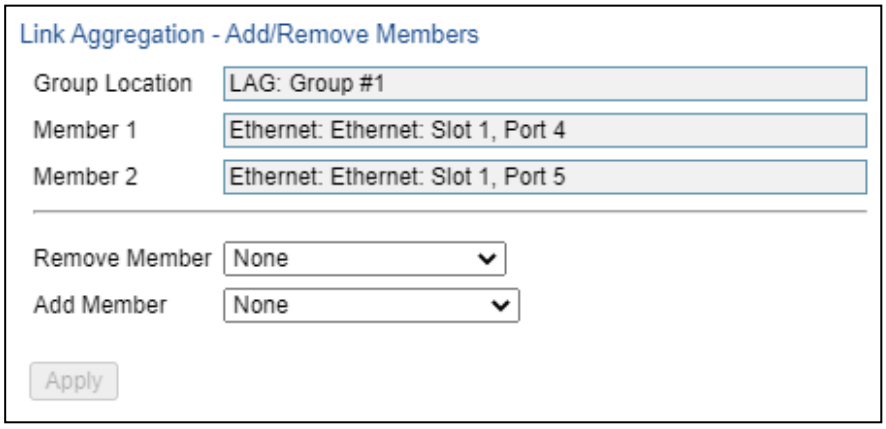


Figure 286: Link Aggregation – Add/Remove Members Page

3 Do any of the following:

- To remove an interface from the LAG Group, select the interface in the **Remove Member** field.
- To add an interface to the LAG Group, select the interface in the **Add Member** field.

4 Click **Apply**.
5 To remove or add additional interfaces, repeat steps 3 and 4.

Notes: When removing an interface from a LAG group, the removed interface is assigned the default interface values.

Enabling and Disabling LAG Group Shutdown in Case of Degradation Event



Note

LAG Group Shutdown in Case of Degradation Event cannot be used

with LACP.

A LAG group can be configured to be automatically closed in the event of LAG degradation. This option is used if you want traffic from the switch to be re-routed during such time as the link is providing less than a certain capacity.

By default, the LAG group shutdown in case of degradation event option is disabled. When enabled, the LAG is automatically closed in the event that any one or more ports in the LAG fail. When all ports in the LAG are again operational, the LAG is automatically re-opened.



Note

Failure of a port in the LAG also triggers a lag-degraded alarm, Alarm

ID 100.

To enable or disable the LAG group shutdown in case of degradation event option:

Select **Ethernet > Groups > LAG** to open the LAG page.

Select the LAG group in the Link Aggregation table.

Click **Edit** underneath the Link Aggregation table. The Link Aggregation - Edit page opens (*Figure 91*).

In the **LAG degrade** field, select **Enable** to enable the LAG group shutdown in case of degradation event option or **Disable** to disable the LAG group shutdown in case of degradation event option.

Click **Apply**.

Configuring Enhanced LAG Distribution

You can change the distribution function by selecting from ten pre-defined LAG distribution schemes. The feature includes a display of the TX throughput for each interface in the LAG, to help you identify the best LAG distribution scheme for the specific link.



Note

Enhanced LAG distribution is only available for LAG groups that consist of exactly two interfaces. It cannot be used with LACP.

To configure enhanced LAG distribution:

Select **Ethernet > Groups > LAG**. The LAG page opens.

Click **LAG DF** underneath the Link Aggregation table. The LAG Distribution Function (DF) page opens.

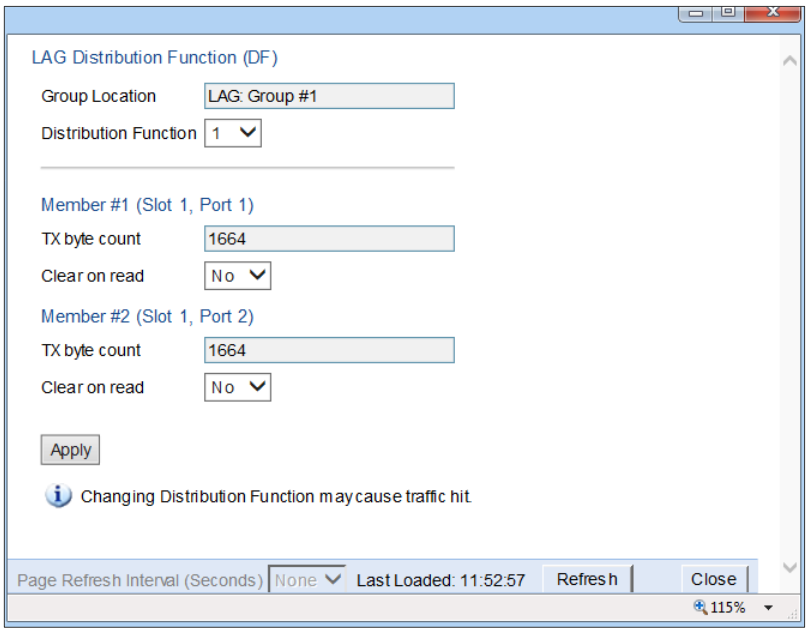


Figure 287 LAG Distribution Function (DF) Page

In the **Distribution Function** field, select a pre-set distribution scheme, from 1 to 10. It is recommended to experiment with the various schemes, monitoring the **TX byte count** fields for each interface to determine the efficiency of each distribution scheme for the link. The default distribution scheme is 1. The default LAG distribution pattern is 1.

To clear the TX byte counts, select **Clear on read** for one or both interfaces. The byte counts will be cleared when you close the LAG Distribution Function (DF) page or click **Refresh**.

Note

This counter will also be cleared for the members of the LAG in the Port RMON Statistics page.

Click **Apply** to apply the selected distribution scheme.

Deleting a LAG Group

In order to delete a LAG group, you must first make sure that no service points are attached to the LAG group.

To delete a LAG group:

1. Select **Ethernet** > **Groups** > **LAG**. The LAG page opens.
2. Select the LAG group you want to delete in the Link Aggregation table.
3. Click **Delete** underneath the Link Aggregation table. The LAG group is deleted. To delete multiple LAG groups:
4. Select the LAG groups in the Link Aggregation table or select all the LAG groups by selecting the check box in the top row.

5. Click Delete underneath the Link Aggregation table.

Displaying LACP Parameters and Statistics

You can display the following LACP parameters and statistics:

- LACP Aggregation (per LAG)
- LACP Port Status
- LACP Port Statistics
- LACP Port Debug Statistics

Note

PTP 850S does not support any LACP write parameters.

Displaying LACP Aggregation Status Parameters

To display LACP aggregation status parameters:

Select **Ethernet > Protocols > LACP > Aggregation** to open the LACP Aggregation page.

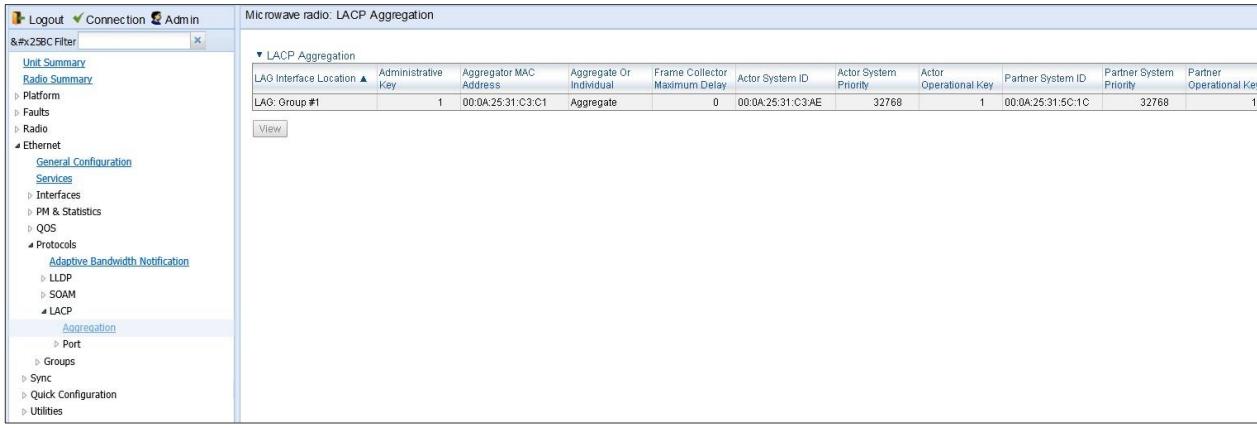


Figure 288 LACP Aggregation Page

Table 25 LACP Aggregation Status Parameters

Parameter	Definition
LAG Interface Location	Identifies the LAG group.
Administrative Key	The current administrative value of the key for the Aggregator.
Aggregator MAC Address	The individual MAC address assigned to the Aggregator.
Aggregate or Individual	Indicates whether the Aggregator represents an aggregate or an individual link.
Frame Collector Maximum Delay	The maximum delay, in tens of microseconds.
Actor System ID	The MAC address value used as a unique identifier for the system that contains this Aggregator.
Actor System Priority	The priority value associated with the Actor's System ID.

Actor Operational Key	The current operational value of the Key for the Aggregator.
Partner System ID	The MAC address value consisting of the unique identifier for the current protocol Partner of this Aggregator.
Partner System Priority	The priority value associated with the Partner's System ID.
Partner Operational Key	The current operational value of the Key for the Aggregator's current Protocol partner.

Displaying LACP Port Status Parameters

To display LACP port status parameters:

Select **Ethernet > Protocols > LACP > Port > Status** to open the LACP Port Status page.

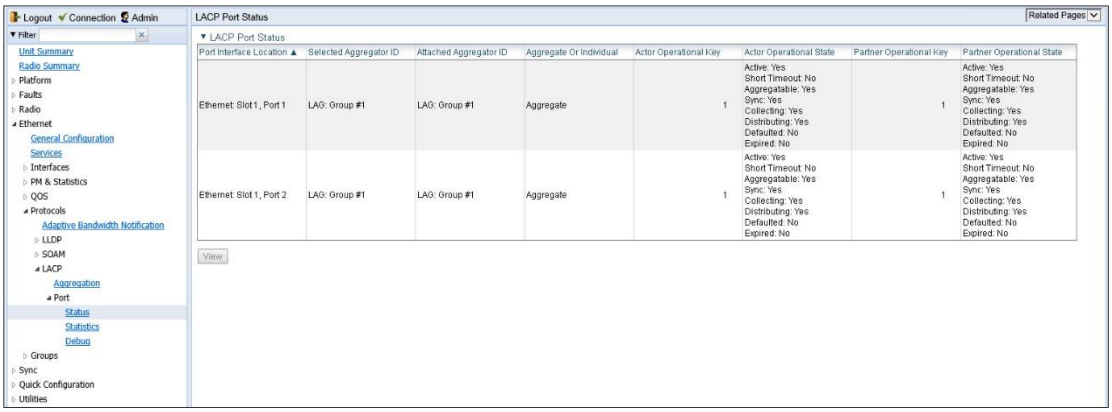


Figure 289 LACP Port Status Page

The LACP Port Status page displays the major port status parameters, per port. display all the available LACP port status parameters, select a port and click View. The LACP Port Status – View page is displayed.

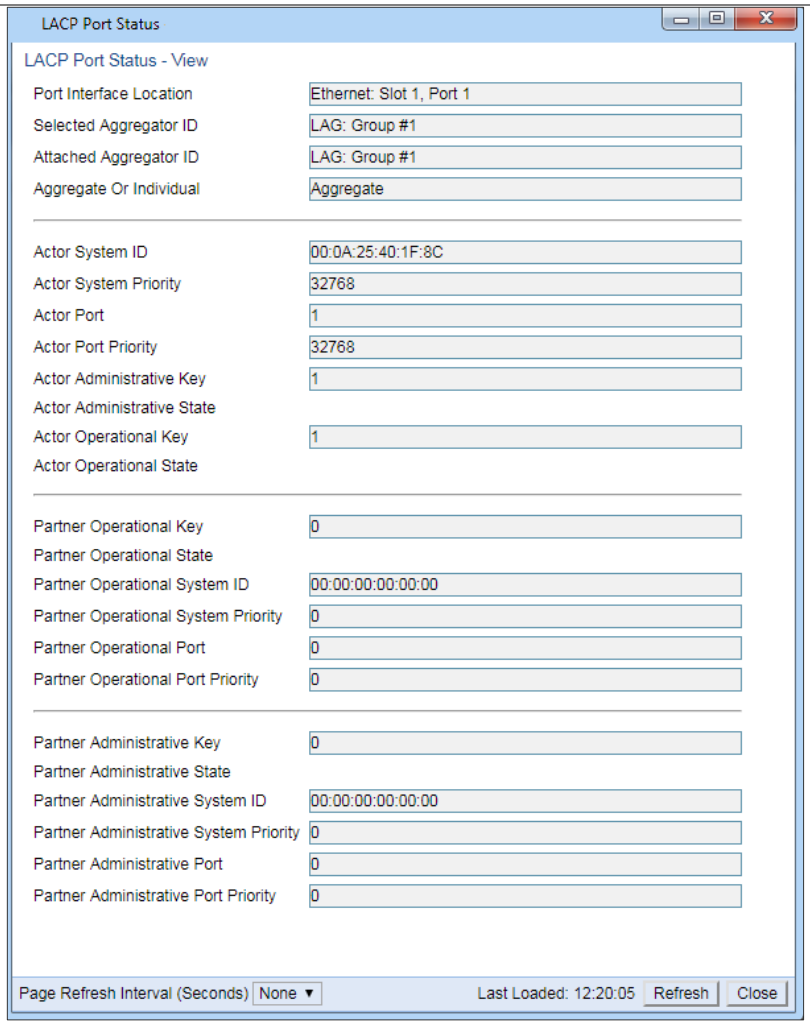


Figure 290 *LACP Port Status – View Page*

Table 26 LACP Port Status Parameters

Parameter	Definition
Port Interface	The location of the port.
Selected Aggregator ID	The identifier value of the Aggregator that this Aggregation port has currently selected.
Attached Aggregator ID	The identifier value of the Aggregator that this Aggregation port is currently attached to.
Aggregate or Individual	Indicates whether the Aggregation Port is able to aggregate or is only able to operate as an individual link.
Actor System ID	The MAC Address value that defines the value of the System ID for the system that contains this Aggregation Port.
Actor System Priority	The priority value associated with the Actor's System ID.
Actor Port	The port number locally assigned to the Aggregation Port.

Actor Port Priority	The priority value assigned to this Aggregation Port.
Actor Administrative	The current administrative value of the Key for the Aggregation Port.
Actor Administrative	The administrative values of the Actor's state as transmitted by the Actor via LACPDUs.
Actor Operational Key	The current operational value of the Key for the Aggregation Port.
Actor Operational State	The current operational values of the Actor's state as transmitted by the Actor via LACPDUs.
Partner Operational Key	The current operational value of the Key for the protocol Partner.
Partner Operational State	The current values of Actor State in the most recently received LACPDU transmitted by the protocol Partner.
Partner Operational	The MAC Address value representing the current value of the Aggregation Port's protocol Partner's System ID.
Partner Operational	The operational value of priority associated with the Partner's System ID.
Partner Operational Port	The operational port number assigned to this Aggregation port by the Aggregation port's port Partner.
Partner Operational Port	The Priority value assigned to this Aggregation port by the Partner.
Partner Administrative	The current administrative value of the Key for the protocol Partner.
Partner Administrative	The current administrative value of Actor state for the protocol Partner.
Partner Administrative System ID	The MAC Address value representing the administrative value of the Aggregation Port's Protocol partner's System ID.
Partner Administrative System Priority	The administrative priority value associated with the Partner's System ID.
Partner Administrative Port	The current administrative value of the port number for the protocol partner.
Partner Administrative Port Priority	The current administrative value of the port priority for the protocol partner.

Displaying LACP Port Statistics

To display LACP port statistics:

1 Select **Ethernet > Protocols > LACP > Port > Statistics** to open the LACP Port Statistics page.

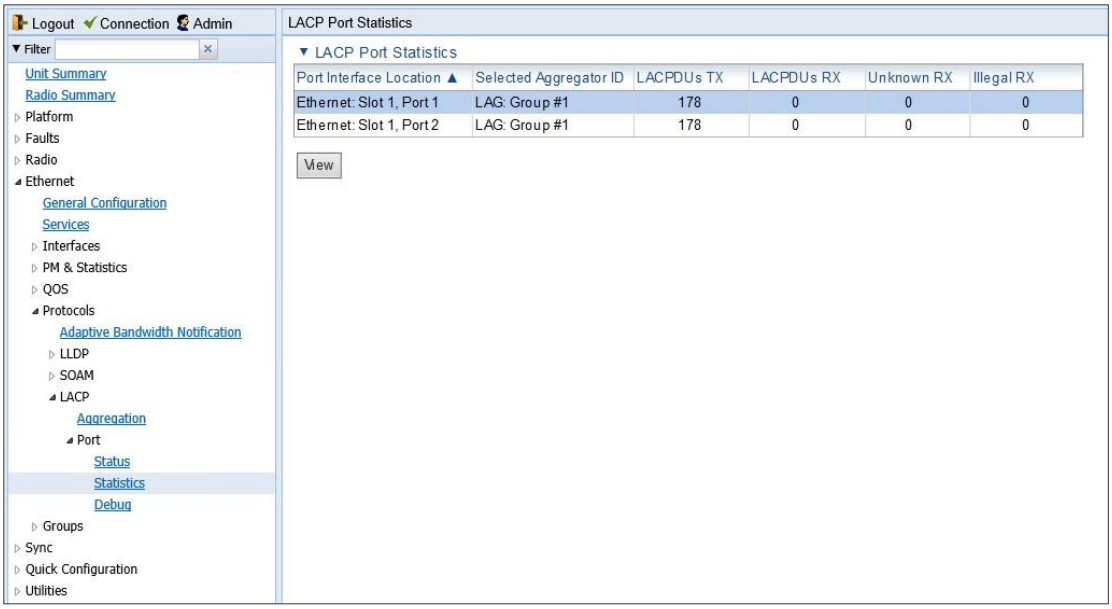


Figure 291 LACP Port Statistics Page

Table 27 LACP Port Statistics

Parameter	Definition
Port Interface	The location of the port.
Selected Aggregator ID	The identifier value of the Aggregator that this Aggregation port has currently selected.
LACPDUs TX	The number of LACPDUs that this port has transmitted.
LACPDUs RX	The number of LACPDUs that this port has received.
Unknown RX	The number of unknown protocol frames that this port has
Illegal RX	The number of illegal protocol frames that this port has received.

Displaying LACP Port Debug Statistics

To display LACP port debug statistics:

1 Select **Ethernet > Protocols > LACP > Port > Debug** to open the LACP Port Debug page.

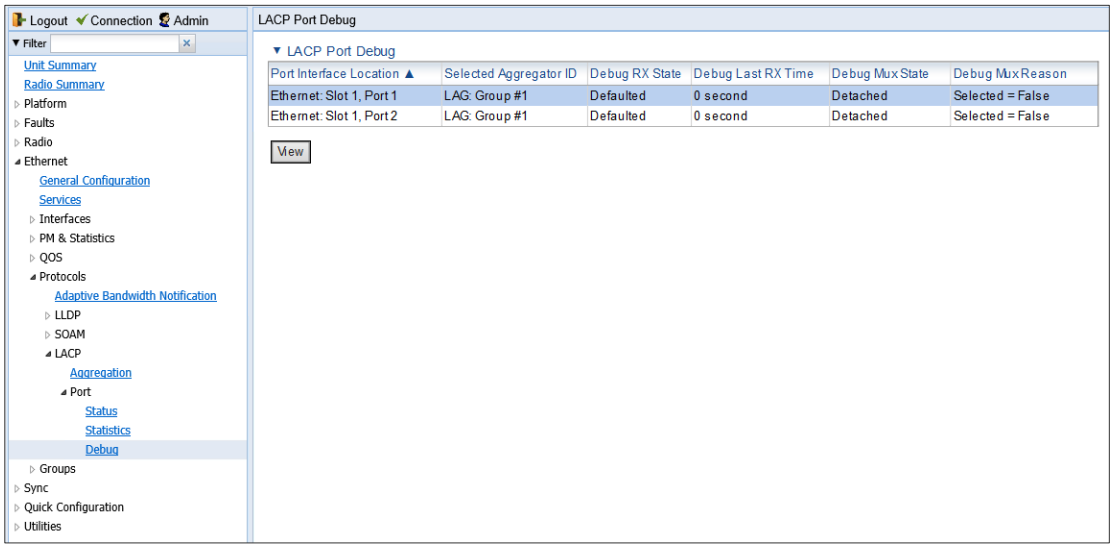


Figure 292 LACP Port Debug Page

Table 28 LACP Port Debug Statistics

Parameter	Definition
Port Interface	The location of the port.
Selected Aggregator ID	The identifier value of the Aggregator that this Aggregation port has currently selected.
Debug RX State	The state of the receive state machine for the Aggregation port. Possible values are: **Current** – An LACPDU was received before expiration of the most recent timeout period. **Expired** – No LACPDU was received before expiration of the most recent timeout period. **Defaulted** – No LACPDU was received during the two most recent timeout periods.
Debug Last RX Time	The value of a TimeSinceSystemReset (F.2.1) when the last LACPDU was received by this Aggregation port.
Debug Mux State	The state of the Mux state machine for the Aggregation port. Possible values are Collecting, Distributing, Attached, and Detached.
Debug Mux Reason	A text string indicating the reason for the most reason change in the state of the Mux machine.

8. Unit Management

This section includes:

- Defining the IP Protocol Version for Initiating Communications
- Configuring the Remote Unit's IP Address
- Configuring SNMP
- Configuring Trap Managers
- Installing and Configuring an FTP or SFTP Server
- Configuring the Internal Ports for FTP or SFTP
- Upgrading the Software
- Backing Up and Restoring Configurations
- Setting the Unit to the Factory Default Configuration
- Performing a Hard (Cold) Reset
- Configuring Unit Parameters
- Configuring NTP
- Displaying Unit Inventory
- Displaying SFP DDM and Inventory Information
- Defining a Login Banner

Related topics:

- Setting the Time and Date (Optional)
- Enabling the Interfaces (Interface Manager)
- Uploading Unit Info
- Changing the Management IP Address

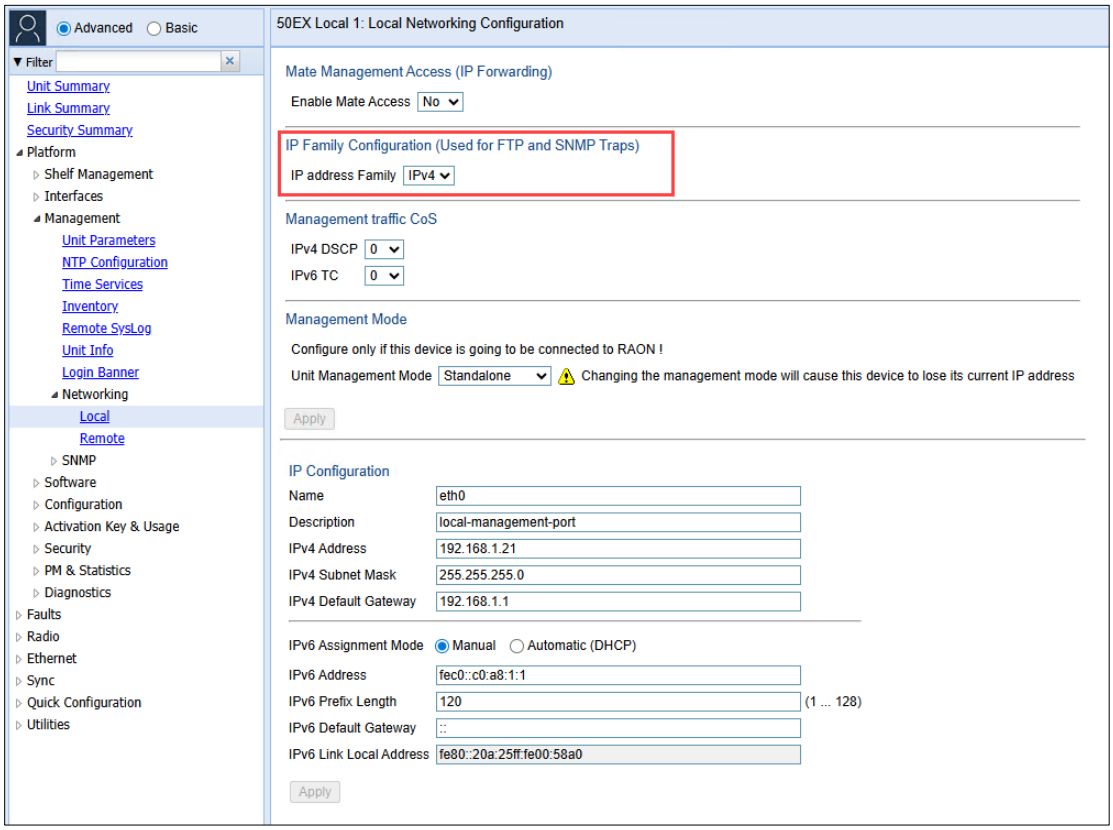
8.1 Defining the IP Protocol Version for Initiating Communications

You can specify which IP protocol the unit will use when initiating communications, such as downloading software, sending traps, pinging, or exporting configurations. The options are IPv4 or IPv6.

To set the IP protocol version of the local unit:

1. Select **Platform** > **Management** > **Networking** > **Local**. The Local Networking Configuration page opens.

Figure 293 Local Networking Configuration Page



2. In the **IP address Family** field, select the IP protocol the unit will use when initiating communications. The options are **IPv4** or **IPv6**.

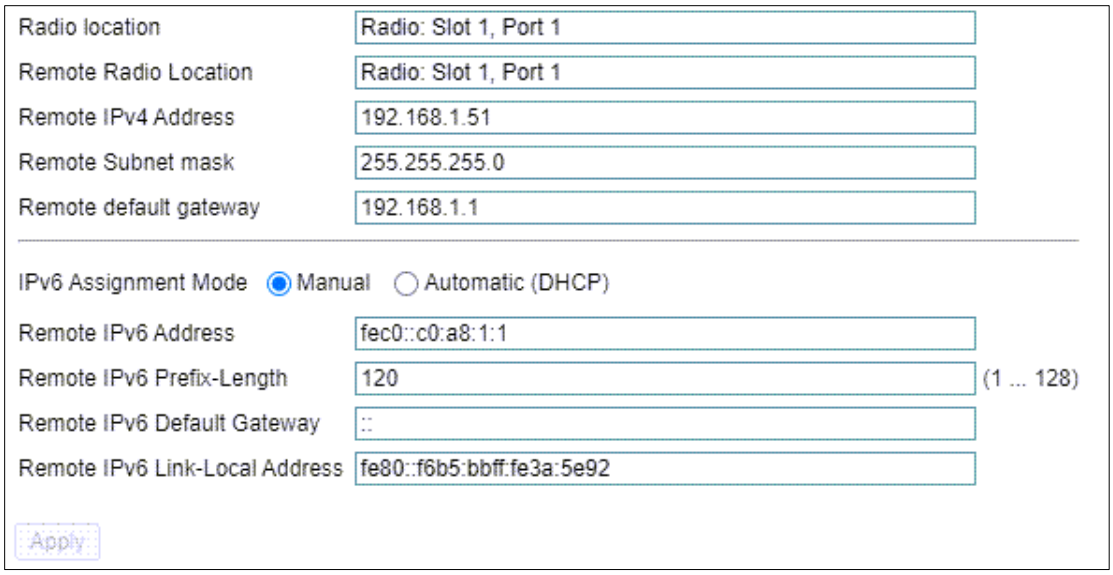
8.2 Configuring the Remote Unit's IP Address

You can configure the IP address of a remote unit.

To configure the IP address of a remote unit:

1. Select **Platform** > **Management** > **Networking** > **Remote**. The Remote Networking Configuration page opens.

Figure 294 Remote Networking Configuration Page



2. In the **Remote IPv4 address** field, enter an IPv4 address for the remote unit. You can enter the address in IPv4 format in this field, and/or in IPv6 format in the **IPv6 Address** field. The remote unit will receive communications whether they are sent to its IPv4 address or its IPv6 address.
3. In the **Remote Subnet mask** field, enter the subnet mask of the remote radio.
4. Optionally, in the **Remote default gateway** field, enter the default gateway address for the remote radio.
5. Optionally, in the **Remote IPv6 Address** field, enter an IPv6 address for the remote unit. You can enter the address in IPv6 format in this field, and/or in IPv4 format in the **Remote IPv4 Address** field. The unit will receive communications whether they are sent to its IPv4 address or its IPv6 address.
6. If you entered an IPv6 address, enter the IPv6 prefix length in the **Remote IPv6 Prefix-Length** field.
7. Optionally, if you entered an IPv6 address, enter the default gateway in IPv6 format in the **Remote IPv6 Default Gateway** field.
8. Click **Apply**.

8.2.1 Changing the Subnet of the Remote IP Address

If you wish to change the **Remote IPv4 Address** to a different subnet:

1. Change the address of the **Remote Default Gateway** to 0.0.0.0.
2. Click **Apply**.
3. Set the **Remote IPv4 Address** as desired, and the **Remote Default Gateway** as desired.

Similarly, if you wish to change the **Remote IPv6 Address** to a different subnet:

1. Change the address of the **Remote IPv6 Default Gateway** to 0:0:0:0:0:0:0:0.
2. Click **Apply**.
3. Set the **Remote IPv6 Address** as desired, and the **Remote IPv6 Default Gateway** as desired.

8.3 Configuring SNMP

PTP 850E support SNMP v1, V2c, and v3. You can set community strings for access to PTP 850 units.

PTP 850E support the following MIBs:

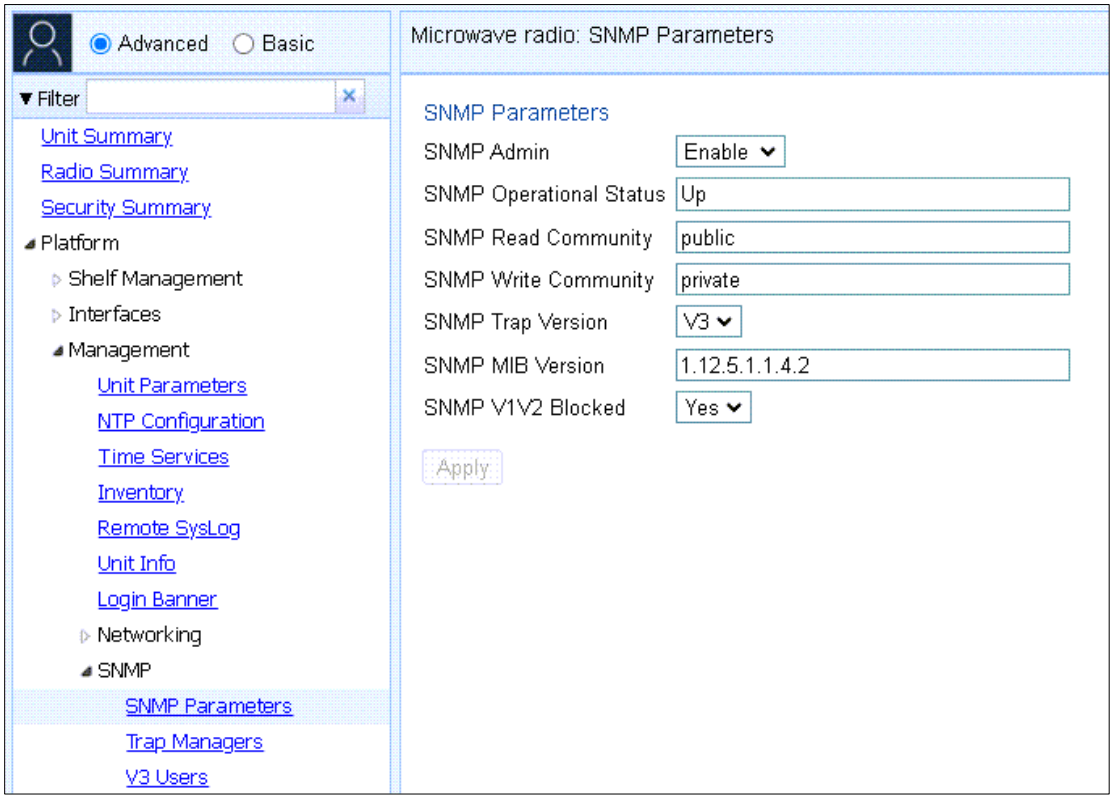
- RFC-1213 (MIB II).
- RMON MIB.
- Proprietary MIB.

Access to the unit is provided by making use of the community and context fields in SNMPv1 and SNMPv2c/SNMPv3, respectively.

To configure SNMP:

1. Select **Platform > Management > SNMP > SNMP Parameters**. The SNMP Parameters page opens.

Figure 295 SNMP Parameters Page



2. In the **Admin** field, select **Enable** to enable SNMP monitoring, or **Disable** to disable SNMP monitoring.

Note

The **Operational Status** field indicates whether SNMP monitoring is currently active (**Up**) or inactive (**Down**).

3. In the **SNMP Read Community** field, enter the community string for the SNMP read community.
4. In the **SNMP Write Community** field, enter the community string for the SNMP write community
5. In the **SNMP Trap Version** field, select **V1**, **V2**, or **V3** to specify the SNMP version.

Note

The **SNMP MIB Version** field displays the current SNMP MIB version the unit is using.

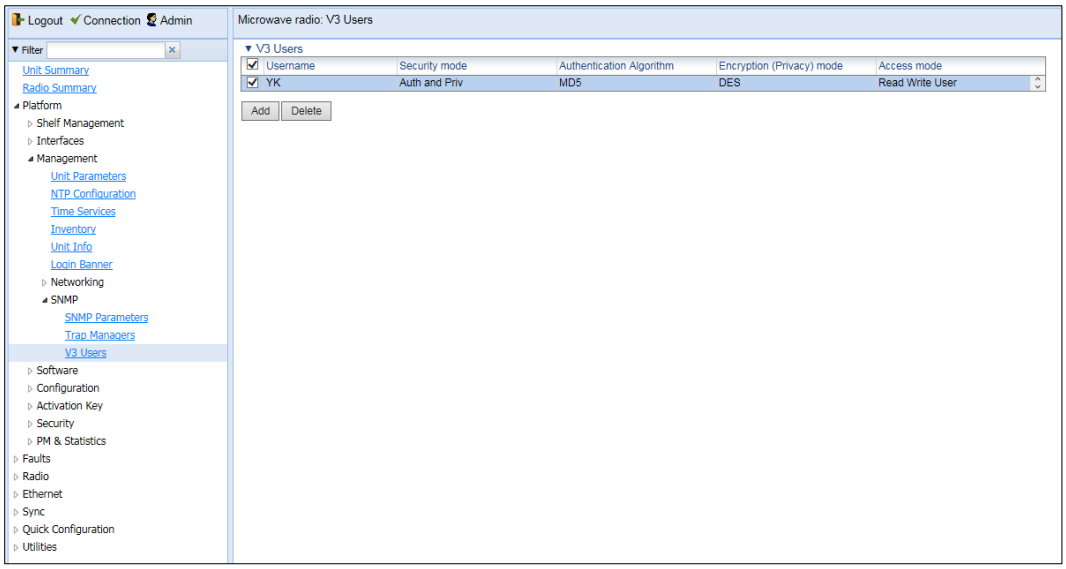
6. **In** the **V1V2 Blocked** field, select **Yes** if you want to block SNMPv1 and SNMPv2 access so that only SNMPv3 access will be enabled.
7. Click **Apply**.

If you are using SNMPv3, you must also configure SNMPv3 users. SNMPv3 security parameters are configured per SNMPv3 user.

To add an SNMP user:

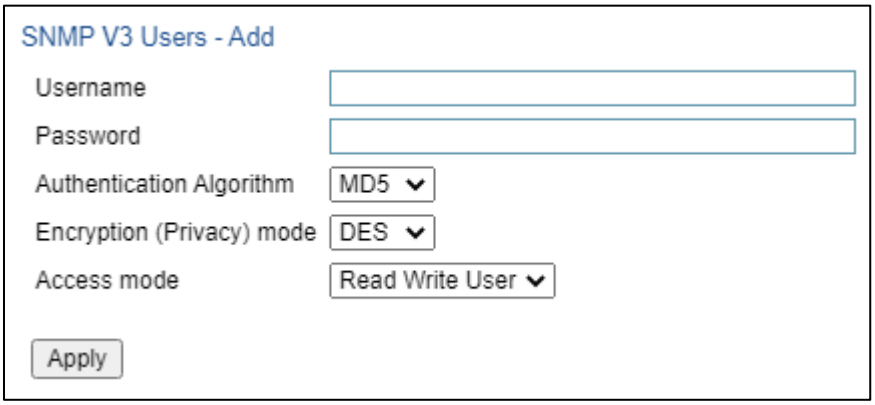
1. Select **Platform > Management SNMP > V3 Users**. The V3 Users page opens.

Figure 296 V3 Users Page



2. Click **Add**. The V3 Users - Add page opens.

Figure 297 V3 Users - Add Page



3. Configure the SNMP V3 Authentication parameters, as described below.
4. Click **Apply**, then **Close**.

Table 29 SNMP V3 Authentication Parameters

Parameter	Definition
User Name	Enter the SNMPv3 user name.
Password	Enter a password for SNMPv3 authentication. The password must be at least eight characters.
Authentication Algorithm	Select an authentication algorithm for the user. Options are: **None** **SHA** **SHA256** **MD5**
Encryption (Privacy) Mode	Select an encryption (privacy) protocol for the user. Options are: **None** **DES** **AES**
Access Mode	Select an access permission level for the user. Options are: **Read Write User** **Read Only User**

.

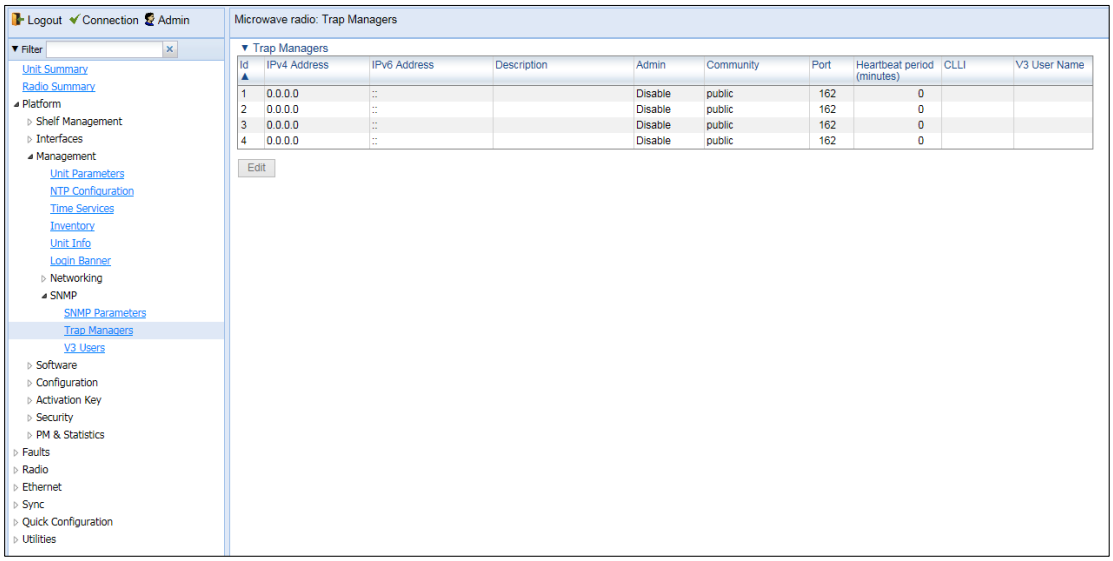
8.4 Configuring Trap Managers

You can configure trap forwarding parameters by editing the Trap Managers table. Each line in the Trap Managers table displays the setup for a manager defined in the system.

To configure trap managers:

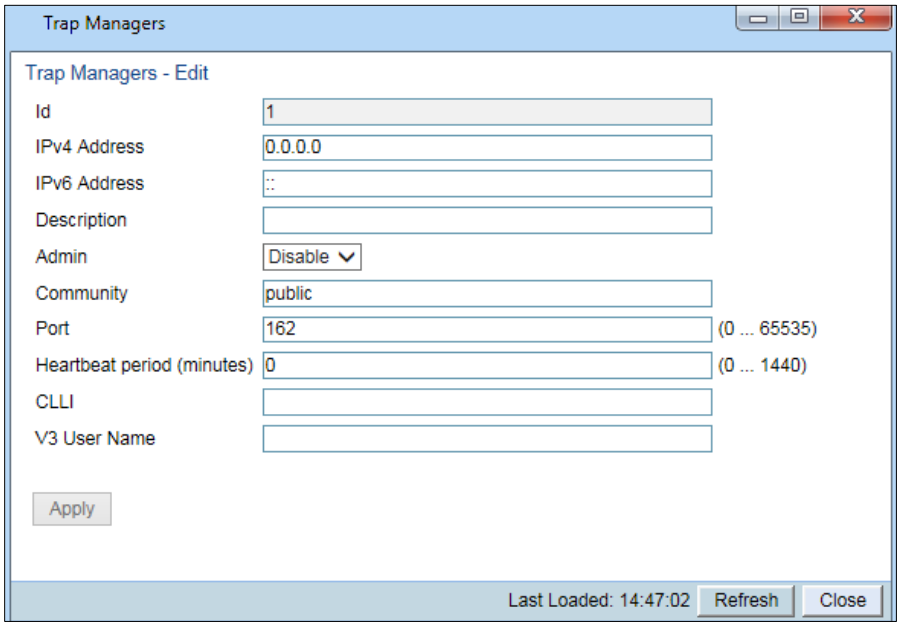
1. Select **Platform > Management SNMP > Trap Managers**. The Trap Managers page opens.

Figure 298 Trap Managers Page



2. Select a trap manager and click Edit. The Trap Managers Edit page opens.

Figure 299 Trap Managers - Edit Page



3. Configure the trap manager parameters, as described in Table 30 Trap Manager Parameters.
4. Click **Apply**, then **Close**.

Table 30 Trap Manager Parameters

Parameter	Definition
IPv4 Address	If the IP address family is configured to be IPv4, enter the destination IPv4 address. Traps will be sent to this IP address. See Defining the IP Protocol Version for Initiating Communications.
IPv6 Address	If the IP address family is configured to be IPv6, enter the destination IPv6 address. Traps will be sent to this IP address. See Defining the IP Protocol Version for Initiating Communications.
Description	Enter a description of the trap manager (optional).
Admin	Select **Enable** or **Disable** to enable or disable the selected trap manager.
Community	Enter the community string for the SNMP read community.
Port	Enter the number of the port through which traps will be sent.

Parameter	Definition
Heartbeat Period	Enter the interval, in minutes, between each heartbeat trap.
CLLI	Enter a Common Language Location Identifier (CLLI). The CLLI is free text that will be sent with the trap. You can enter up to 100 characters.
V3 User Name	If the SNMP Trap version selected in Figure 295 SNMP Parameters Page page is **V3**, enter the name of a V3 user defined in the system. To view or define a V3 user, use the Figure 296 V3 Users Page page. **Note**: Make sure that an identical V3 user is also defined on the manager's side.

8.5 Installing and Configuring an FTP or SFTP Server

Several tasks, such as software upgrade (except when performed using HTTP or HTTPS) and configuration backup, export, and import, require the use of FTP or SFTP. The PTP 850 can function as an FTP or SFTP client. If you wish to use FTP/SFTP, you must install FTP/SFTP server software on the PC or laptop you are using.



Note

For FTP, it is recommended to use FileZilla_Server software that can be downloaded from the web (freeware).
For SFTP, it is recommended to use SolarWinds SFTP/SFCP server (freeware).

If you are using IPv6 to perform the operation, make sure to use FileZilla version 0.9.38 or higher to ensure IPv6 support. If you are using another type of FTP or SFTP server, make sure the application version supports IPv6.

To install and configure FTP or SFTP server software on the PC or laptop:

1. Create a user and (optional) password on the FTP/SFTP server. For example, in FileZilla Server, perform the following:

From the Edit menu, select Users.

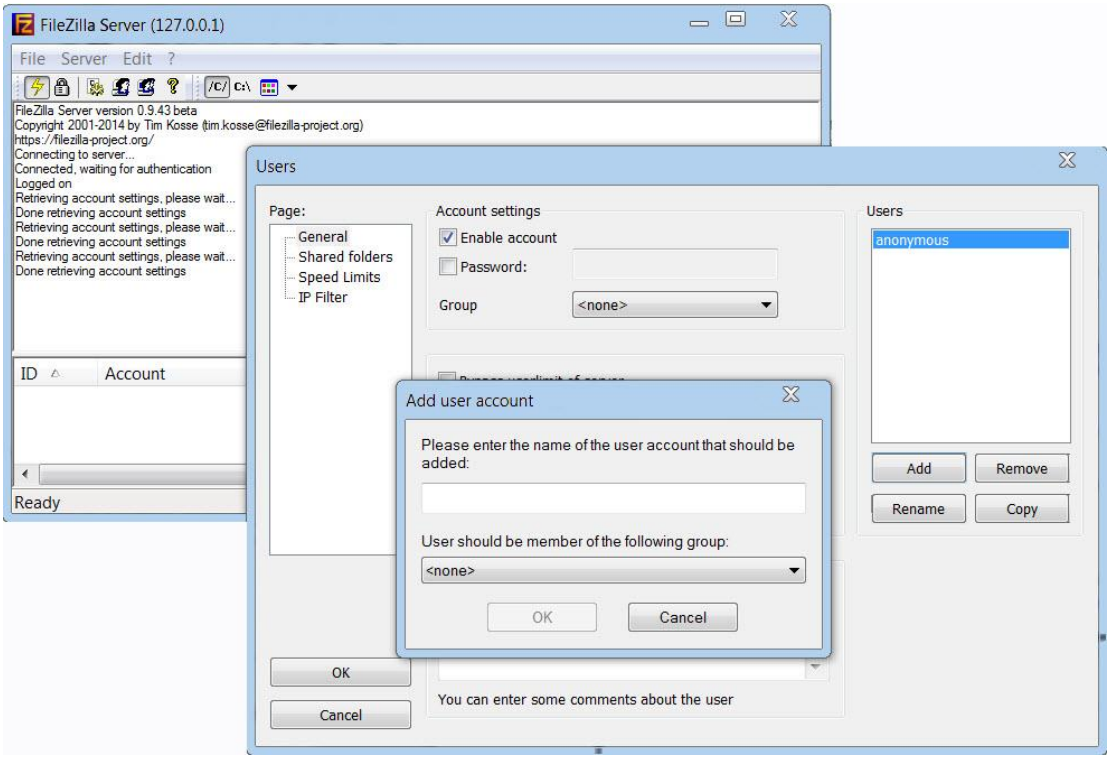
I. In the Users window, click Add.

II. In the Add user account window, enter a user name and click OK.

III. In the Users window, select Enable account and, optionally, select Password and enter a password.

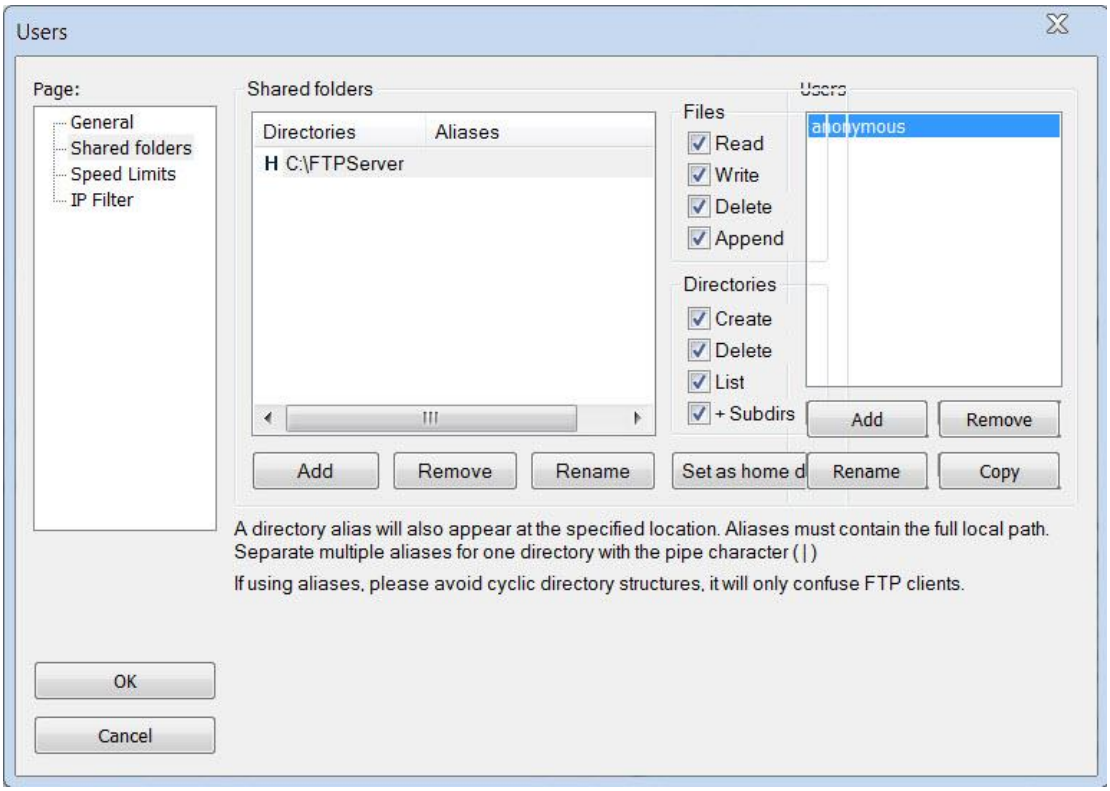
IV. In the Users window, click OK.

Figure 300 FileZilla Server User Configuration



2. Create a shared FTP/SFTP folder on the PC or laptop you are using to perform the software upgrade (for example, *C:\FTPServer*).
3. In the FTP/SFTP server, set up the permissions for the shared FTP/SFTP folder. For example, in FileZilla Server:
   I. From the **Edit** menu, select **Users**.
   II. In the Users window, select **Shared folders**.
   III. Underneath the Shared folders section, click **Add** and browse for your shared FTP folder.
   IV. Select the folder and click **OK**.
   V. In the Shared folders section, select your shared FTP folder.
   VI. In the Files and Directories sections, select all of the permissions.
   VII. Click Set as home directory to make the Shared folder the root directory for your FTP server
   VIII. Click **OK** to close the Users window.

Figure 301 FileZilla Server Shared Folder Setup



8.6 Configuring the Internal Ports for FTP or SFTP

By default, the following PTP 850 ports are used for FTP and SFTP when the PTP 850 unit is acting as an FTP or SFTP client (e.g., software downloads, configuration file backup and restore operations):

FTP – 21

SFTP – 22

You can change either or both of these ports from the following pages:

Platform > Management > Unit Info

Platform > Management > Unit Info

Platform > Software > Download & Install

Platform > Configuration > Configuration Management

Platform > Security > General > Security Log Upload

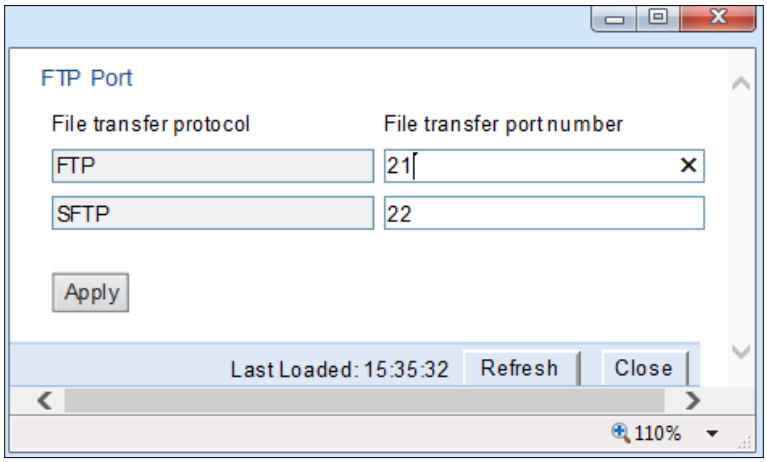
Platform > Security > General > Configuration Log Upload

Platform > Security > X.509 Certificate > CSR

Platform > Security > X.509 Certificate > Download & Install

From any of these pages, click **FTP Port**. The FTP Port page opens.

Figure 302 FTP Port Page



Edit the **File transfer port number** for FTP and or SFTP and click **Apply**.

8.7 Upgrading the Software

PTP 850 software and firmware releases are provided in a single bundle that includes software and firmware for all components in the system. Software is first downloaded to the system, then installed. After installation, a reset is automatically performed on all components whose software was upgraded.

This section includes:

Viewing Current Software Versions

Software Upgrade Overview

Downloading and Installing Software

Configuring a Timed Installation

8.7.1 Viewing Current Software Versions

To display a list of software packages currently installed and running on the system modules:

1. Select **Platform** > **Software** > **Versions**. The Versions page opens. For a description of the information provided in the Versions page, see Table 31 Software Versions Page Columns.

Figure 303 Versions Page

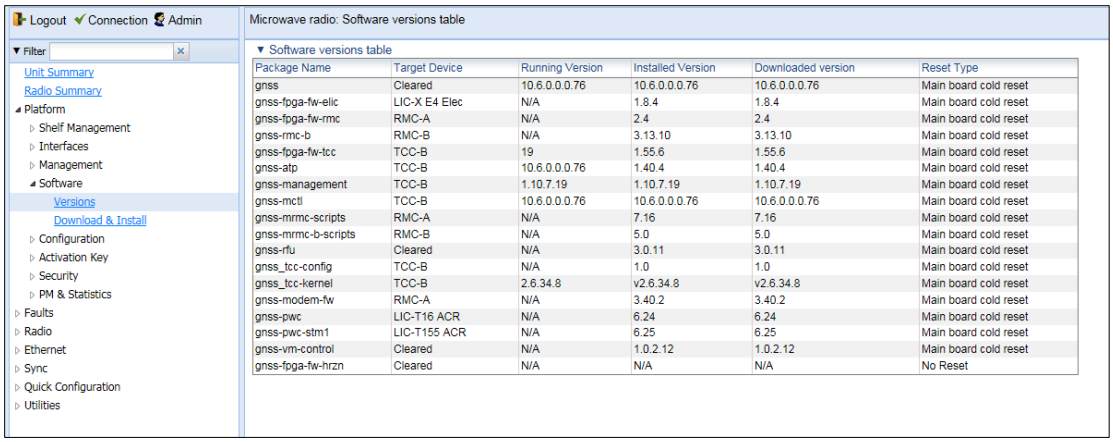


Table 31 Software Versions Page Columns

Parameter	Definition
Package Name	The name of the software package.
Target Device	The specific component on which the software runs.
Running Version	The software version currently running on the component.
Installed Version	The software version currently installed for the component. If the installed version is not already the running version, it will become the running version after the next reset takes place.
Downloaded Version	The version, if any, that has been downloaded from the server but not yet installed. Upon installation, this version will become the Installed Version.
Reset Type	The level of reset required by the component in order for the Installed Version to become the Active Version. A cold (hard) reset powers down and powers back up the component. A warm (soft) reset simply reboots the software or firmware in the component.

8.7.2 Software Upgrade Overview

The PTP 850 software installation process includes the following steps:

1. **Download** – The files required for the installation or upgrade are downloaded from a remote server.
2. **Installation** – The downloaded software and firmware files are installed in all modules and components of the PTP 850 that are currently running an older version.

3. **Reset** – The PTP 850 is restarted in order to boot the new software and firmware versions.

Software and firmware releases are provided in a single bundle that includes software and firmware for all components in the system. When you download a software bundle, the system verifies the validity of the bundle. The system also compares the files in the bundle to the files currently installed in the PTP 850 and its components, so that only files that need to be updated are actually downloaded. A message is displayed for each file that is actually downloaded.



Note

When downloading an older version, all files in the bundle may be downloaded, including files that are already installed.

Software bundles can be downloaded via HTTP, HTTPS, FTP or SFTP. After the software download is complete, you can initiate the installation.

8.7.3 Downloading and Installing Software

You can download software using HTTP, HTTPS, FTP or SFTP.

When downloading software via HTTPS or HTTPS, the PTP 850E functions as the server, and you can download the software directly to the PTP 850E unit.

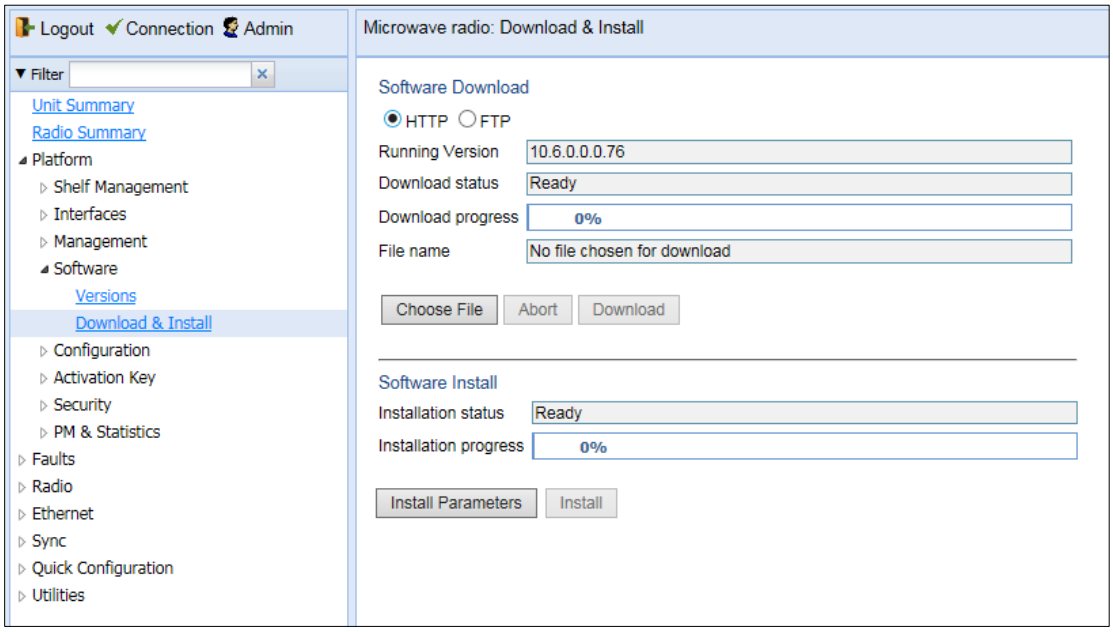
When downloading software via FTP or SFTP, the PTP 850E functions as an FTP or SFTP client. You must install FTP or SFTP server software on the PC or laptop you are using to perform the software upgrade. For details, see Installing and Configuring an FTP or SFTP Server.

8.7.4 Downloading Software Via HTTP or HTTPS

To download and install a new software version using HTTP or HTTPS:

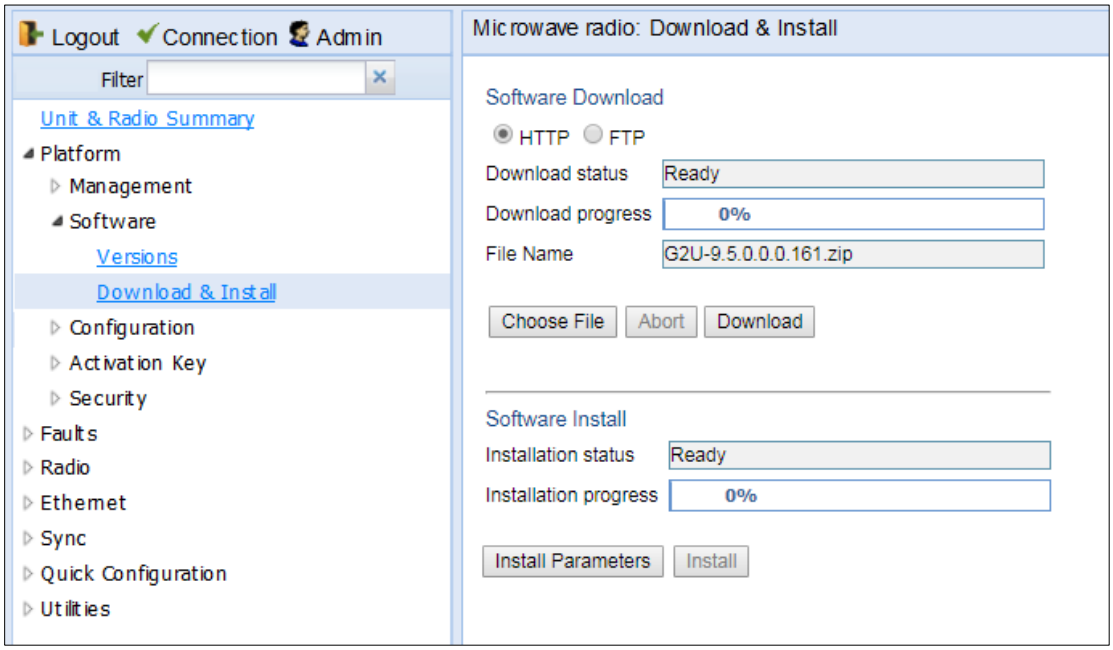
1. Before performing a software upgrade, it is important to verify that the system date and time are correct.
2. In the PTP 850's Web EMS, select **Platform > Software > Download & Install**. The Download & Install page opens.

Figure 304 Download & Install Page – HTTP/ HTTPS Download – No File Selected



3. Select **HTTP**
4. Click **Choose File.** A browser window opens.
5. Navigate to the directory in which the software file is located and selected the file. The selected file must be a ZIP file.
6. Click **Open**. The file name of the selected file appears in the **File Name** field.

Figure 305 Download & Install page – HTTP/ HTTPS Download – File Selected



7. Click **Download**. The download begins. You can view the status of the download in the **Download Status** field.

> **Note**
>
> To Discontinue the download process, Click **Abort.**

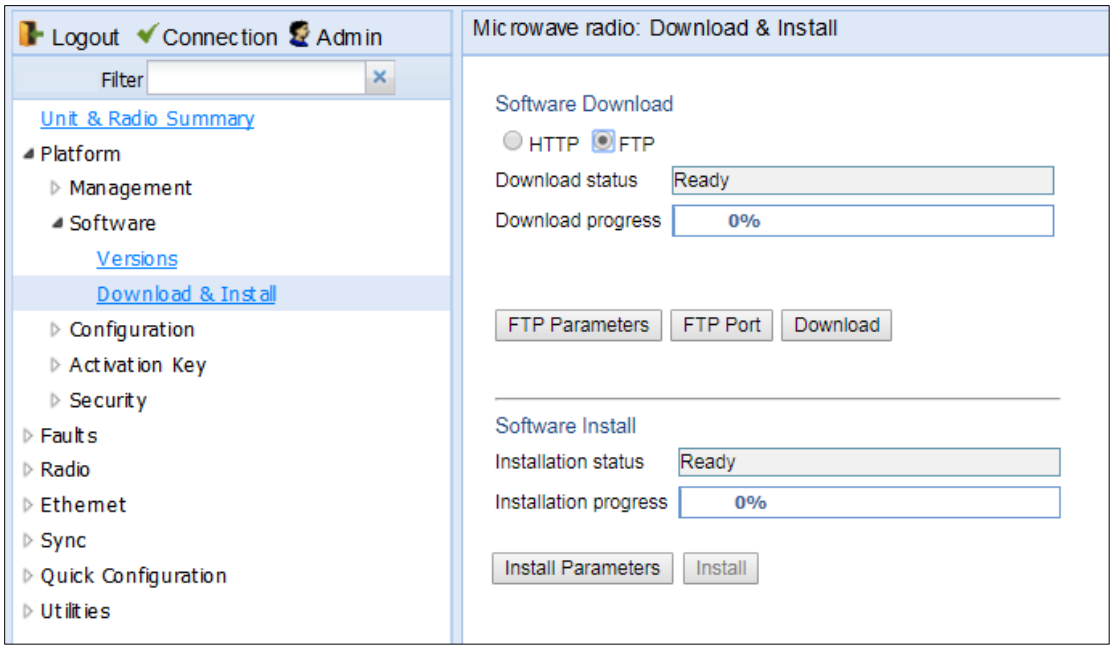
8. Once the download has been completed, verify that the version you want to install has been downloaded. You can check the downloaded version for each component by viewing the Downloaded Version column in the Versions page. See Viewing Current Software versions.

8.7.5 Downloading Software Via FTP or SFTP

To download and install a new software version using FTP or SFTP:

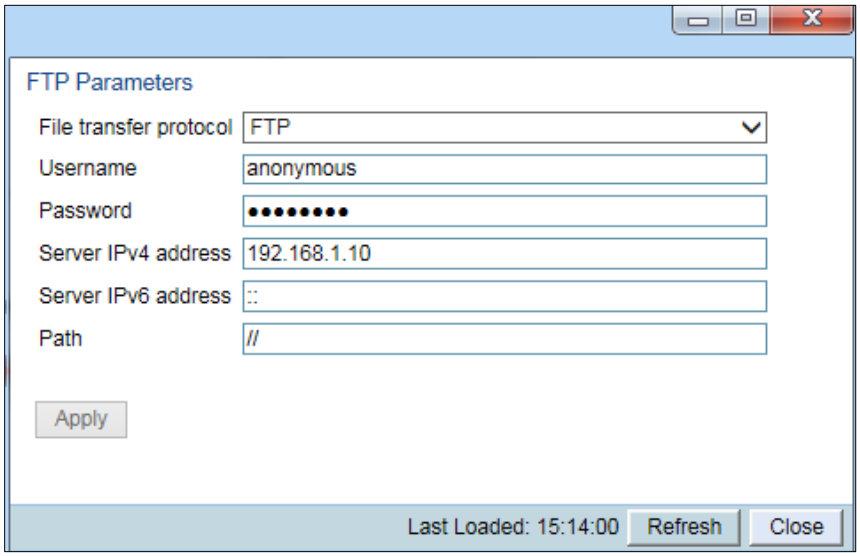
1. Before performing a software upgrade, it is important to verify that the system date and time are correct..
2. Install and configure FTP or SFTP server software on the PC or laptop you are using to perform the software upgrade, as described in Installing and Configuring an FTP or SFTP Server.
3. Unzip the new software package for PTP 850 into your shared FTP or SFTP folder.
4. In the PTP 850's Web EMS, select **Platform > Software > Download & Install**. The Download & Install page opens.
5. Select **FTP**.

Figure 306 Download & Install Page - FTP



6. Click **FTP Parameters** to view the FTP Parameters page.

Figure 307 FTP Parameters Page



7. In the **File Transfer Protocol** field, select the file transfer protocol you want to use (**FTP** or **SFTP**).
8. In the **Username** field, enter the user name you configured in the FTP server.
9. In the **password** field, enter the password you configured in the FTP server. If you did not configure a password for your FTP/SFTP user, simply leave this field blank.
10. If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the FTP/SFTP server in the **Server IPv4 address** field. See Defining the IP Protocol Version for Initiating Communications.
11. If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the FTP/SFTP server in the **Server IPv6 Address** field. See Defining the IP Protocol Version for Initiating Communications.
12. In the **Path** field, enter the directory path from which you are downloading the files. Enter the path relative to the FTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
13. Click **Apply** to save your settings, and **Close** to close the FTP Parameters page.
14. Click **Download**. The download begins. You can view the status of the download in the **Download Status** field of the Download & Install page. See Table 32 Download & Install Status Parameters.
15. Once the download has been completed, verify that the version you want to install has been downloaded. You can check the downloaded version for each component by viewing the Downloaded Version column in the Versions page. See Viewing Current Software Versions.

8.7.7 Installing Software

Note

For Instructions on how to configure a timed installation, see Configuring a Timed Installation.

To Install software:

1. Download the software version you want to install. See Downloading and installing Software.
2. Select **Platform > Software > Download & Install**. The Download & Install page opens. (Figure 306).
3. Click **Install**. The installation begins. You can view the status of the installation in the Download & Install - Status Parameters section of the Download & Install Download & Install page. See Table 32 Download & Install Status Parameters.

Upon completion of the installation, the system performs an automatic reset.

Note

DO NOT reboot the unit during the software installation process. As soon as the process is successfully completed, the unit will reboot itself.

Sometimes the installation process can take up to 30 minutes.

Only in the event that software installation was not successfully finished and more than 30 minutes have passed can the unit be rebooted..

Table 32 Download & Install Status Parameters

Parameter	Definition
Download status	The status of any pending software download. Possible values are: • **Ready** – The default value, which appears when no download is in progress. • **Verifying download files** – The system is verifying the files to be downloaded. • **Download in progress** – The download files have been verified, and the download is in progress. If an error occurs during the download, an appropriate error message is displayed in this field. When the download is complete, one of the following status indications appears: • **Download Success** • **Download Failure** • **All components already found in the system** When the system is reset, the **Download Status** returns to **Ready**.
Download progress	Displays the progress of the current software download.
Install status	The status of any pending software installation. Possible values are: • **Ready** – The default value, which appears when no installation is in progress. • **Verifying installation files** – The system is verifying the files to be installed. • **Installation in progress** – The installation files have been verified, and the installation is in progress. If an error occurs during the installation, an appropriate error message is displayed in this field. When the installation is complete, one of the following status indications appears: • **Installation Success** • **Installation Partial Success** • **Installation Failure** • **incomplete-sw-version** When the system is reset, the **Installation Status** returns to **Ready**.

Parameter	Definition
Install progress	Displays the progress of the current software installation.

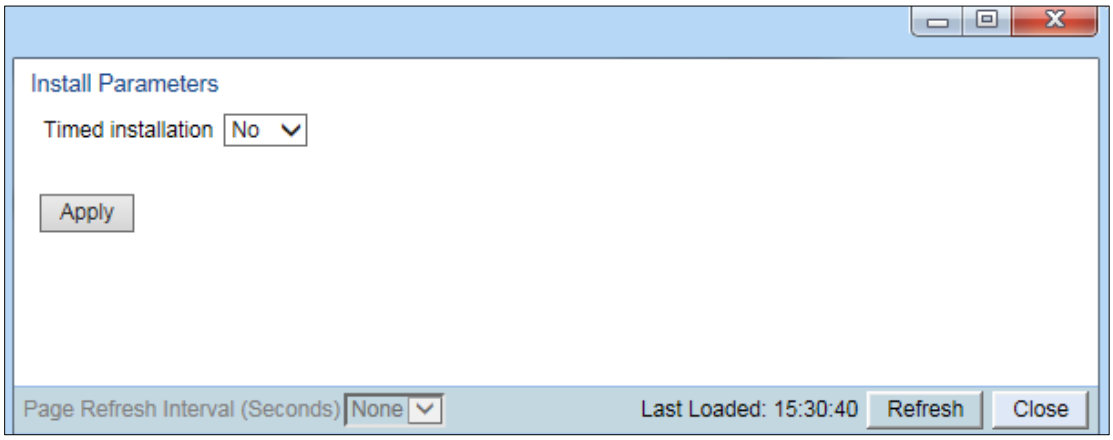
8.7.8 Configuring a Timed Installation

You can schedule a timed (deferred) software installation to take place at any time within 24 hours after you configure the installation.

To schedule a timed software installation:

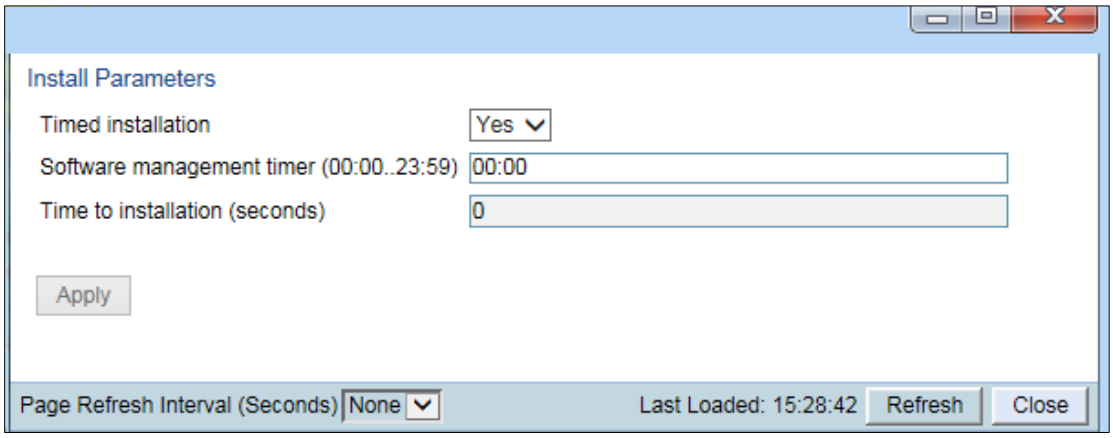
1. Download the software version you want to install. See Downloading and Installing Software.
2. Select **Platform > Software > Download & Install. The Download & Install page opens.**
3. Click **Install Parameters**. The Install Parameters page opens.

Figure 308 Install parameters Page.



4. Select **Yes** in the **Timed Installation** field.
5. Click **Apply**. The **Software Management timer field** appears.

Figure 309 Install parameters page- Software Management Timer.



6. In the **Software management timer** field, enter the amount of time, in hours and minutes, you want to defer the installation. For example, inFigure 116, the timer is set for two hours after the timer was configured (02:00).
7. Click **Apply**, then **Close** to close the Install Parameters page.

8.8 Backing Up and Restoring Configurations

You can import and export PTP 850 configuration files. This enables you to copy the system configuration to multiple PTP 850 units. You can also backup and save configuration files.

Configuration files can only be copied between units of the same type, i.e., PTP 850E to PTP 850E to PTP 850E.

This section includes:

- Configuration Management Overview (CLI)
- Setting the Configuration Management Parameters (CLI)
- Backing up and Exporting a Configuration File (CLI)
- Importing and Restoring a Configuration File (CLI)
- Editing CLI Scripts (CLI)

8.8.1 Configuration Management Overview

System configuration files consist of a zip file that contains three components:

A binary configuration file used by the system to restore the configuration.

A text file which enables users to examine the system configuration in a readable format. The file includes the value of all system parameters at the time of creation of the backup file.

An additional text file which enables you to write CLI scripts in order to make desired changes in the backed-up configuration. This file is executed by the system after restoring the configuration.

The system provides three restore points to manage different configuration files. Each restore point contains a single configuration file. Files can be added to the restore points by creating backups of the current system state or by importing them from an external server. For example, you may want to use one restore point to keep a last good configuration, another to import changes from an external server, and the third to store the current configuration.

You can apply a configuration file to the system from any of the restore points.

8.8.2 Viewing Current Backup Files

The system provides three restore points to manage different configuration files. Each restore point contains a single configuration file. Files can be added to the restore points by creating backups of the current system state or by importing them from an external server. For example, you may want to use one restore point to keep a last good configuration, another to import changes from an external server, and the third to store the current configuration.

To display the configuration files currently saved at the system restore points:

1. Select **Platform > Configuration > Backup Files**. The Backup Files page opens. For a description of the information provided in the Backup Files page, see Table 33 Backup Files Page Columns.

Figure 310 Backup Files Page

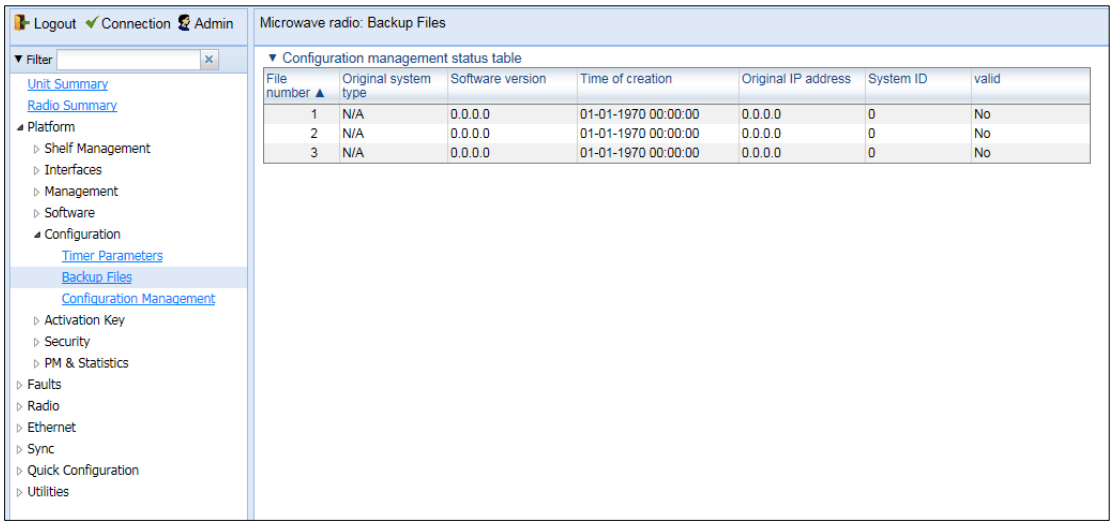


Table 33 Backup Files Page Columns

Parameter	Definition
File number	A number from 1 to 3 that identifies the restore point.
Original system type	The type of unit from which the backup configuration file was created.
Software version	The software version of the unit from which the backup configuration file was created.
Time of creation	The time and date on which the configuration file was created.
Original IP address	The IP address of the unit from which the configuration file was created.
System ID	The System ID, if any, of the unit from which the configuration file was created. This is taken from the **Name** field in the Unit Parameters page. See Configuring Unit Parameters.
Valid	Reserved for future use.

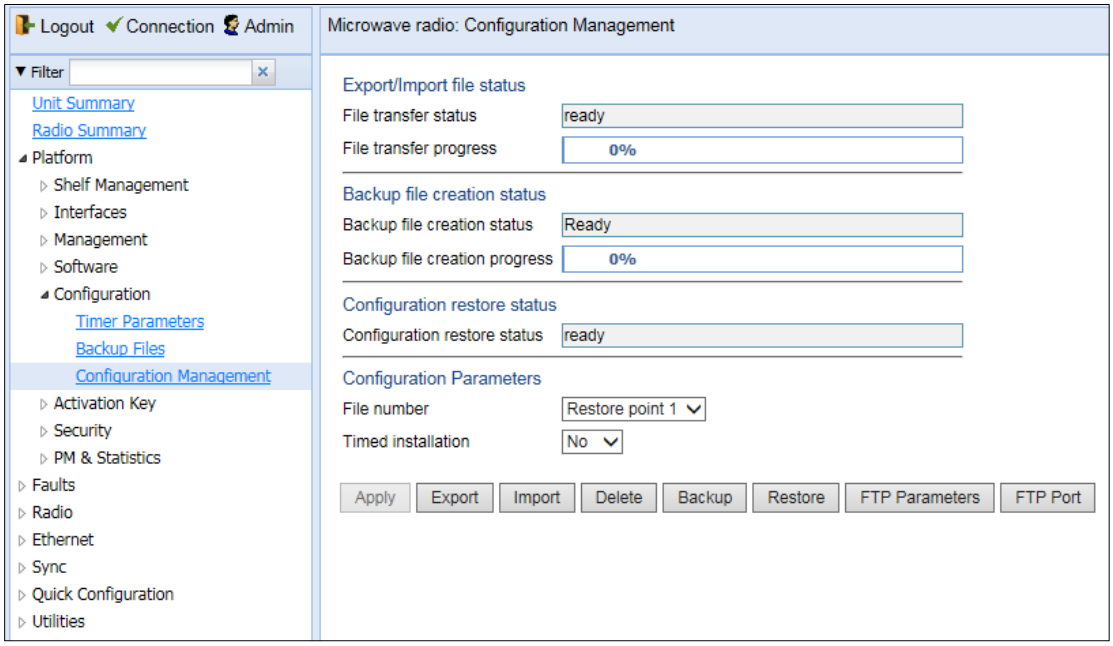
8.8.3 Setting the Configuration Management Parameters

When importing and exporting configuration files, the PTP 850 functions as an FTP or SFTP client. You must install FTP or SFTP server software on the PC or laptop you are using to perform the import or export. For details, see Installing and Configuring an FTP or SFTP Server.

Before importing or exporting a configuration file, you must perform the following steps:

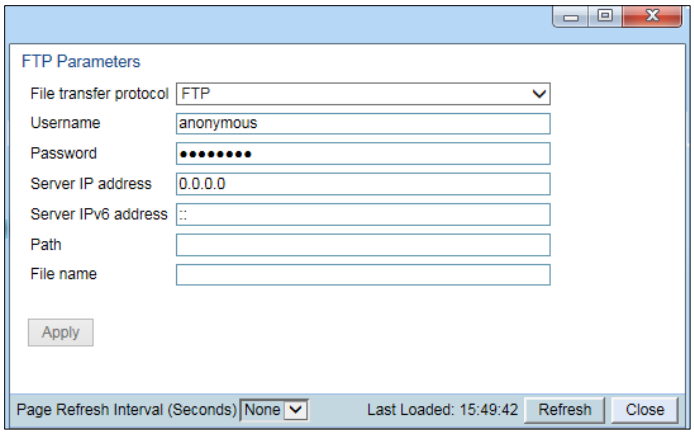
1. Verify that the system date and time are correct..
2. Install and configure an FTP server on the PC or laptop you are using to perform the import or export.
3. In the PTP 850E Web EMS, select **Platform > Configuration > Configuration Management**. The Configuration Management page opens.

Figure 311 Configuration Management Page



4. Click **FTP Parameters** to display the FTP Parameters page.

Figure 312 FTP Parameters Page



5. In the **File transfer protocol** field, select the file transfer protocol you want to use (**FTP** or **SFTP**).
6. In the **Username** field, enter the user name you configured in the FTP server.
7. In the **Password** field, enter the password you configured in the FTP server. If you did not configure a password for your FTP user, simply leave this field blank.
8. If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the FTP server in the **Server IP address** field. See Defining the IP Protocol Version for Initiating Communications.
9. If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the FTP server in the **Server IPv6 Address** field. See Defining the IP Protocol Version for Initiating Communications.
10. In the **Path** field, enter the location of the file you are downloading or uploading. If the location is the root shared folder, it should be left empty. If the location is a sub-folder under the root shared folder, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
11. In the **File name** field, enter the name of the file you are importing, or the name you want to give the file you are exporting.



Note

You must add the suffix **.zip** to the file name. Otherwise, the file import may fail. You can export the file using any name, then add the suffix **.zip** manually.

12. Click **Apply**, then **Close**, to save the FTP parameters and return to the Configuration Management page
13. In the **File number** field, select from three system restore points:

When you import a configuration file, the file is saved to the selected restore point, and overwrites whichever file was previously held in that restore point.

When you export a configuration file, the file is exported from the selected restore point.

When you back up the current configuration, the backup configuration file is saved to the selected restore point, and overwrites whichever file was previously held in that restore point.

When you restore a configuration, the configuration file in the selected restore point is the file that is restored.



Note

The **Timed installation** field is reserved for future use.

14. Click **Apply** to save your settings.

8.8.4 Exporting a Configuration File

You can export a saved configuration file from one of the system's three restore points to a PC or laptop.

To export a configuration file:

Exporting a Configuration File Via HTTP or HTTPS

To export a configuration file using HTTP or HTTPS:

1 Select Platform > Configuration > Configuration Management. The Configuration Management page opens.

2 Select **HTTP**.

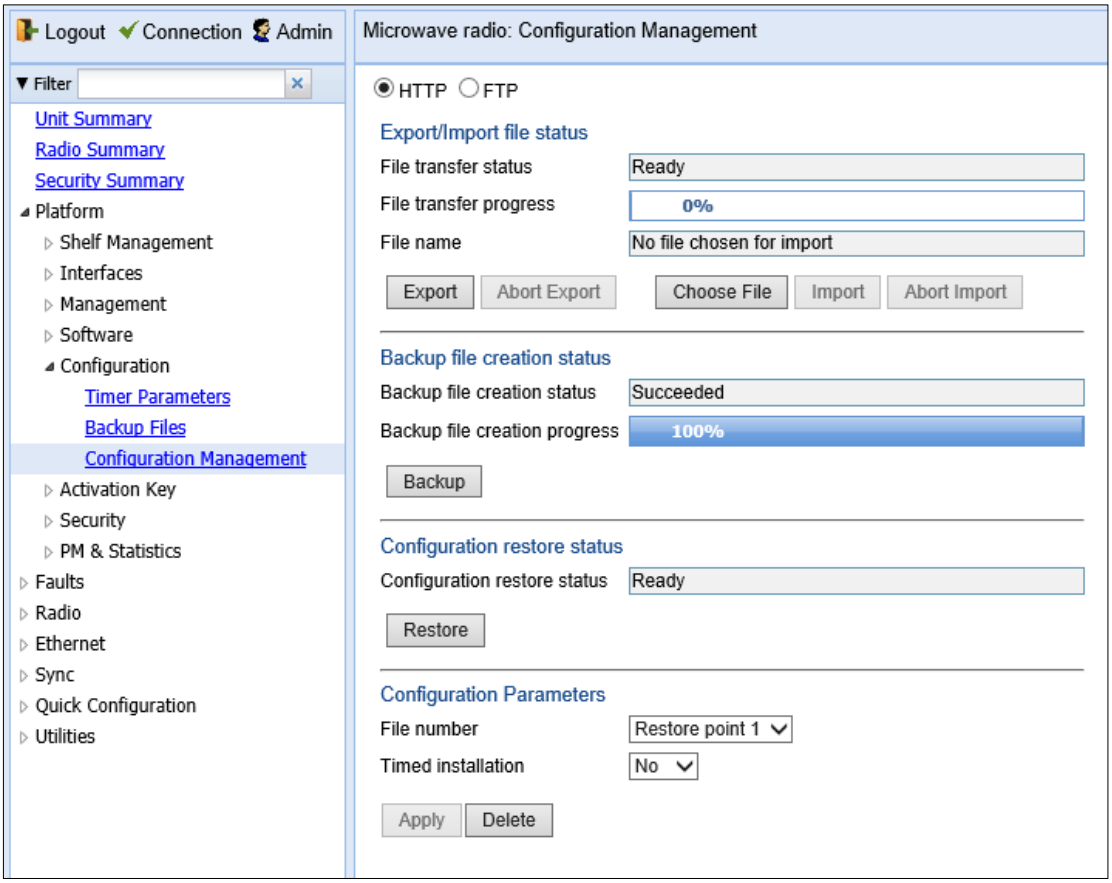


Figure 313 Configuration Management Page – HTTP/HTTPS

3 In the **File number** field, select the restore point from which to export the file.

Note: The Timed installation field is reserved for future use.

4 Click **Export**. The export begins. You can view the status of the export in the **File Transfer status** field in the Export/Import file status section. Possible values are:

- **Ready** - The default value, which appears when no import or export is in progress.
- **File-in-Transfer** – The file export is in progress.
- If an error occurs during the import or export, an appropriate error message is displayed in this field.

When the import or export is complete, one of the following status indications appears:

- Succeeded
- Failure

The next time the system is reset, the File Transfer status field returns to

Ready.

5 To abort the export, click Abort Export.

Exporting a Configuration File Via FTP or SFTP

To export a configuration file via FTP or SFTP:

1 Verify that you have followed all the steps in *Setting the FTP/SFTP Configuration Management Parameters*.

2 Select Platform > Configuration > Configuration Management. The Configuration Management page opens (*Figure 116*).

3 Select **FTP**.

4 In the File Number field, select the restore point from which you want to export the file.

Note: The Timed installation field is reserved for future use.

5 Click Apply to save your settings.

6 Click Export. The export begins. You can view the status of the export in the File Transfer status field in the Export/Import file status section. Possible values are:

- Ready – The default value, which appears when no import or export is in progress.
- File-in-Transfer – The file export is in progress.
- If an error occurs during the import or export, an appropriate error message is displayed in this field.

When the import or export is complete, one of the following status indications appears:

- Succeeded
- Failure

The next time the system is reset, the File Transfer status field returns to Ready.

8.8.5 Importing a Configuration File

You can import a saved configuration file from a PC or laptop to one of the system's three restore points. You can use FTP, SFTP, HTTP, or HTTPS to export a configuration file.To import a configuration file:

Importing a Configuration File Via HTTP or HTTPS

1. Select **Platform > Configuration > Configuration Management**. The Configuration Management page opens (Figure 311).
2. In the **File Number** field, select the restore point to which you want to import the file.
3. Click **Apply** to save your settings.
4. Click **Import**. The import begins. You can view the status of the import in the **File Transfer status** field in the Export/Import file status section. Possible values are:

Ready – The default value, which appears when no import or export is in progress.

File-in-Transfer – The file import is in progress.

If an **error** occurs during the import or export, an appropriate error message is displayed in this field.

When the import or export is complete, one of the following status indications appears:

Succeeded

Failure

The next time the system is reset, the File Transfer status field returns to

Ready.

After importing the configuration file, you can apply the configuration by restoring the file from the restore point to which you saved it. See Restoring a Saved Configuration.

Importing a Configuration File Via FTP or SFTP

To import a configuration file using FTP or SFTP:

Verify that you have followed all the steps in Setting the FTP/SFTP Configuration Management Parameters.

Select Platform > Configuration > Configuration Management. The Configuration Management page opens (Figure 202).

Select FTP.

In the File Number field, select the restore point to which you want to import the file. The imported file will be saved to the selected restore point, and will overwrite whatever file was previously held in that restore point.

Click Apply to save your settings.

Click Import. The import begins. You can view the status of the import in the File Transfer status field in the Export/Import file status section. Possible values are:

Ready – The default value, which appears when no import or export is in progress.

File-in-Transfer – The file import is in progress.

If an error occurs during the import or export, an appropriate error message is displayed in this field.

When the import or export is complete, one of the following status indications appears:

Succeeded

Failure

The next time the system is reset, the File Transfer status field returns to Ready.

After importing the configuration file, you can apply the configuration by restoring the file from the restore point to which you saved it.

8.8.6 Deleting a Configuration File

You can delete a saved configuration file from any of the system's three restore points:

To delete a configuration file:

1. Select **Platform > Configuration > Configuration Management**. The Configuration Management page opens (Figure 311).
2. In the **File Number** field, select the restore point that holds the configuration file you want to delete.
3. Click **Delete**. The file is deleted.

8.8.7 Backing Up the Current Configuration

You can back up the current configuration file to one of the system's three restore points.

To back up a configuration file:

1. Select **Platform > Configuration > Configuration Management**. The Configuration Management page opens (Figure 311).
2. In the **File Number** field, select the restore point to which you want to back up the file. If another configuration file is already saved to that restore point, it will be overwritten by the file you back up.
3. Click **Backup**. The backup begins. You can view the status of the backup in the **Backup file creation status** field. Possible values in the status field are:

Ready – The default value, which appears when no backup is in progress.

Generating file – The system is verifying the files to be backed up.

If an error occurs during the backup, an appropriate error message is displayed in this field.

When the backup is complete, one of the following status indications appears:

Succeeded

Failure

The next time the system is reset, the **Backup file creation status** field returns to **Ready**.

8.8.8 Restoring a Saved Configuration

You can replace the current configuration with any configuration file saved to one of the system's three restore points by restoring the configuration file from the restore point.

To restore a configuration file:

1. Select **Platform > Configuration > Configuration Management**. The Configuration Management page opens (Figure 311 Configuration Management Page).
2. In the **File Number** field, select the restore point that holds the configuration you want to restore.
3. Click **Restore**. The configuration restoration begins. You can view the status of the restoration in the **Configuration restore status** field.



Note

While a configuration restoration is taking place, no user can make any changes to the configuration. All system configuration parameters are read-only during the configuration restoration.

8.8.9 Editing CLI Scripts

The configuration file package includes a text file that enables you to write CLI scripts in a backed-up configuration that are executed after restoring the configuration.

To edit a CLI script:

1. Back up the current configuration to one of the restore points.
2. Export the configuration from the restore point to a PC or laptop.
3. On the PC or laptop, unzip the file *Configuration_files.zip*.
4. Edit *the cli_script.txt* file using clish commands, one per line.
5. Save and close the *cli_script.txt* file, and add it back into the *Configuration_files.zip* file.
6. Import the updated Configuration_files.zip file back into the unit.
7. Restore the imported configuration file. The unit is automatically reset. During initialization, the CLI script is executed, line by line.



Note

If any specific command in the CLI script requires reset, the unit is reset when that that command is executed. During initialization following the reset, execution of the CLI script continues from the following command.

8.9 Setting the Unit to the Factory Default Configuration

You can restore the unit to its factory default configuration, while retaining the unit's IP address settings and logs.

To restore the factory default settings:

1 Select **Platform > Shelf Management > Chassis Configuration**. The Chassis Configuration page opens.

Note: This page is only available in Advanced mode. A limited version, without the drag-and-drop functionality, is available in Basic view by selecting **Device View**.

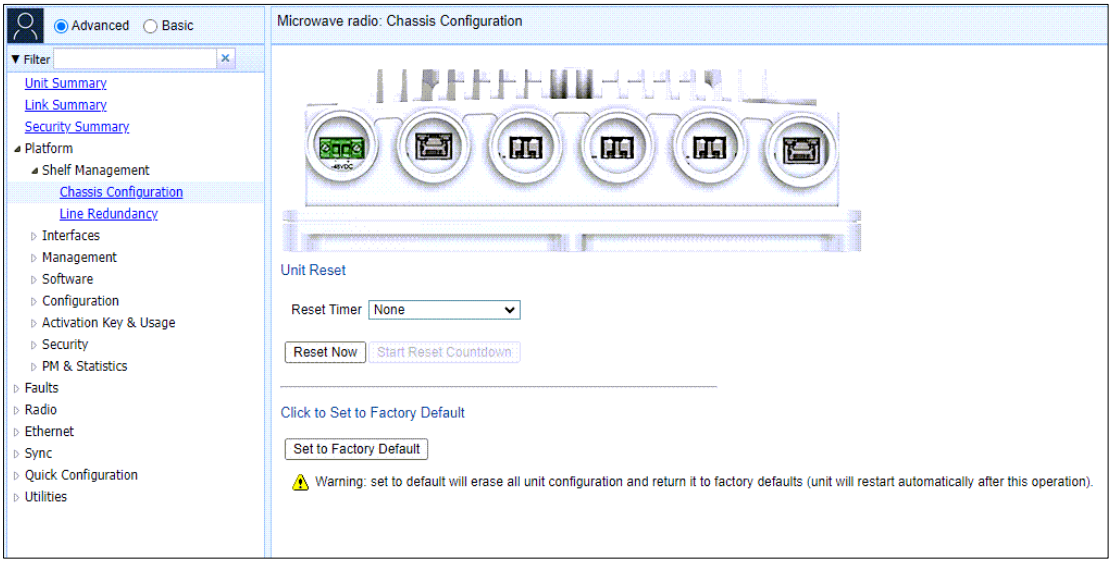


Figure 314: Chassis Configuration Page – PTP 850C

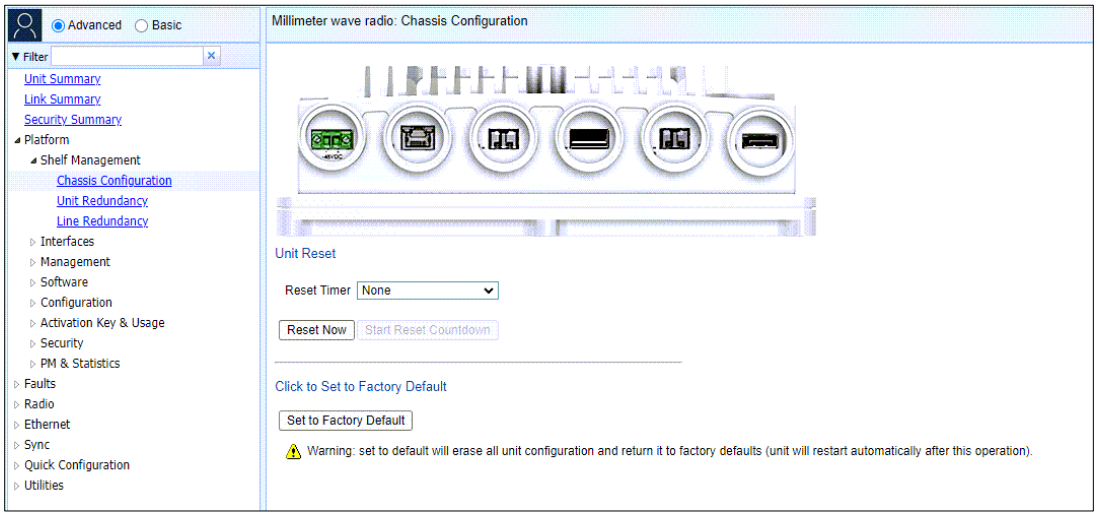


Figure 315: Chassis Configuration Page – PTP 850E

2 Click **Set to Factory Default**. The unit is restored to its factory default settings. This does not change the unit's IP address or FIPS configuration.

8.10 Performing a Unit Reset

You can reset the unit. You can also use a timer to schedule a unit reset at a later time.

To initiate an immediate reset of the unit:

1 Select **Platform > Shelf Management > Chassis Configuration**. The Chassis Configuration page opens.
2 Click **Reset Now**.
3 A prompt appears asking if you want to proceed with the reset. Click **Yes** to initiate the reset.

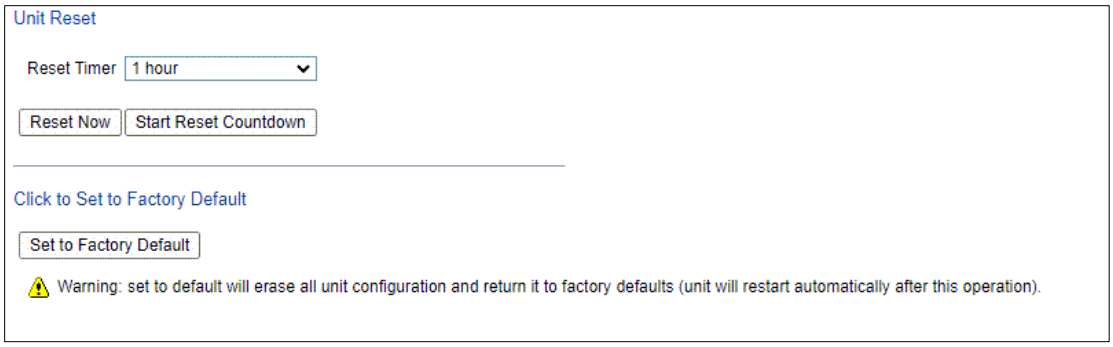
The unit is reset.

To configure a timed reset of the unit:

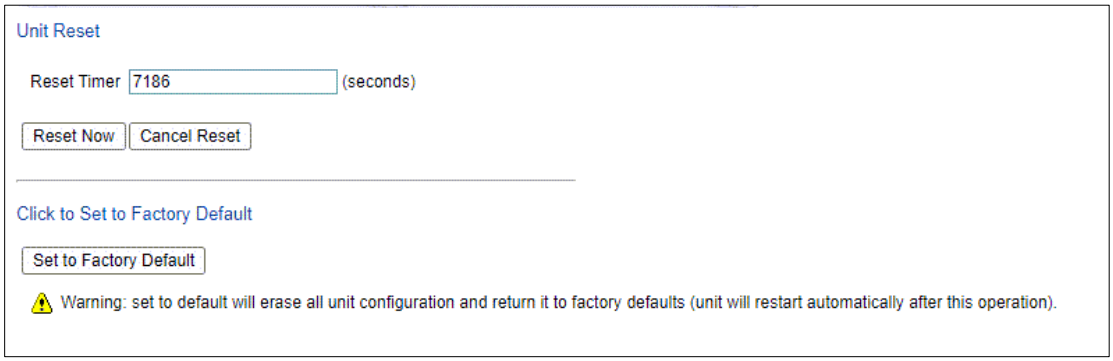
1 Select **Platform > Shelf Management > Chassis Configuration**. The Chassis Configuration page opens.
2 In the **Reset Timer** field, select from the following options:

- 30 seconds
- 1 minute
- 5 minutes
- 10 minutes
- 15 minutes
- 30 minutes
- 45 minutes
- 1 hour
- 2 hours
- 4 hours
- 8 hours
- 12 hours
- 24 hours

3 When you select a value, a new field appears called **Start Reset Countdown**. Click **Start Reset Countdown** to start the timer.



4 A prompt appears asking if you want to proceed with the reset. Click **Yes** to initiate the reset timer.
5 Once you click **Yes**, a new field appears called **Cancel Reset**. If you want to cancel the reset timer, click **Cancel Reset**.



Note: You can set a reset timer with granularity of one second and longer available timers via the CLI.

Configuring Unit Parameters

To view and configure system information:

1. Select **Platform > Management > Unit Parameters**. The Unit Parameters page opens. Table **34** describes the fields in the Unit Parameters page.

Figure 316 Unit Parameters Page

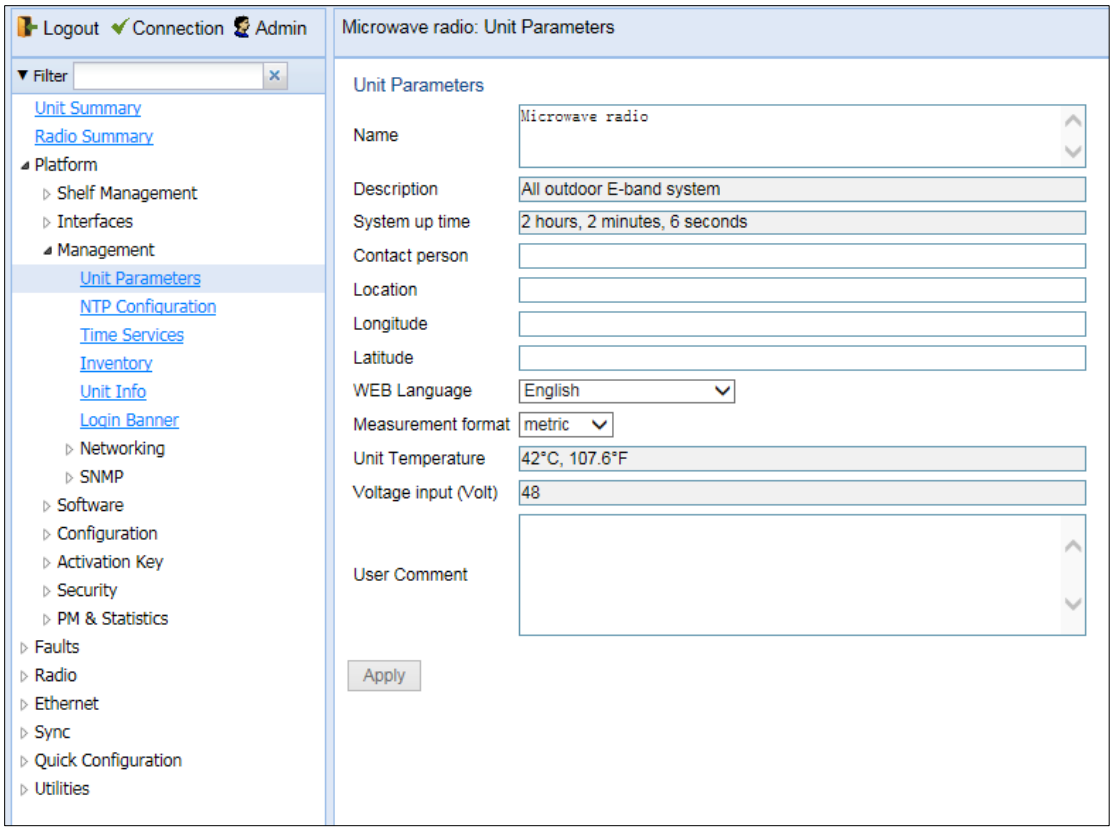


Table 34 Unit Parameters

Parameter	Definition
Name	A name for the unit (optional, up to 128 characters). This name appears at the top of every Web EMS page.
Description	Descriptive information about the unit. This information is used for debugging, and should include information such as the unit type.
System up time	The time since the system was last reinitialized.
Contact person	The name of the person to be contacted if and when a problem with the system occurs (optional).
Location	The actual physical location of the node or agent (optional).
Longitude	The unit's longitude coordinates.
Latitude	The unit's latitude coordinates.

Parameter	Definition
Web Language	Enables you to select the language in which the Web EMS is displayed. In release 11.1, the following languages are available: •English (default) •Russian
Measurement format	The type of measurement you want the system to use: **Metric** or **Imperial**.
Unit Temperature	The current temperature of the unit. If the unit temperature goes lower than -40°C or higher than 90°C, the unit raises an extreme temperature alarm (Alarm ID 25). This alarm is cleared when the unit temperature rises above -37°C or goes below 87°C.
Voltage input (Volt)	The voltage input of the unit.
User Comment	A free text field for any information you want to record (up to 500 characters).

8.11 Configuring NTP

PTP 850E supports Network Time Protocol (NTP). NTP distributes Coordinated Universal Time (UTC) throughout the system, using a jitter buffer to neutralize the effects of variable latency.

You can configure up to four NTP servers. Each server can be configured using IPv4 or IPv6. When multiple servers are configured, the unit chooses the best server according to the implementation of Version 4.2.6p1 of the NTPD (Network Time Protocol Daemon). The servers are continually polled. The polling interval is determined by the NTPD, to achieve maximum accuracy consistent with minimum network overhead.

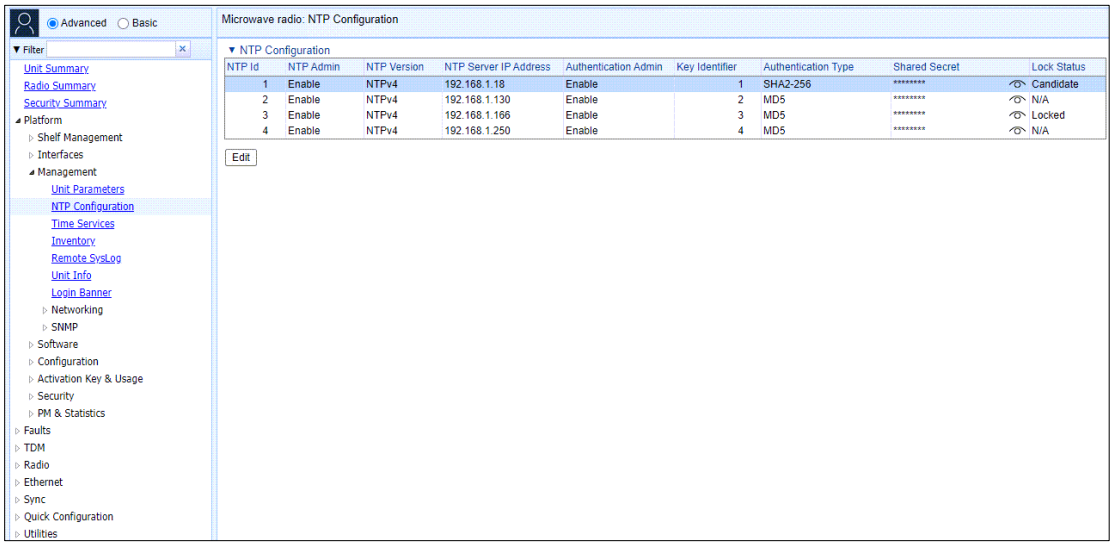
Optionally, for extra security you can enable NTP authentication, as defined in the NTP specification (IETF RFC 5905). NTP authentication enables the client to verify the authenticity of the NTP server before synchronizing its clock with the server's time. This can help prevent man-in-the-middle attacks and other types of threats that could manipulate the client's clock by providing it with false time information.

NTP authentication requires the client and server to have a shared secret key that is used to authenticate the NTP messages exchanged between them. You can define the shared key for the client on the device, as described below.

To view and configure the NTP Parameters:

1. Select **Platform > Management > NTP Configuration**. The NTP Configuration page opens.

Figure 317 NTP Configuration Page



Select a row in the NTP Configuration table and click **Edit**. The NTP Configuration Edit page opens.

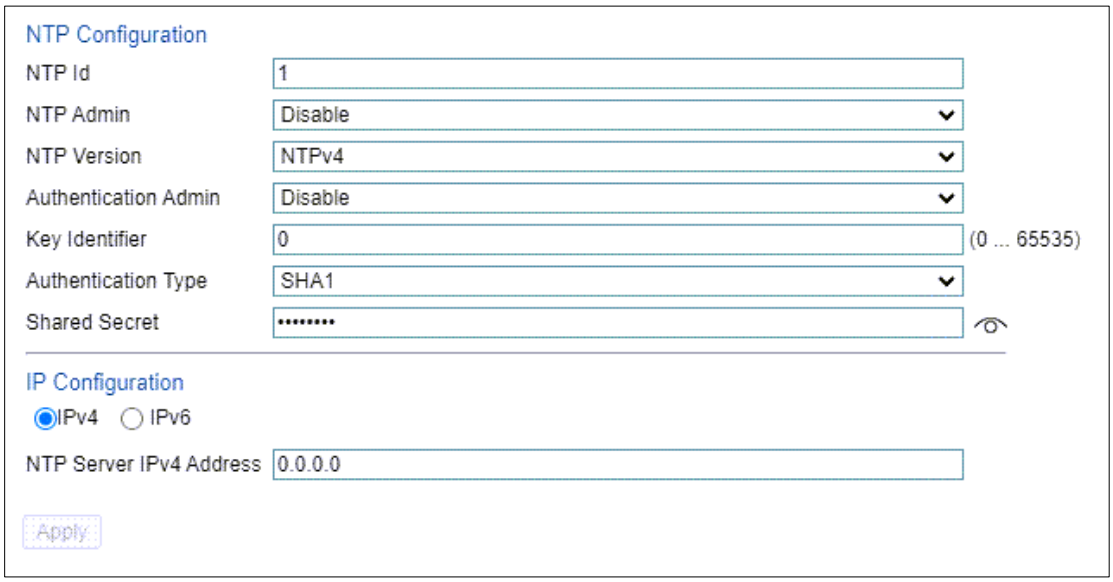


Figure 318: NTP Configuration Edit Page (Disabled)

1 In the **NTP Admin** field, select **Enable**.
2 In the **NTP version** field, select the NTP version you want to use. Options are **NTPv3** and **NTPv4**. NTPv4 provides interoperability with NTPv3 and with SNTP.
3 In the **Authentication Admin** field, select **Enable** to enable NTP authentication or **Disable** to disable NTP authentication. By default, NTP authentication is disabled.

4 If you are enabling NTP authentication, enter a key identifier (1-65535) in the **Key Identifier** field. The key identifier as included in the client requests and identifies the shared secret the client is using for message authentication.

   If you are not enabling NTP authentication, leave the default value of 0 in the **Key Identifier** field.

5 If you are enabling NTP authentication, select a message authentication code type in the **Authentication Type** field. Options are:

   - **MD5**
   - **SHA1 (default)**
   - **SHA2-256**

   If you are not enabling NTP authentication, you can leave the default value of **SHA1**.

6 If you are enabling NTP authentication, enter the shared secret in the **Shared Secret** field. The length of the shared secret depends on the authentication type:

   - **MD5** – 8-32 characters
   - **SHA1 (default)** – 8-40 characters
   - **SHA2-256** – 8-64 characters

7 In the **IP Configuration** section, select **IPv4** or **IPv6**.

Note: For each NTP server, you can define an IPv4 address or an IPv6 address but not both.

8 In the **NTP server IPv4 address** or **NTP server IPv6 address** field, enter the IP address of the NTP server.

9 Click **Apply**. Once you click **Apply**, the NTP Status Parameters appear. Table 35 describes the NTP Status Parameters.

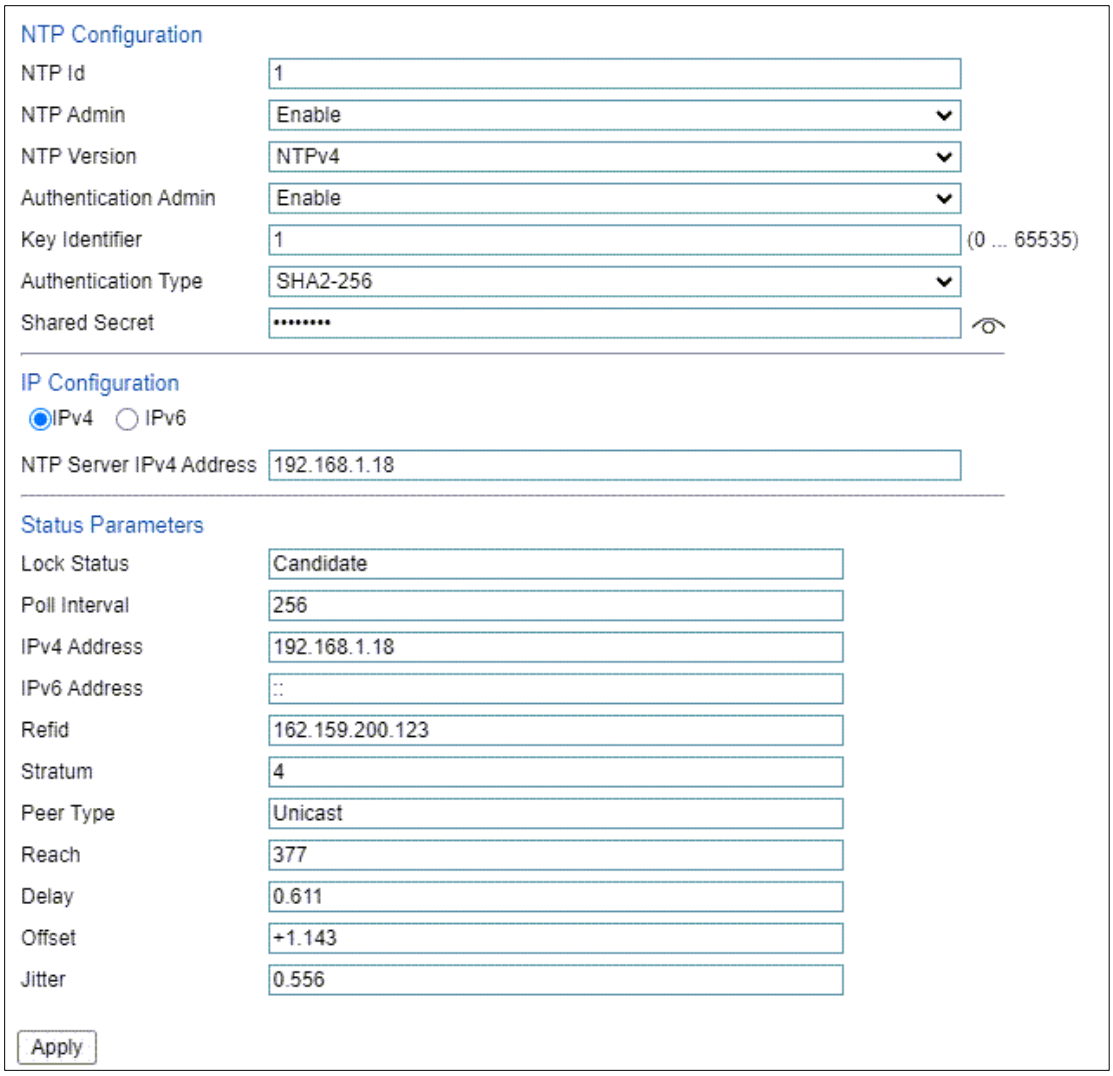


Figure 319: NTP Configuration Edit Page (Enabled)

10 Repeat these steps for each NTP server you want to configure, up to four servers.

Table 35 NTP Status Parameters

Para	Definition
Lock status	Indicates the status of each NTP server. Possible values are: • Locked – The NTP client is locked on this server. • Candidate – This server is next in line to be selected if the currently locked server is discarded. • Secondary – This server is not the next in line to be selected but is considered a good server if needed. • Unreliable – This server was checked but was determined not to be reliable.

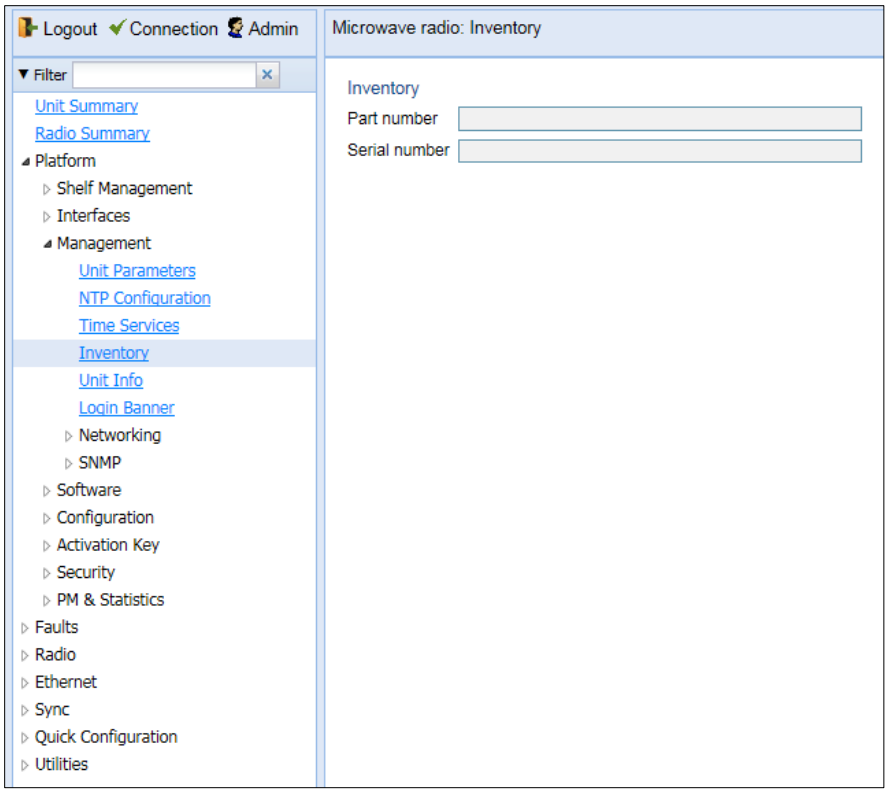
Poll Interval	The amount of time between successive requests made by the device, as NTP client, to an NTP server in order to remain synchronized. This parameter is set automatically and is read-only.
IPv4	The IPv4 address of the NTP server (if configured).
IPv6	The IPv6 address of the NTP server (if configured).
Refid	The NTP client time server.
Stratu	The NTP client statum..
Peer	The server peer type.
Reach	The result of the last 8 polls in octal form.
Delay	The round trip delay to peer in milliseconds.
Offset	Offset to the client in milliseconds.
Jitter	Variance in latency on the network.

8.12 Displaying Unit Inventory

To view the unit's part number and serial number:

Select **Platform > Management > Inventory**. The Inventory page opens, showing the unit's part number and serial number.

Figure 320 Inventory Page



8.13 Displaying SFP DDM and Inventory Information

Static and dynamic monitoring is available for SFP, SFP+, QSFP, and CSFP transceivers used in ports P3 (Eth2), P4 (Eth3, Eth4, Eth5, Eth6), and P5 (Eth7).

Dynamic monitoring (DDM) PMs are also available.

Note

DDM parameters are not relevant for electrical SFPs.

8.13.1 SFP DDM Alarms

The following alarms are available in connection with SFP DDM and inventory monitoring. The polling interval for these alarms is one minute.

- Alarm #803- SFP port RX power level is too low.
- Alarm #804 – SFP port RX power level is too high.
- Alarm #805- SFP port TX power level is too low.
- Alarm #806 – SFP port TX power level is too high.
- Alarm #809 – SFP port supply voltage is too low.
- Alarm #810 – SFP port supply voltage is too high.
- Alarm #811 – SFP Rx power low threshold crossing.

- Alarm #812 – SFP Rx power high threshold crossing.

  Alarms 803 through 810are based on thresholds defined by the SFP transceivers vendor, which are static.

  Alarms 811 and 812 are based on user-configurable thresholds. For more information and instructions how to configure these thresholds, see Displaying PMs about an SFP transceivers and Configuring SFP RX Power Thresholds.

  If there is no signal on the interface, a Loss of Carrier alarm (LOC) is raised, and this alarm masks the DDM alarms, except the SFP port supply voltage alarms.

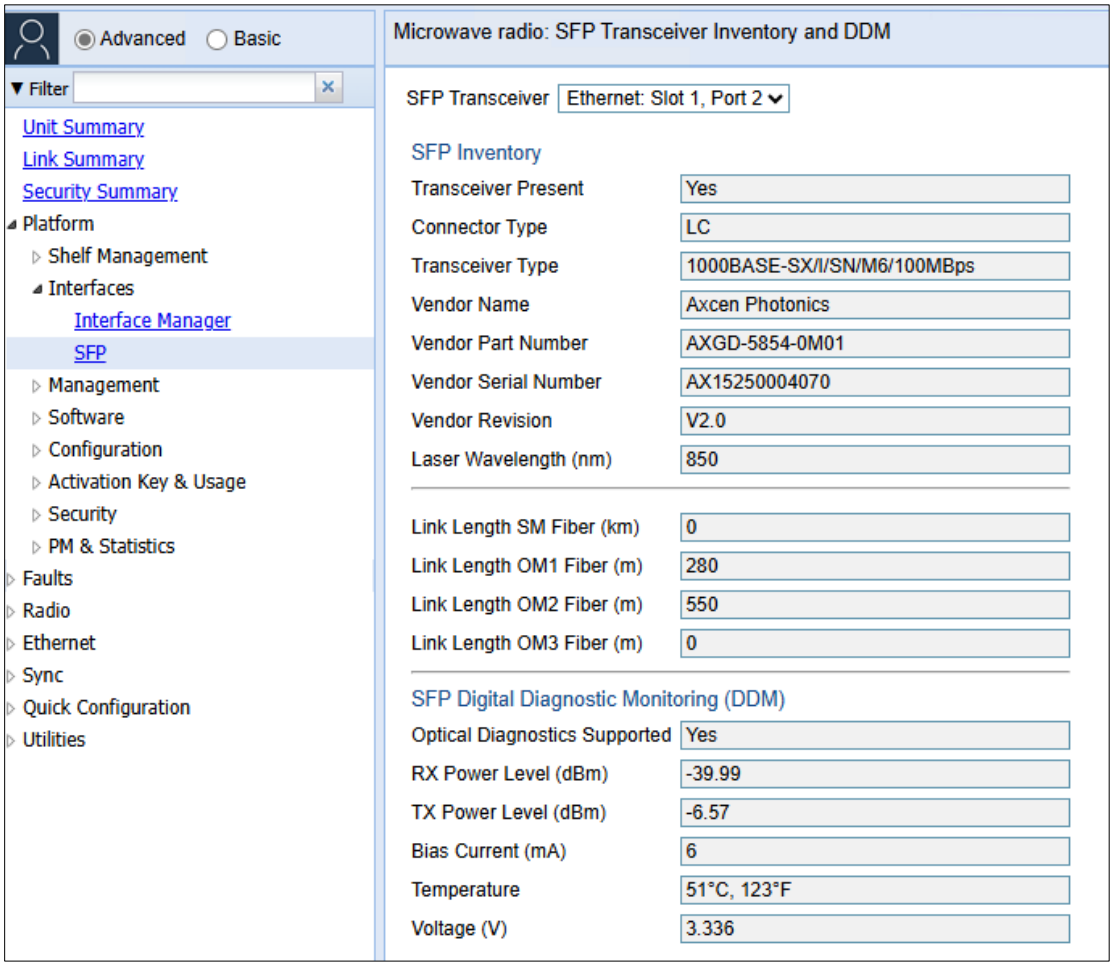
8.13.2 Displaying Information about an SFP transceiver

To display information about an SFP transceiver:

1. Select **Platform** > **Interfaces** > **SFP**. The SFP Transceiver Inventory and DDM page opens.

   - The SFP Inventory section displays static information about the SFP transceiver.
   - The SFP Digital Diagnostic Monitoring (DDM) section displays dynamic information about the current state of the SFP transceiver.

Figure 321 SFP Transceiver Inventory and DDM Page



In the SFP **Transceiver** field, select the SFP interface about which you want to display information.

Table 36 SFP Inventory Parameters

Parameter	Description
Transceiver Present	Indicates whether an SFP transceiver is attached to the interface.
Connector Type	Always displays LC.
Transceiver Type	Displays a description of the SFP transceiver.
Vendor Name	Displays the name of the SFP's vendor.
Vendor Part Number	Displays the vendor's part number for the SFP transceiver.
Vendor Serial Number	Displays the vendor's serial number for the SFP transceiver.
Vendor Revision	Displays the revision number of the serial number provided by the vendor for the SFP transceiver.
Laser Wavelength (nm)	Display's the SFP module's laser wavelength. This parameters is not relevant for copper SFPs.
Link Length SM Fiber (km)	The maximum length of the cable (in km) for single mode fiber cables.
Link Length OM1 Fiber (m)	The maximum length of the cable (in meters) for OM1 multi-mode fiber cables.
Link Length OM2 Fiber (m)	The maximum length of the cable (in meters) for OM2 multi-mode fiber cables.
Link Length OM3 Fiber (m)	The maximum length of the cable (in meters) for OM3 multi-mode fiber cables.

Table 37 SFP Digital Diagnostic Monitoring (DDM) Parameters

Parameter	Description
Optical Diagnostics Supported	Displays whether the SFP transceiver supports DDM monitoring. For modules that do not support DDM monitoring, the parameters below are not available.
RX Power Level (dBm)	The SFP transceivers current RX power signal strength (in dBm).
TX Power Level (dBm)	The SFP transceivers current TX power signal strength (in dBm).
Bias Current (mA)	The laser bias current of the SFP transceivers (in mA)
Temperature	The current temperature of the SFP transceivers (displayed in both C° and F°).
Voltage (V)	The supply voltage (VCC) currently being received by the SFP transceivers (if available).



Note

Tx Power level DDM is not supported for QSFP (P4) – not part of the standard.

If no signal is being received, RX Power Level is displayed as -40 dBm.

If the Admin status of the port is Down, the TX Power Level is displayed as -40 DBm and the Bias Current is displayed as 0 mA.

The Temperature is always shown as long as the SFP transceivers is inserted in the port.

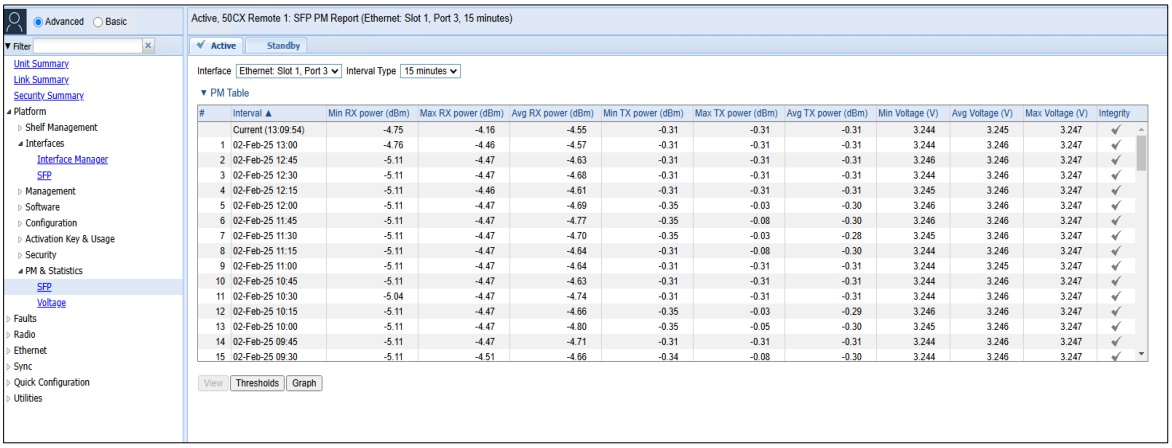
8.13.3 Displaying PMs about an SFP transceiver and Configuring SFP RX Signal Power Thresholds

The SFP PM Report page displays DDM PMs and enables you to configure high and low SFP RX power thresholds for each interface with an SFP. If these thresholds are exceeded, an alarm is raised. For details, see SFP DDM Alarms.

To display DDM PMs:

1. Select **Platform** > **PM & Statistics** > **SFP**. The SFP PM Report page opens.

Figure 322 SFP PM Report Page



2. In the **Interface** field, select the interface for which you want to display PMs.
3. In the **Interval Type** field:
   - To display reports for the past 24 hours, in 15 minute intervals, select **15 minutes**.
   - To display reports for the past month, in daily intervals, select **24 hours**.

Note

No entries are displayed if the SFP device does not support DDM, or if the Admin status of the interface is Down.

DDM PMs are not persistent, which means they are not saved in the event of unit reset. RX and TX power levels are collected five times per 15-minute interval. 15-minute PM data is saved for 24 hours. 24-hour PM data, which is updated every 15 minutes, is saved for 30 days.

To set the high and low SFP RX power thresholds:

1 In the **Interface** field of the SFP PM Report page, click **Thresholds**. The Thresholds Configuration – Edit page opens.

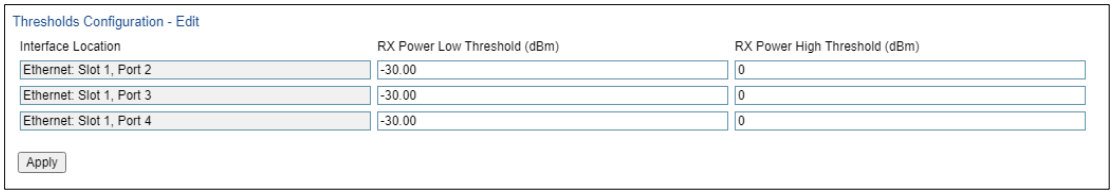


Figure 323: SFP RX Power Thresholds Configuration – Edit Page (PTP 850C)

2 For each interface with an SFP, enter the thresholds:
   - **RX Power Low Threshold** – -40 dBm to +10 dBm. Default value: 0 dBm.
   - **RX Power High Threshold** – -40 dBm to +10 dBm. Default value: -25 dBm.

3 Click **Apply**, then **Close**.

Table 38 DDM PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Min RX Power (dBm)	The minimum RX power during the interval (dBm).
Max RX Power (dBm)	The maximum RX power during the interval (dBm).
Avg RX Power (dBm)	The average RX power during the interval (dBm).
Min TX Power (dBm)	The minimum TX power during the interval (dBm).
Max TX Power (dBm)	The maximum TX power during the interval (dBm).
Avg TX Power (dBm)	The average TX power during the interval (dBm).
Min Voltage (V)	The minimum voltage (VCC) received by the SFP transceiver during the interval.
Avg Voltage (V)	The average voltage (VCC) received by the SFP transceiver during the interval.
Max Voltage (V)	The maximum voltage (VCC) received by the SFP transceiver during the interval.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable. Possible causes are (i) an LOC alarm, (ii) changing the Admin status of the interface, or (iii) unit reset.

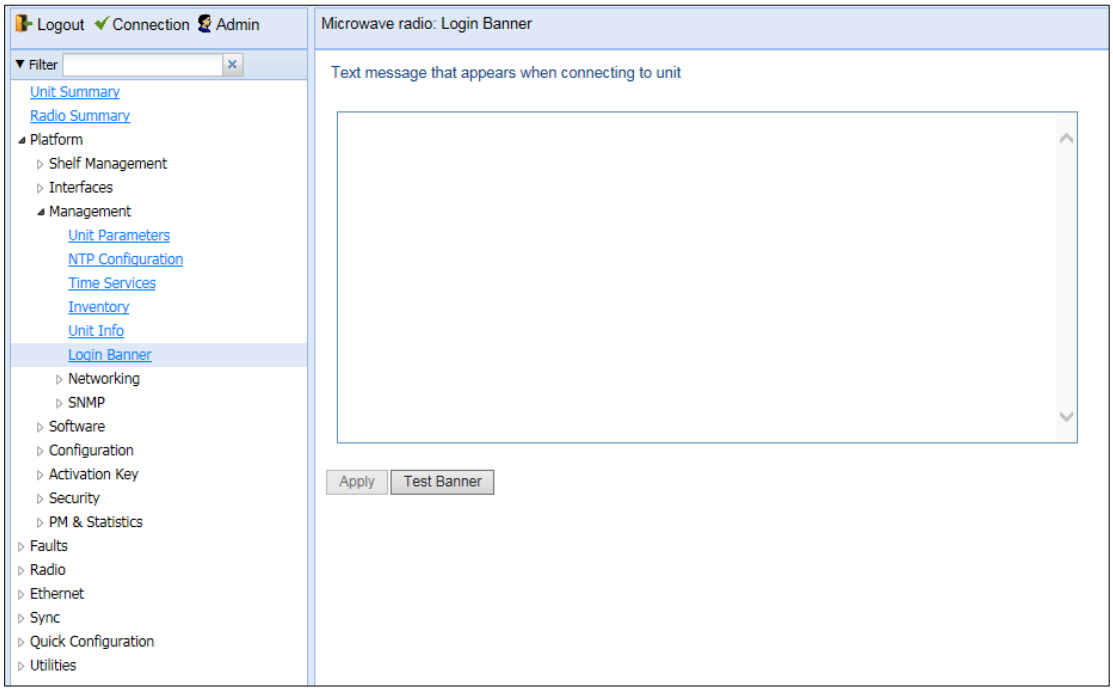
8.14 Defining a Login Banner

You can define a login banner of up to 2,000 bytes. This banner will appear every time a user establishes a connection with the Web EMS. The banner appears before the login prompt, so that users will always see the login banner and must manually close the banner before logging in to the Web EMS.

To define a login banner:

1 Select **Platform** > **Management** > **Login Banner**. The Login Banner page opens.

Figure 324 Login Banner Page



2 Enter a text message of up to 2,000 bytes.
3 To display a test banner as it will appear to users, click **Test Banner**.
4 Click **Apply**.

9. Radio Configuration

This section includes:

- Viewing the Radio Status and Settings
- Configuring the Remote Radio Parameters
- Configuring ATPC and ATPC Override Timer
- Configuring AES-256 Payload Encryption
- Configuring and Viewing Radio PMs and Statistics

Related topics:

- Configuring the Radio Parameters
- Configuring the Radio (MRMC) Script(s)
- Configuring XPIC
- Configuring 1+1 HSB Unit Protection
- Performing Radio Loopback

9.1 Viewing the Radio Status and Settings

You can configure the radios and display the radio parameters in the Radio Parameters page.

Note

For instructions how to configure the radio parameters.

To display the radio parameters:

1. Select **Radio > Radio Parameters**. The Radio Parameters page opens. Select the carrier you want to configure and click **Edit** to display the Radio Parameters page for that carrier.

Note

To clear all defective blocks that have been counted for all radio carriers, click **Clear All Defective Blocks**.

Figure 325 Radio Parameters Page

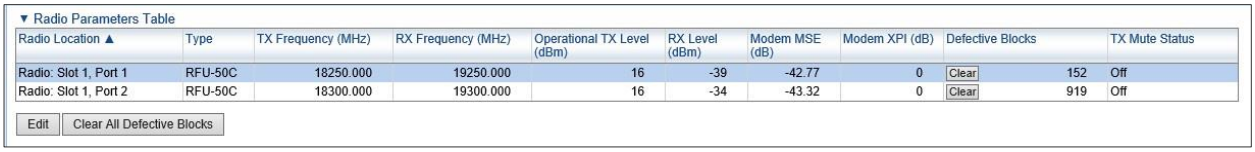


Figure 326 Radio Parameters Page – PTP 850C

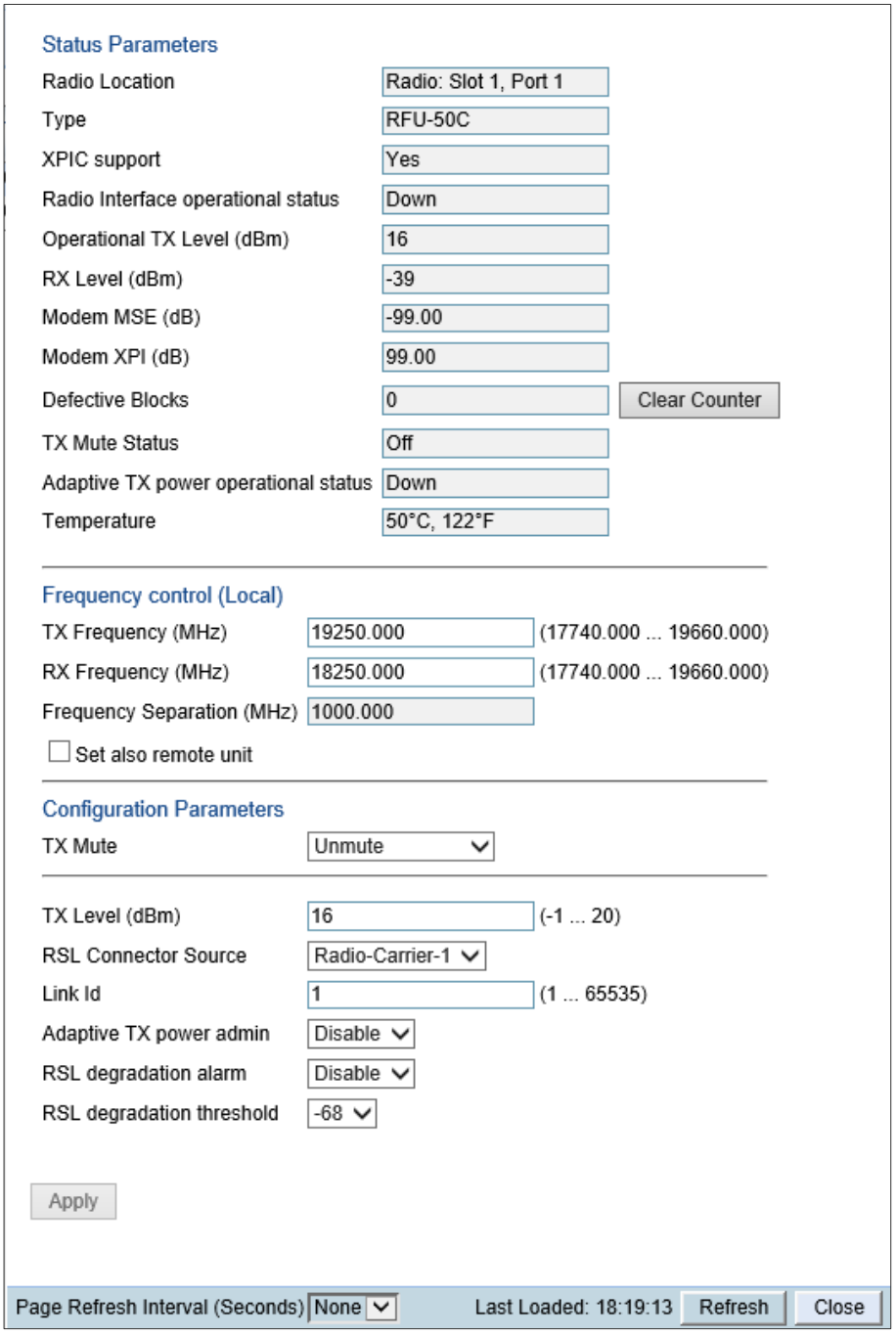


Figure 327 Radio Parameters Page – PTP 850S

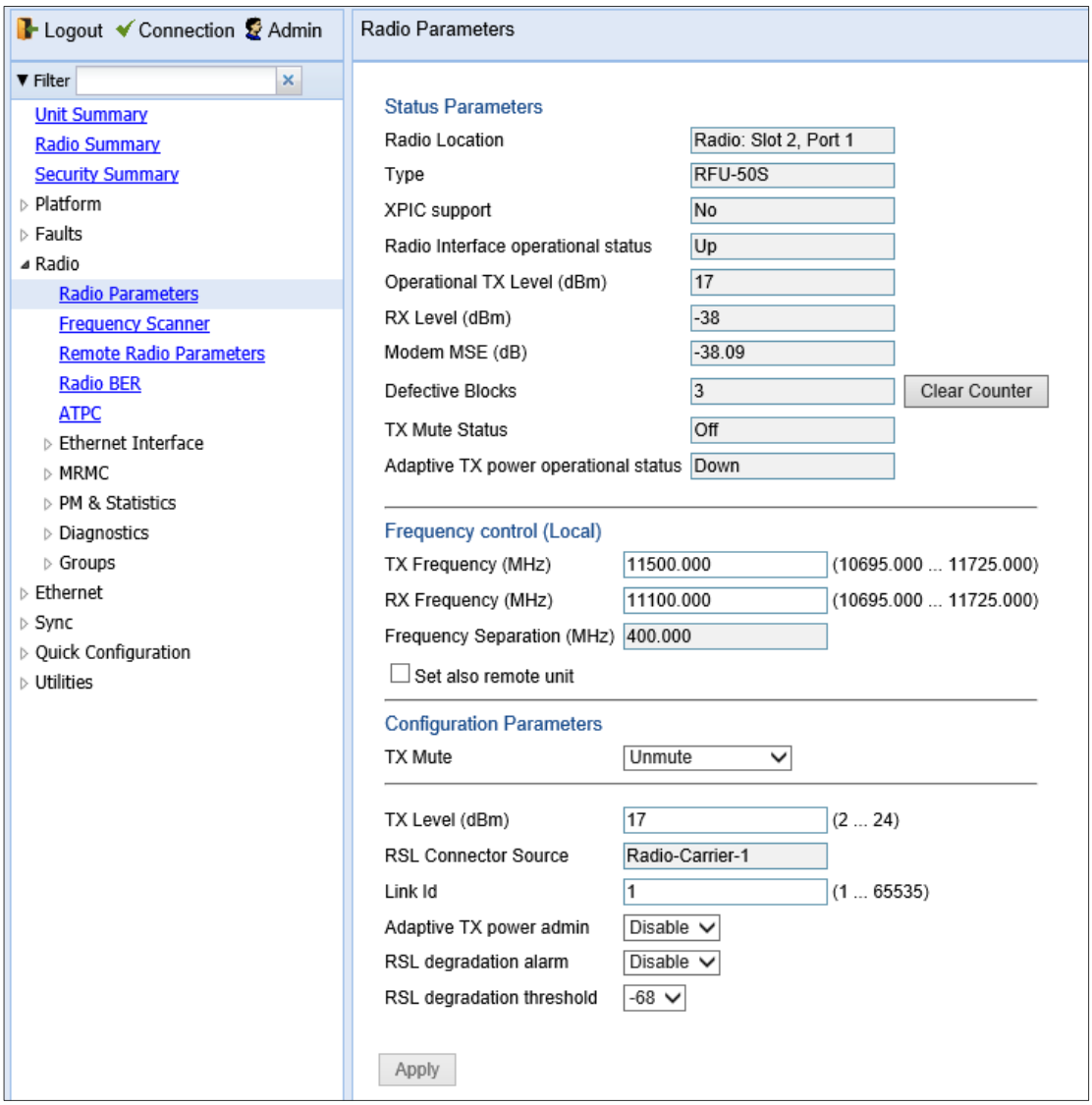


Figure 328 Radio Parameters Page – PTP 850E

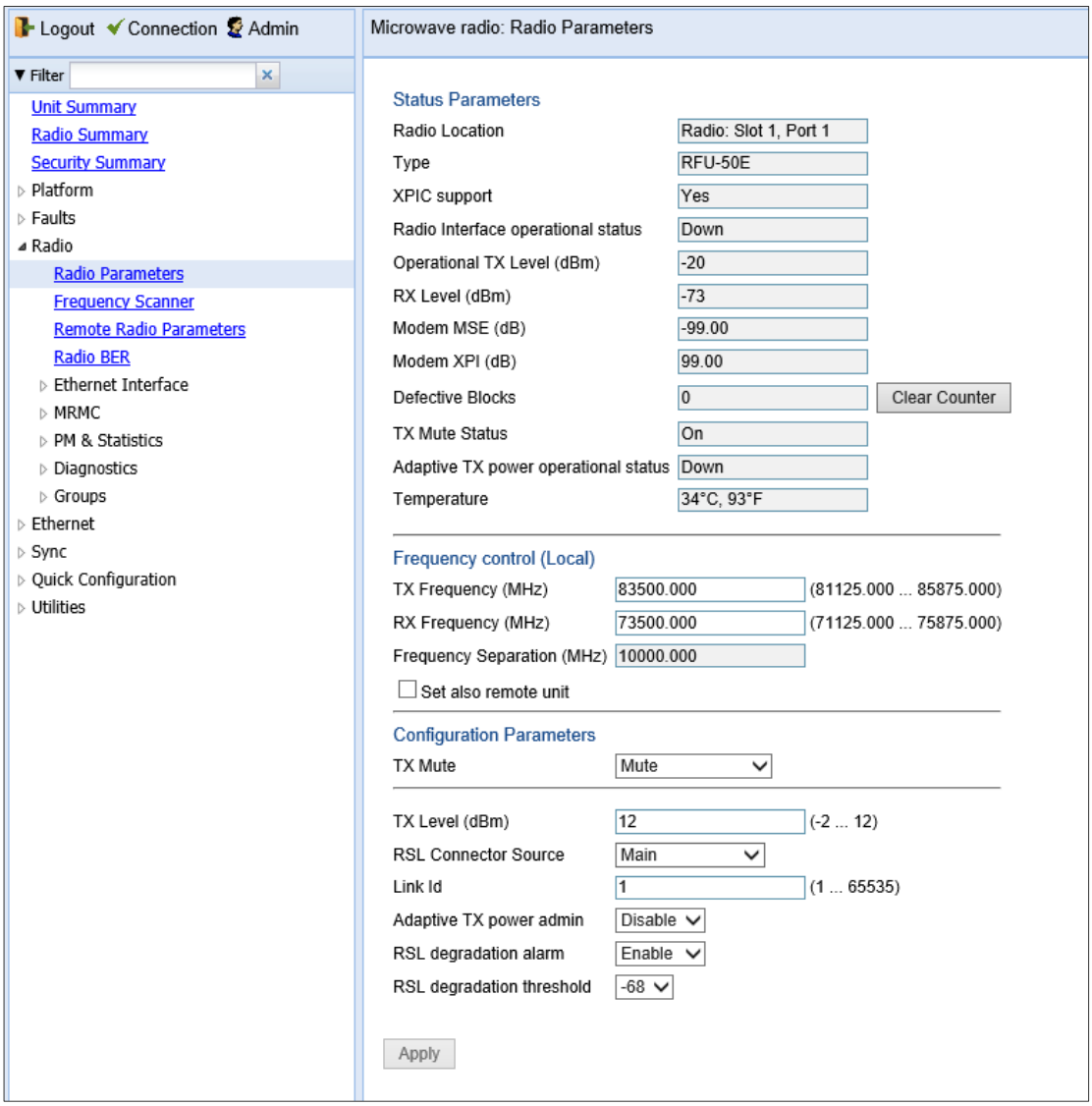


Table 39 lists and describes the parameters displayed in the **Status parameters** section of the Radio Parameters page.

Table 39 Radio Status Parameters

Parameter	Description
Type	The RF module type.
XPIC Support	Reserved for future use.
Radio Interface operational status	Indicates whether the carrier is operational (Up) or not operational (Down).
Operational TX Level (dBm)	The actual TX signal level (TSL) of the carrier (in dBm).
RX Level (dBm)	The actual measured RX signal level (RSL) of the carrier (in dBm).
Modem MSE (dB)	The MSE (Mean Square Error) of the RX signal, measured in dB. A value of 0 means that the modem is not locked.
Modem XPI (dB)	The XPI (Cross Polarization Interference) level, measured in dB.
Defective Blocks	The number of defective radio blocks that have been counted. Click **Clear Counter** to reset this counter.
TX Mute Status	Indicates whether radio transmission is muted.
Adaptive TX power operational status	Indicates whether Adaptive TX power is currently operational.
Temperature	The internal temperature of the unit.
TX Frequency	The configured TX radio frequency (MHz). The TX radio frequency is configured in the Frequency control (Local) section of the Radio Parameters page.
RX Frequency	The configured RX radio frequency (MHz). The RX radio frequency is configured in the Frequency control (Local) section of the Radio Parameters page.
Frequency Separation	The frequency separation, based on the configured TX and RX frequencies.

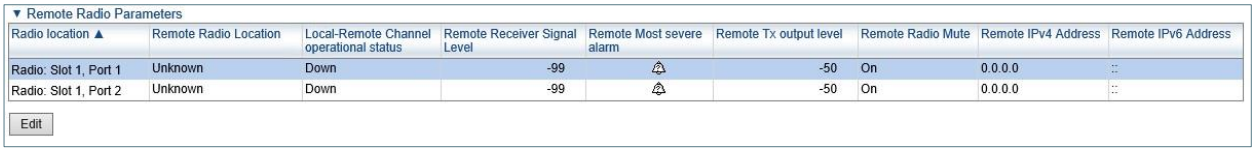
9.2 Configuring the Remote Radio Parameters

You can view and configure the parameters of the carrier or carriers at the remote side of the link in the Remote Radio Parameters page.

To display the remote radio parameters:

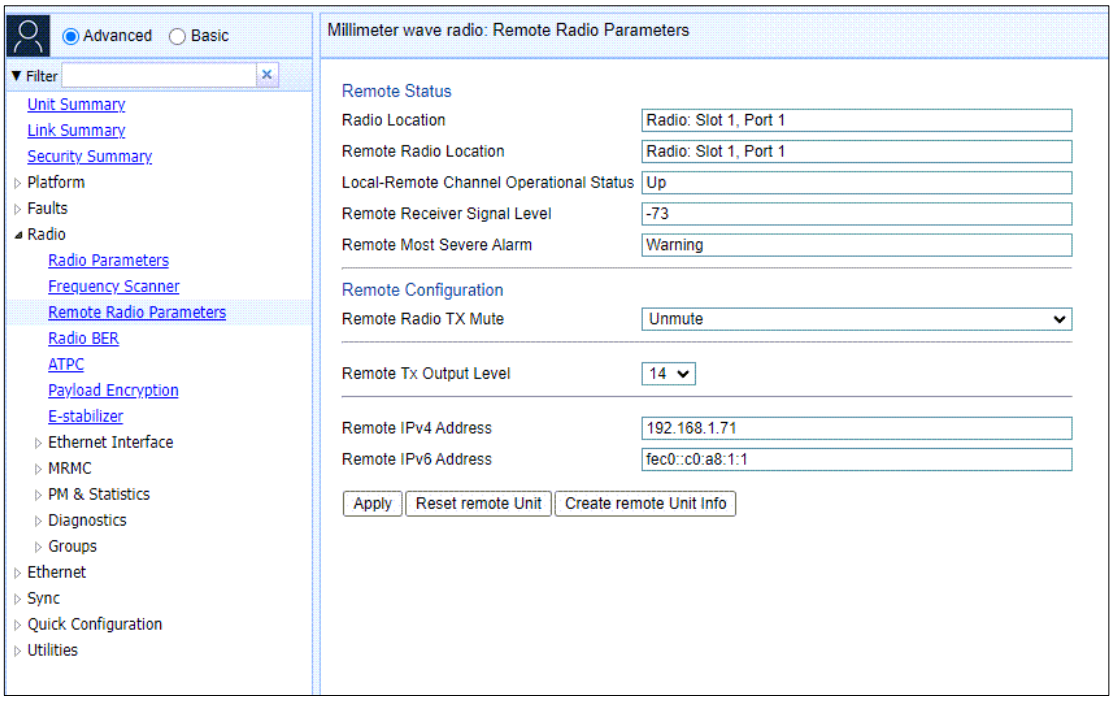
1. Select **Radio > Remote Radio Parameters**.

a. For PTP 850C, the Radio Parameters Table opens. Select the carrier you want to configure and click **Edit** to display the Remote Radio Parameters page for that carrier.



b. For other PTP 850 products, the Remote Radio Parameters page opens right away.

Figure 329 Remote Radio Parameters Page (PTP 850E)



2. Configure the remote radio parameters. For a description of these parameters, see Table 40 Remote Radio Parameters.

3. Click **Apply**.

To reset the remote unit, click **Reset Remote Unit**.

To create a Unit Info file on the remote unit, click **Create Remote Unit Info**. This is useful in the event that management to the remote unit has been lost or the remote unit is not broadcasting but is still able to receive on the radio link. In these scenarios, the request to create a Unit Info file can be transmitted via the local-remote radio link, and the file can be retrieved later to help with troubleshooting.

In this scenario, it may be advisable to reset the remote unit. Make sure to wait about one minute between the **Create Remote Unit Info** command and clicking **Reset Remote Unit**, in order to provide time for the Unit Info file to be created on the remote unit. Once management has been restored, you can retrieve the Unit Info file from the remote unit.

Table 40 Remote Radio Parameters

Parameter	Definition
Radio Location	Read-only. Identifies the carrier.
Remote Radio Location	Read-only. Identifies the location of the remote radio.
Local Remote Channel Operational Status	Read-only. The operational status of the local-remote channel.
Remote Receiver Signal Level	Read-only. The Rx level of the remote radio, in dBm.
Remote Most Severe Alarm	Read-only. The level of the most severe alarm currently active on the remote unit.
Remote Tx Output Level	Set the remote unit's Tx output level (in dBm).
Remote Radio Mute	To mute the TX output of the remote radio, select **On**. To unmute the TX output of the remote radio, select **Off**.
Remote IP Address	The IPv4 IP address of the remote unit.
Remote IPv6 Address	The IPv6 IP address of the remote unit.

9.3 Configuring ATPC and ATPC Override Timer



Note

This section is only relevant for PTP 850S.

ATPC is a closed-loop mechanism by which each carrier changes the TX power according to the indication received across the link, in order to achieve a desired RSL on the other side of the link.

With ATPC, if the radio increases its TX power up to the configured TX power, it can lead to a period of sustained transmission at maximum power, resulting in unacceptable interference with other systems.

In order to minimize interference, PTP 850 provides an ATPC override mechanism. When ATPC override is enabled, a timer begins when ATPC raises the TX power to its maximum. When the timer expires, the radio enters ATPC override state. In ATPC override state, the radio transmits no higher than the pre-determined ATPC override TX level, and an ATPC override alarm is raised. The radio remains in ATPC override state until the ATPC override state is manually cancelled by the user (or until the unit is reset). The radio then returns to normal ATPC operation.

In a configuration with unit protection, the ATPC override state is propagated to the standby unit in the event of switchover.

Note

When canceling an ATPC override state, you should ensure that the underlying problem has been corrected. Otherwise, ATPC may be overridden again.

To enable and configure ATPC and display ATPC settings:

1 Select **Radio > ATPC**. The ATPC page opens.

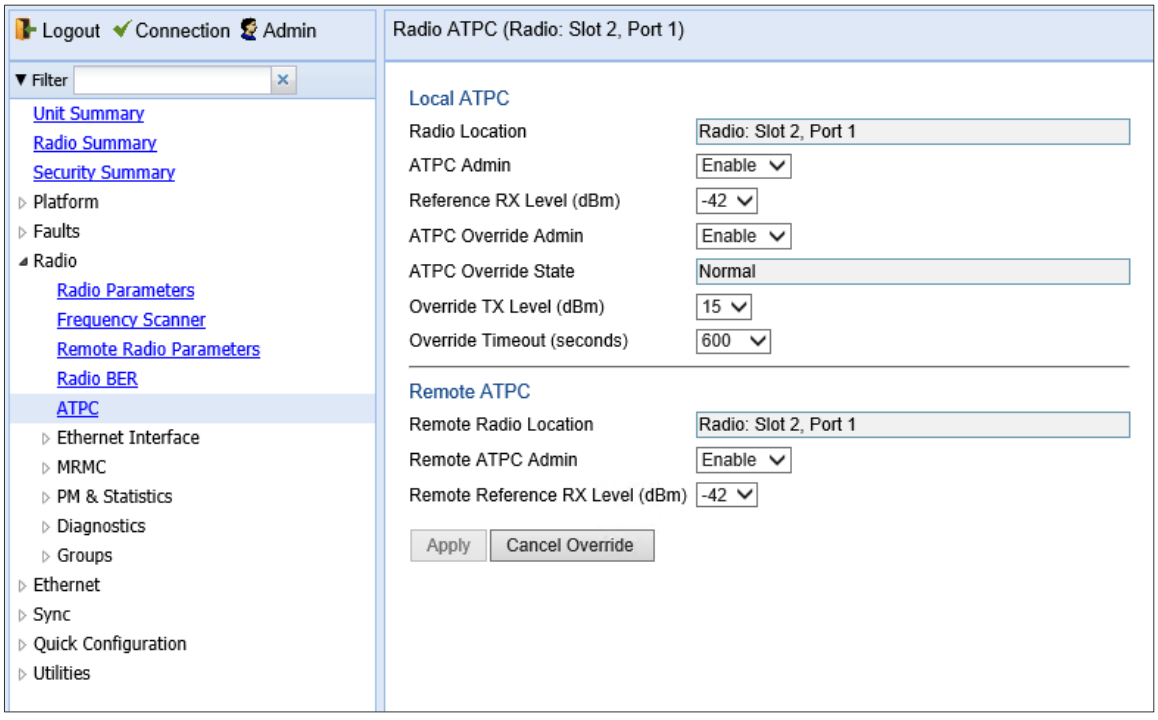


Figure 330 ATPC Page

In the **ATPC Admin** field, select **Enable** to enable ATPC or **Disable** to disable

2 Click **Apply**. If you selected **ATPC -Admin** – **Enable**, the **Reference RX Level (dBm)** and **ATPC Override**

Admin fields are now displayed.

3 In the Reference RX Level (dBm) field, enter a number between -70 and -30 as the reference value for the ATPC mechanism. When ATPC is enabled, it adjusts the TX power dynamically to preserve this RSL level. The range of values depends on the frequency, MRMC script, and RFU type.

4 In the **ATPC Override Admin** field, select **Enable** to enable ATPC override or **Disable** to disable ATPC override. You can only enable ATPC override if ATPC itself is enabled.



Note

Make sure to set an appropriate value in the Override Timeout field before enabling ATPC override. Failure to do so can lead to unexpected reduction of the TX power with corresponding loss of capacity if TX override is enabled with the timer set to a lower-than-desired value.

5 Click **Apply**. If you selected **ATPC Override Admin** – **Enable**, the **ATPC Override State**, **Override TX Level,** and **ATPC Override Admin** fields are now displayed.

6 In the Override TX Level field, select the TX power, in dBm, to be used when the unit is in an ATPC override state. The range of values depends on the frequency, MRMC script, and RFU type.

7 In the **Override Timeout** field, select the amount of time, in seconds, the timer counts from the moment the radio reaches its maximum configured TX power until ATPC override goes into effect. You can select from 0 to 1800 seconds.

8 In the **Remote ATPC Admin** field, select **Enable** to enable ATPC or **Disable** to disable ATPC on the remote radio carrier.

9 Click **Apply**. If you selected **Remote ATPC Admin** – **Enable**, the **Remote Reference RX Level (dBm)** field is now displayed.

10 In the **Remote Reference RX Level (dBm)** field, enter a number between -70 and -30 as the reference value for the ATPC mechanism on the remote radio carrier.

11 Click **Apply**.

To cancel an ATPC override state on the local unit, click **Cancel Override**.

9.4 Configuring Header De-Duplication and Frame Cut-Through



Note

This section is only relevant for PTP 850S.

Header De-Duplication enables operators to significantly improve Ethernet throughout over the radio link without affecting user traffic. Header

De-Duplication can be configured to operate on various layers of the protocol stack, saving bandwidth by reducing unnecessary header overhead. Header De- duplication is also sometimes known as header compression.

Note

The Header De-Duplication and Frame Cut-Through configuration must be identical on both sides of the link.

If Frame Cut-Through is used together with 1588 Transparent Clock, the 1588 packets must be given a CoS that is not assigned to the fourth priority queue.

Using the Frame Cut-Through feature, frames assigned to queues with 4th priority pre-empt frames already in transmission over the radio from other queues. After the 4th queue frames have been transmitted, transmission of the pre-empted frames resumes.

Note

Frame Cut-Through cannot be used together with 1588 Transparent Clock.

To configure Header De-Duplication and Frame Cut-Through:

1 Select **Radio > Ethernet Interface > Configuration**. The Radio Ethernet Interface Configuration page opens.

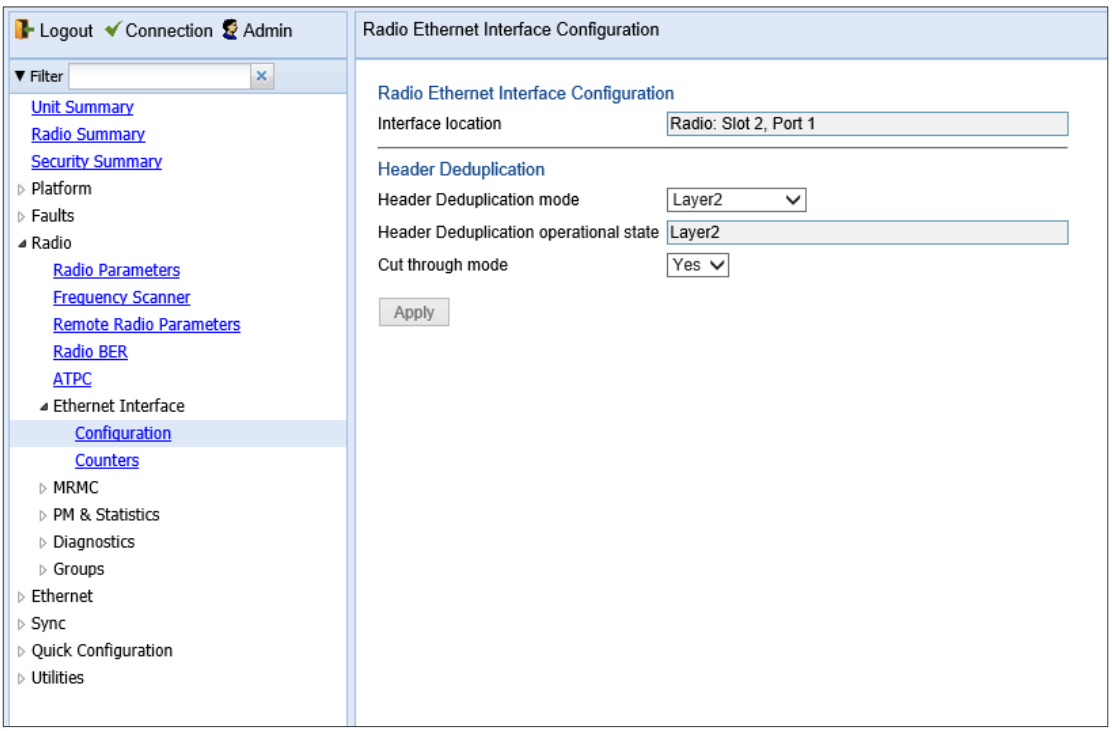


Figure 331 Radio Ethernet Interface Configuration Page

2 In the **Cut through mode** field, select **Yes** to enable Frame Cut-Through or **No** to disable Frame Cut-Through.

3 In the **Header Deduplication mode** field, select from the following options:

- **Disabled** – Header De-Duplication is disabled.

- **Layer2** – Header De-Duplication operates on the Ethernet level.
- **MPLS** – Header De-Duplication operates on the Ethernet and MPLS levels.
- **Layer3** – Header De-Duplication operates on the Ethernet and IP levels.
- **Layer4** – Header De-Duplication operates on all supported layers up to Layer 4.
- **Tunnel** – Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel layer for packets carrying GTP or GRE frames.
- **Tunnel-Layer3** – Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel and T-3 layers for packets carrying GTP or GRE frames.
- **Tunnel-Layer4** – Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel, T-3, and T-4 layers for packets carrying GTP or GRE frames.

4 Click Apply, then Close



Note

The **Utilization threshold** field is not applicable.

Viewing Header De-Duplication and Frame Cut-Through Counters

You can view PMs on the usage of Header De-Duplication and Frame Cut-Through. To view Header De-Duplication and Frame Cut-Through counters:

1 Select **Radio > Ethernet Interface > Counters**. The Radio Ethernet Interface Configuration page opens.

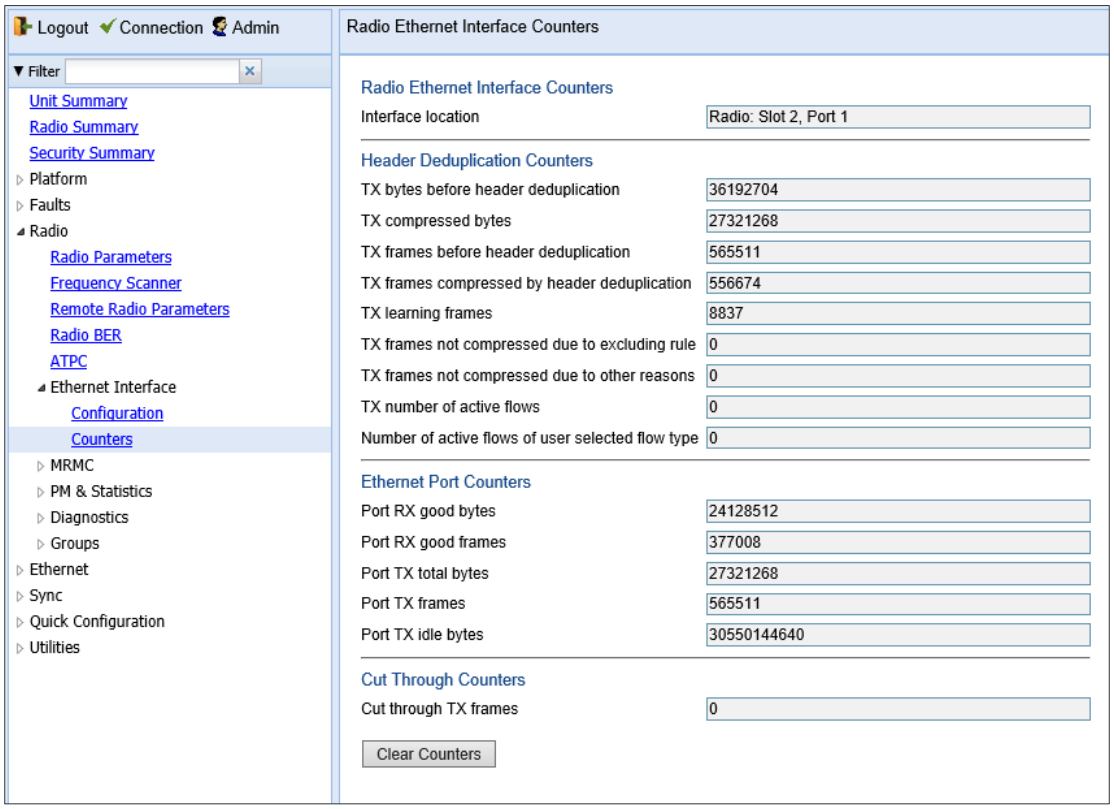


Figure 332 Radio Ethernet Interface Counters Page

Below table lists and describes the fields in the Radio Ethernet Interface Counters page.

Table 41 Radio Ethernet Interface Counters Fields

Parameter	Description
Interface	Identifies the radio interface.
Header Compression Counters	
TX bytes before	Bytes on the TX side before Header De-Duplication.
TX comp	Bytes on the TX side that were compressed by Header De-Duplication.
TX frames before	Frames on the TX side before Header De-Duplication.
TX frames comp	Frames on the TX side that were compressed by Header De-Duplication.

TX learning frames	The number of frames that have been used to learn unique data flows. Once a particular flow type has been learned, subsequent frames with that flow type are compressed by Header De-Duplication.
TX frames not compress	Frames on the TX side that were not compressed due to exclusion rules. **Note**: The use of exclusion rules for Header De-Duplication is planned for future release.
TX frames not compress	Frames on the TX side that were not compressed for reasons other than the use of exclusion rules.
TX number of active	The number of Header De-Duplication flows that are active on the TX side.
Number of active flows of	Not supported.
Ethernet Port Counters	
Port RX good bytes	The number of good bytes received on the port since the last time the Radio Ethernet Interface counters were cleared.
Port RX good frames	The number of good frames received on the port since the last time the Radio Ethernet Interface counters were cleared.
Port TX total bytes	The number of bytes transmitted since the last time the Radio Ethernet Interface counters were cleared.
Port TX frames	The number of frames transmitted since the last time the Radio Ethernet Interface counters were cleared.
Port TX idle bytes	The number of idle bytes transmitted since the last time the Radio Ethernet Interface counters were cleared.
Cut Through Counters	
Cut through TX frames	The number of frames that have been transmitted via Frame Cut-Through since the last time the Radio Ethernet Interface counters were cleared.

9.5 Configuring AES-256 Payload Encryption



Note

This feature is only relevant for PTP 850E units.

This feature is not supported with 2+0 XPIC and Multiband links.

This feature requires:

- Requires an activation key. If no valid AES activation key has been applied to the unit, AES will not operate on the unit. See *Configuring the Activation Key*.



Note

In order for the AES activation key to become active, you must reset the unit after configuring a valid AES activation key. Until the unit is reset, an alarm will be present if you enable AES. This is not the case for other activation keys.

PTP 850E supports AES-256 payload encryption, using a dual-key encryption mechanism:

- The user provides a master key. The master key can also be generated by the system upon user command. The master key is a 32-byte symmetric encryption key. The same master key must be manually configured on both ends of the encrypted link.
- The session key is a 32-byte symmetric encryption key used to encrypt the actual data. Each link uses two session keys, one for each direction. For each direction, the session key is generated by the transmit side unit and propagated automatically, via a Key Exchange Protocol, to the other side of the link. The Key Exchange Protocol exchanges session keys by encrypting them with the master key, using the AES-256 encryption algorithm. Session keys are regenerated at user-configured intervals.

The first KEP exchange that takes place after a new master key is configured causes traffic to be blocked for up to one minute, until the Crypto Validation State becomes Valid. Subsequent KEP exchanges that take place when a session key expires do not affect traffic. KEP exchanges have no effect upon ACM, RSL, and MSE.

To configure payload encryption:

1 Verify that both the local and remote units are running with no alarms. If any alarm is present, take corrective actions to clear the alarms before proceeding.

2 If the link is using in-band management, identify which unit is local and which unit is remote from the management point of view.

3 On the remote unit, select **Radio > Payload Encryption**. The Payload Encryption page opens.

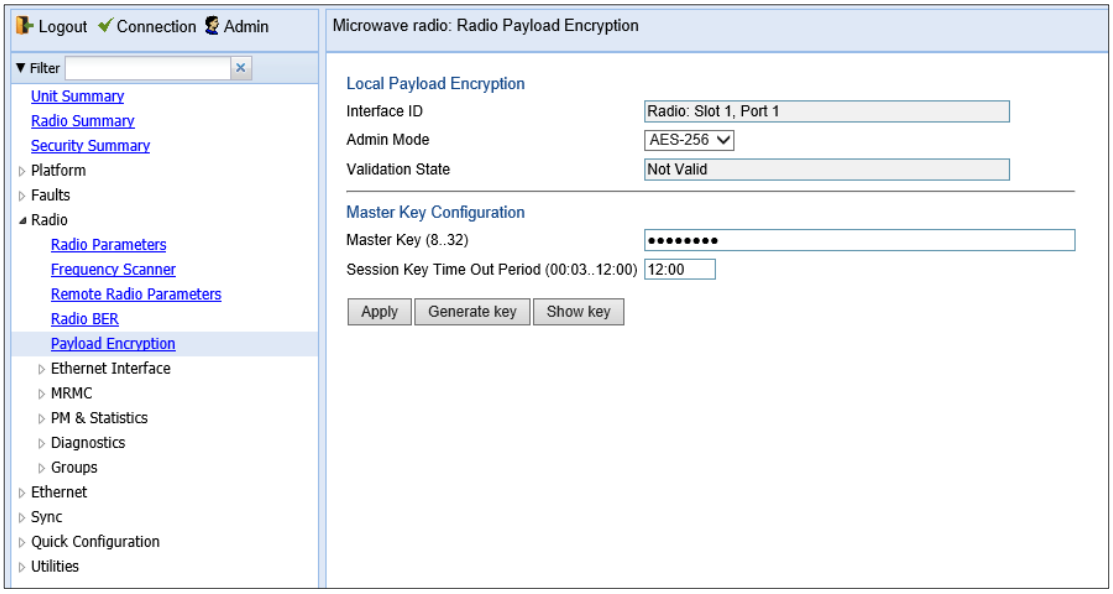


Figure 333 Payload Encryption Page

4 Configure the master key by doing one of the following:

- Enter a master key in the **Master Key** field. You must enter between 8 and 32 ASCII characters.
- Click **Generate key** to generate a master key automatically.

You must use the same master key on both sides of the link. This means that if you generate a master key automatically on one side of the link, you must copy that key and for use on the other side of the link. Once payload encryption has been enabled on both sides of the link, the Key Exchange Protocol periodically verifies that both ends of the link have the same master key. If a mismatch is detected, an alarm is raised and traffic transmission is stopped for the mismatched carrier at both sides of the link. The link becomes non-valid and traffic stops being forwarded.

When you enter a master key, or when the master key is automatically generated, the key is hidden behind dots. To copy the master key, you must display the key. To display the master key, click **Show Key**. A new **Master key** field appears, displaying the master key. You can copy the key to the clipboard from this field.

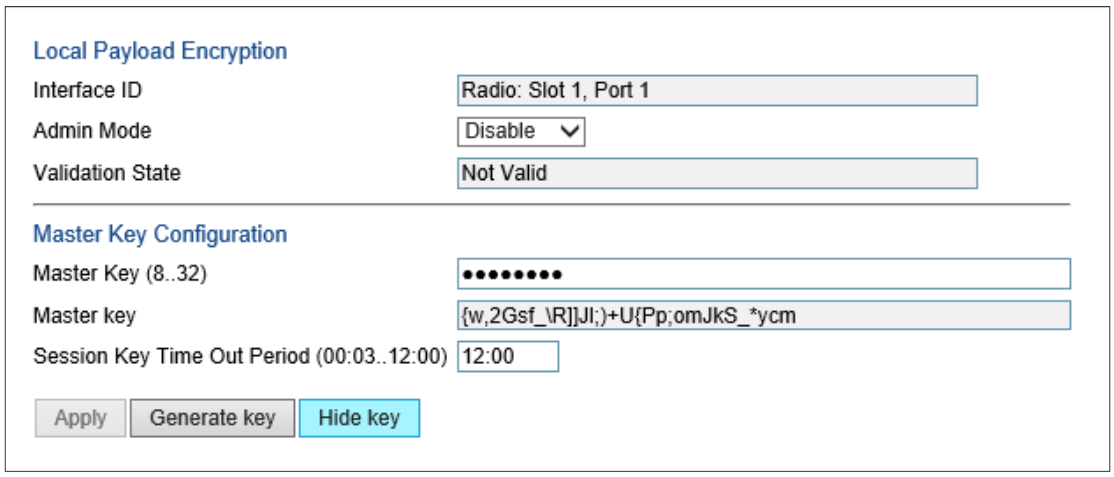


Figure 334 Radio Payload Encryption Page with Master Key Displayed

5 Record and save the master key generated in Step 4.

6 On the local unit, follow Steps 3 through 4 to configure the same master key configured on the remote unit also on the local unit.

7 Enable payload encryption on the remote unit:

i In the Admin **Mode** field, select **AES-256** to enable payload encryption.

ii In the Session **Key Period** field, configure a time interval in hours and minutes (HH:MM). This is the interval at which the session key is automatically regenerated. The Session Key Period can be from 3 minutes (00:03) to 12 hours (12:00).

iii When you are finished, click **Apply**.

This step will cause the link status to be Down until payload encryption is successfully enabled on the local unit. However, the RSL measured on the link should remain at an acceptable level.

Note

The **Validation State** field indicates whether the interface is functioning properly, with AES-256 encryption. In order for this field to display **Valid**, both the interface itself and AES-256 encryption must be enabled, the hardware must be in place and functioning properly, initialization must be finished, and AES-256 encryption must be functioning properly, with no loopback on the interface.

8 Enable payload encryption on the local unit by following the procedure described in Step 7. Verify that on both the local and remote active units, the link status returns to Up and user traffic is restored. In links using in-band management, verify also that in-band management returns.

9 Verify that there are no alarms on the link.

9.6 Configuring and Viewing Radio PMs and Statistics

This section includes:

- Configuring BER Thresholds and Displaying Current BER
- Displaying MRMC Status
- Displaying MRMC PMs
- Displaying and Clearing Defective Block Counters
- Displaying Signal Level PMs and Configuring Signal Level PM Thresholds
- Displaying Modem BER (Aggregate) PMs
- Displaying MSE PMs and Configuring MSE PM Thresholds
- Displaying XPI PMs and Configuring XPI PM Thresholds
- Displaying Traffic PMs
- Displaying Ethernet Interface Counters



Note

The **Radio** > **PM & Statistics** > **Diversity** and **Radio** > **PM & Statistics** > **Combined** pages are reserved for future use.

9.6.1 Configuring BER Thresholds and Displaying Current BER

You can configure PM thresholds, BER thresholds, and Excessive BER Administration. This enables you to define the levels at which certain PMs are counted, such as the number of seconds in which the configured threshold RX and TX levels are exceeded. This also enables you to define the levels at which certain alarms are triggered.

Signal level PM thresholds, such as RX and TX level thresholds, are configured from the Signal Level PM Report page. See Displaying Signal Level PMs and Configuring Signal Level PM Thresholds.

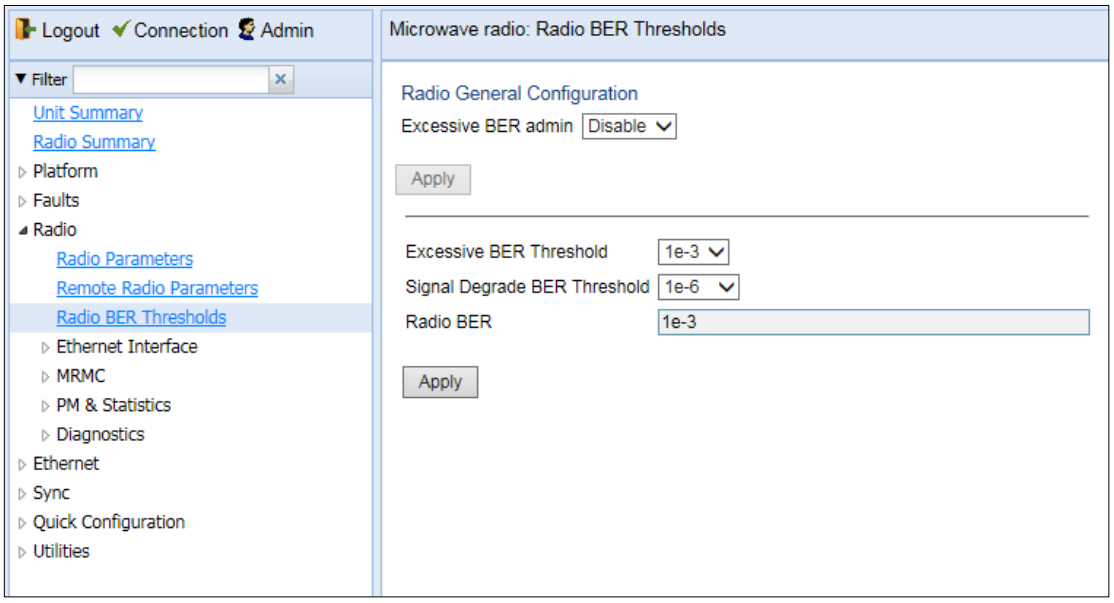
MSE PM Thresholds are configured from the MSE PM Report page. See Displaying MSE PMs and Configuring MSE PM Thresholds.

You can also display the current BER level.

To configure the BER thresholds and Excessive BER Administration, and display current BER levels

1. Select **Radio > Radio BER Thresholds**. The Radio BER Thresholds page opens. The current BER level is displayed, per radio, in the Radio BER column.

Figure 335 Radio BER Thresholds Page



2. In the **Excessive BER admin** field, select **Enable** to enable excessive BER administration or **Disable** to disable excessive BER administration. Excessive BER administration determines whether or not excessive BER is propagated as a fault and considered a system event. For example, if excessive BER administration is enabled, excessive BER can trigger a protection switchover and can cause a synchronization source to go into a failure status. Excessive BER administration is enabled or disabled for the entire unit rather than for specific radios.

3. In the **Excessive BER Threshold field**, select the level above which an excessive BER alarm is issued for errors detected over the radio link.
4. In the **Signal Degrade BER Threshold** field, select the level above which a Signal Degrade alarm is issued for errors detected over the radio link.
5. Click **Apply**, then **Close**.

9.6.2 Displaying MRMC Status

Related Topics:

Configuring the Radio (MRMC) Script(s)

To display the current modulation and bit rate per radio:

1. Select **Radio > MRMC > MRMC Status**. The MRMC Status page opens.

Figure 336 MRMC Status Page

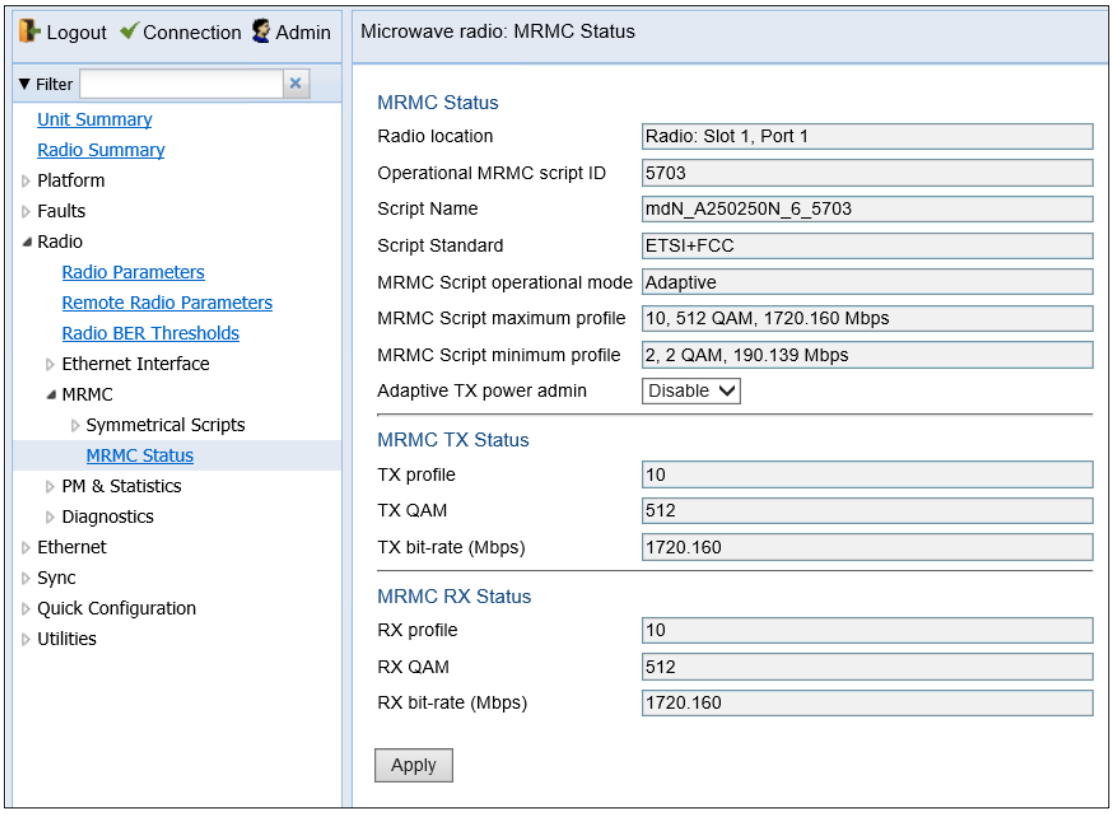


Table 42 describes the MRMC status parameters.

Note

To display the same parameters for an individual radio in a separate page, select the radio in the MRMC script status table and click **Edit**.

Table 42 MRMC Status Parameters

Parameter	Definition
Radio Location	Displays the location of the radio.
Operational MRMC Script ID	The current MRMC script.
Script Name	The name of the script.
Script Standard	Indicates whether the script is compatible with ETSI or FCC (ANSI) standards, or both.
MRMC Script operational mode	The ACM mode: **Fixed** or **Adaptive**. Fixed ACM mode applies constant TX and RX rates. However, unlike regular scripts, with a Fixed ACM script you can specify a maximum profile to inhibit inefficient transmission levels. In Adaptive ACM mode, TX and RX rates are dynamic. An ACM-enabled radio system automatically chooses which profile to use according to the channel fading conditions.
MRMC Script profile	Fixed ACM mode only: The profile in which the system will operate.
MRMC Script maximum profile	Adaptive ACM mode only: The maximum profile for the script. For example, if you select a maximum profile of 5, the system will not climb above profile 5, even if channel fading conditions allow it.
MRMC Script minimum profile	Adaptive ACM mode only: The minimum profile for the script. For example, if you select a minimum profile of 3, the system will not go below profile 3 regardless of the channel fading conditions. The minimum profile cannot be greater than the maximum profile, but it can be equal to it. **Note:** The default minimum profile is 2.

Parameter	Definition
Adaptive Tx Power Admin	Enables or disables Adaptive TX Power. When Adaptive TX Power is enabled, the radio adjusts its TX power dynamically based on the current modulation. When the modulation is at a high level, the TX power is adjusted to the level required with the high modulation. If the modulation goes down to a lower level, the TX power increases to compensate for the lower modulation. The TX level configured in the **TX Level (dBm)** field of the Radio Parameters page determines the maximum TX level, but the actual TX level as shown in the **Operational TX Level (dBm)** field of the Radio Parameters page can be expected to be lower when the radio is operating at high modulations requiring less TX power.
TX profile	The current TX profile.
TX QAM	The current TX modulation.
TX bit-rate	The current TX bit-rate (Mbps).
RX profile	The current RX profile.
RX QAM	The current RX modulation.
RX bit-rate	The current RX bit-rate (Mbps).

9.6.3 Displaying MRMC PMs and Configuring ACM Profile Thresholds

Related Topics:

Configuring the Radio (MRMC) Script(s)

To display Multi-Rate Multi-Constellation PMs, including information on ACM profile fluctuations per interval per radio:

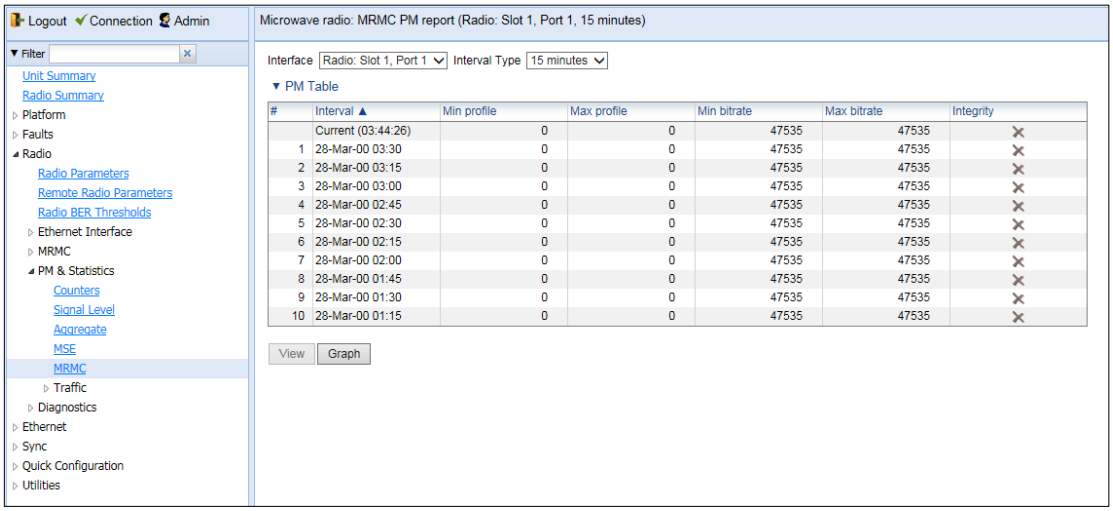
For each radio carrier, you can display the minimum and maximum ACM profile and the minimum and maximum bitrate (throughput) per 15-minute or daily intervals.

You can also define two ACM profile thresholds for each radio carrier, and display the number of seconds per interval that the radio's ACM profile was below each of these thresholds. These thresholds trigger the following alarms:

- Threshold 1 – When the ACM profile goes beneath this threshold, Alarm ID 1313 (Major) is raised. The alarm is cleared when the ACM profile is at or above this threshold.
- Threshold 2 – When the ACM profile goes beneath this threshold, Alarm ID 1314 (Critical) is raised. The alarm is cleared when the ACM profile is at or above this threshold.

1. Select **Radio > PM & Statistics > MRMC**. The MRMC PM Report page opens.

Figure 337 MRMC PM Report Page



2. In the **Interval Type** field:

To display reports in 15-minute intervals, select **15 minutes**.

To display reports in daily intervals, select **24 hours**.

Table 43 describes the MRMC PMs.



Note

To display the same parameters for a specific interval in a separate page, select the interval in the MRMC PM table and click **View**.

Table 43 MRMC PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Min profile	Displays the minimum ACM profile that was measured during the interval.
Max profile	Displays the maximum ACM profile that was measured during the interval.
Min bitrate	Displays the minimum total radio throughput (Mbps) delivered during the interval.
Max bitrate	Displays the maximum total radio throughput (Mbps) delivered during the interval.
Seconds above Threshold 1	Displays the number of seconds the radio was above both ACM profile thresholds during the interval.

Parameter	Definition
Seconds below Threshold 1	Displays the number of seconds the radio was below ACM profile threshold 1 during the interval.
Seconds below Threshold 2	Displays the number of seconds the radio was below ACM profile threshold 2 during the interval.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.

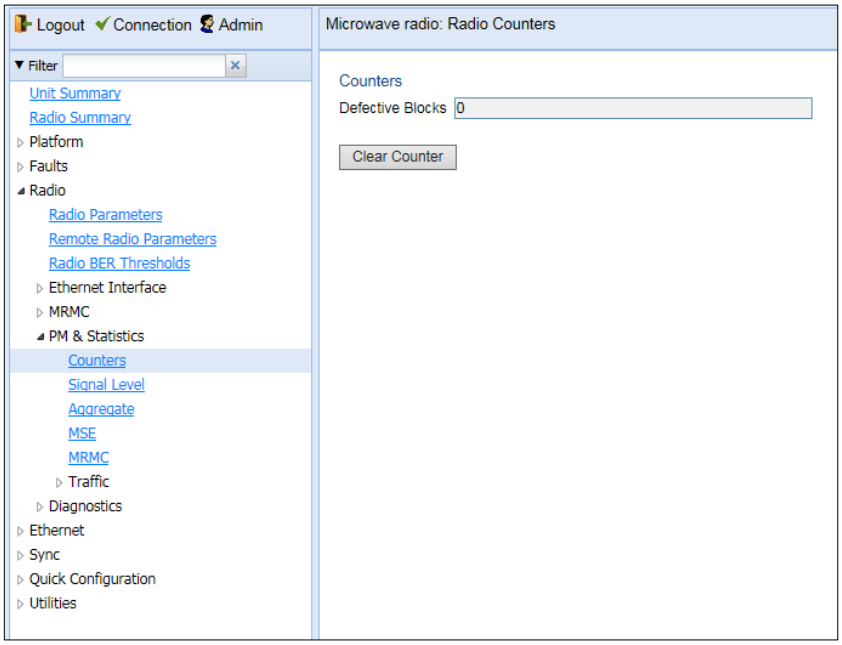
9.6.4 Displaying and Clearing Defective Block Counters

The Counters page displays the number of blocks in which errors were detected. The larger the amount, the poorer the radio link quality.

To display the number of blocks in which errors were detected per radio:

1. Select **Radio > PM & Statistics > Counters**. The Counters page opens.

Figure 338 Counters Page



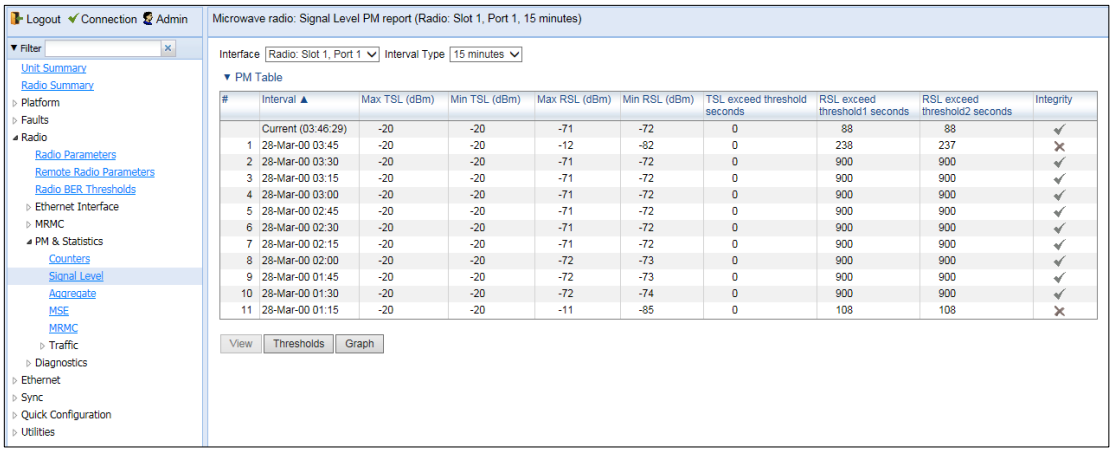
2. To clear the counters, click **Clear Counters**.

9.6.5 Displaying Signal Level PMs and Configuring Signal Level PM Thresholds

To display signal level PMs per radio:

1. Select **Radio > PM & Statistics > Signal Level**. The Signal Level PM report page opens.

Figure 339 Signal Level PM Report Page



2. In the **Interval Type** field:
   - To display reports in 15-minute intervals, select **15 minutes**.
   - To display reports in daily intervals, select **24 hours**.

Table 44 describes the Signal Level PMs.



Note

To display the same parameters for a specific interval in a separate page, select the interval in the RF PM table and click **View**.

Table 44 Signal Level PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Max TSL (dBm)	The maximum TSL (Transmit Signal Level) that was measured during the interval.
Min TSL (dBm)	The minimum TSL (Transmit Signal Level) that was measured during the interval.
Max RSL (dBm)	The maximum RSL (Received Signal Level) that was measured during the interval.
Min RSL (dBm)	The minimum RSL (Received Signal Level) that was measured during the interval.

Parameter	Definition
TSL exceed threshold seconds	The number of seconds the measured TSL exceeded the TX Level Threshold during the interval.
RSL exceed threshold1 seconds	The number of seconds the measured RSL exceeded RX Level Threshold 1 during the interval.
RSL exceed threshold2 seconds	The number of seconds the measured RSL exceeded RX Level Threshold 2 during the interval.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.

To set the Signal Level PM thresholds, click **Thresholds**. The Signal Level Thresholds Configuration – Edit Page opens. Set the thresholds, described in Table 45, and click **Apply**.

Figure 340 Signal Level Thresholds Configuration - Edit Page

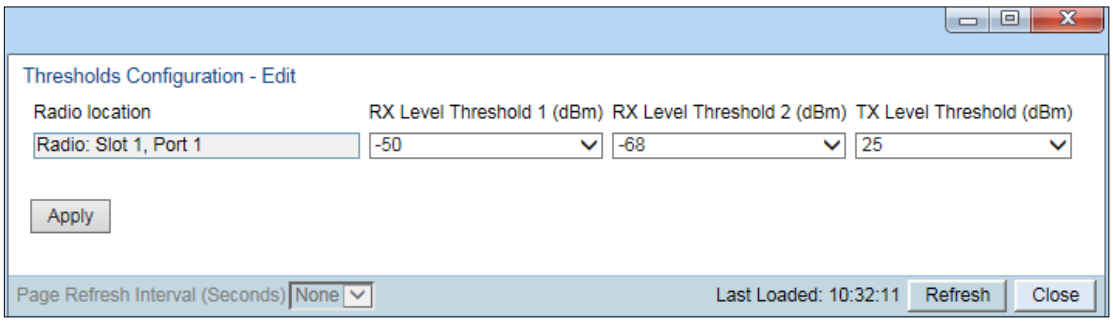


Table 45 Signal Level Thresholds

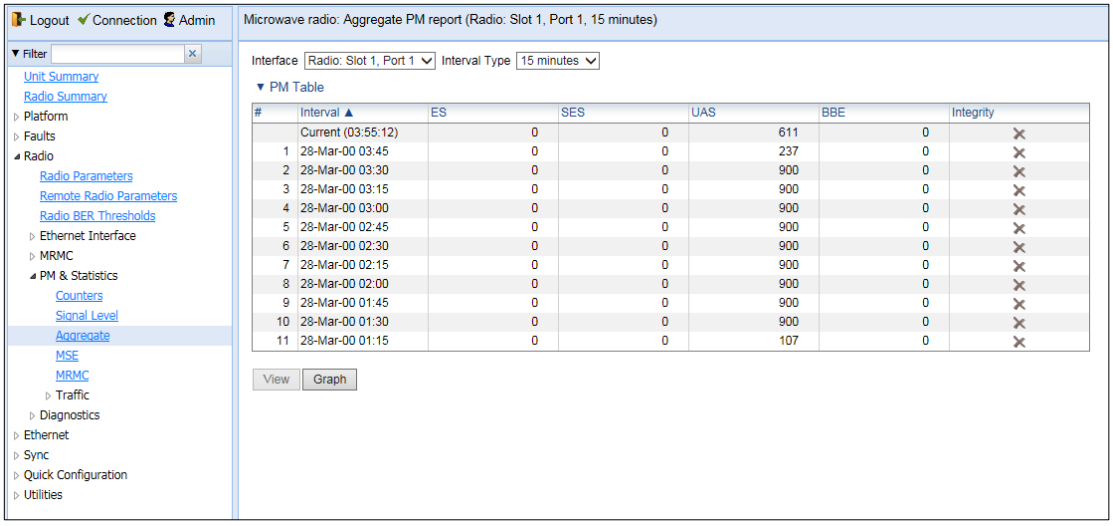
Parameter	Definition
RX Level Threshold 1 (dBm)	Specify the threshold for counting exceeded seconds if the RSL is below this level.
RX Level Threshold 2 (dBm)	Specify a second threshold for counting exceeded seconds if the RSL is below this level.
TX Level Threshold (dBm)	Specify the threshold for counting exceeded seconds if the TSL is below this level.

9.6.6 Displaying Modem BER (Aggregate) PMs

To display modem BER (Bit Error Rate) PMs per radio:

1. Select **Radio > PM & Statistics > Aggregate**. The Aggregate PM report page opens.

Figure 341 Aggregate PM Report Page



2. In the **Interval Type** field:
   - To display reports in 15-minute intervals, select **15 minutes**.
   - To display reports in daily intervals, select **24 hours**.

Table 46 describes the Modem BER (Aggregate) PMs.



Note

To display the same parameters for a specific interval in a separate page, select the interval in the Modem BER PM table and click **View**.

Table 46 Modem BER (Aggregate) PMs

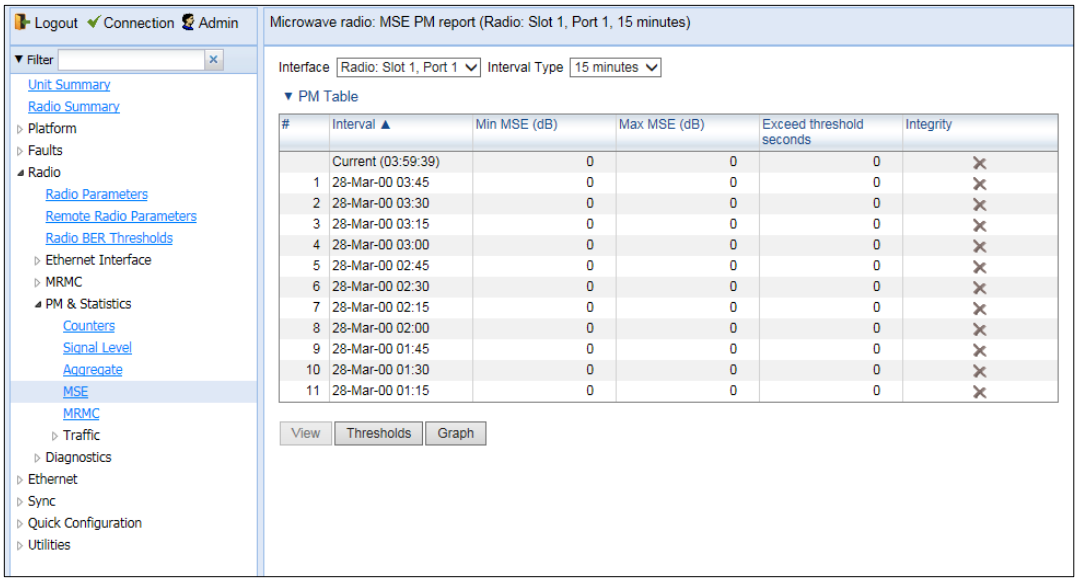
Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
ES	Displays the number of seconds in the measuring interval during which errors occurred.
SES	Displays the number of severe error seconds in the measuring interval.
UAS	Displays the Unavailable Seconds value of the measured interval. The value can be between 0 and 900 seconds (15 minutes).
BBE	Displays the number of background block errors during the measured interval.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.

9.6.7 Displaying MSE PMs and Configuring MSE PM Thresholds

To display modem MSE (Minimum Square Error) PMs per radio:

1. Select **Radio** > **PM & Statistics** > **MSE**. The MSE PM report page opens.

Figure 342 MSE PM Report Page



2. In the **Interval Type** field:

To display reports in 15-minute intervals, select **15 minutes**.

To display reports in daily intervals, select **24 hours**.

Table 47 describes the Modem MSE PMs.



Note

To display the same parameters for a specific interval in a separate page, select the interval in the Modem MSE PM table and click **View**.

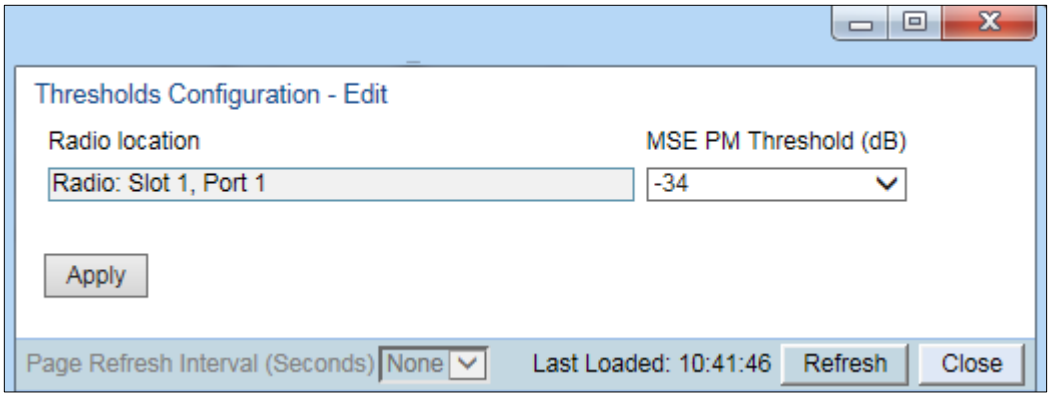
Table 47 Modem MSE PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Min MSE (dB)	Displays the minimum MSE in dB, measured during the interval. A 0 in this field and an X in the **Integrity** field may also indicate that the modem was unlocked during the entire interval.

Parameter	Definition
Max MSE (dB)	Displays the maximum MSE in dB, measured during the interval. A 0 in this field and an X in the **Integrity** field may also indicate that the modem was unlocked.
Exceed threshold seconds	Displays the number of seconds the MSE exceeded the MSE PM threshold during the interval. The MSE PM is configured in the Radio Thresholds page. See Configuring BER Thresholds AND Displaying Cureent BER.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time. An X and a 0 value in the **Max MSE** field may also indicate that the modem was unlocked.

To set the Modem MSE PM thresholds, click **Thresholds**. The Modem MSE Thresholds Configuration–Edit Page opens. For each radio, specify the modem MSE (Mean Square Error) threshold for calculating MSE Exceed Threshold seconds, and click **Apply**.

Figure 343 Modem MSE Thresholds Configuration – Edit Page



9.6.8 Displaying XPI PMs and Configuring XPI PM Thresholds

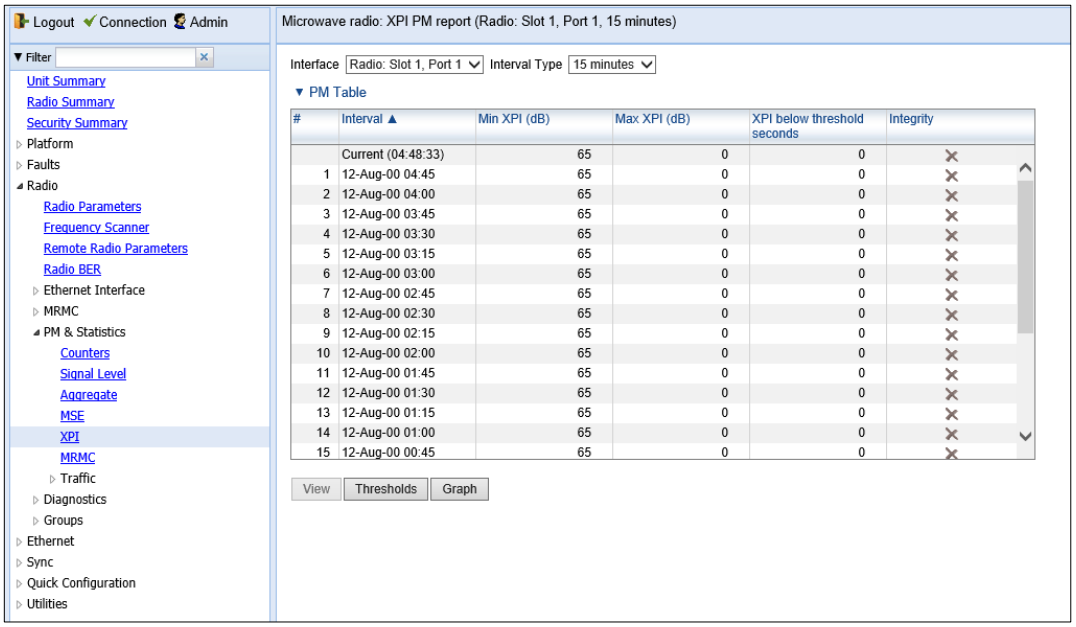
Related topics:

- Configuring XPIC

To display XPI (Cross Polarization Interface) PMs per radio:

1. Select Radio > PM & Statistics > XPI. The XPI PM report page opens.

Figure 344 XPI PM Report Page



2. In the **Interval Type** field:
   - To display reports in 15-minute intervals, select 15 minutes.
   - To display reports in daily intervals, select 24 hours.

Note

To display the same parameters for a specific interval in a separate page, select the interval in the Modem XPI PM table and click View.

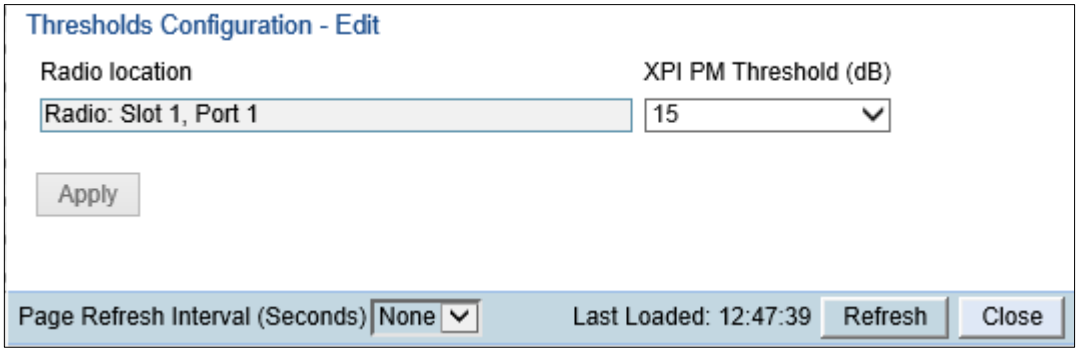
Table 48 XPI PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Min XPI (dB)	The minimum XPI level that was measured during the interval.
Max XPI (dB)	The maximum XPI level that was measured during the interval.

Parameter	Definition
XPI below threshold seconds	The number of seconds the measured XPI level was below the threshold during the interval.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.

To set the XPI PM thresholds, click **Thresholds**. The XPI Thresholds Configuration– Edit Page opens. Specify the modem XPI threshold for calculating XPI Exceed Threshold seconds and click **Apply**.

Figure 345 XPI Thresholds Configuration – Edit Page



9.6.9 Displaying Traffic PMs

This section includes:

- Displaying Capacity and Throughput PMs
- Displaying Utilization PMs

9.6.9.1 Displaying Capacity and Throughput PMs

You can display PMs for capacity and throughput for a radio, an Enhanced Multi-Carrier ABC or Multiband group, or the Traffic port of an PTP 850E in a Multiband group, based on:

- The total Layer 1 bandwidth (payload plus overheads) sent through the interface (Mbps).
- The total effective Layer 2 traffic sent through the interface.

You can also configure thresholds for capacity and throughput PMs. The number of seconds during which these thresholds are exceeded are among the displayed PMs.

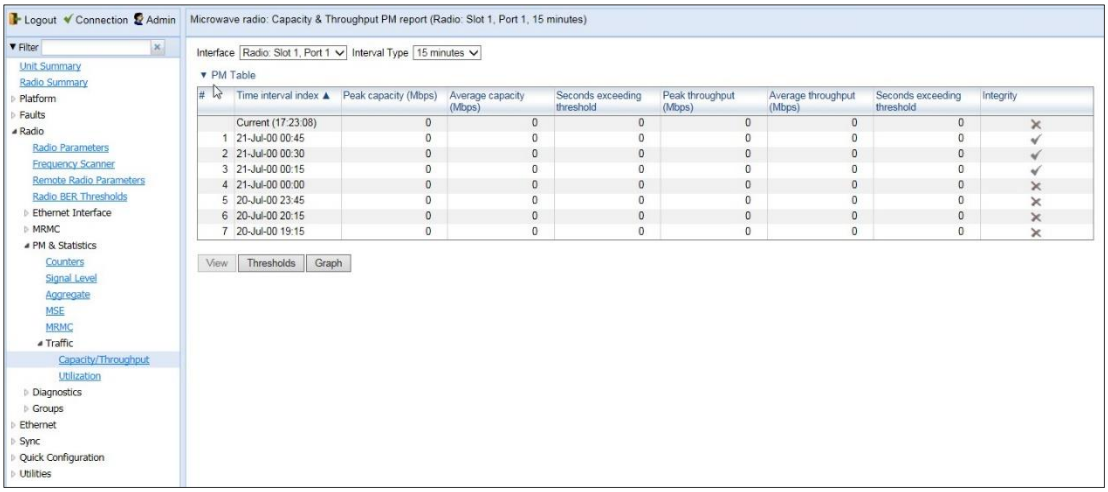
Peak counters display the maximum data rate for each interval, with a resolution of one second. This means the PM mechanism records the number of bytes sent during each second of the interval and displays the number of bytes for the highest one-second period during that interval. So, for example, when measuring 15-minute intervals, the PM mechanism chooses the peak value from 900 recorded values in that interval (60 seconds multiplied by 15 60-second record periods).

Average counters display the average number of bytes received on the interface measured with a resolution of one second. This means the PM mechanism divides the total number of bytes received during the interval by the total number of seconds in the interval. So, for example, when measuring 15-minute intervals, the PM mechanism divides the total number of bytes received during the 15-minute interval by 900.

To display capacity and throughput PMs per interface:

1 Select **Radio > PM & Statistics > Traffic > Capacity/Throughput**. The Capacity PM report page opens.

Figure 346 Capacity PM Report Page



2 In the **Interface** field, select the radio or, if Multiband is configured, select the Multiband group. If Multiband is configured, you can also select the individual members of the Multiband (Enhanced Layer 1 Link Aggregation) group, including the radio and the Traffic port.

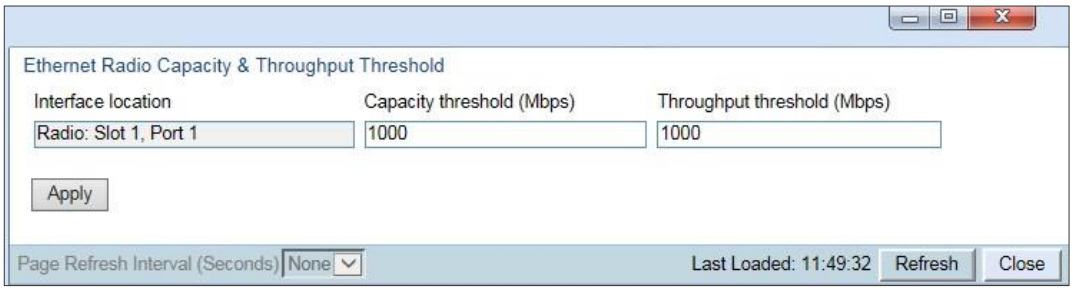
3 In the Interval Type field:

- To display reports in 15-minute intervals, select **15 minutes**.
- To display reports in daily intervals, select **24 hours**.

To set the thresholds for capacity and throughput PMs:

1 Select **Thresholds**. The Ethernet Radio Capacity & Throughput Threshold page opens.

Figure 347 Ethernet Radio Capacity and Throughput Threshold Page



2 Enter the capacity and throughput thresholds you want, in Mbps. The range of values is 0 to 4294967295. The default value for is 1000.

3 Click Apply, then Close.

Note

To display the same parameters for a specific interval in a separate page, select the interval in the PM table and click View

Table 49 Capacity/Throughput PMs

Parameter	Definition
Time interval index	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Peak capacity (Mbps)	Displays the highest L1 bandwidth, in Mbps, sent through the selected interface during the measured time interval.
Averag e	Displays the average L1 bandwidth, in Mbps, during the measured time interval.
Seconds exceedin	Displays the number of seconds during the measured time interval during which the L1 bandwidth exceeded the configured capacity
Peak throug	Displays the highest throughput, in Mbps, that occurred for the selected interface during the measured time interval.
Average throughpu	Displays the average throughput, in Mbps, for the selected interface during the measured time interval.
Seconds exceedin	Displays the number of seconds during the measured time interval during which the throughput exceeded the configured throughput
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the

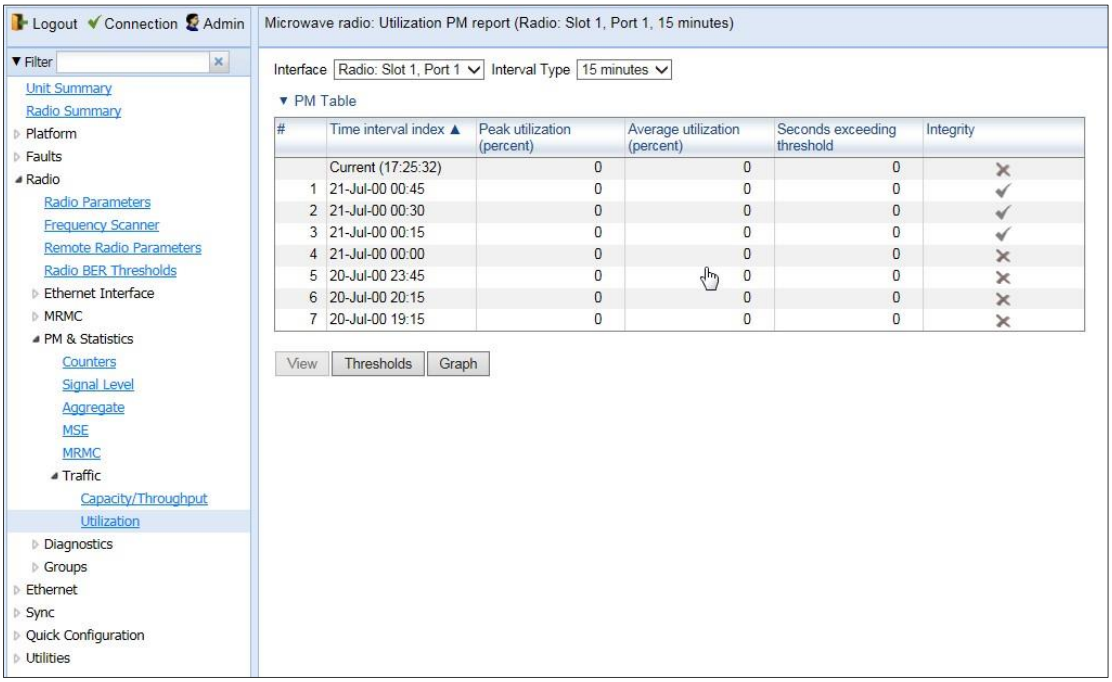
9.6.9.2 Displaying Utilization PMs and Configuring Utilization Thresholds

You can configure three radio capacity utilization thresholds, in percentage. The Utilization PM Report displays, for each radio carrier and Multi-Carrier ABC group, the number of seconds in which the radio or group exceeded each threshold in each interval. It also displays the peak and average utilization, in percentage, per interval.

To display radio capacity utilization PMs per radio:

1 Select **Radio > PM & Statistics > Traffic > Utilization**. The Utilization PM report page opens.

Figure 348 Utilization PM Report Page



2 In the **Interface** field, select the radio or, if Multiband is configured, select the Multiband group. If Multiband is configured, you can also select the individual members of the Multiband group, including the radio or the Traffic port.

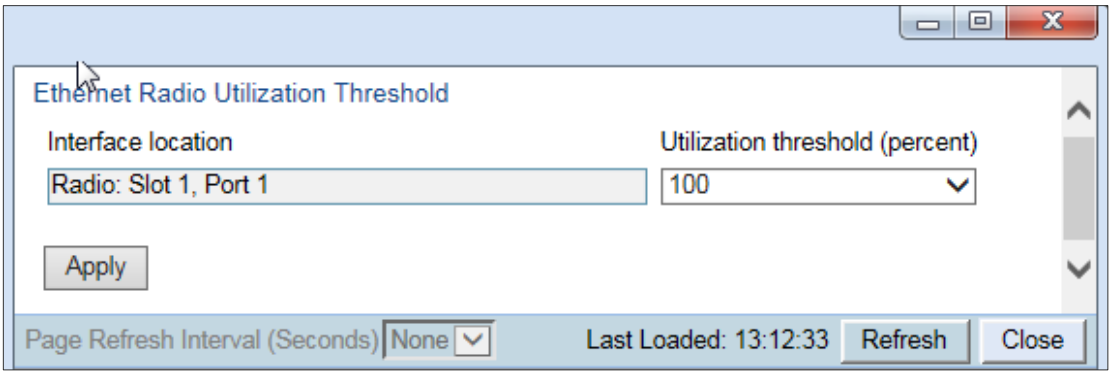
3 In the Interval Type field:

- To display reports in 15-minute intervals, select 15 minutes.
- To display reports in daily intervals, select 24 hours.

To set the thresholds for utilization PMs:

1 Select **Threshold**. The Utilization Threshold page opens.

Figure 349 Ethernet Radio Utilization Threshold Page



2 Select the utilization threshold you want, in % (1-100). The default value for is 100.

3 Click Apply, then Close.

Note

To display the same parameters for a specific interval in a separate page, select the interval in the PM table and click View.

Table 50 Utilization PMs

Parameter	Definition
Time interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Peak utilizatio	Indicates the highest utilization of the radio capacity that occurred for the selected interface or group during the measured time interval.
Average utilizatio	Indicates the average utilization of the radio capacity for the selected interface or group during the measured time interval.
Seconds exceedin g	Displays the number of seconds during the measured time interval during which the L1 bandwidth exceeded the configured utilization threshold.
Seconds exceedin g	Displays the number of seconds during the measured time interval during which the L1 bandwidth exceeded Threshold 2.
Seconds exceedin g	Displays the number of seconds during the measured time interval during which the L1 bandwidth exceeded Threshold 3 (the lowest threshold).
Seconds below Threshol	Displays the number of seconds during the measured time interval during which the L1 bandwidth was less than Threshold 3 (the lowest threshold).

Integrity	Indicates whether the values received at time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.

9.6.10 Displaying Frame Error Rate PMs

To display frame error rate PMs per radio or Multi-Carrier ABC group:

1 Select **Radio > PM & Statistics > Traffic > Frame error rate**. The Frame error rate PM report page opens.

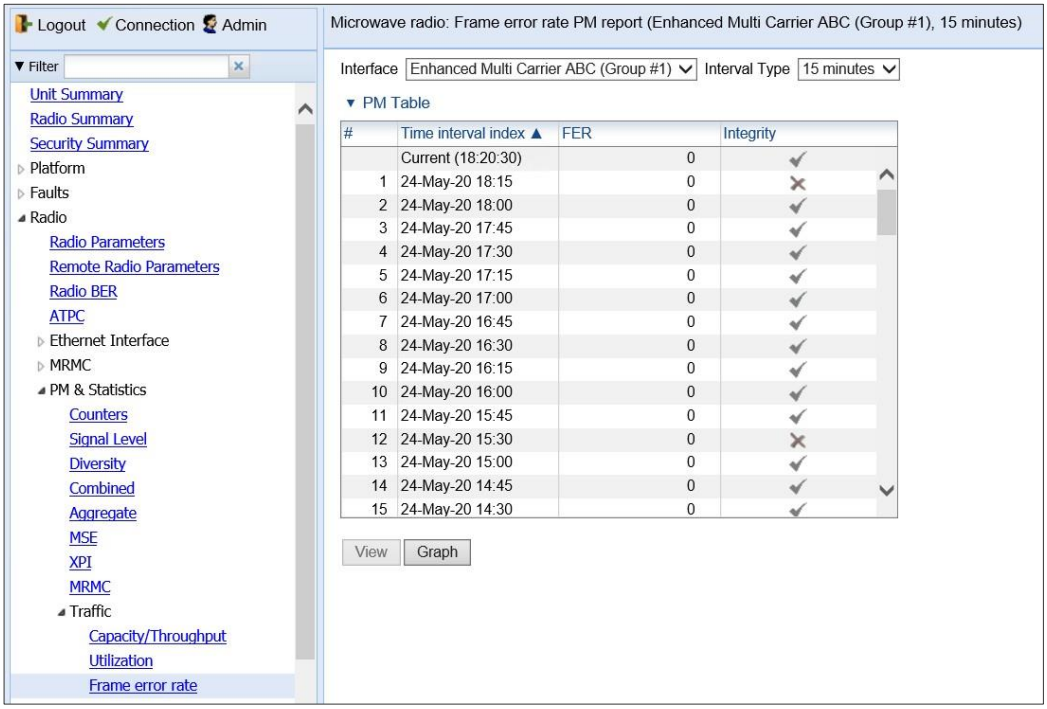


Figure 350 Frame Error PM Report Page

2 In the **Interface** field, select the radio or, if Multi-Carrier ABC (PTP 850C) or Multiband (PTP 850E) is configured, select the ABC or Multiband group.

Note: For PTP 850C, only radio carrier 1 and the Multi-Carrier ABC group (if configured) is available.

3 In the Interval Type field:

- To display reports in 15-minute intervals, select **15 minutes**.
- To display reports in daily intervals, select **24 hours**.

Table 45 describes the capacity and throughput PMs.

Table 51 Frame Error Rate PMs

Parameter	Definition

Time interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
FER	Displays the frame error rate (%) during the measured time interval.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.

9.6.11 Displaying Ethernet Interface Counters

You can view PMs on Ethernet frames entering the radio interface.

Note

In a Multiband configuration, this page displays PMs for the Multiband group rather than the individual interface.

To view Ethernet interface counters:

1 Select **Radio > Ethernet Interface > Counters**. The Radio Ethernet Interface Counters page opens.

Figure 351 Radio Ethernet Interface Counters Page

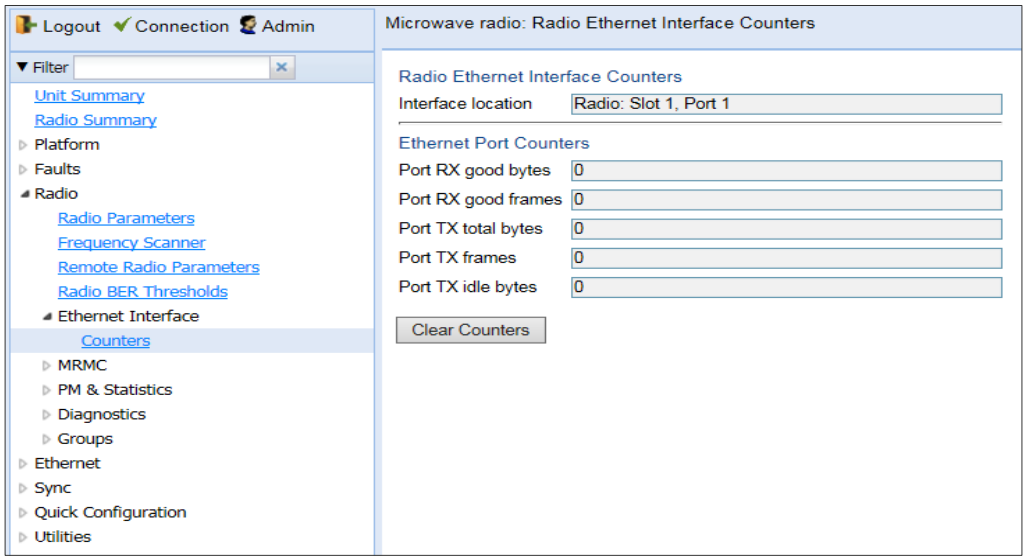


Table 52 Ethernet Interface Counter Fields

Parameter	Description
Port RX good	The number of good bytes received on the port since the last time the Ethernet Interface counters were cleared.
Port RX good	The number of good frames received on the port since the last time the Ethernet Interface counters were
Port TX total bytes	The number of bytes transmitted since the last time the Ethernet Interface counters were cleared.
Port TX frames	The number of frames transmitted since the last time the Radio Ethernet Interface counters were cleared.

Port TX idle bytes	The number of idle bytes transmitted since the last time the Radio Ethernet Interface counters were cleared.

10. Ethernet Services and Interfaces

This section includes:

- Configuring Ethernet Service(s)
- Setting the MRU Size and the S-VLAN Ethertype
- Configuring Ethernet Interfaces
- Configuring Automatic State Propagation and Link Loss Forwarding.
- Viewing Ethernet PMs and Statistics

Related topics:

- Quality of Service (QoS)
- Performing Ethernet Loopback

10.1 Configuring Ethernet Service(s)

This section includes:

- Ethernet Services Overview
- General Guidelines for Provisioning Ethernet Services
- The Ethernet Services Page
- Adding an Ethernet Service
- Editing a Service
- Deleting a Service
- Enabling, Disabling, or Deleting Multiple Services
- Viewing Service Details
- Configuring Service Points

10.1.1 Ethernet Services Overview

Users can define the following number of Ethernet services.

- PTP 850C and PTP 850E: Up to 1024.
- PTP 850S: Up to 64.

Each service constitutes a virtual bridge that defines the connectivity between logical ports in the PTP 850 network element.

This version of PTP 850 supports the following service types:

Multipoint (MP)

Point-to-Point (P2P)

Management (MNG)

In addition to user-defined services, PTP 850 contains a pre-defined management service (Service ID 1025). By default, this service is operational.



Note

You can use the management service for in-band management. For instructions on configuring in-band management, see Configuring In-Band Management.

A service point is a logical entity attached to a physical or logical interface. Service points define the movement of frames through the service. Each service point includes both ingress and egress attributes. A Point-to-Point or Multipoint service can hold up to 32 service points. A Management service can hold up 30 service points.

For a more detailed overview of PTP 850's service-oriented Ethernet switching engine, refer to the Technical Description for the PTP 850.

10.1.2 General Guidelines for Provisioning Ethernet Services

When provisioning Ethernet services, it is recommended to follow these guidelines:

Use the same Service ID for all service fragments along the path of the service.

Do not re-use the same Service ID within the same region. A region is defined as consisting of all PTP 850 devices having Ethernet connectivity between them.

Use meaningful EVC IDs.

Give the same EVC ID (service name) to all service fragments along the path of the service.

Do not reuse the same EVC ID within the same region.

It is recommended to follow these guidelines for creating service points:

Always use SNP service points on NNI ports and SAP service points on UNI ports.

For each logical interface associated with a specific service, there should never be more than a single service point.

The transport VLAN ID should be unique per service within a single region. That is, no two services should use the same transport VLAN ID.

10.1.3 The Ethernet Services Page

The Ethernet Services page is the starting point for defining Ethernet services on the PTP 850.

To open the Ethernet Services page:

1. Select **Ethernet > Services**. The Ethernet Services page opens.

Figure 352 Ethernet Services Page

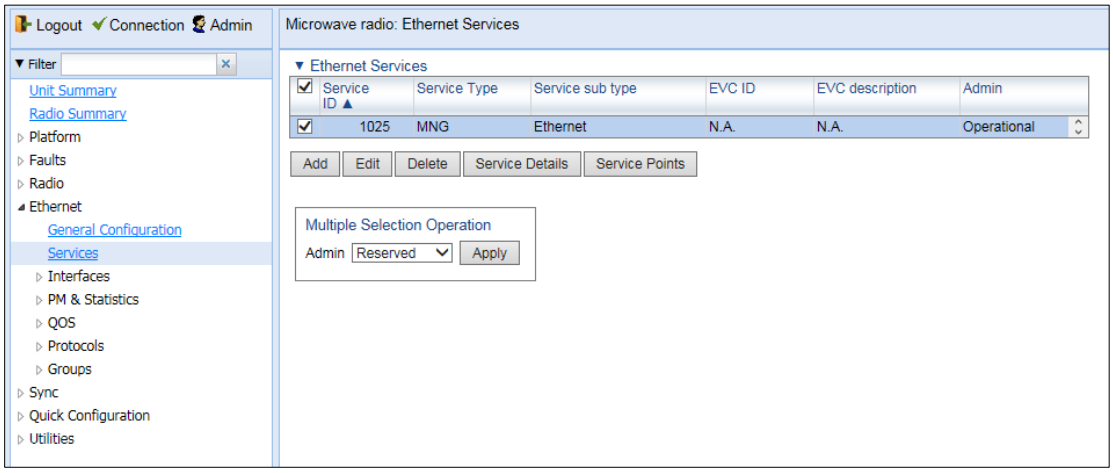


Table 53 Ethernet Services Page Parameters

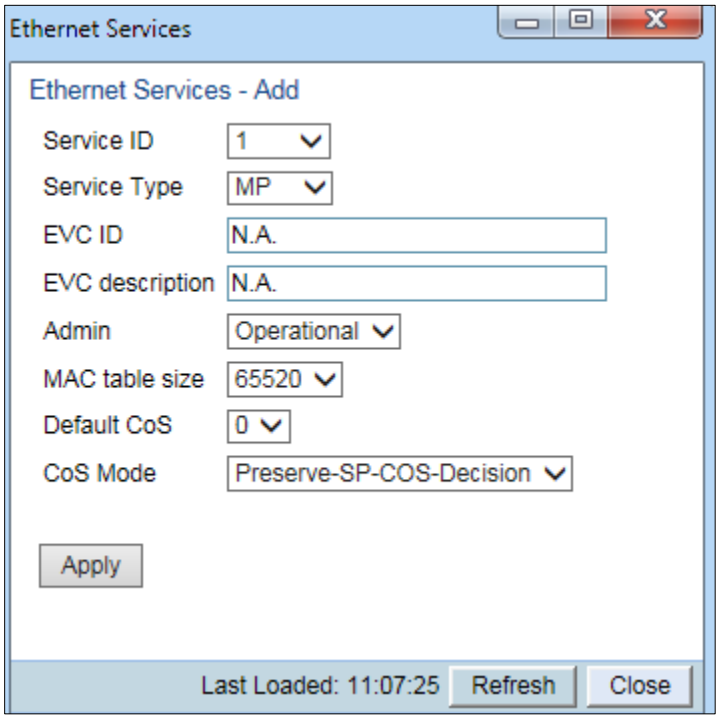
Parameter	Definition
Services ID	A unique ID for the service.
Service Type	The service type: • **MP** – Multipoint • **P2P** – Point-to-Point • **MNG** – Management
Service sub type	Indicates the type of service (**Ethernet**).
EVC ID	The Ethernet Virtual Connection (EVC) ID. This parameter does not affect the network element's behavior, but is used by the NMS for topology management.
EVC description	The Ethernet Virtual Connection (EVC) description. This parameter does not affect the network element's behavior, but is used by the NMS for topology management.
Admin	Indicates whether the service is enabled (**Operational**) or disabled (**Reserved**). You can configure services for later use by defining the service as **Reserved**. In Reserved mode, the service occupies system resources but is unable to transmit and receive data.

10.1.4 Adding an Ethernet Service

To add an Ethernet service:

1. Select **Ethernet** > **Services**. The Ethernet Services page opens (Figure 352).
2. In the Ethernet Services page, click **Add**. The Ethernet Services – Add page opens.

Figure 353 Ethernet Services - Add page



3. In the **Service ID** field, select a unique ID for the service. You can choose any unused value from 1 to 4095. Once you have added the service, you cannot change the Service ID. Service ID 1025 is reserved for a pre-defined management service.
4. In the **Service Type** field, select the service type:

MP – Multipoint

MNG – Management

P2P – Point-to-Point

5. Optionally, in the **EVC ID** field, enter an Ethernet Virtual Connection (EVC) ID (up to 20 characters). This parameter does not affect the network element's behavior, but is used by the NMS for topology management.
6. Optionally, in the **EVC Description** field, enter a text description of the service (up to 64 characters). This parameter does not affect the network element's behavior, but is used by the NMS for topology management.
7. In the **Admin** field, select one of the following options:

Operational - The service is functional.

Reserved - The service is disabled until this parameter is changed to **Operational**. In this mode, the service occupies system resources but is unable to receive and transmit data.

8. In the **MAC table size** field, enter the maximum MAC address table size for the service. The MAC address table is a source MAC address learning table used to forward frames from one service point to another. You can select a value from 16 to 65,520 in multiples of 16. This maximum only applies to dynamic, not static, MAC address table entries.

Note

Additional configuration of the MAC address table can be performed via the CLI. See Defining the MAC Address Forwarding Table for a Service.

9. In the **Default CoS** field, enter a default Class of Service (CoS) value (0-7). This value is assigned to frames at the service level if CoS Mode is set to Default-CoS. Otherwise, this value is not used, and frames retain whatever CoS value they were assigned at the service point or logical interface level.
10. In the **CoS Mode** field, select one of the following options. This parameter determines whether or not frames passing through the service have their CoS modified at the service level. The CoS determines the priority queue to which frames are assigned.

Default CoS – Frames passing through the service are assigned the default CoS defined above. This CoS value overrides whatever CoS may have been assigned at the service point or interface level.

Preserve-SP-COS-Decision – The CoS of frames passing through the service is not modified by the service's default CoS.

11. Click **Apply**, then **Close** to close the Ethernet Services - Add page.
12. Add service points. You must add service points to the service in order for the service to carry traffic. See Configuring Service Points.

10.1.5 Editing a Service

To edit a service:

1. Select **Ethernet** > **Services**. The Ethernet Services page opens (Figure 352).
2. Select the service in the Service Configuration Table.
3. In the Ethernet Services page, click **Edit**. The Ethernet Services - Edit page opens.
4. This page is identical to the Ethernet Services - Add page (Figure 353). You can edit any parameter that can be configured in the Add page, except the **Service ID**.

10.1.6 Deleting a Service

Before deleting a service, you must first delete any service points attached to the service.

To delete a service:

1. Delete all service points attached to the service you wish to delete, as described in Deleting a Service Point.
2. Select **Ethernet** > **Services**. The Ethernet Services page opens (Figure 352).
3. Select the service in the Ethernet Service Configuration Table.
4. Click **Delete.** The service is deleted.

10.1.7 Enabling, Disabling, or Deleting Multiple Services

To enable, disable, or delete multiple services:

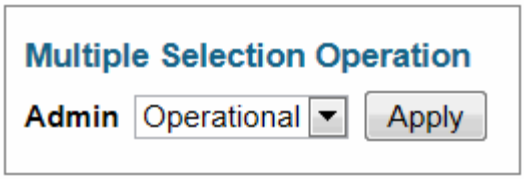
1. Select **Ethernet** > **Services**. The Ethernet Services page opens (Figure 352).
2. Select the services in the Ethernet Services Configuration table, or select all the services by selecting the check box in the top row.

To enable the selected services, in the Multiple Selection Operation section underneath the Ethernet Services Configuration Table, select **Operational** and click **Apply**.

To disable the selected services, in the Multiple Selection Operation section underneath the Ethernet Services Configuration Table, select **Reserved** and click **Apply**.

To delete the selected services, select **Delete** underneath the Ethernet Services Configuration Table. Before deleting a service, you must delete any service points attached to the service, as described in Deleting a Service Point.

Figure 354 Multiple Selection Operation Section (Ethernet Services)



Note

When setting multiple services to **Reserve** state, make sure to avoid setting the management service to **Reserve** state.

When setting multiple services to **Reserve** state, make sure to avoid setting the management service to **Reserve** state

10.1.8 Viewing Service Details

To view the full service parameters:

1. Select **Ethernet > Services**. The Ethernet Services page opens (Figure 352).
2. Select the service in the Ethernet Services Configuration table.
3. In the Ethernet Services page, click **Service Details**. The Ethernet Services – Service Details page opens. The Service Details page contains the same fields as the Add page (Figure 352). However, in the Service Details page, these fields are read-only.

10.1.9 Configuring Service Points

This section includes:

- Ethernet Services Points Overview
- The Ethernet Service Points Page

- Adding a Service Point
- Editing a Service Point
- Deleting a Service Point
- Attaching VLANs

Ethernet Services Points Overview

Service points are logical interfaces within a service. A service point is a logical entity attached to a physical or logical interface. Service points define the movement of frames through the service. Each service point includes both ingress and egress attributes.

Each service point for a Point-to-Point or Multipoint service can be either a Service Access Point (SAP) or a Service Network Point (SNP). A Point-to-Point service can also use Pipe service points.

An SAP is equivalent to a UNI in MEF terminology and defines the connection of the user network with its access points. SAPs are used for Point-to-Point and Multipoint traffic services.

An SNP is equivalent to an NNI or E-NNI in MEF terminology and defines the connection between the network elements in the user network. SNPs are used for Point-to-Point and Multipoint traffic services.

A Pipe service point is used to create traffic connectivity between two ports in a port-based manner (Smart Pipe). In other words, all the traffic from one port passes to the other port.

Management services utilize Management (MNG) service points.

A Point-to-Point or Multipoint service can hold up to 32 service points. A management service can hold up to 30 service points.

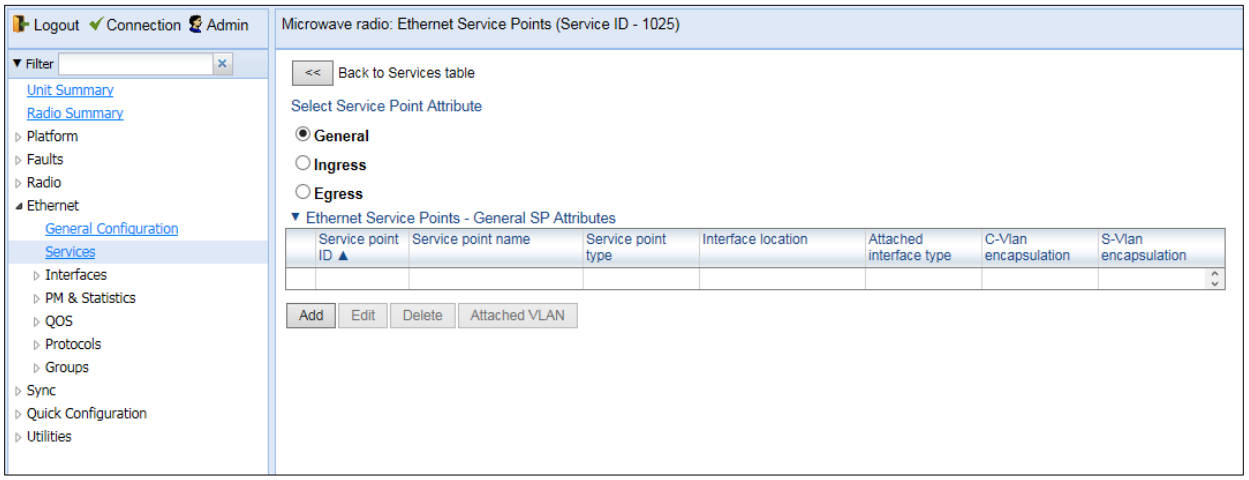
The Ethernet Service Points Page

The Ethernet Service Points page is the starting point for configuring Ethernet service points.

To open the Ethernet Service Points page:

1. Select **Ethernet > Services**. The Ethernet Services page opens (Figure 352).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens.

Figure 355 Ethernet Service Points Page



You can choose to display the following sets of attributes by selecting the appropriate button above the SP Attributes table:

General – See Ethernet Service Points – General SP Attributes Table

Ingress – See 2. Ethernet Service Points – Ingress Attributes

Egress – See 3. Ethernet Service Points – Egress Attributes

To return to the Ethernet Services page at any time, click **Back to Services table** at the top of the Ethernet Service Points page.

1. Ethernet Service Points – General SP Attributes Table

The General SP Attributes table is shown in Figure 355 Ethernet Service Points Page. Table 54 describes the parameters displayed in the General SP Attributes table.

Table 54 General Service Point Attributes

Parameter	Definition
Service point ID	This ID is unique within the service. For Point-to-Point and Multipoint services, the range of values is 1-32. For Management services, the range of values is 1-30. When adding a service point, you can select a service point ID from the available options in the **Service point ID** drop-down list in the Ethernet Service Points – Add page. Once you have added the service point, you cannot change the service point ID.
Service point name	A descriptive name for the service point (optional). The Service Point Name can be up to 20 characters.

Parameter	Definition
Service point type	The service point type. Options are: • **SAP** – Service Access Point. • **SNP** – Service Network Point. • **MNG** – Management service point. • **PIPE** – Pipe service point. The following rules apply to the mixing of different types of service points on a single logical interface: You cannot configure both SAPs and SNPs on the same logical interface. • You can configure both SAPs or SNPs on the same logical interface as a MNG service point. • If you configure a Pipe service point on an interface, you cannot configure an SAP, SNP, or another Pipe service point on the same interface. You can, however, configure an MNG service point on the same interface. • You cannot configure more than one MNG service point on a single logical interface. • Once you have added the service point, you cannot change this parameter.
Interface location	The physical or logical interface on which the service point is located. Once you have added the service point, you cannot change this parameter.
Attached interface type	The encapsulation type (Ethertype) for frames entering the service point. Once you have added the service point, you cannot change this parameter. The Attached Interface Type determines which frames enter the service via this service point, based on the frame's VLAN tagging. Since more than one service point may be associated with a single interface, frames are assigned to the earliest defined service point in case of conflict. For a list of available Attached Interface Types, the types of frames to which each one applies, and the service point types for which each one is available, see Table 55.

Parameter	Definition
C-Vlan encapsulation	The C-VLAN classified into the service point. Options are 1-4094, **Untagged**, or **N.A.** (Not Applicable). Once you have added the service point, you cannot change this parameter. If you selected **Bundle-C** in the **Attached Interface Type** field, select **Untagged** or **N.A**. You can then add multiple C-VLANs via the **Attach VLAN** option. See Attaching VLANs.
S-Vlan encapsulation	The S-VLAN classified into the service point. Options are 1-4094, **Untagged**, or **N.A.** (Not Applicable). Once you have added the service point, you cannot change this parameter. If you selected **Bundle-S** in the **Attached Interface Type** field, select the S-VLAN value to classify into the service point (1-4094), or select **Untagged**. You can then add multiple C-VLANs via the **Attach VLAN** option. See Attaching VLANs.

Table 55 describes the available Attached Interface Types.

Table 55 Attached Interface Types

Attached Interface Type	Types of Frames	Available for Service Point Types
dot1q	A single C-VLAN is classified into the service point.	All
s-tag	A single S-VLAN is classified into the service point.	SNP, PIPE, and MNG
Bundle-C	A set of C-VLANs is classified into the service point.	SAP
Bundle-S	A single S-VLAN and a set of C-VLANs are classified into the service point.	SAP
All-to-One	All C-VLANs and untagged frames that enter the interface are classified into the service point.	SAP

Attached Interface Type	Types of Frames	Available for Service Point Types
Q-in-Q	A single S-VLAN and C-VLAN combination is classified into the service point.	SAP and MNG

2. Ethernet Service Points – Ingress Attributes

Select **Ingress** in the Ethernet Service Points page to display the Ethernet Service Points – Ingress Attributes table. Table 56 describes the parameters displayed in the Ingress SP Attributes table.

Figure 356 Ethernet Service Points Page – Ingress Attributes

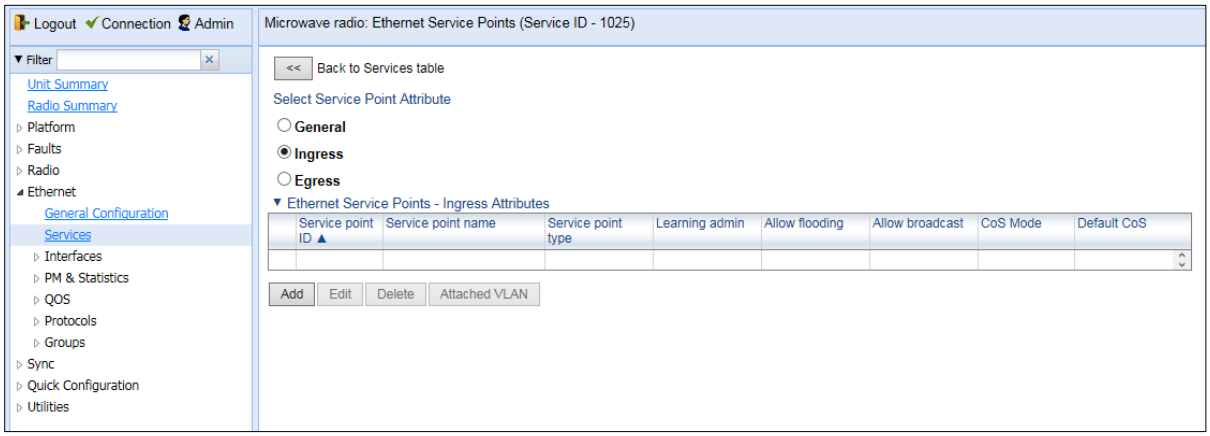


Table 56 Service Point Ingress Attributes

Parameter	Definition
Service point ID	This ID is unique within the service. For Point-to-Point and Multipoint services, the range of values is 1-32. For Management services, the range of values is 1-30.
Service point name	A descriptive name for the service point (optional). The Service Point Name can be up to 20 characters.
Service point type	The service point type. Options are: **SAP** – Service Access Point. **SNP** – Service Network Point. **MNG** – Management service point. **PIPE** – Pipe service point.
Learning admin	Determines whether MAC address learning for incoming frames is enabled (**Enable**) or disabled (**Disable**). When enabled, the service point learns the source MAC addresses of incoming frames and adds them to a MAC address forwarding table.
Allow flooding	Determines whether incoming frames with unknown MAC addresses are forwarded to other service points via flooding. Select **Allow** to allow flooding or **Disable** to disable flooding.
Allow broadcast	Indicates whether frames with a broadcast destination MAC address are allowed to ingress the service via this service point. Select **Allow** to allow broadcast or **Disable** to disable broadcast.

Parameter	Definition
CoS Mode	Indicates how the service point handles the CoS of frames that pass through the service point. Options are: **sp-def-cos** – The service point re-defines the CoS of frames that pass through the service point, according to the Default CoS (below). This decision can be overwritten on the service level. **Interface-Decision** – The service point preserves the CoS decision made at the interface level. The decision can still be overwritten at the service level. **PCL** – Reserved for future use. **TCAM** – Reserved for future use.
Default CoS	The default CoS. If the **CoS Mode** is **sp-def-cos**, this is the CoS assigned to frames that pass through the service point. This decision can be overwritten at the service level. Possible values are 0 to 7.

3. Ethernet Service Points – Egress Attributes

Select **Egress** in the Ethernet Service Points page to display the Ethernet Service Points – Egress Attributes table. Table 57 describes the parameters displayed in the General SP Attributes table.

Figure 357 Ethernet Service Points Page – Egress Attributes

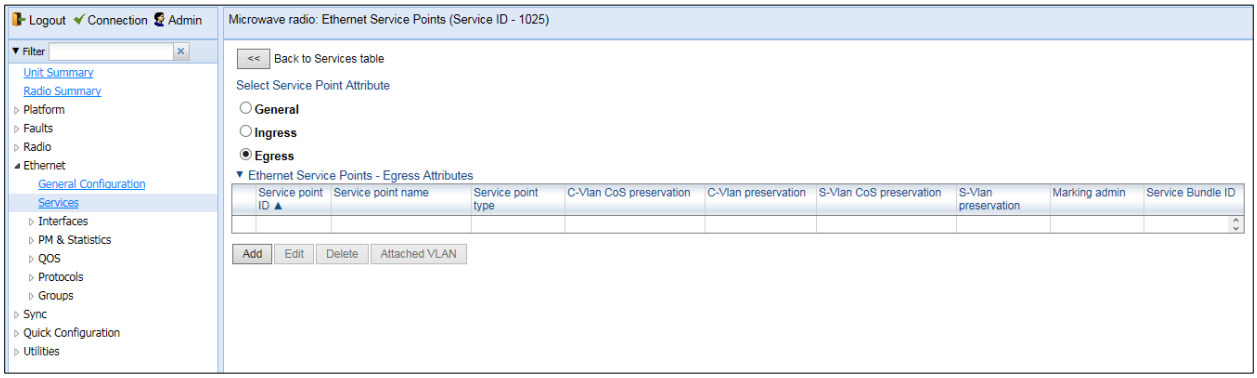


Table 57 Service Point Egress Attributes

Parameter	Definition
Service point ID	This ID is unique within the service. For Point-to-Point and Multipoint services, the range of values is 1-32. For Management services, the range of values is 1-30.
Service point name	A descriptive name for the service point (optional). The Service Point Name can be up to 20 characters.

Parameter	Definition
Service point type	The service point type. Options are: **SAP** – Service Access Point. **SNP** – Service Network Point. **MNG** – Management service point. **PIPE** – Pipe service point.
C-Vlan CoS preservation	Determines whether the original C-VLAN CoS value is preserved or restored for frames egressing from the service point. If C-VLAN CoS preservation is enabled, the C-VLAN CoS value of frames egressing the service point is the same as the value when the frame entered the service. If C-VLAN CoS preservation is disabled, the C-VLAN CoS value of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking.
C-Vlan preservation	Determines whether the original C-VLAN ID is preserved or restored for frames egressing from the service point. If C-VLAN preservation is enabled, the C-VLAN ID of frames egressing the service point is the same as the C-VLAN ID when the frame entered the service. If C-VLAN preservation is disabled, the C-VLAN ID of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking
S-Vlan CoS preservation	Determines whether the original S-VLAN CoS value is preserved or restored for frames egressing from the service point. If S-VLAN CoS preservation is enabled, the S-VLAN CoS value of frames egressing the service point is the same as the value when the frame entered the service. If S-VLAN CoS preservation is disabled, the C-VLAN CoS value of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking

Parameter	Definition
S-Vlan preservation	Read-only. Indicates whether the original S-VLAN ID is preserved or restored for frames egressing from the service point. If S-VLAN preservation is enabled, the S-VLAN ID of frames egressing the service point is the same as the S-VLAN ID when the frame entered the service. If S-VLAN preservation is disabled, the S-VLAN ID of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking
Marking admin	Determines whether re-marking of the outer VLAN (C-VLAN or S-VLAN) of tagged frames that pass through the service point is enabled. If **Marking admin** is set to **Enable**, and CoS preservation for the relevant outer VLAN is set to **Disable**, the SAP re-marks the C-VLAN or S-VLAN 802.1p UP bits of egress frames according to the calculated CoS and Color, and the user-configurable 802.1Q and 802.1AD marking tables. You can configure these tables by selecting **Ethernet > QoS > Marking** from the menu on the left side of the Web EMS. If **Marking admin** and CoS preservation for the relevant outer VLAN are both set to **Enable**, re-marking is not performed. If **Marking admin** and CoS preservation for the relevant outer VLAN are both set to **Disable**, re-marking is applied, but only according to the values defined for Green frames in the 802.1Q and 802.1AD marking tables.
Service Bundle ID	If H-QoS is enabled on the interface to which the service point is assigned, you can select Service Bundle ID 1-6. Otherwise, only Service Bundle ID 1 is supported. Once a service point has been created, you cannot edit the Service Bundle ID. Instead, you must delete the service point and create a new service point with the desired Service Bundle ID. Note: In System Release 11.9, H-QoS is only supported with PTP 850C. For PTP 850E, H-QoS is planned for future release.

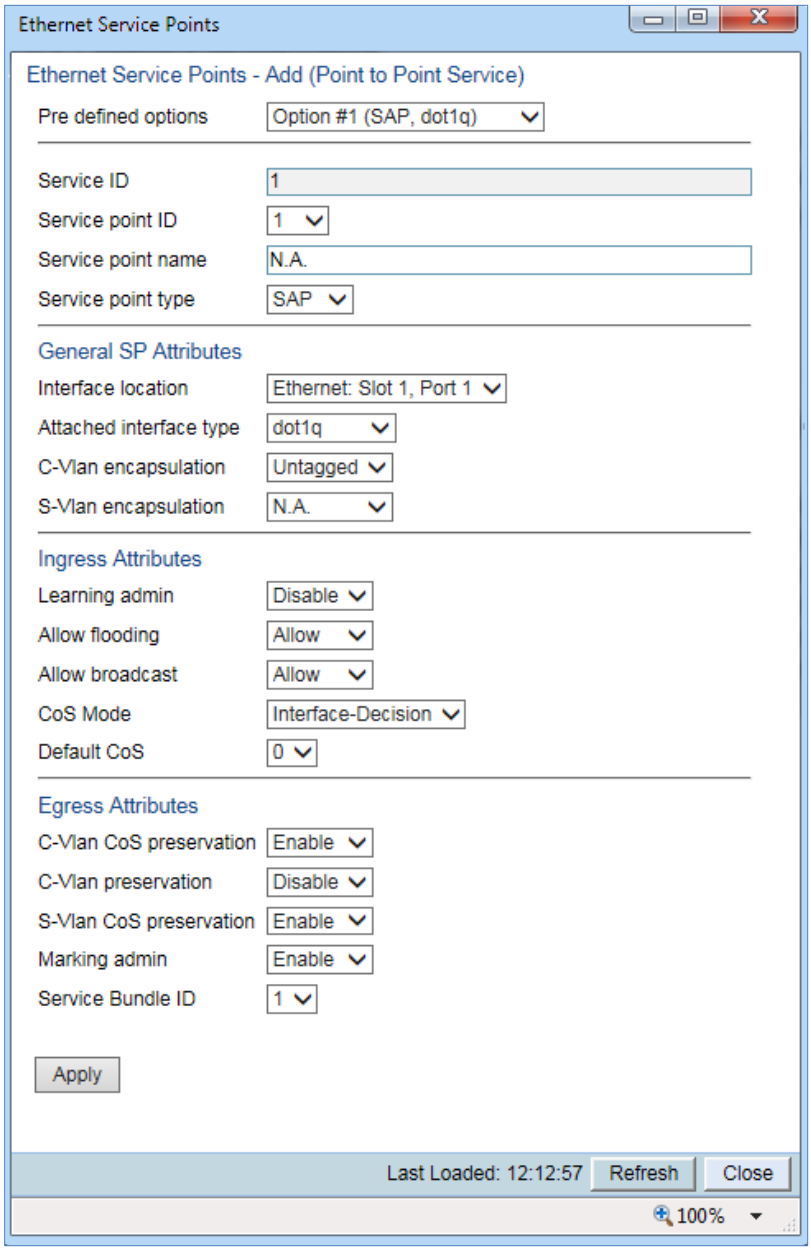
Adding a Service Point

To add a service point:

1. Select **Ethernet > Services**. The Ethernet Services page opens.
2. Select the relevant service in the Ethernet Services Configuration table.

3. Click **Service Points**. The Ethernet Service Points page opens.
4. Select the relevant service point in the Ethernet Services Points – General SP Attributes table.
5. Click **Add**. The Ethernet Service Points – Add page opens.

Figure 358 Ethernet Service Points - Add Page



6. Configure the service point attributes, as described in Table 54, Table 56, and Table 57.



Note

Optionally, you can select from a list of pre-defined service point options in the **Pre defined options** field at the top of the Ethernet Service Points - Add page. The system automatically populates the remaining service point parameters according to the system-defined parameters. However, you can manually change these parameter values. The pre-defined options are customized to the type of service to which you are adding the service point.

7. Click **Apply**, then **Close**.

Editing a Service Point

To edit a service point:

1. Select **Ethernet > Services**. The Ethernet Services page opens (Figure 352).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens (Figure 355).
4. Select the relevant service point in the Ethernet Services Points – General SP Attributes table.
5. Click **Edit**. The Ethernet Service Points– Edit page opens. The Ethernet Service Points – Edit page is similar to the Ethernet Service Points - Add page (Figure 358). You can edit any parameter that can be configured in the Add Service Point page, except **Service Point ID**, **Service Point Type**, and the **General SP Attributes**.
6. Edit the service point attributes, as described in Table 54, Table 56, and Table 57.
7. Click **Apply**, then **Close**.

Deleting a Service Point

You can only delete a service point with an **Attached Interface Type** of **Bundle-C** or **Bundle-S** if no VLANs are attached to the service point. See Attaching VLANs.

To delete a service point:

1. Select **Ethernet > Services**. The Ethernet Services page opens (Figure 352).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens (Figure 355).
4. Select the relevant service point in the Ethernet Services Points – General SP Attributes table.
5. Click **Delete**. The service point is deleted.

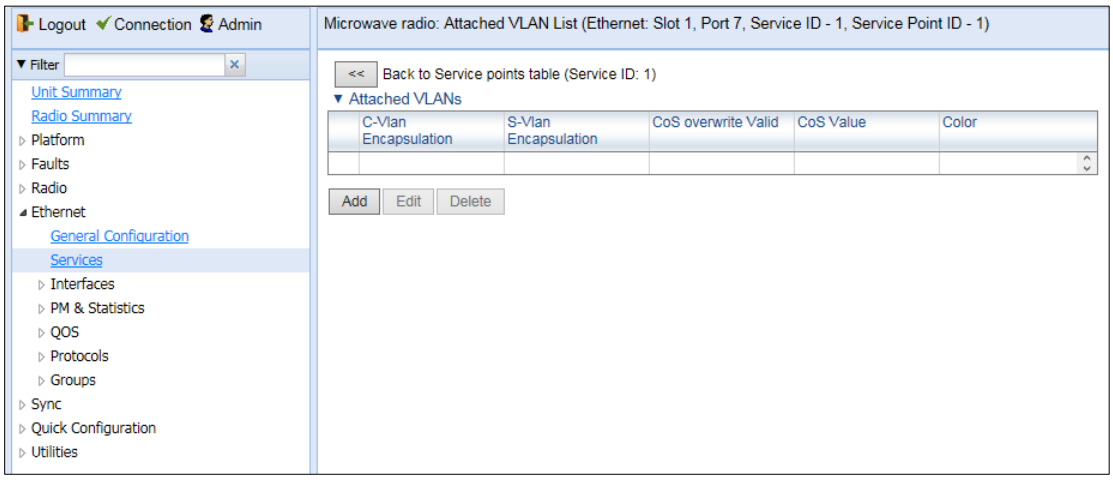
Attaching VLANs

When the Attached Interface Type for a service point is set to Bundle-C or Bundle-S, you can add multiple C-VLANs to the service point.

To add multiple C-VLANs:

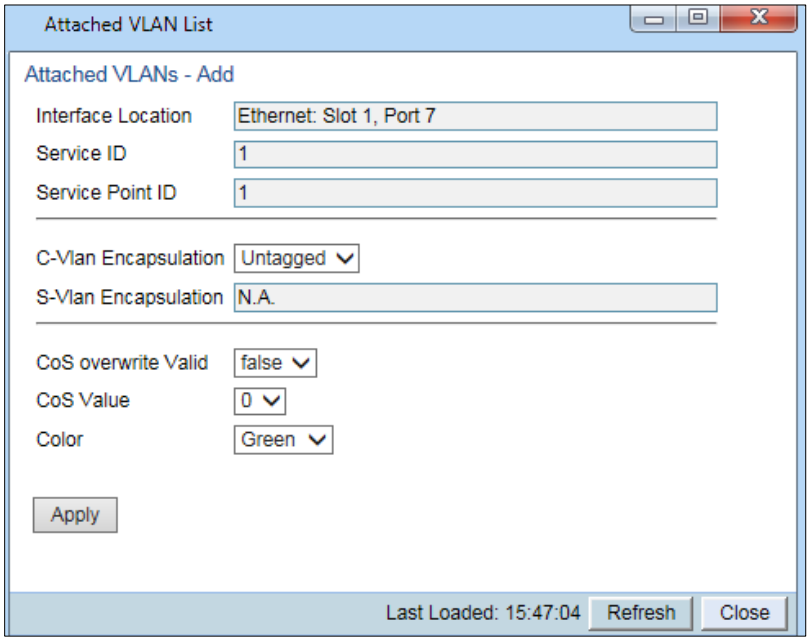
1. Select **Ethernet > Services**. The Ethernet Services page opens (Figure 352).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens (Figure 355).
4. Select the relevant service point in the Ethernet Services Points – General SP Attributes table.
5. Click **Attached VLAN**. The Attached VLAN List page opens.

Figure 359 Attached VLAN List Page



6. Click **Add**. The Attached VLAN List - Add page opens.

Figure 360 Attached VLAN List - Add Page



7. Configure the VLAN Classification parameters, described in Table 58.
8. Click **Apply**, then **Close**.

Table 58 VLAN Classification Parameters

Parameter	Definition
Interface Location	Read-only. The physical or logical interface on which the service point is located.
Service ID	Read-only. The ID of the service to which the service point belongs.
Service Point ID	Read-only. The ID of the service point.
C-Vlan Encapsulation	Select the C-VLAN you want to add to the service point.
S-Vlan Encapsulation	Read-only. If the **Attached Interface Type** for the service point is **Bundle-S**, this field displays the S-VLAN encapsulation selected when the service point was created. If the **Attached Interface Type** for the service point is **Bundle-C**, this field is inactive.
CoS Overwrite Valid	If you want to assign a specific CoS and Color to frames with the C-VLAN or S-VLAN defined in the **C-VLAN Encapsulation** field, select **true**. This CoS and Color values defined below override the CoS and Color decisions made at the interface level. However, if the service point or service are configured to apply their own CoS and Color decisions, those decisions override the decision made here.
CoS Value	If **CoS Overwrite Valid** is set to **true**, the CoS value defined in this field is applied to frames with the C-VLAN defined in the **C-VLAN Encapsulation** field. This CoS overrides the CoS decision made at the interface level. However, if the service point or service are configured to apply their own CoS, that decision overrides the decision made here. If CoS Overwrite Valid is set to false, this parameter has no effect.
Color	If **CoS Overwrite Valid** is set to **true**, the Color value defined in this field is applied to frames with the C-VLAN defined in the **C-VLAN Encapsulation** field. This Color overrides the Color decision made at the interface level. However, if the service point or service are configured to apply their own Color, that decision overrides the decision made here. If **CoS Overwrite Valid** is set to **false**, this parameter has no effect.

To edit a VLAN Classification table entry, select the entry in the VLAN Classification table and click **Edit**. You can edit all the fields that can be configured in the Attached VLAN List – Add page, except the **C-VLAN Encapsulation** field.

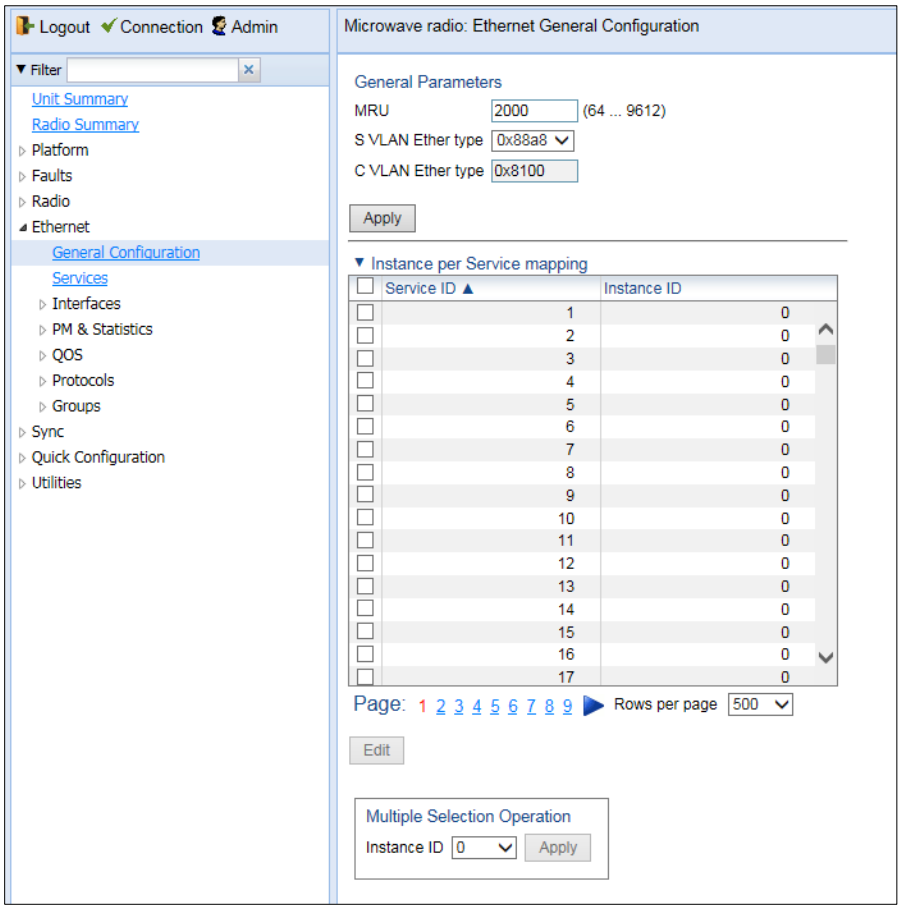
To delete a VLAN Classification table entry, select the entry in the VLAN Classification table and click **Delete**.

10.2 Setting the MRU Size and the S-VLAN Ethertype

To configure the size of the MRU (Maximum Receive Unit) and the S-VLAN Ethertype:

1. Select **Ethernet > General Configuration**. The Ethernet General Configuration page opens.

Figure 361 Ethernet General Configuration Page



2. In the **MRU** field, enter the global size (in bytes) of the Maximum Receive Unit (MRU). Permitted values are 64 to 9612. The default value is 2000. Frames that are larger than the global MRU will be discarded.

Note: For PTP 850C and PTP 850E, after setting the MRU to a value higher than 2000, the unit should be reset. Similarly, if the MRU is changed from a value higher than 2000 to 2000 or lower, the unit should be reset.

3. In the **S VLAN Ether type** field, select the S-VLAN Ethertype. This defines the ethertype recognized by the system as the S-VLAN ethertype. Options are: 0x8100, 0x88A8, 0x9100, and 0x9200. The default value is 0x88A8.



Note

The C-VLAN Ethertype is set at 0x8100 and cannot be modified.

4. Click **Apply**.

10.2.1 S-VLAN Ethertype 0x8100 (CISCO Mode)

When the S-VLAN Ethertype is set to 0x8100 (CISCO mode), another VLAN tag is added at the egress s-tag service point.

In the case of an All-to-One service point to an s-tag service point, the additional VLAN tag can be removed by the ingress s-tag service point on the remote unit:

1 Select **Ethernet** > **Services**. The Ethernet Services page opens
2 Select the relevant service in the Ethernet Services Configuration table.
3 Click **Service Points**. The Ethernet Service Points page opens
4 Select the relevant service point in the Ethernet Services Points – General SP Attributes table.
5 Click **Edit**. The Ethernet Service Points– Edit page opens. The Ethernet Service Points – Edit page is similar to the Ethernet Service Points.
6 In the **Remove outer VLAN** field, select **Enable**.
7 Click **Apply**, then **Close**.

In the case of an s-tag service point to an s-tag service point, addition of another VLAN tag can be avoided by disabling C-VLAN preservation. This should be done on both service points in order to address both traffic directions.

To disable C-VLAN preservation:

1 Select **Ethernet** > **Services**. The Ethernet Services page opens.
2 Select the relevant service in the Ethernet Services Configuration table.
3 Click **Service Points**. The Ethernet Service Points page opens.
4 Select the relevant service point in the Ethernet Services Points – General SP Attributes table.
5 Click **Edit**. The Ethernet Service Points– Edit page opens. The Ethernet Service Points – Edit page is similar to the Ethernet Service Points - Add page.
6 In the **C-VLAN preservation** field, select **Disable**.
7 Click **Apply**, then **Close**.

10.3 Configuring Ethernet Interfaces

Related Topics:

- Enabling the Interfaces (Interface Manager)
- Performing Ethernet Loopback
- Configuring Ethernet Service(s)
- Quality of Service (QoS)

The PTP 850's switching fabric distinguishes between physical interfaces and logical interfaces. Physical and logical interfaces serve different purposes in the switching fabric. In some cases, a physical interface corresponds to a logical interface on a one-to-one basis. For some features, such as LAG, a group of physical interfaces can be joined into a single logical interface.

The basic interface characteristics, such as media type, port speed, duplex, and auto negotiation, are configured for the physical interface via the Physical Interfaces page. Ethernet services, QoS, and OAM characteristics are configured on the logical interface level.

The QSFP interface (P4) on an PTP 850E requires special configuration of the QSFP mode before configuring the normal physical interface parameters. Before changing the **QSFP Mode**, you must verify that:

- The **Admin** status of Eth 3, Eth 4, Eth 5, and Eth 6 is **Down**. See Enabling the Interfaces (Interface Manager).

Note: If the QSFP interface is already set to **40Gbps Ethernet**, Eth 4, Eth 5, and Eth 6 do not appear in the Interface Manager, and are not relevant.

- No service point is attached to the interface. See Configuring Service Points.
- No ASP pair is assigned to the interface. See **Error! Reference source not found.**.
- No Policer is attached to the interface. See Assigning Policers to Interfaces.
- No Shaper is attached to the interface. See **Error! Reference source not found.**.
- The interface is not part of a LAG group. See **Error! Reference source not found.**.
- No synchronization is configured on the interface. See **Error! Reference source not found.**.

To configure the QSFP interface:

1 Select **Platform > Interfaces > QSFP**. The QSFP Module Configuration page opens.

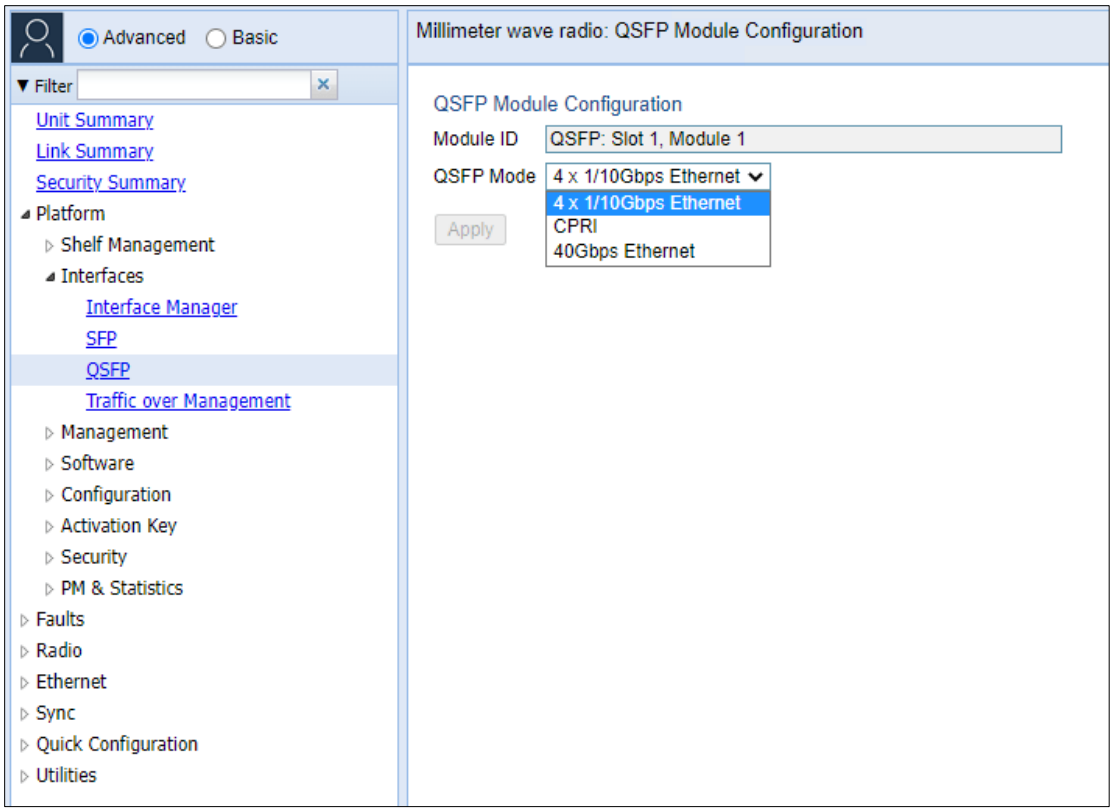


Figure 362: QSFP Module Configuration Page

2 Select from the following options:

- **10Gbps Ethernet** – Select this for 4x1/10 and 1x1/10 Gbps configurations. Then click **Apply** and proceed to the Physical Interfaces page to configure the parameters of the interface(s).
- **CPRI** – See Error! Reference source not found..
- **40Gbps Ethernet** – Select this for 1x40 Gbps configurations. Then click **Apply**. There is no need to procced to the Physical Interfaces page because the parameters of the interface are set:
  - Auto Negotiation is Off
  - Speed is 40 Gbps
  - Full Duplex

To configure the physical interface parameters:

1 Select **Ethernet** > **Interfaces** > **Physical Interfaces**. The Physical Interfaces page opens.

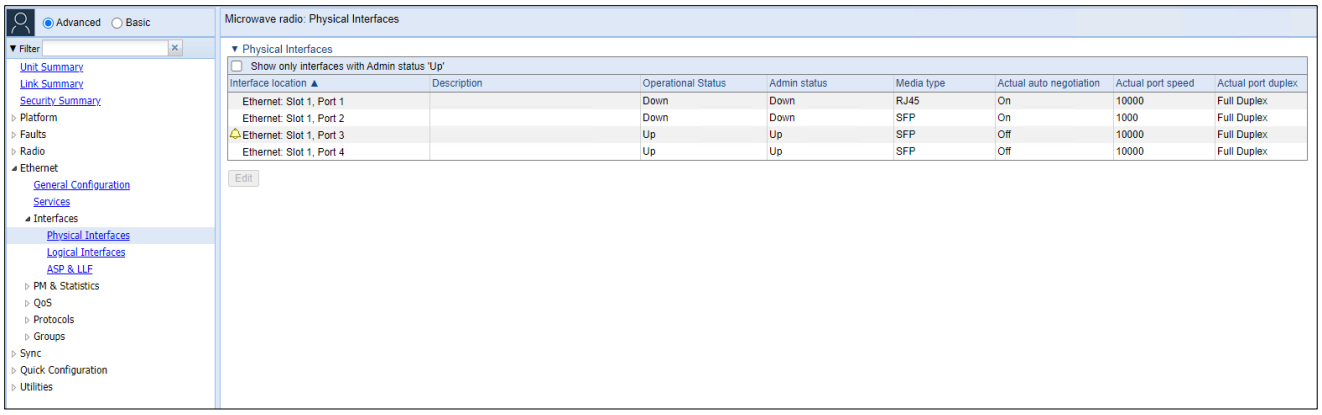


Figure 363: Physical Interfaces Page – PTP 850C

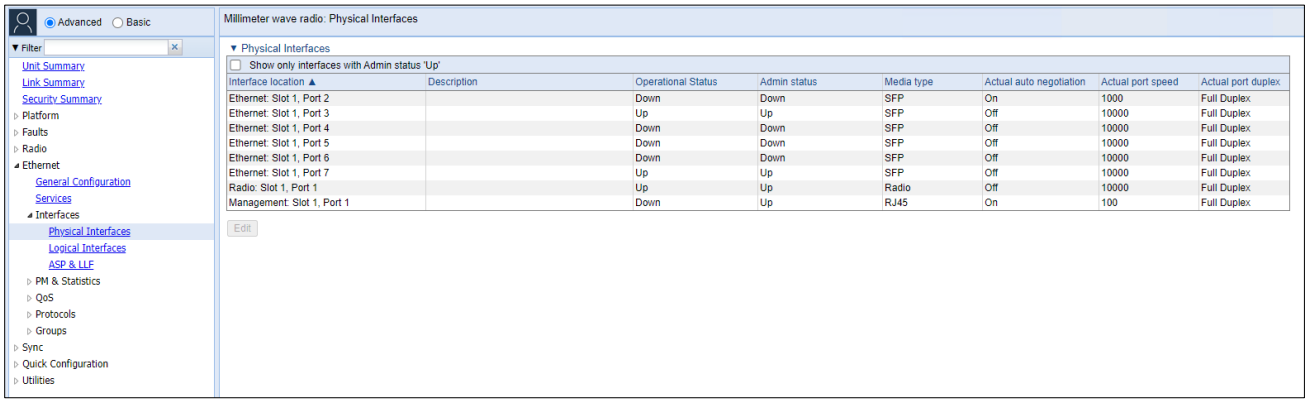


Figure 364: Physical Interfaces Page – PTP 850E

If an alarm is currently raised on an interface, an alarm icon appears to the left of the interface location. To display details about the alarm or alarms in tooltip format, hover the mouse over the alarm icon.

Note: In Release 12.9:

For PTP 850C, Ethernet Slot 1, Ports 1, 2, 3, and 4 are supported.

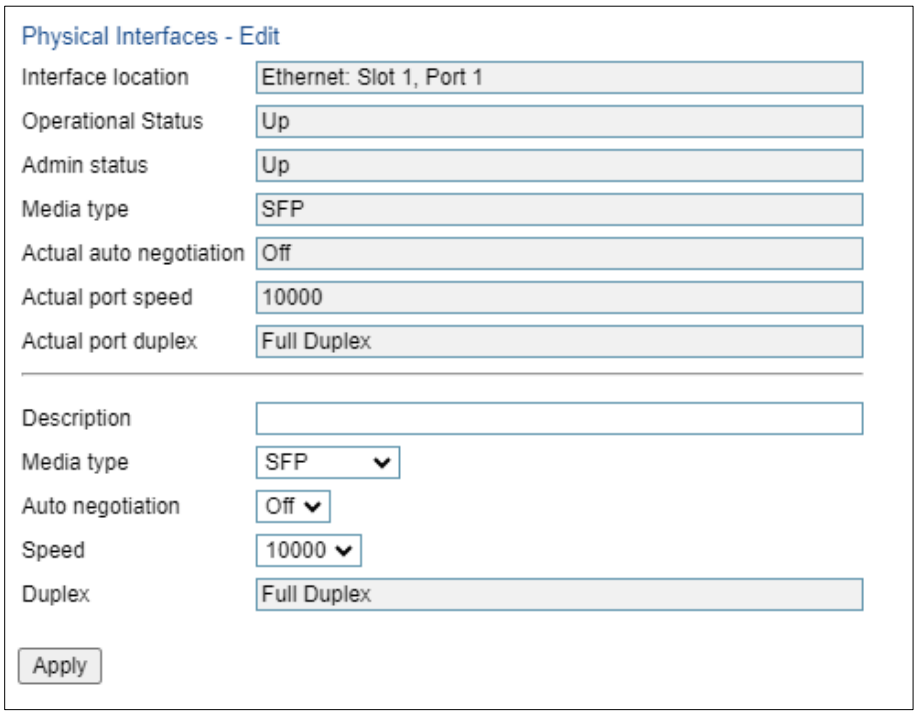
For PTP 850E, Ethernet Slot 1, Ports 2 through 7 are supported. The Management port (Management: Slot 1 Port 1) can also be used for traffic. For details on using the Management port for traffic, see **Error! Reference source not found.**.

The QSFP port (Port 4) on PTP 850E devices is displayed as follows.

- In a 4x1/10G configuration the QSFP port can provide four Ethernet interfaces: Eth 3, Eth 4, Eth 5, and Eth 6. In this configuration, a QSFP transceiver is attached to the QSFP port, and an MPO-MPO cable is connected between the transceiver and a splitter. The splitter splits the traffic between four Ethernet cables connecting the splitter to the customer equipment.
- The QSFP port can also be used with a QSFP-to-SFP adaptor to provide a 1x1/10G configuration. In this configuration, the port is displayed as Ethernet Slot 1, Port 3.
- In 1x40G configurations, the port is displayed as Ethernet Slot 1, Port 3. Once the port has been configured in the QSFP Module Configuration page, no further port configuration is necessary.

2 Select the interface you want to configure and click **Edit**. The Physical Interfaces - Edit page opens.

Figure 365 Physical Interfaces - Edit Page



9. Optionally, in the **Description** field, enter a description of the interface.

10. In the **Media type** field, select the physical interface layer 1 media type. Options are:

Auto-Type – NA.

RJ45 – An electrical (RJ-45) Ethernet interface.

SFP – An optical (SFP) Ethernet interface.

Radio – A radio interface.

11. In the **Auto negotiation** field, select **On** to enable or **Off** to disable Auto-Negotiation. When the Media-Type is **Radio**, Auto Negotiation is always **Off**.

a. For Ethernet interfaces, the default value is **Off**:

   i. For Ports 3 to 6 (the QSFP ports), **Off** is the only supported value.

ii. For Port 7 if the Speed is set to 10000 (10G), Auto Negotiation is not available, and the setting must remain **Off**. If the speed is set to 1000 (1G), **Auto negotiation** can be set to **Off** (default) or **On**.

12. In the **Speed** field, select the maximum speed of the interface in Mbps. Options are:

Ethernet RJ-45 interfaces –**100** and **1000**.

Ethernet SFP interfaces – Only **1000**is supported.

Ethernet SFP+ and QSFP interfaces – Only **1000** and **10000** are supported.

Radio interfaces – The parameter is read-only and set by the system to **1000FD**.



Note

After changing the speed of an SFP+ interface, you must reset the unit in order for the change to take effect.

13. In the **Duplex** field, select the interface's duplex setting (**Full-Duplex** or **Half-Duplex**). Only Full-Duplex is available in this release.

14. Click **Apply**, then **Close**.

The following tables summarize the Speed and Auto-Negotiation options for the Ethernet traffic ports.

Table 59 Ethernet Interface Speed and Auto-Negotiation Options – PTP 850C

Interface	Physical Port Number	Notes	Speed (Mbps)	Auto-Negotiation
Eth 1	P2	RJ-45	1000/2500/10000	On
Eth 2	P3	SFP	2500	Depends on speed.
Eth 3	P4	SFP+	1000/10000	Off

Table 60 Ethernet Interface Speed and Auto-Negotiation Options – PTP 850S

Interface	Physical Port Number	Notes	Speed (Mbps)	Auto-Negotiation
Eth 1	P3	SFP+	1000/10000	On/Off
Eth2	P2	SFP/CSFP	100/1000	Off only
Eth3	P3	Only available with CSFP.	100/1000	Off only

Parameter	Definition
Interface location	The location of the interface.
Operational Status	Indicates whether the interface is currently operational (**Up**) or non-operational (**Down**).
Admin Status	Indicates whether the interface is currently enabled (**Up**) or disabled (**Down**). You can enable or disable an interface from the Interface Manager page. See Enabling the Interfaces (Interface Manager).
Media Type	The physical interface layer 1 media type.
Actual auto negotiation	Displays the actual auto negotiation state of the interface. For electrical SFPs, this is determined by the module's specifications rather than the configured value. All Cambium-approved electrical SFP transceivers operate with Auto Negotiation on. For other interface types, this should be identical to the configured value.
Actual port speed	Displays the actual speed of the interface for the link as agreed by the two sides of the link after the auto negotiation process.
Actual port duplex	Displays the actual duplex status of the interface for the link as agreed by the two sides of the link after the auto negotiation process.

Ethernet Interface Speed and Auto-Negotiation Options – PTP 850E

Interface	Physical Port Number	Notes	Speed (Mbps)	Auto-Negotiation
Eth 2	P3	P3. Multiband interface (SFP). Only supported for PTP 850E.	1000	Off only
Eth3	P4	QSFP.	1000/10000/40000	Off only
Eth4	P4	QSFP. Only availabl	1000/10000	Off only

		e with QSFP transceiver in P4.		
Eth5	P4	QSFP. Only available with QSFP transceiver in P4.	1000/10000	Off only

Table 61 describes the status parameters that appear in the Physical Interfaces page.

Table 61 Physical Interface Status Parameters

10.4 Configuring Automatic State Propagation and Link Loss Forwarding

Automatic state propagation enables propagation of radio failures back to the Ethernet port. You can also configure Automatic State Propagation to close the Ethernet port based on a radio failure at the remote carrier.

Automatic state propagation is configured as pairs of interfaces. Each interface pair includes one Monitored Interface and one Controlled Interface. You can create multiple pairs using the same monitored interface and multiple controlled interfaces.

The Monitored Interface is a radio interface, or a radio protection or Multi-Carrier ABC group. The Controlled Interface is an Ethernet interface or LAG. An Ethernet interface can only be assigned to one Monitored interface.

Each Controlled Interface is assigned an LLF ID. If **ASP trigger by remote fault** is enabled on the remote side of the link, the ASP state of the Controlled Interface is propagated to the Controlled Interface with the same LLF ID at the remote side of the link. This means if ASP is triggered locally, it is propagated to the remote side of the link, but only to Controlled Interfaces with LLF IDs that match the LLF IDs of the affected Controlled Interfaces on the local side of the link.



Note

LLF requires an activation key (SL-LLF). Without this activation key, only LLF ID 1 is available.

The following events in the Monitored Interface trigger ASP:

- Radio LOF
- Radio Excessive BER

- Radio LOC
- Remote Radio LOF
- Remote Excessive BER
- Remote LOC

The user can also configure the ASP pair so that Radio LOF, Radio Excessive BER, or loss of the Ethernet connection at the remote side of the link will also trigger ASP.

In addition, ASP is triggered if the Controlled Interface is a LAG, and the physical interfaces that belong to the LAG are set to **Admin = Down** in the Interface Manager.

When a triggering event takes place:

If the Controlled Interface is an electrical GbE port, the port is closed.

If the Controlled Interface is an optical GbE port, the port is muted.

The Controlled Interface remains closed or muted until all triggering events are cleared.

In addition, when a local triggering event takes place, the ASP mechanism sends an indication to the remote side of the link. Even when no triggering event has taken place, the ASP mechanism sends periodic update messages indicating that no triggering event has taken place.

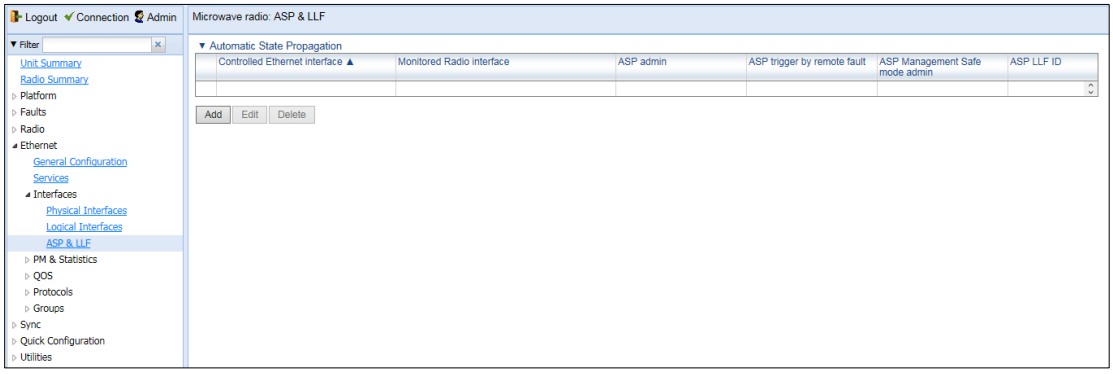
A trigger delay time can be configured, so that when a triggering event takes place, the ASP mechanism does not propagate the event until this delay time has elapsed. A trigger delay from 0 to 10,000 ms can be set per LLD ID. The delay time must be configured via CLI. See Configuring Automatic State Propogation and Link Loss Forwarding (CLI).

It is recommended to configure both ends of the link to the same Automatic State Propagation configuration.

To configure an Automatic State Propagation interface pair:

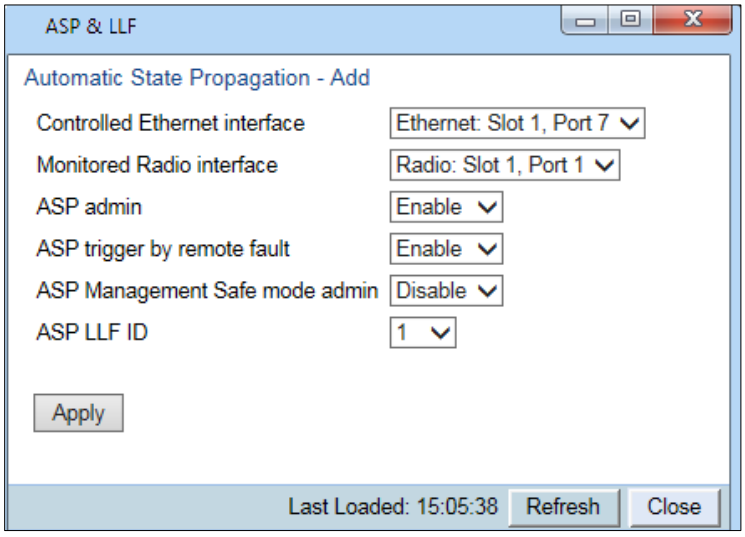
1. Select **Ethernet > Interfaces > Automatic State Propagation**. The Automatic State Propagation page opens.

Figure 366 Automatic State Propagation Page



2. Click **Add**. The Automatic State Propagation - Add page opens.

Figure 367 Automatic State Propagation - Add Page



3. In the **Controlled Ethernet interface** field, select an interface that will be disabled upon failure of the Monitored Radio Interface, defined below.
4. In the **Monitored Radio interface** field, select the Monitored Radio Interface. The Controlled Ethernet Interface, defined above, is disabled upon a failure indication on the Monitored Radio Interface.
5. In the **ASP admin** field, select **Enable** to enable Automatic State Propagation on the interface pair, or **Disable** to disable Automatic State Propagation on the pair.
6. Optionally, in the**ASP trigger by remote fault** field, select **Enable** if you want to configure the system to disable the Controlled Ethernet Interface upon a radio failure at the remote side of the link from the Monitored Radio Interface. ASP events will only be propagated to Controlled Interfaces with LLF IDs that match LLF IDs of affected Controlled Interfaces at the other side of the link.
7. Optionally, in the **ASP Management Safe mode admin** field, select **Enable** or **Disable** to enable or disable ASP Management Safe mode. In ASP Management Safe mode, the ASP mechanism does not physically shut down the Controlled Interface when ASP is triggered. Instead, the ASP mechanism sends a failure indication message. This message is used to propagate the failure indication to external equipment.
8. In the **ASP LLF ID** field, select an ID for Link Loss Forwarding (LLF). When **ASP trigger by remote fault** is set to **Enable**, ASP events at the other side of the link are propagated to Controlled Interfaces with LLF IDs that match the LLF IDs of affected Controlled Interfaces at the other side of the link. LLF IDs are unique per Monitored Interface. That is, if LLF ID 1 has been used for a Controlled Interface that is grouped with radio interface 1, that ID cannot be used again for another Controlled Interface grouped fixed radio interface 1. However, it *can* be used for Controlled Interface grouped with radio interface 2. You can select an LLF ID between 1 and 30.
9. Repeat this procedure to assign additional Controlled Interfaces to the Monitored Interface, or to set up additional ASP pair with other interfaces. Controlled Interfaces can only be assigned to one ASP pair. Monitored Interfaces can be assigned to multiple ASP pairs.

To edit an Automatic State Propagation interface pair:

1. Select the interface pair in the Automatic state propagation configuration table.
2. Click **Edit**. The Automatic State Propagation – Edit page opens. The Edit page is similar to the Add page (Figure 367), but the **Controlled Ethernet Interface** and **Monitored Radio Interface** parameters are read-only.

To delete an Automatic State Propagation interface pair:

1. Select the interface pair in the Automatic state propagation configuration table.
2. Click **Delete**. The interface pair is removed from the Automatic state propagation configuration table.

To delete multiple interface pairs:

1. Select the interface pairs in the Automatic state propagation configuration table or select all the interfaces by selecting the check box in the top row.
2. Click **Delete**. The interface pairs are removed from the Automatic state propagation configuration table.

10.5 Viewing Ethernet PMs and Statistics

PTP 850 stores and displays statistics in accordance with RMON and RMON2 standards. You can display various peak TX and RX rates (per second) and average TX and RX rates (per second), both in bytes and in packets, for each measured time interval. You can also display the number of seconds in the interval during which TX and RX rates exceeded the configured threshold.

This section includes:

- RMON Statistics
- Port TX Statistics
- Port RX Statistics

10.5.1 RMON Statistics

RMON counters per frame size are not available for individual radio interfaces and radio groups. For Link Bonding groups, TX counters are available but not RX counters. For radio members of Link Bonding groups, all counters are available.

In Multiband (non-Link Bonding) and Layer 1 Link Aggregation configurations, there is no distinction between regular and idle packets in RMON statistics for the Ethernet interface connected to the attached unit (the Traffic interface). Therefore, it is recommended to rely on Capacity, Throughput, and Utilization PMs for the Traffic interface. See ***Error! Reference source not found.***.

To view and reset RMON statistics:

1. Select **Ethernet > PM & Statistics > RMON**. The RMON page opens.

Figure 368 RMON Page PTP 850C

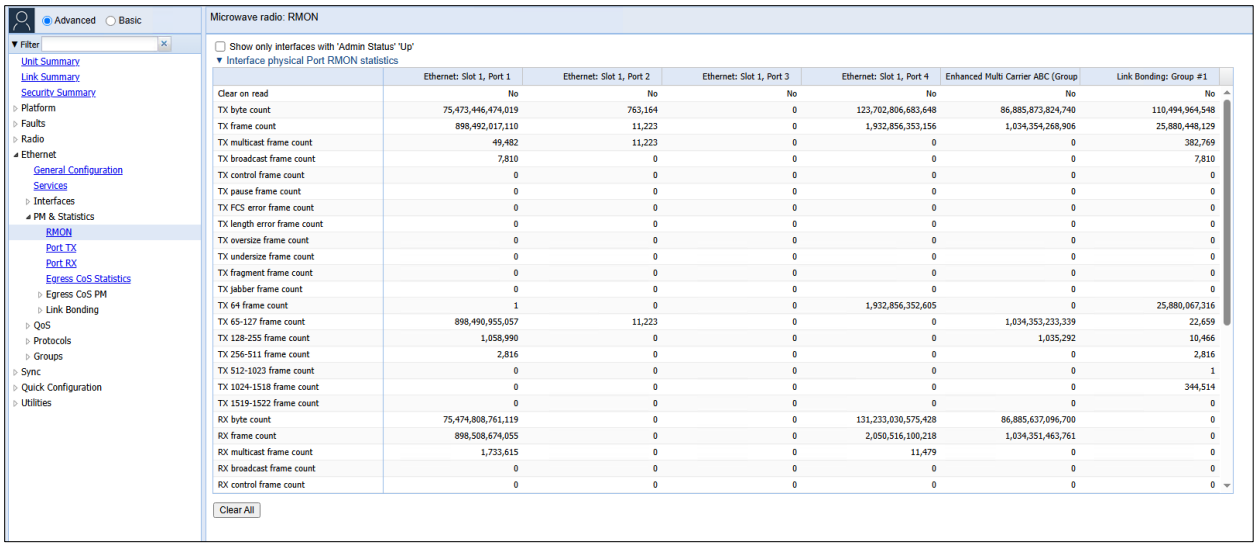
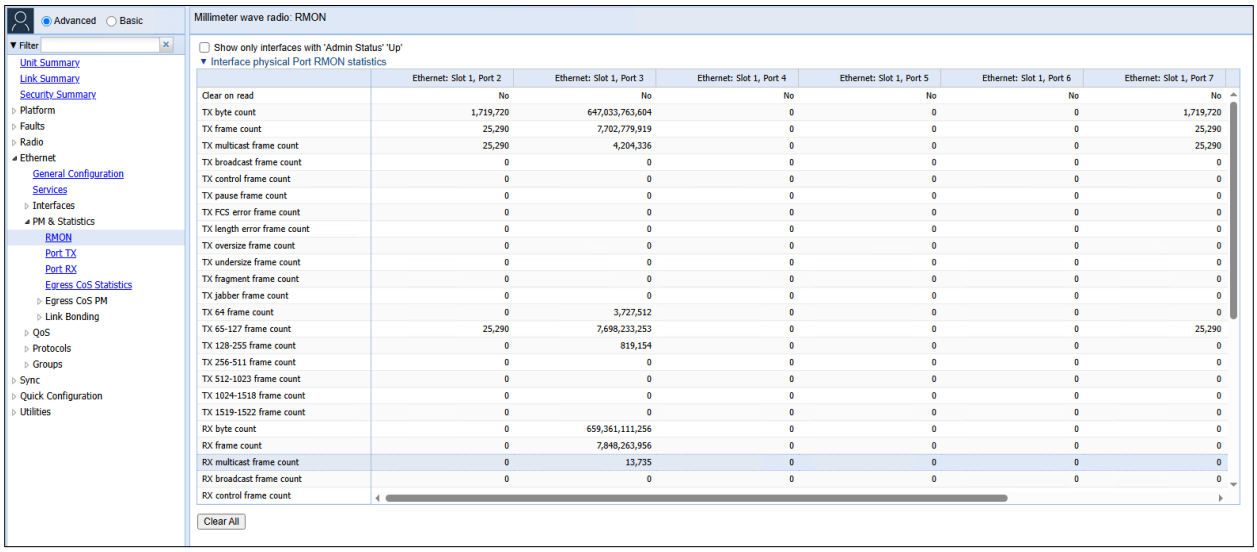


Figure 369 RMON Page PTP 850E



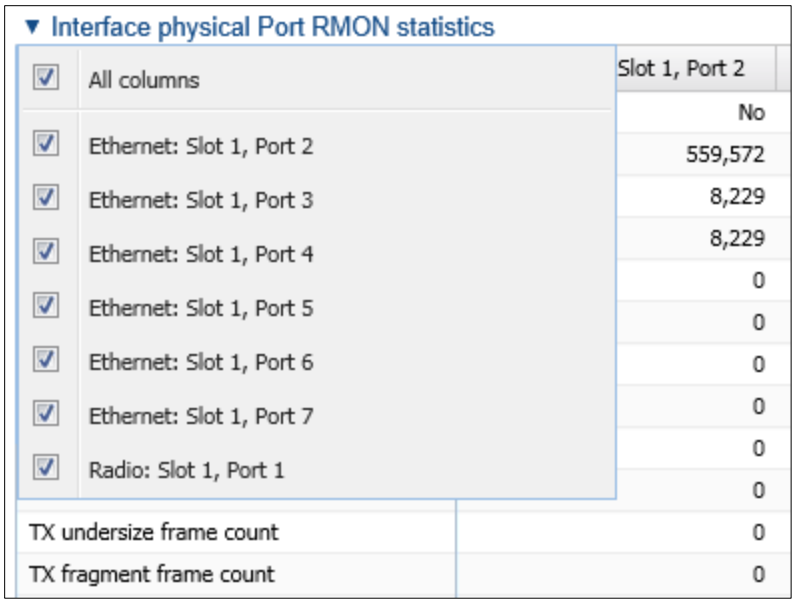
To clear the statistics, click **Clear All** at the bottom of the page.

To refresh the statistics, click **Refresh** at the bottom of the page.

Each column in the RMON page displays RMON statistics for one of the unit's interfaces. To hide or display columns:

1. Click the arrow next to the table title (**Interface Physical Port RMON Statistics**).
2. Mark the interfaces you want to display and clear the interfaces you do not want to display.

Figure 370 RMON Page – Hiding and Displaying Columns



Note

If you click the table title itself, all columns are hidden. To un-hide the columns, click the table title again.

10.5.2 Egress CoS Statistics

You can display packet egress statistics per CoS value. For each CoS value, the following statistics are displayed per Color (Green and Yellow):

- Number of packets transmitted
- Number of packets dropped
- Number of bytes transmitted
- Number of bytes dropped

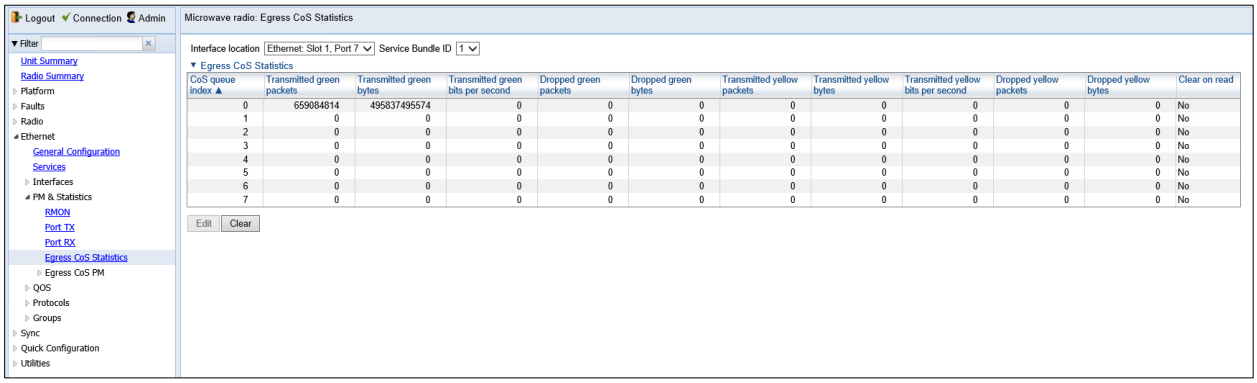
Note

Transmitted bits per second are not supported in the current release.

To display egress CoS statistics:

1. Select **Ethernet > PM & Statistics > Egress CoS Statistics**. The Egress CoS Statistics page opens.

Figure 371 Egress Cos Statistics Page



2. In the **Show Service bundle ID** field, select select the Service Bundle ID for which you want to display statistics.

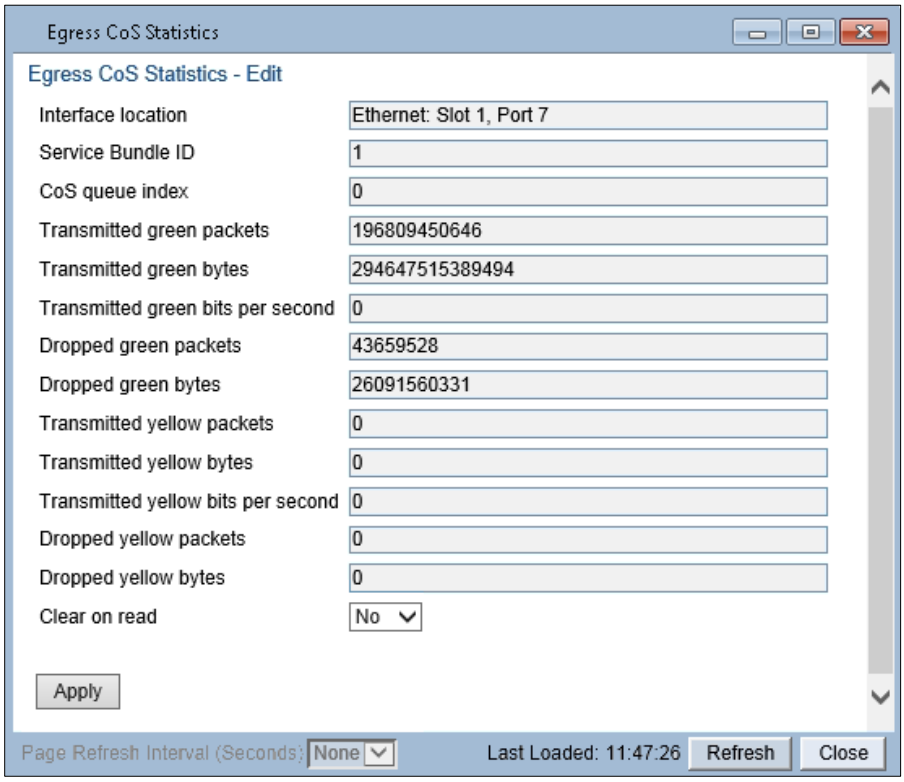
Note

Service Bundles are bundles of queues, grouped together in order to configure common egress characteristics for specific services. If H-QoS is enabled on the interface, you can select Service Bundle ID 1-6. Otherwise, only Service Bundle ID 1 is supported.
To view statistics for the pre-defined management service point, select Service Bundle ID 7. Egress CoS statistics are displayed for Service Bundle ID 7, regardless of which Service Bundle ID is actually assigned to the management service point.
In Systerm Release 11.9, H-QoS is only supported with PTP 850C. For PTP 850E, H-QoS is planned for future release.

By default, the egress CoS statistics are cumulative. That is, they are not automatically cleared. You can set each individual CoS number to be cleared whenever the Egress CoS Statistics page is opened by changing the Clear on read value to **Yes**.

1. To change the clear on read value, select the CoS number in the CoS queue index column and click **Edit**. The Egress CoS Statistics – Edit page opens.

Figure 372 Egress CoS Statistics – Edit Page



2. In the **Clear on read** field, select **Yes** to have statistics for the CoS value cleared every time you open the page.
3. Click **Apply**.

10.5.3 Port TX Statistics

The Ethernet Port TX PM report page displays PMs that measure various peak transmission rates (per second) and average transmission rates (per second), both in bytes and in packets, for each measured time interval.

The page also displays the number of seconds in the interval during which transmission rates exceeded the configured threshold.

This section includes:

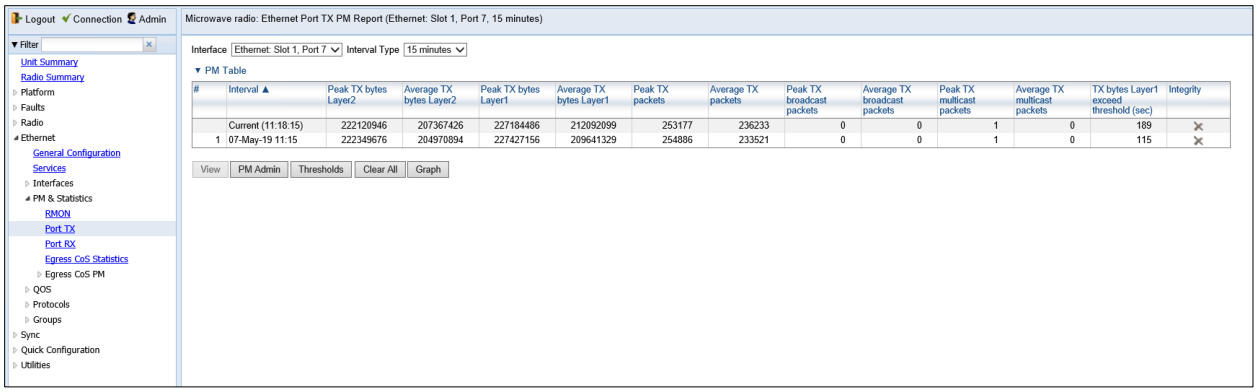
- Displaying Ethernet Port TX PMs
- Enabling or Disabling Gathering of Port TX PM Statistics per Interface
- Setting the Ethernet Port TX Threshold

Displaying Ethernet Port TX PMs

To display Ethernet Port TX PMs:

1. Select **Ethernet** > **PM & Statistics** > **Port TX**. The Ethernet Port TX PM Report page opens.

Figure 373 Ethernet Port TX PM Report Page



2. In the **Interface** field, select the interface for which you want to display PMs.
3. In the **Interval Type** field:

To display reports for the past 24 hours, in 15 minute intervals, select **15 minutes**.

To display reports for the past month, in daily intervals, select **24 hours**.

Table 62 describes the Ethernet TX port PMs.

Table 62 Ethernet TX Port PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Peak... Average... bytes... Packets...	Various peak transmission rates (per second) and average transmission rates (per second), both in bytes and in packets, for each measured time interval.
TX bytes Layer 1 exceed threshold (sec)	The number of seconds the TX bytes exceeded the specified threshold during the interval. For instructions on setting the threshold, see Setting the Ethernet Port TX Threshold.
Invalid data flag	Indicates whether the values received during the measured interval are valid. An x in the column indicates that the values are not valid (for example, because of a power surge or power failure that occurred during the interval).

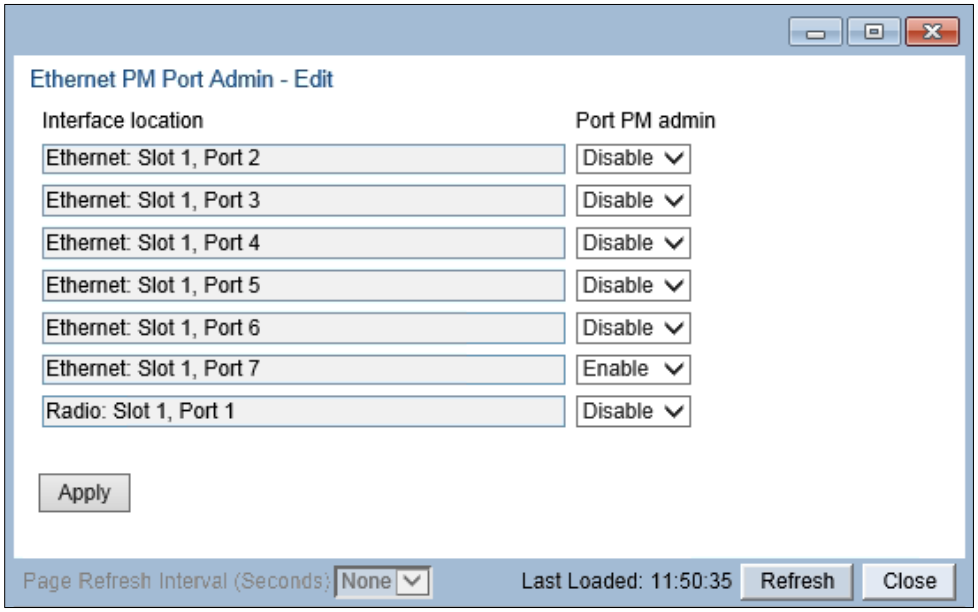
To clear the PMs, click **Clear All**.

Enabling or Disabling Gathering of Port TX PM Statistics per Interface

To select the interfaces for which to gather and display Port TX PMs:

1. In the Ethernet Port TX PM Report page, click **PM Admin**. The Ethernet PM Port Admin page opens.

Figure 374 Ethernet PM Port Admin Page



2. Select the interface.
3. Click **Enable Port PM** or **Disable Port PM** to enable or disable the gathering of Port TX PMs on the selected interface.
4. Click **Close**.

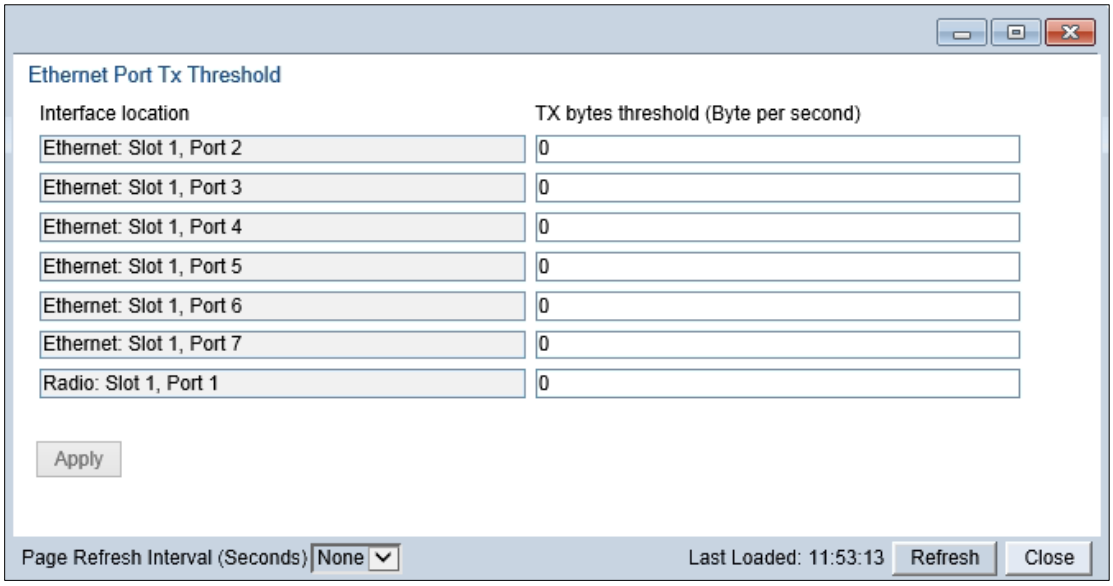
Setting the Ethernet Port TX Threshold

The **TX bytes Layer 1 exceed threshold (sec)** column shows, for each interval, the number of seconds the TX bytes exceeded the specified threshold during the interval:

To view and set this threshold:

1. In the Ethernet Port TX PM Report page, click **Threshold**. The Ethernet Port Tx Threshold page opens.

Figure 375 Ethernet Port Tx Threshold Page



2. Enter a threshold, between 0 and 4294967295.
3. Click **Apply**, then **Close**.

10.5.4 Port RX Statistics

The Ethernet Port RX PM report page displays PMs that measure various peak transmission rates (per second) and average RX rates (per second), both in bytes and in packets, for each measured time interval.

The page also displays the number of seconds in the interval during which RX rates exceeded the configured threshold.

This section includes:

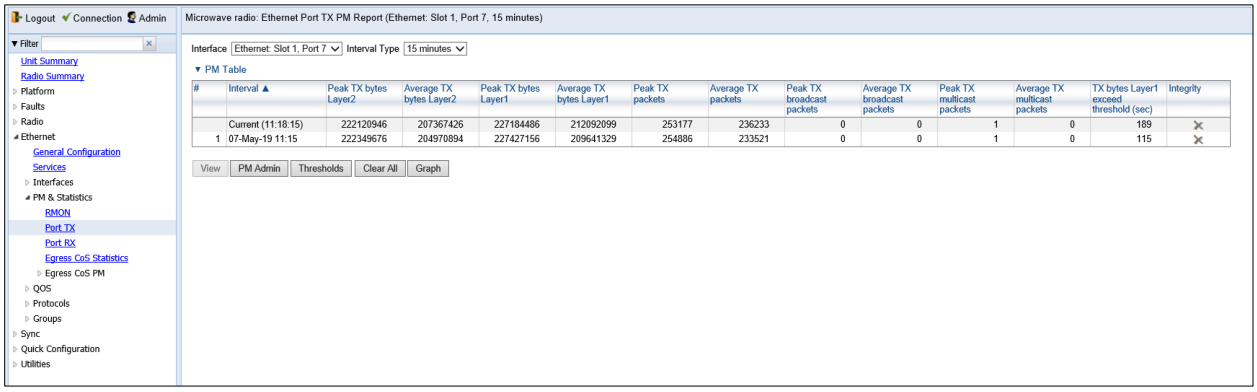
- Displaying Ethernet Port RX PMs
- Enabling or Disabling Gathering of Port RX PM Statistics per Interface
- Setting the Ethernet Port RX Threshold

Displaying Ethernet Port RX PMs

To display Ethernet Port RX PMs:

1. Select **Ethernet > PM & Statistics > Port RX**. The Ethernet Port RX PM Report page opens.

Figure 376: Ethernet Port RX PM Report Page



2. In the **Interface** field, select the interface for which you want to display PMs.
3. In the **Interval Type** field:

To display reports for the past 24 hours, in 15 minute intervals, select **15 minutes**.

To display reports for the past month, in daily intervals, select **24 hours**.

Table 63 describes the Ethernet RX port PMs.

Table 63 Ethernet RX Port PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Peak... Average... bytes... Packets...	Various peak transmission rates (per second) and average RX rates (per second), both in bytes and in packets, for each measured time interval.
RX bytes Layer 1 exceed threshold (sec)	The number of seconds the RX bytes exceeded the specified threshold during the interval. For instructions on setting the threshold, see Setting the Ethernet Port RX Threshold.
Invalid data flag	Indicates whether the values received during the measured interval are valid. An x in the column indicates that the values are not valid (for example, because of a power surge or power failure that occurred during the interval).

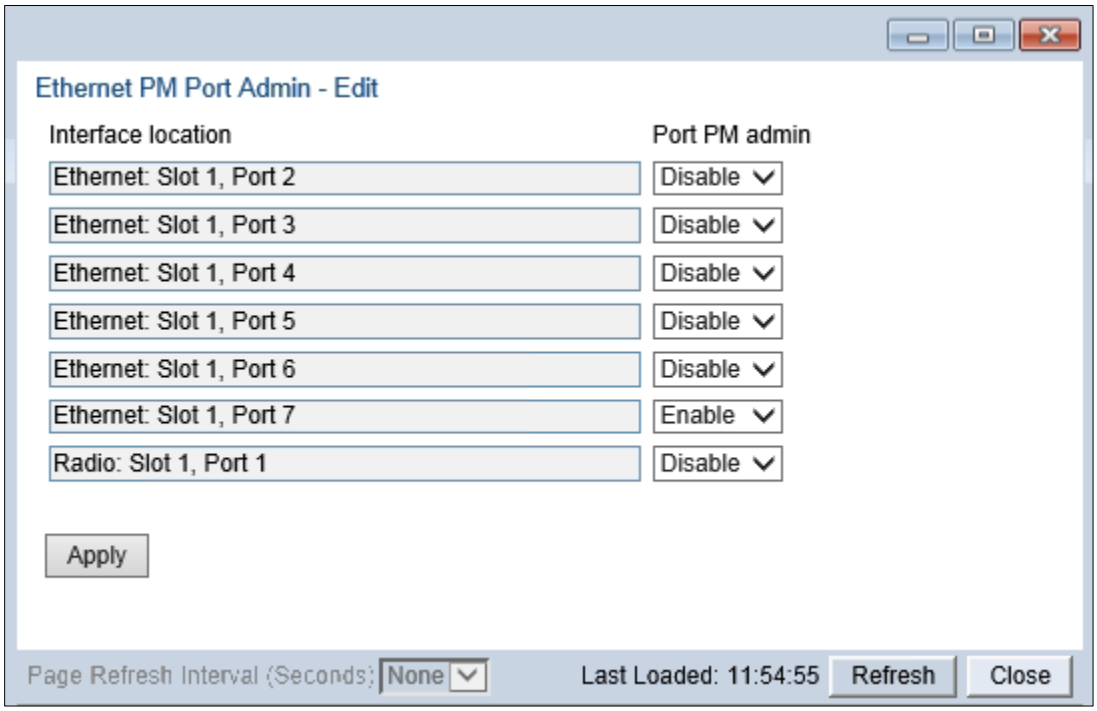
To clear the PMs, click **Clear All**.

Enabling or Disabling Gathering of Port RX PM Statistics per Interface

To select the interfaces for which to gather and display Port RX PMs:

1. In the Ethernet Port RX PM Report page, click **PM Admin**. The Ethernet PM Port Admin page opens.

Figure 377 Ethernet PM Port Admin Page



2. In the field to the right of the interface, select **Enable** or **Disable** to enable or disable the gathering of Port PMs on the interface.
3. Click **Close**.

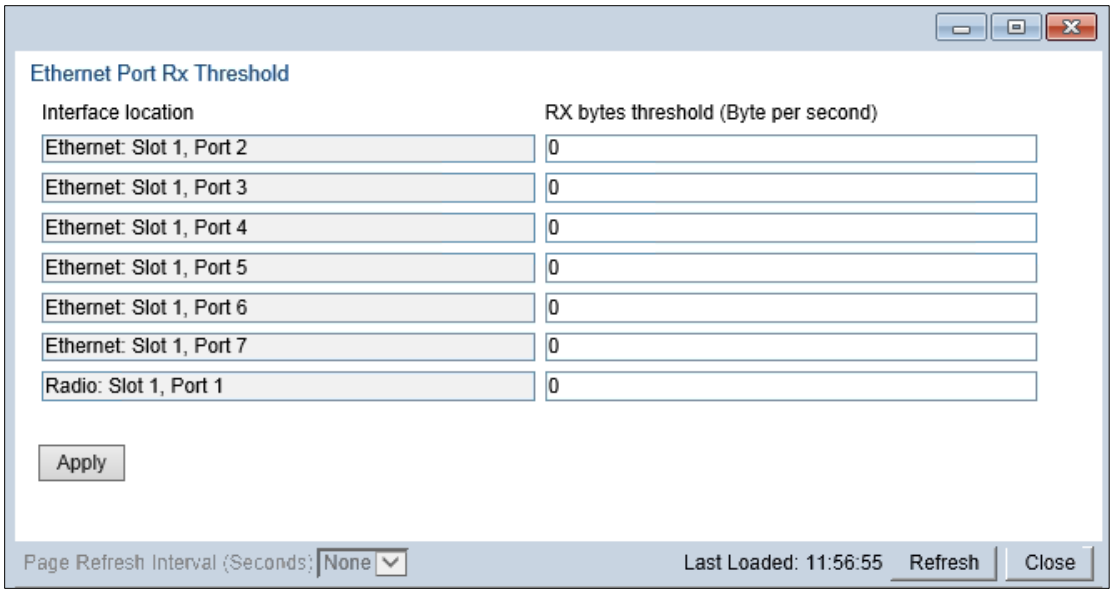
Setting the Ethernet Port RX Threshold

The **RX bytes Layer 1 exceed threshold (sec)** column shows for each interval, the number of seconds the RX bytes exceeded the specified threshold during the interval:

To view and set this threshold:

1. In the Ethernet Port RX PM Report page, click **Threshold**. The Ethernet Port Rx Threshold page opens.

Figure 378 Ethernet Port Rx Threshold Page



2. For each interface, you can enter a threshold, in bytes per second, between 0 and 4294967295.
3. Click **Apply**, then **Close**.

11. Quality of Service (QoS)

This section includes:

- QoS Overview
- Configuring Classification
- Configuring Policers (Rate Metering)
- Configuring Marking
- Configuring WRED
- Configuring Egress Shaping
- Configuring Scheduling
- Enabling Hierarchical QoS (H-QoS
- Configuring and Displaying Queue-Level PMs

11.1 QoS Overview

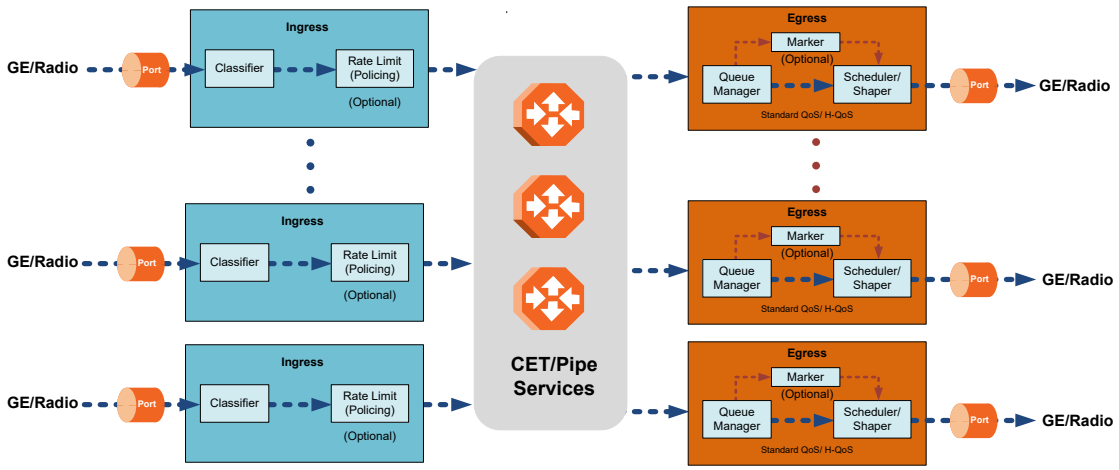
Quality of Service (QoS) deals with the way frames are handled within the switching fabric. QoS is required in order to deal with many different network scenarios, such as traffic congestion, packet availability, and delay restrictions.

PTP 850's personalized QoS enables operators to handle a wide and diverse range of scenarios. PTP 850's smart QoS mechanism operates from the frame's ingress into the switching fabric until the moment the frame egresses via the destination port.

QoS capability is very important due to the diverse topologies that exist in today's network scenarios. These can include, for example, streams from two different ports that egress via single port, or a port-to-port connection that holds hundreds of services. In each topology, a customized approach to handling QoS will provide the best results.

Figure 379 shows the basic flow of PTP 850's QoS mechanism. Traffic ingresses (left to right) via the Ethernet or radio interfaces, on the "ingress path." Based on the services model, the system determines how to route the traffic. Traffic is then directed to the most appropriate output queue via the "egress path."

Figure 379 QoS Block Diagram



The ingress path consists of the following QoS building blocks:

Ingress Classifier – A hierarchical mechanism that deals with ingress traffic on three different levels: interface, service point, and service. The classifier determines the exact traffic stream and associates it with the appropriate service. It also calculates an ingress frame CoS and Color. CoS and Color classification can be performed on three levels, according to the user's configuration.

Ingress Rate Metering – A hierarchical mechanism that deals with ingress traffic on three different levels: interface, service point, and service point CoS. The rate metering mechanism enables the system to measure the incoming frame rate on different levels using a TrTCM standard MEF rate meter, and to determine whether to modify the color calculated during the classification stage.

Note

Ingress rate meters can be configure per service point or per service point CoS, but not on both.

The egress path consists of the following QoS building blocks:

Queue Manager – This is the mechanism responsible for managing the transmission queues, utilizing smart WRED per queue and per packet color (Green or Yellow).

Scheduling and Shaping – A hierarchical mechanism that is responsible for scheduling the transmission of frames from the transmission queues, based on priority among queues, Weighted Fair Queuing (WFQ) in bytes per each transmission queue, and eligibility to transmit based on required shaping on several different levels (per queue, per service bundle, and per port).

Marker – This mechanism provides the ability to modify priority bits in frames based on the calculated CoS and Color.

For a more detailed description of QoS in the PTP 850, refer to the Technical Description for the PTP 850 product type you are using.

The following two modes of operation are available on the egress path:

- **Standard QoS** – This mode provides eight transmission queues per port.
- **Hierarchical QoS (H-QoS)** – In this mode, users can associate services from the service model to configurable groups of eight transmission queues (service bundles), from a total 8K queues. In H-QoS mode, PTP 850C performs QoS in a hierarchical manner in which the egress path is managed on three levels: ports, service bundles, and specific queues. This enables users to fully distinguish between streams, therefore providing a true SLA to operators.

Note: In System Release 11.9, H-QoS is only available for PTP 850C. Support for H-QoS with PTP 850E is planned for future release.

The following figure illustrates the difference between how standard QoS and H-QoS handle traffic:

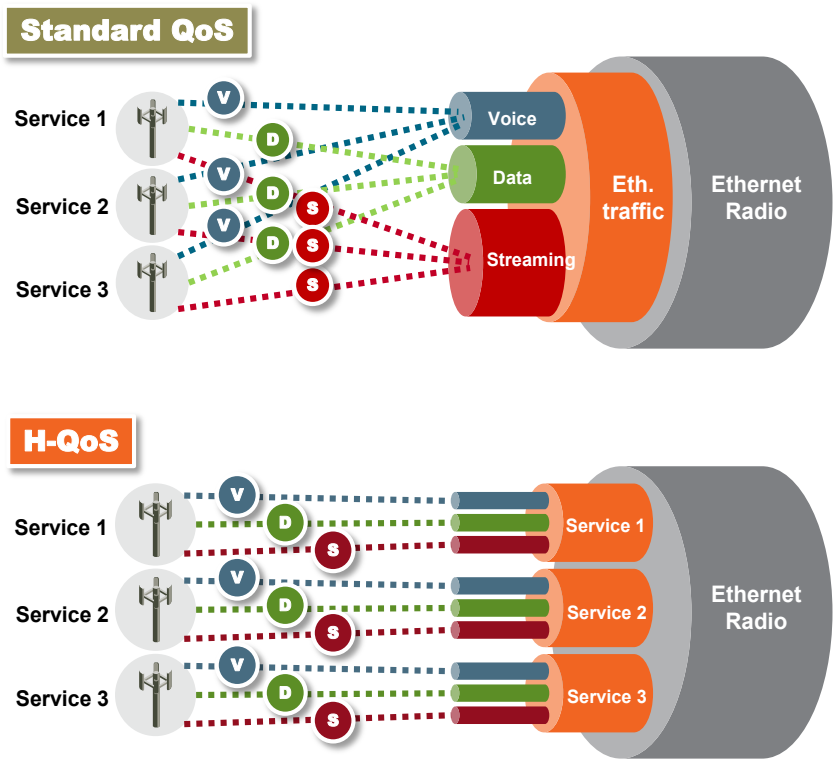


Figure 380: Standard QoS and H-QoS Comparison

H-QoS must be enabled on the logical interface level. For instructions, see Enabling Hierarchical QoS (H-QoS.

11.2 Configuring Classification

The hierarchical classifier consists of the following levels:

Logical interface-level classification

Service point-level classification

Service level classification

This section explains how to configure classification at the logical interface level.

For instructions how to configure classification at the service point level, see 2. Ethernet Service Points – Ingress Attributes.

For instructions how to configure classification at the service level, see Adding an Ethernet Service.

This section includes:

- Classification Overview
- Configuring Ingress Path Classification on a Logical Interface
- Modifying the C-VLAN 802.1Q UP and CFI Bit Classification Table
- Modifying the S-VLAN 802.1 UP and DEI Bit Classification Table
- Modifying the DSCP Classification Table
- Modifying the MPLS EXP Bit Classification Table

In addition to the procedures described in this section, you can specify a specific CoS and Color for a specific VLAN ID. This is the highest classification priority on the logical interface level, and overrides any other classification criteria at the logical interface level. Classification by VLAN ID can only be configured via CLI. See Configuring VLAN Classification and Override (CLI).

11.2.1 Classification Overview

PTP 850 supports a hierarchical classification mechanism. The classification mechanism examines incoming frames and determines their CoS and Color. The benefit of hierarchical classification is that it provides the ability to “zoom in” or “zoom out”, enabling classification at higher or lower levels of the hierarchy. The nature of each traffic stream defines which level of the hierarchical classifier to apply, or whether to use several levels of the classification hierarchy in parallel.

Classification takes place on the logical interface level according to the following priorities:

- VLAN ID (CLI-only – see Configuring VLAN Classification and Override (CLI))
- 802.1p bits
- DSCP bits (only considered if MPLS is not present, regardless of trust setting)
- MPLS EXP field
- Default interface CoS

For PTP 850S, classification is performed according to the following priorities:

- VLAN ID (CLI-only – see Configuring VLAN Classification and Override (CLI))
- 802.1p bits
- DSCP bits

PTP 850 performs the classification on each frame ingressing the system via the logical interface. Classification is performed step by step from the highest priority to the lowest priority classification method. Once a match is found, the classifier determines the CoS and Color decision for the frame for the logical interface-level.

You can disable some of these classification methods by configuring them as un-trusted. For example, if 802.1p classification is configured as un-trusted for a specific interface, the classification mechanism does not perform classification by UP bits. This is useful, for example, if classification is based on DSCP priority bits.

If no match is found at the logical interface level, the default CoS is applied to incoming frames at this level. In this case, the Color of the frame is assumed to be Green.

For PTP 850S, classification may also be performed by Destination MAC Address (MAC DA) at the service point level. When MAC DA classification is enabled on a service point, the classification mechanism checks each frame ingressing the interface on which the service point is defined against a list of user-defined MAC DAs. If there is a match, the mechanism applies to the frame the CoS and Color defined for that MAC DA. Classification by MAC DA overrides the other classification criteria at the service point level.

Up to 64 MAC addresses can be defined per device, including four predefined MAC addresses. You can assign each of these MAC addresses a CoS value and a Color.

The following MAC addresses are predefined, with a high priority (CoS=7, Color=Green). You can edit or delete these MAC addresses:

- 09:00:2B:00:00:04
- 09:00:2B:00:00:05
- 01:80:C2:00:00:14
- 01:80:C2:00:00:15

These are protocol MAC addresses used to transport IS-IS frames as defined in ISO 9542 and ISO/IEC 10589.

11.2.2 Configuring Ingress Path Classification on a Logical Interface

This section explains how to configure the classification criteria per each logical interface. The following sections explain how to modify the classification tables per bit type.

To configure the classification criteria for a logical interface:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens.

Figure 381 Logical Interfaces Page-PTP 850C

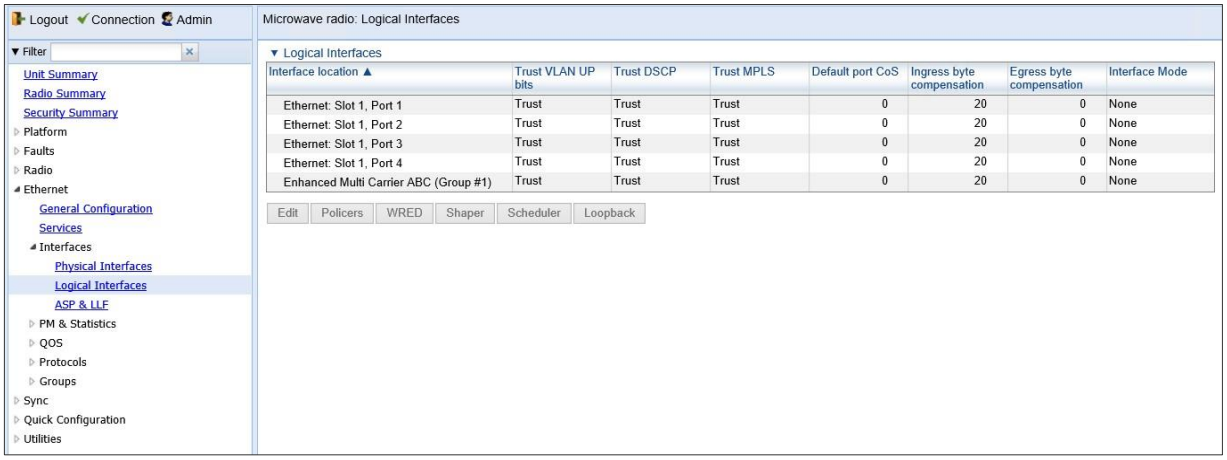


Table 64 Logical Interfaces Page-PTP 850S

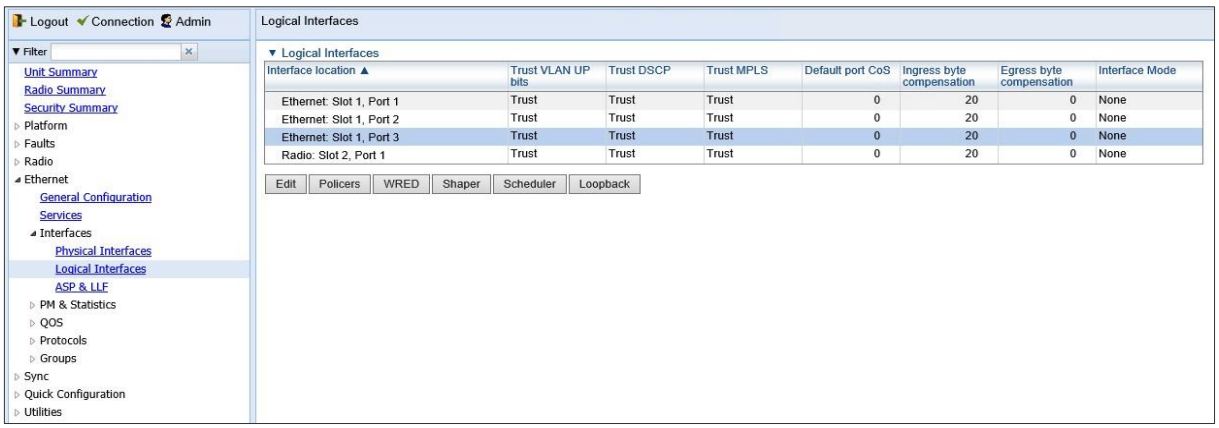
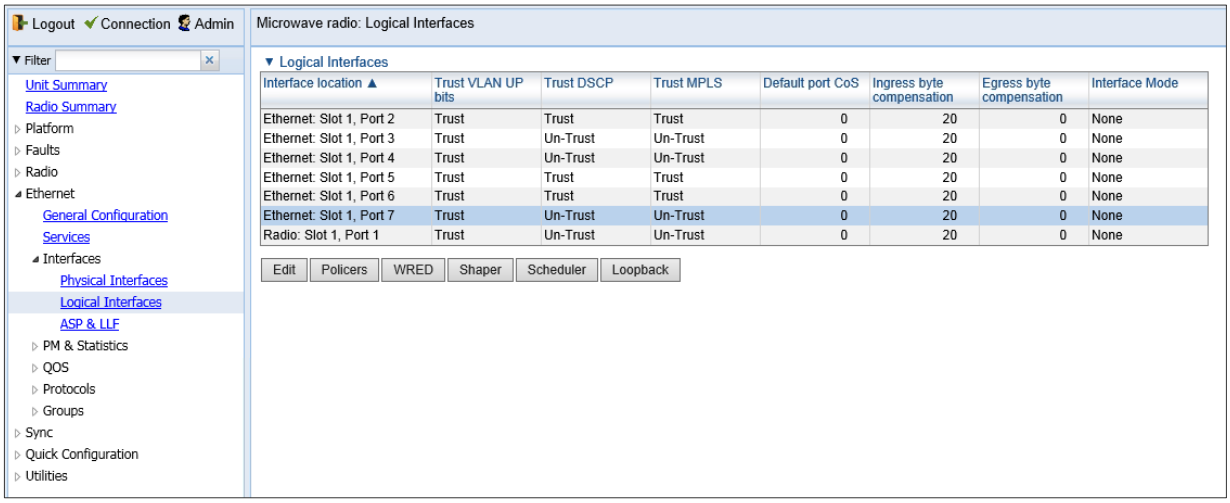
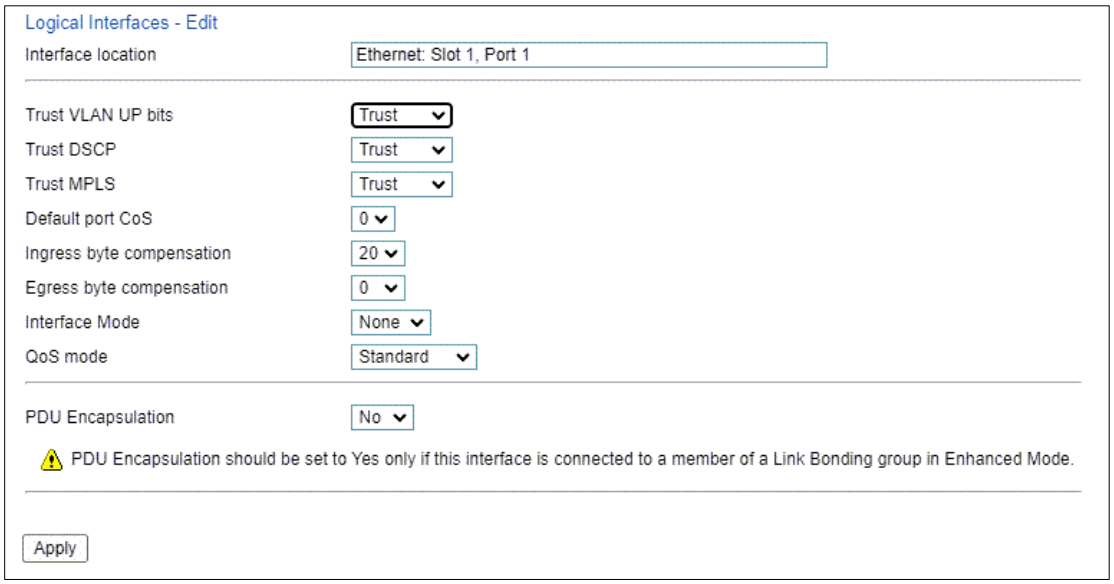


Table 65 Logical Interfaces Page-PTP 850E



2. Select the interface you want to configure and click **Edit**. The Logical Interfaces - Edit page opens.

Figure 382 Logical Interfaces - Edit Page



3. Configure the parameters described in Table 66.
4. Click **Apply**, then **Close**.

Note

The **Ingress byte compensation** and **Egress byte compensation** fields are described in Configuring the Ingress and Egress Byte Compensation.

Table 66 Logical Interface Classification Parameters

Parameter	Definition
Trust VLAN UP bits	Select the interface's trust mode for user priority (UP) bits: Trust – The interface performs QoS and color classification according to UP and CFI/DEI bits according to user-configurable tables for 802.1q UP bits (C-VLAN frames) or 802.1AD UP bits (S-VLAN frames). MPLS and DSCP classification has priority over 802.1p Trust Mode, so that if a match is found with the MPLS or DSCPI, 802.1p bits are not considered. Un-Trust – The interface does not consider 802.1 UP bits during classification.

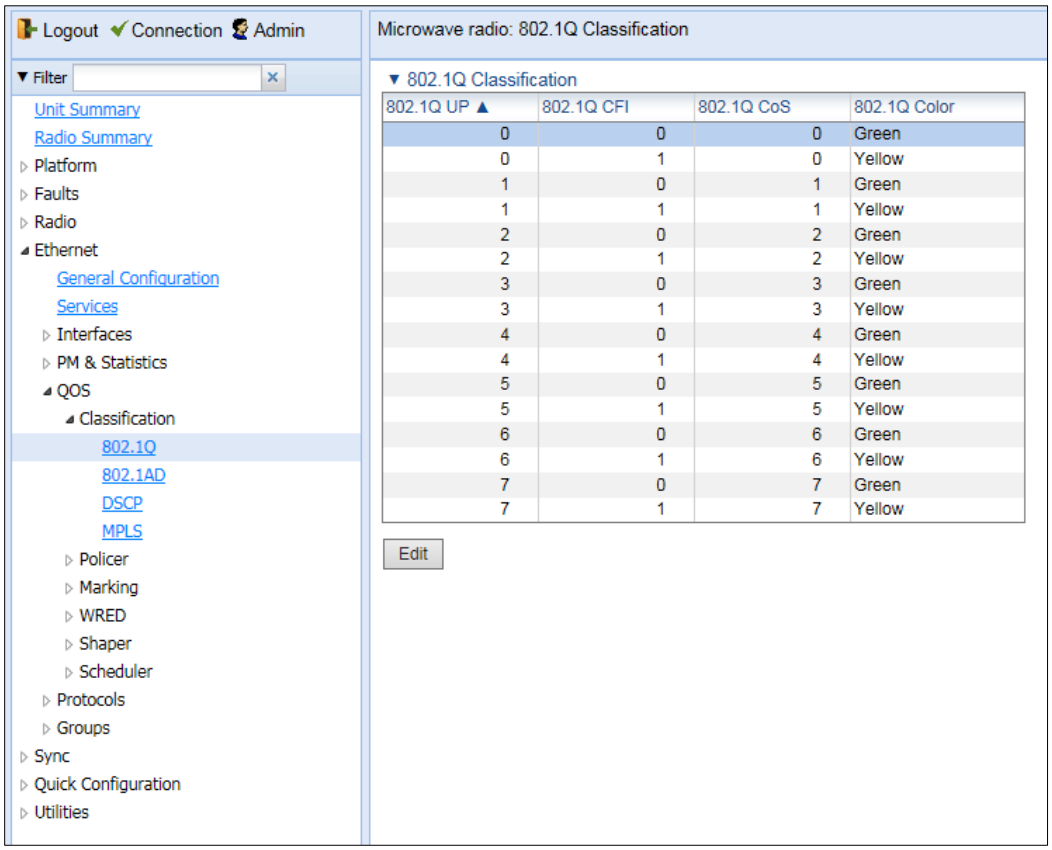
Parameter	Definition
Trust DSCP	Select the interface's trust mode for DSCP: **Trust** – The interface performs QoS and color classification according to a user-configurable table for DSCP to CoS and color classification. DSCP classification has priority over MPLS classification, so that if a match is found with the DSCP value of the ingressing frame, MPLS bits are not considered. **Un-Trust** – The interface does not consider DSCP during classification. **Note:** If you change the trust mode for DSCP, the trust mode for MPLS is automatically changed to the same setting.
Trust MPLS	Select the interface's trust mode for MPLS bits: **Trust** – The interface performs QoS and color classification according to a user-configurable table for MPLS EXP to CoS and color classification. **Un-Trust** – The interface does not consider MPLS bits during classification. **Note:** If you change the trust mode for MPLS, the trust mode for DSCP is automatically changed to the same setting.
Default port CoS	Select the default CoS value for frames passing through the interface (0 to 7). This value can be overwritten on the service point and service level.
Ingress Byte Compensation	See Configuring the Ingress and Egress Byte Compensation.
Egress Byte Compensation	See Configuring the Ingress and Egress Byte Compensation.
Interface Mode	Reserved for future use.
QoS Mode	See Enabling Hierarchical QoS (H-QoS).
PDU Encapsulation	Should be set to No unless the interface is connected to a member of a Link Bonding group in Enhanced mode.

11.2.3 Modifying the C-VLAN 802.1Q UP and CFI Bit Classification Table

To modify the classification criteria for 802.1Q User Priority (UP) bits:

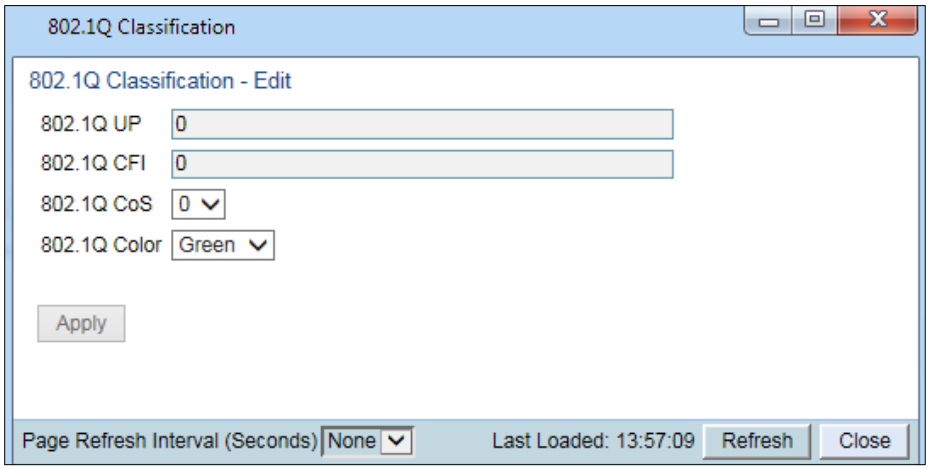
1. Select **Ethernet** > **QoS** > **Classification** > **802.1Q**. The 802.1Q Classification page opens.

Figure 383 802.1Q Classification Page



2. Select the row you want to modify and click **Edit**. The 802.1Q Classification – Edit page opens.

Figure 384 802.1Q Classification - Edit Page



3. Modify the parameters you want to change:

802.1Q UP – Read-only. The User Priority (UP) bit to be mapped.

802.1Q CFI – Read-only. The CFI bit to be mapped.

802.1Q CoS – The CoS assigned to frames with the designated UP and CFI.

802.1Q Color – The Color assigned to frames with the designated UP and CFI.

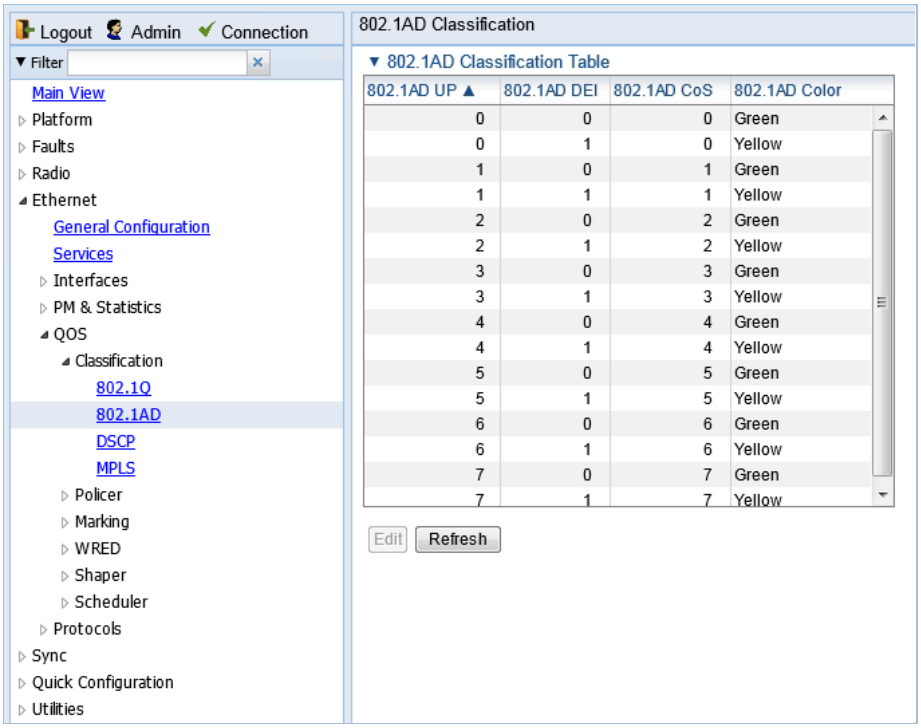
4. Click **Apply**, then **Close**.

11.2.4 Modifying the S-VLAN 802.1 UP and DEI Bit Classification Table

To modify the classification criteria for 802.1AD User Priority (UP) bits:

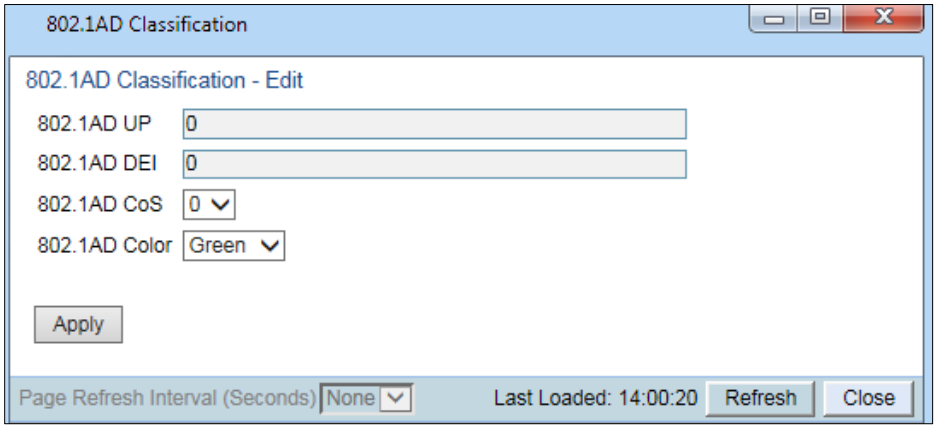
1. Select **Ethernet** > **QoS** > **Classification** > **802.1AD**. The 802.1AD Classification page opens.

Figure 385 802.1AD Classification Page



2. Select the row you want to modify and click **Edit**. The 802.1AD Classification - Edit page opens.

Figure 386 802.1Q Classification - Edit Page



3. Modify the parameters you want to change:

802.1AD UP – Read-only. The User Priority (UP) bit to be mapped.

802.1ADQ DEI – Read-only. The DEI bit to be mapped.

802.1AD CoS – The CoS assigned to frames with the designated UP and DEI.

802.1AD Color – The Color assigned to frames with the designated UP and DEI.

4. Click **Apply**, then **Close**.

11.2.5 Modifying the DSCP Classification Table

You can configure the classification criteria for Differentiated Service Code Point (DSCP) priority values. The DSCP is a 6-bit length field inside the IP datagram header carrying priority information. Classification by DSCP can be used for untagged frames, as well as 802.1Q tagged or provider VLAN tagged frames.

PTP 850 units have a DSCP classification table with 24 pre-defined entries. Each entry includes the following criteria:

- DSCP – The DSCP value to be mapped.
- Binary – The binary representation of the DSCP value.
- Description – A description of the DSCP value.
- CoS – The CoS assigned to frames with the designated DSCP value.
- Color – The Color assigned to frames with the designated DSCP value.

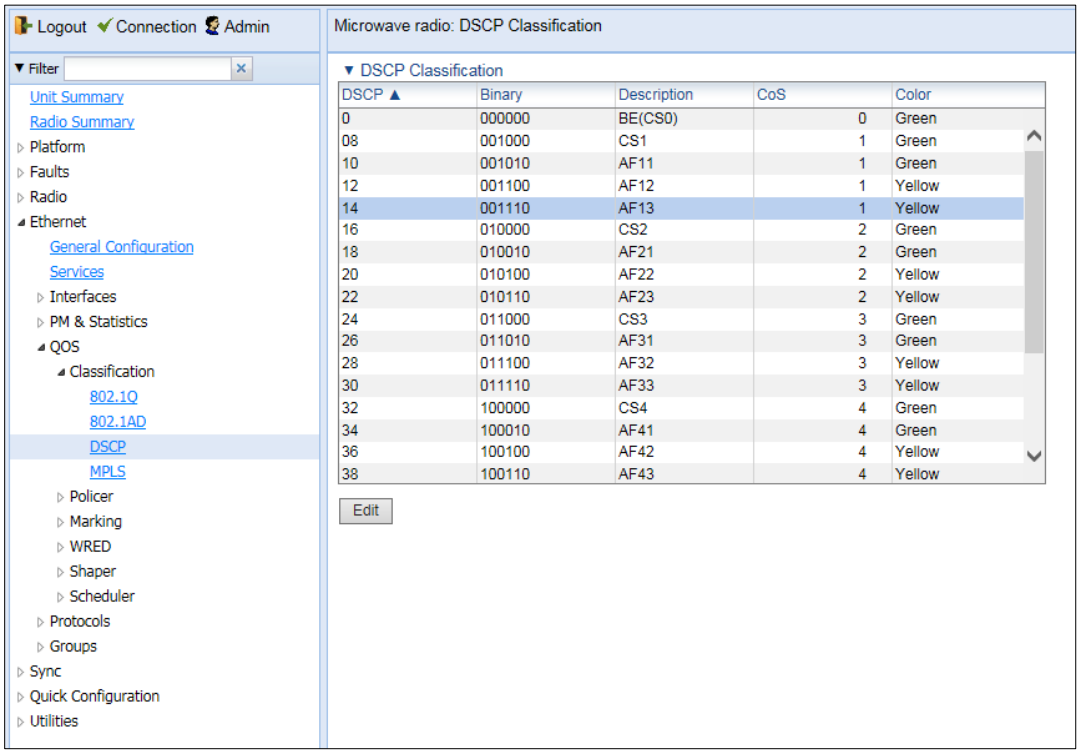
You can modify the Description, CoS, and Color for any of the pre-defined entries. You can also add and delete entries. The maximum number of entries is:

- PTP 850C and PTP 850E: 64.
- PTP 850S: 32

To modify the classification criteria for DSCPs:

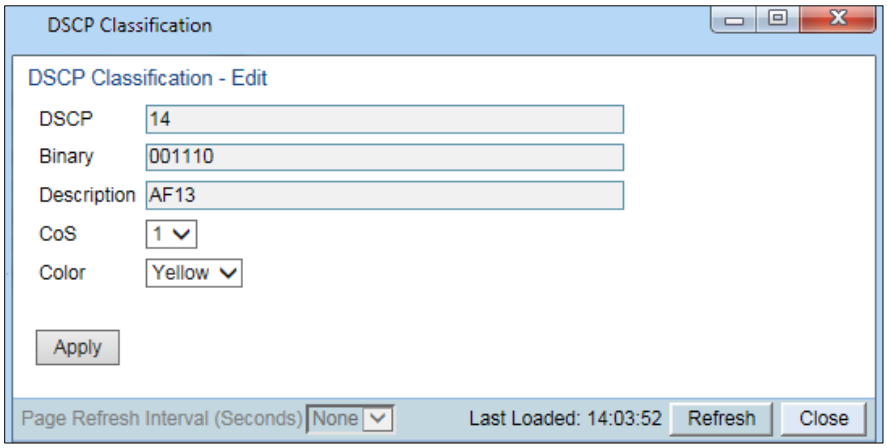
1. Select **Ethernet > QoS > Classification > DSCP**. The DSCP Classification page opens.

Figure 387 DSCP Classification Page



2. Select the row you want to modify and click **Edit**. The DSCP Classification - Edit page opens.

Figure 388 DSCP Classification - Edit Page



3. Modify the parameters you want to change:

DSCP – Read-only. The DSCP value to be mapped.

Binary – Read-only. The binary representation of the DSCP value.

Description – Read-only. The description of the DSCP value.

CoS – The CoS assigned to frames with the designated DSCP value.

Color – The Color assigned to frames with the designated DSCP value.

4. Click **Apply**, then **Close**.

To add an entry to the DSCP Classification table:

1 Select **Ethernet > QoS > Classification > DSCP**. The DSCP Classification page opens (*Figure 259*).

2 Click **Add**. The DSCP Classification - Add page opens.

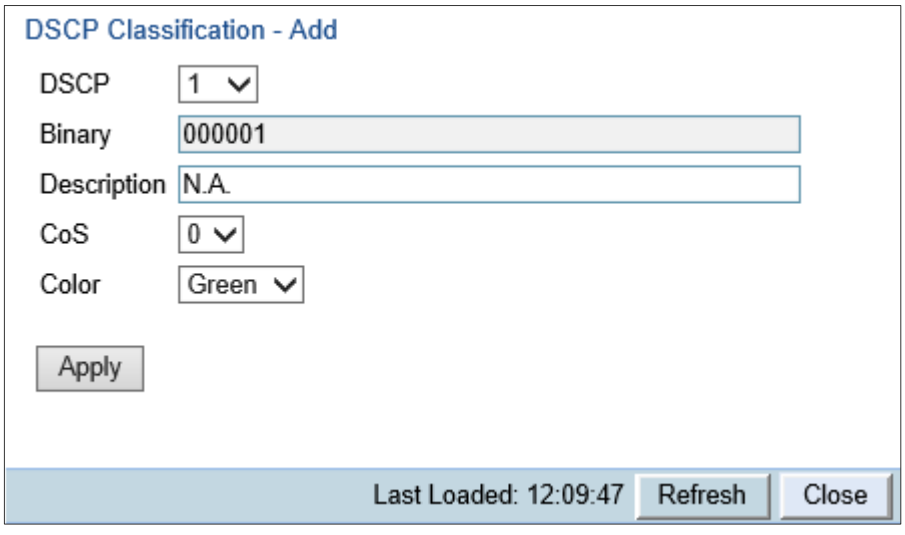


Figure 261: DSCP Classification - Add Page

3 In the **DSCP** field, select the DSCP value you want to add. The **Binary** field is automatically adjusted to display the binary representation of the DSCP value you selected.

4 In the **Description** field, enter a description of the DSCP entry.

5 In the **CoS** field, select a CoS value to assign to frames with the designated DSCP value.

6 In the **Color** field, select a Color to assign to frames with the designated DSCP value.

7 Click **Apply**.

To delete an entry from the DSCP Classification table:

1 Select **Ethernet > QoS > Classification > DSCP**. The DSCP Classification page opens (*Figure 259*).

2 Select the row you want to modify and click **Delete**. A confirmation window opens.

3 Click **OK**. The entry is deleted.

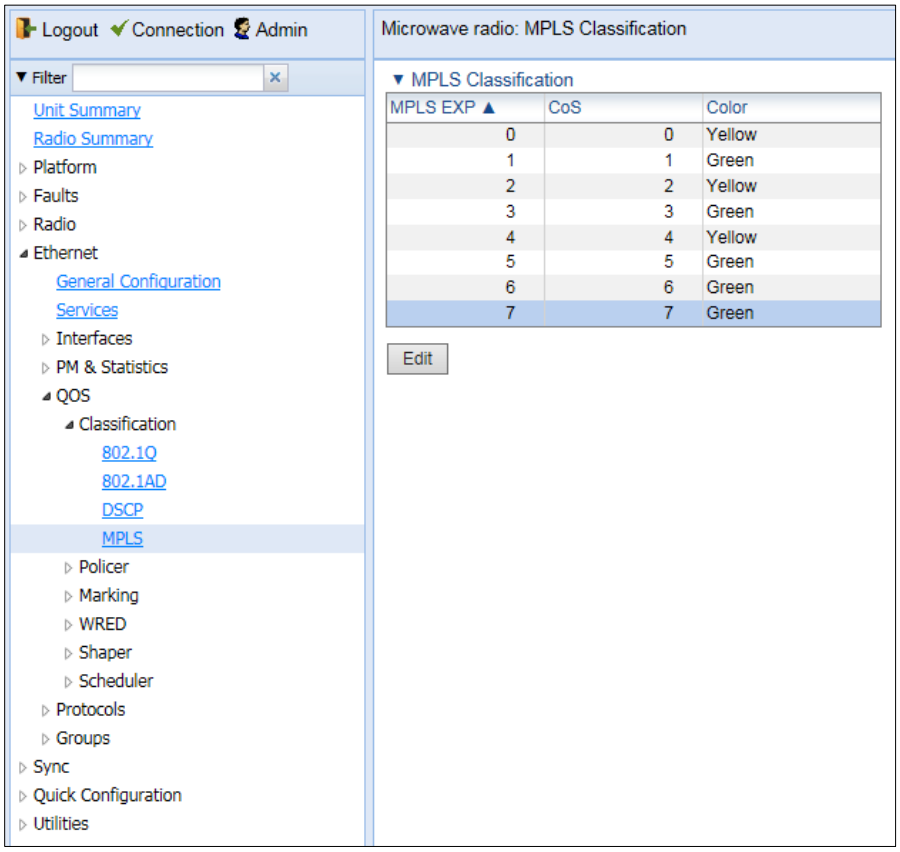
11.2.6 Modifying the MPLS EXP Bit Classification Table

MPLS bits are used to provide QoS capabilities by utilizing the bits set in the MPLS labels. Classification by MPLS bits is supported in both untagged and 802.1Q provider-tagged frames.

To modify the classification criteria for MPLS EXP bits:

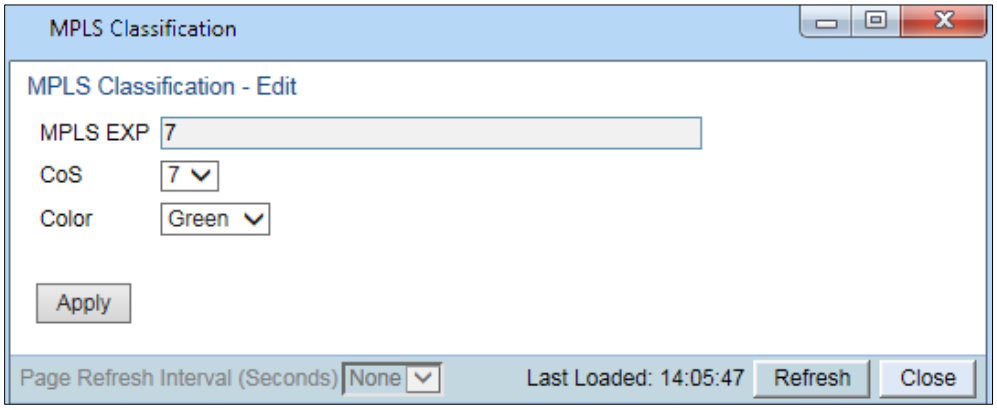
1. Select **Ethernet > QoS > Classification > MPLS**. The MPLS Classification page opens.

Figure 389 MPLS Classification Page



2. Select the row you want to modify and click **Edit**. The MPLS Classification - Edit page opens.

Figure 390 MPLS Classification - Edit Page



3. Modify the parameters you want to change:

MPLS EXP – Read-only. The MPLS (experimental) bit to be mapped.

CoS – The CoS assigned to frames with the designated MPLS EXP value.

Color – The Color assigned to frames with the designated MPLS EXP value.

4. Click **Apply**, then **Close**.

Modifying the MAC DA Classification Table

You can determine whether classification is performed by MAC DA in the **CoS Mode** field of the service point's Ingress Parameters page. See *Classification Overview*.

To add an entry to the MAC DA Classification Table:

1 Select **Ethernet > QoS > Classification > MAC DA**. The MAC DA Classification page opens.

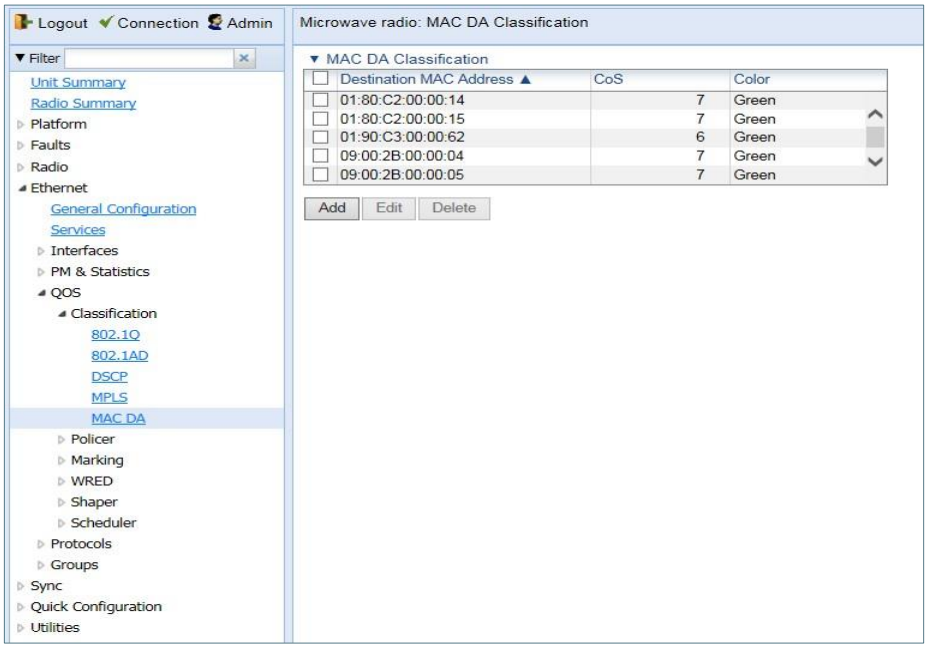


Figure 264: MAC DA Classification Page

2 Click **Add**. The MAC DA Classification – Add page opens.

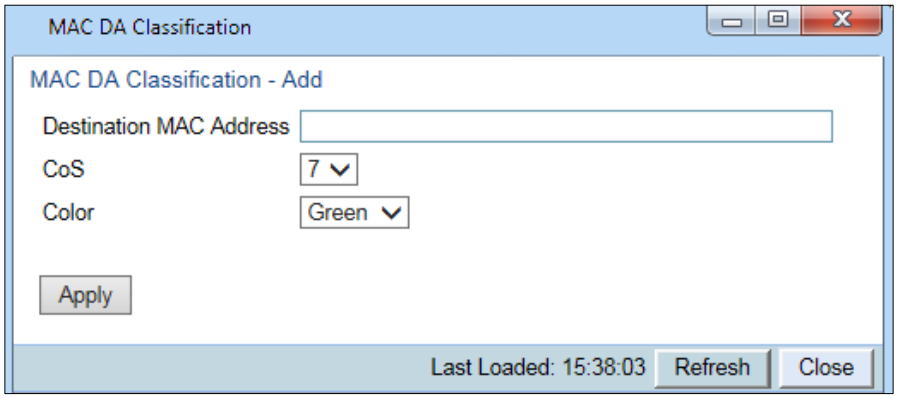


Figure 391 MAC DA Classification – Add Page

In the **Destination MAC Address** field, enter the MAC address.

3 In the **CoS** field, enter the CoS to be assigned to frames with this MAC DA.

4 In the **Color** field, enter the Color to be assigned to frames with this MAC DA.

5 Click Apply, then Close.

To modify an entry in the MAC DA Classification Table:

1 In the MAC DA Classification page, select the row you want to modify and click **Edit**. The MAC DA Classification – Edit page opens.

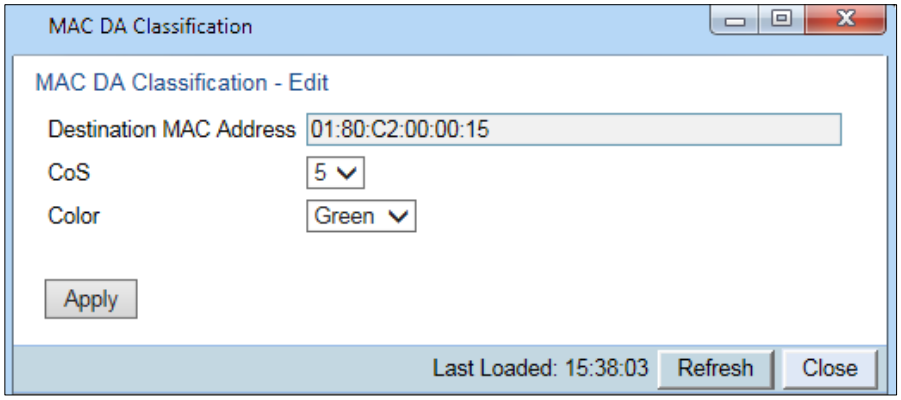


Figure 392 MAC DA Classification – Edit Page

2 Modify the parameters you want to change:

- **CoS** – The CoS assigned to frames with this MAC DA.
- **Color** – The Color assigned to frames with this MAC DA.

3 Click Apply, then Close.

To delete an entry from the MAC DA Classification Table:

1 In the MAC DA Classification page, select the row you want to delete and click

Delete. A confirmation window opens.

2 Click OK.

11.3 Configuring Policers (Rate Metering)

This section includes:

- Policer (Rate Metering) Overview
- Configuring Policer Profiles
- Assigning Policers to Interfaces
- Configuring the Ingress and Egress Byte Compensation

11.3.1 Policer (Rate Metering) Overview

The PTP 850 switching fabric supports hierarchical policing on the logical interface level. You can define up to 250 rate meter (policer) profiles.



Note

Policing on the service point level, and the service point and CoS level, is planned for future release.

PTP 850's policer mechanism is based on a dual leaky bucket mechanism (TrTCM). The policers can change a frame's color and CoS settings based on CIR/EIR + CBS/EBS, which makes the policer mechanism a key tool for implementing bandwidth profiles and enabling operators to meet strict SLA requirements.The output of the policers is a suggested color for the inspected frame. Based on this color, the queue management mechanism decides whether to drop the frame or to pass it to the queue.

11.3.2 Configuring Policer Profiles

This section includes:

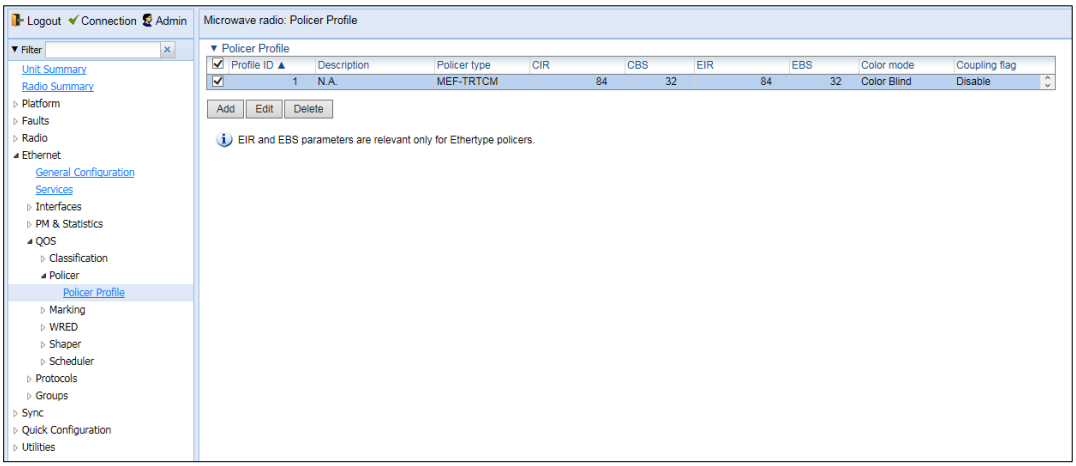
- Adding a Policer Profile
- Editing a Policer Profile
- Deleting a Policer Profile

Adding a Policer Profile

To add a policer profile:

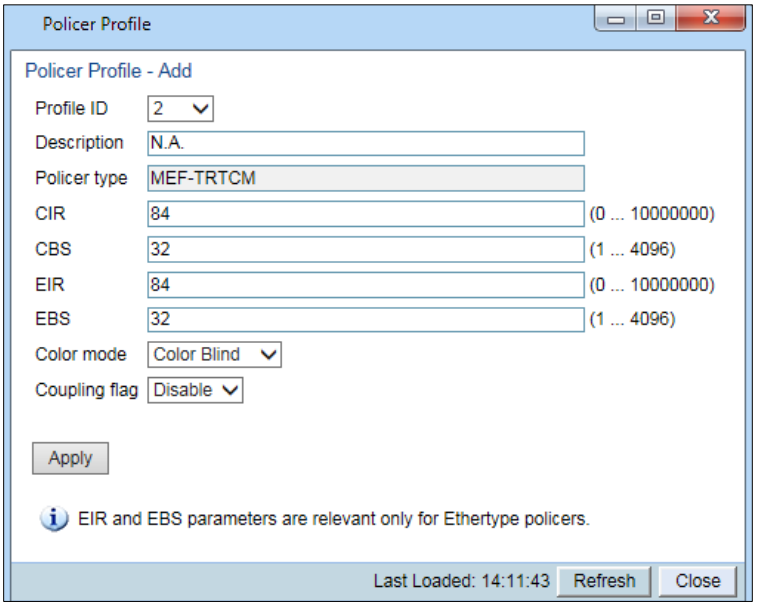
1. Select **Ethernet** > **QoS** > **Policer** > **Policer Profile**. The Policer Profile page opens.

Figure 393 Policer Profile Page



2. Click **Add**. The Policer Profile - Add page opens.

Figure 394 Policer Profile - Add Page



3. Configure the profile's parameters. See Table 67 Policer Profile Parameters for a description of the policer profile parameters.
4. Click **Apply**, then **Close**.

Table 67 Policer Profile Parameters

Parameter	Definition
Profile ID	A unique ID for the policer profile. You can choose from any unused value from 1 to 256. Once you have added the profile, you cannot change the Profile ID.
Description	A description of the policer profile.
Policer type	Read-only. The type of policer. Always set to MEF-TRTCM.
CIR	Enter the Committed Information Rate (CIR) for the policer, in bits per second. Permitted values are 0, or 64,000 through 1,000,000,000 bps. If the value is 0, all incoming CIR traffic is dropped.
CBS	Enter the Committed Burst Rate (CBR) for the policer, in Kbytes. Permitted values are 0 through 4096 Kbytes.
EIR	Enter the Excess Information Rate (EIR) for the policer, in bits per second. Permitted values are 0, or 64,000 through 1,000,000,000 bps. If the value is 0, all incoming EIR traffic is dropped.
EBS	Enter the Excess Burst Rate (EBR) for the policer, in Kbytes. Permitted values are 0 through 4096 Kbytes.
Color mode	Select how the policer treats packets that ingress with a CFI or DEI field set to 1 (yellow). Options are: **Color Aware** – All packets that ingress with a CFI/DEI field set to 1 (yellow) are treated as EIR packets, even if credits remain in the CIR bucket. **Color Blind** – All ingress packets are treated as green regardless of their CFI/DEI value. A color-blind policer discards any former color decisions.
Coupling flag	Select **Enable** or **Disable**. When enabled, frames that ingress as yellow may be converted to green when there are no available yellow credits in the EIR bucket. **Coupling Flag** is only relevant in Color Aware mode.

Editing a Policer Profile

To edit a policer profile, select the profile in the Police Profile table and click **Edit**. The Policer Profile Table Edit page opens.

The Policer Profile Table - Edit page is identical to the Policer Profile Table - Add page (Figure 394). You can edit any parameter that can be configured in the Policer Profile Table Add page, except the **Profile ID**.

Deleting a Policer Profile

You cannot delete a policer profile that is attached to a logical interface. You must first remove the profile from the logical interface, then delete the profile. See Assigning Policers to Interfaces.

To delete a policer profile, select the profile in the Police Profile table and click **Delete**. The profile is deleted.

To delete multiple policer profiles:

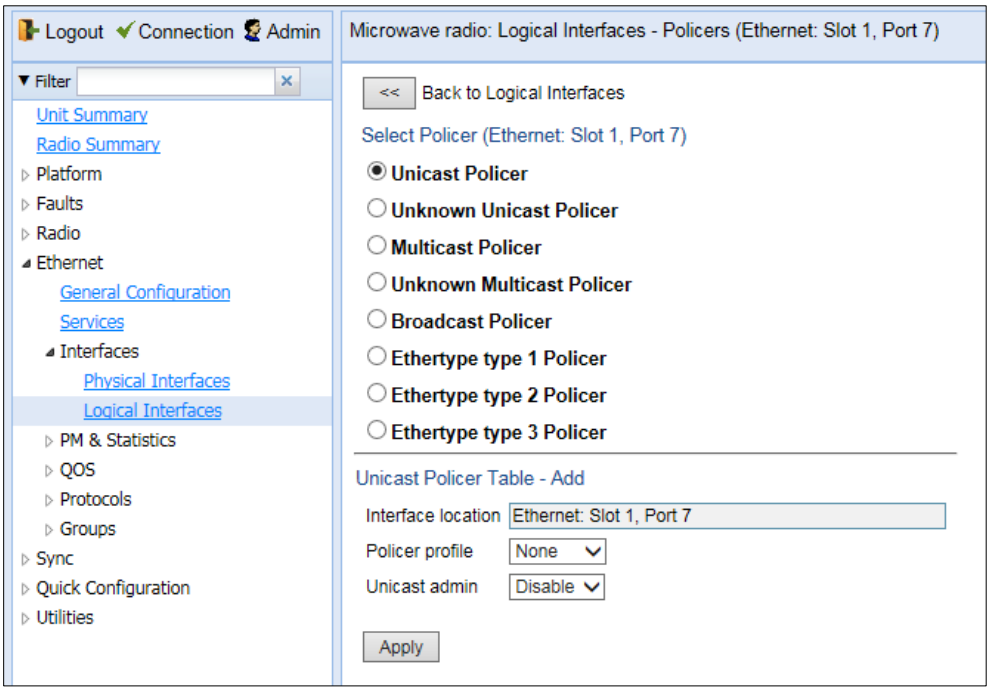
1. Select the profiles in the Policer Profile table or select all the profiles by selecting the check box in the top row.
2. Click **Delete**. The profiles are deleted.

11.3.3 Assigning Policers to Interfaces

To assign policers to a logical interface:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 381).
2. Select the interface in the Ethernet Logical Port Configuration table and click **Policers**. The Policers page opens.

Figure 395 Logical Interfaces – Policers Page – Unicast Policer (Default)



For a logical interface, you can assign policers to the following traffic flows:

Unicast Policer

Unknown Unicast Policer

Multicast Policer

Unknown Multicast Policer

Broadcast Policer

Ethertype Policers

Assigning Unicast Policers

To assign a policer for unicast traffic to a logical interface:

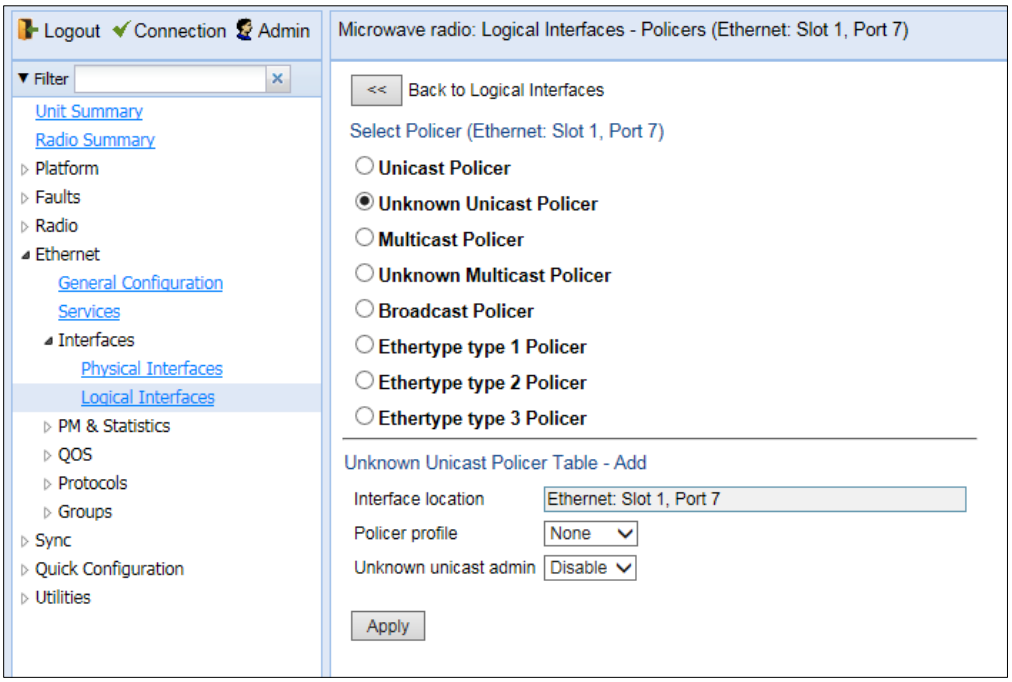
1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 381).
2. Select the interface in the Ethernet Logical Port Configuration Table and click **Policers**. The Policers page opens. By default, the Policers page opens to the Unicast Policer table (Figure 395).
3. In the **Policer profile** field, select a profile from the policer profiles defined in the system. The **Policer profile** drop-down list includes the ID and description of all defined profiles.
4. In the **Unicast admin** field, select **Enable** to enable policing on unicast traffic flows from the logical interface, or **Disable** to disable policing on unicast traffic flows from the logical interface.
5. Click **Apply**.

Assigning Unknown Unicast Policers

Unknown unicast packets are unicast packets with unknown destination MAC addresses. To assign a policer for unknown unicast traffic to a logical interface:

1. Select Ethernet > Interfaces > Logical Interfaces. The Logical Interfaces page opens (Figure 381).
2. Select the interface in the Ethernet Logical Port Configuration table and click Policers. The Policers page opens. By default, the Policers page opens to the Unicast Policer table (Figure 395).
3. Select Unknown Unicast Policer. The Unknown Unicast Policer table appears.

Figure 396 Logical Interfaces – Policers Page – Multicast Policer



4. In the Policer profile field, select a profile from the policer profiles defined in the system. The Policer profile drop-down list includes the ID and description of all defined profiles.
5. In the Multicast admin field, select Enable to enable policing on multicast traffic flows from the logical interface, or Disable to disable policing on multicast traffic flows from the logical interface.
6. Click Apply.

11.3.3.1 Assigning Multicast Policers

To assign a policer for multicast traffic to a logical interface:

1 Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 381).
2 Select the interface in the Ethernet Logical Port Configuration table and click **Policers**. The Policers page opens. By default, the Policers page opens to the Unicast Policer table (Figure 395).
3 Select **Multicast Policer**. The Multicast Policer table appears.

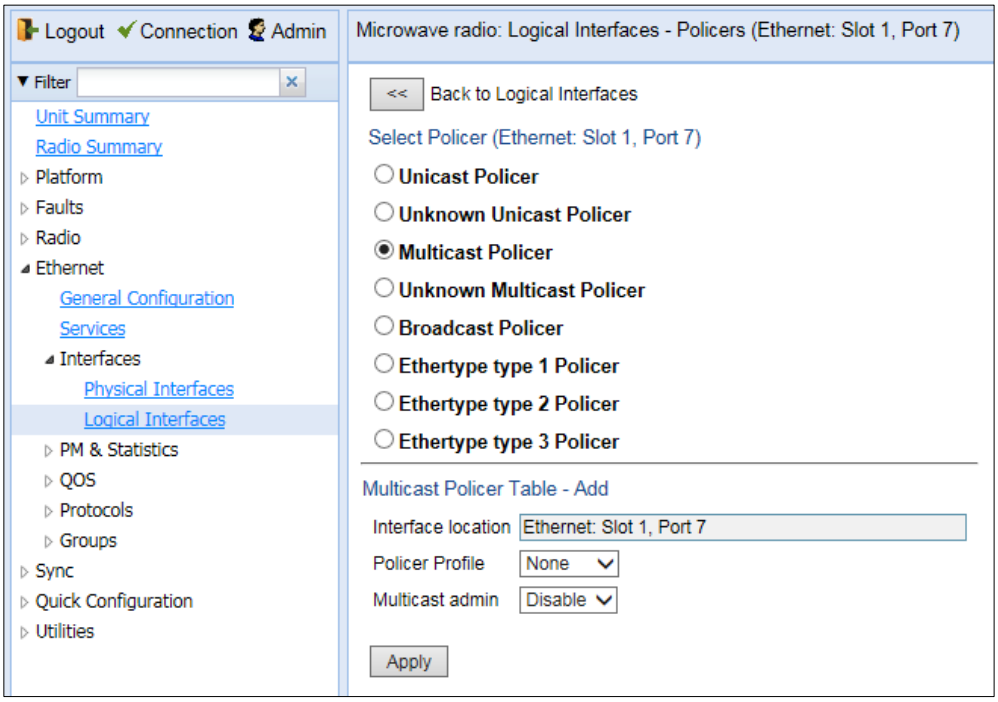


Figure 397: Logical Interfaces – Policers Page – Multicast Policer

4 In the **Policer profile** field, select a profile from the policer profiles defined in the system. The **Policer profile** drop-down list includes the ID and description of all defined profiles.
5 In the **Multicast admin** field, select **Enable** to enable policing on multicast traffic flows from the logical interface, or **Disable** to disable policing on multicast traffic flows from the logical interface.
6 Click **Apply**.

11.3.3.2 Assigning Unknown Multicast Policers

Unknown multicast packets are multicast packets with unknown destination MAC addresses. To assign a policer for unknown multicast traffic to a logical interface:

1 Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 381).
2 Select the interface in the Ethernet Logical Port Configuration table and click **Policers**. The Policers page opens. By default, the Policers page opens to the Unicast Policer table (Figure 395).
3 Select **Unknown Multicast Policer**. The Unknown Multicast Policer table appears.

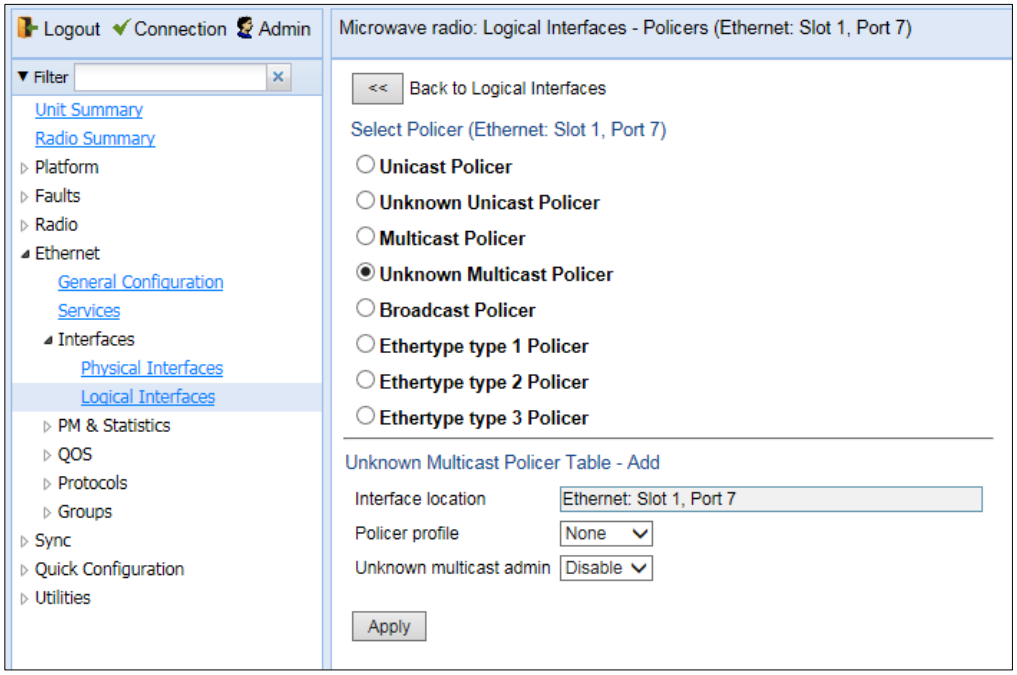


Figure 398: Logical Interfaces – Policers Page – Unknown Multicast Policer

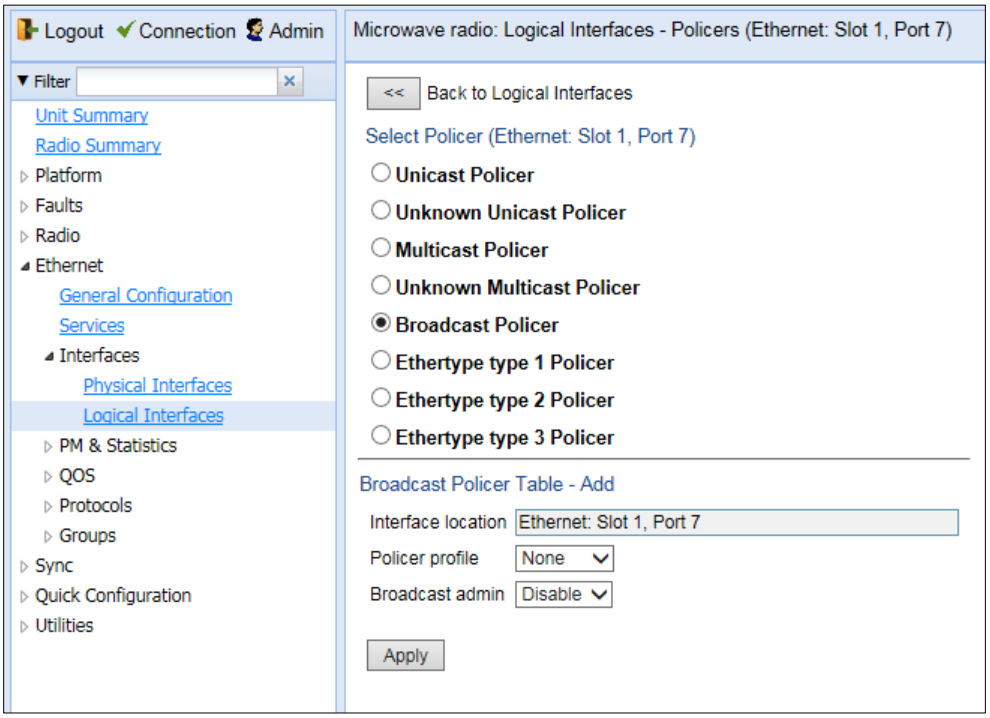
4 In the **Policer profile** field, select a profile from the policer profiles defined in the system. The **Policer profile** drop-down list includes the ID and description of all defined profiles.
5 In the **Unknown multicast admin** field, select **Enable** to enable policing on unknown multicast traffic flows from the logical interface, or **Disable** to disable policing on unknown multicast traffic flows from the logical interface.
6 Click **Apply**.

Assigning Broadcast Policers

To assign a policer for broadcast traffic to a logical interface:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 381).
2. Select the interface in the Ethernet Logical Port Configuration table and click **Policers**. The Policers page opens. By default, the Policers page opens to the Unicast Policer table (Figure 395).
3. Select **Broadcast Policer**. The Broadcast Policer table appears.

Figure 399 Logical Interfaces – Policers Page – Broadcast Policer



4. In the **Policer profile** field, select a profile from the policer profiles defined in the system. The **Policer profile** drop-down list includes the ID and description of all defined profiles.
5. In the **Broadcast admin** field, select **Enable** to enable policing on broadcast traffic flows from the logical interface, or **Disable** to disable policing on broadcast traffic flows from the logical interface.
6. Click **Apply**.

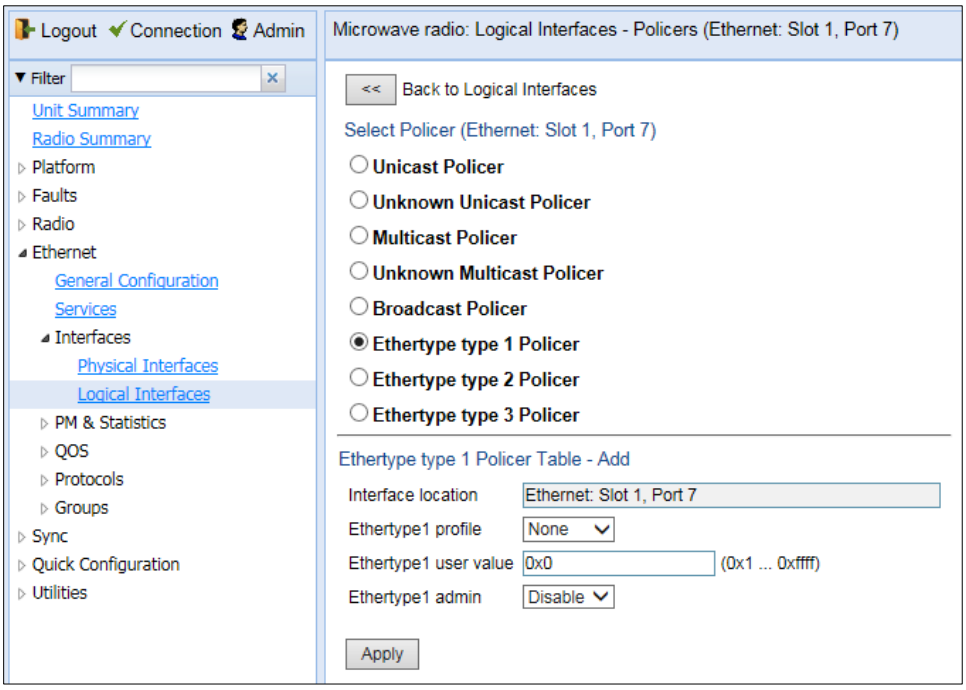
Assigning Ethertype Policers

You can define up to three policers per Ethertype value.

To assign a policer to an Ethertype:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 381).
2. Select the interface in the Ethernet Logical Port Configuration Table and click **Policers**. The Policers page opens. By default, the Policers page opens to the Unicast Policer table (Figure 395).
3. Select **Ethertype type 1 Policer**. The Ethertype type 1 Policer table appears.

Figure 400 Logical Interfaces – Policers Page – Ethertype Policer



4. In the **Ethertype 1 profile** field, select a profile from the policer profiles defined in the system. The **Ethertype 1 profile** drop-down list includes the ID and description of all defined profiles.
5. In the **Ethertype 1 user value** field, enter the Ethertype value to which you want to apply this policer. The field length is 4 nibbles (for example, 0x0806 - ARP).
6. In the **Ethertype 1 admin** field, select **Enable** to enable policing on the logical interface for the specified ethertype, or **Disable** to disable policing on the logical interface for the specified ethertype.
7. Click **Apply**.
8. To assign policers to additional Ethertypes, select **Ethertype type 2 Policer** and **Ethertype type 3 Policer** and repeat the steps above.

11.3.4 Configuring the Ingress and Egress Byte Compensation

You can define the ingress and egress byte compensation value per logical interface. The policer attached to the interface uses these values to compensate for Layer 1 non-effective traffic bytes.

To define the ingress byte compensation value for a logical interface:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 381).
2. Select the interface you want to configure and click **Edit**. The Logical Interfaces - Edit page opens (Figure 382).
3. In the **Ingress byte compensation** field, enter the ingress byte compensation value, in bytes. Permitted values are 0 to 32 bytes. The default value is 20 bytes.
4. In the **Egress byte compensation** field, enter the egress byte compensation value, in bytes. Permitted values are 0 to 32 bytes. The default value is 0 bytes. Only even values are permitted.
5. Click **Apply**, then **Close**.

11.4 Configuring Marking

This section includes:

- Marking Overview
- Enabling Marking
- Modifying the 802.1Q Marking Table
- Modifying the 802.1AD Marking Table

11.4.1 Marking Overview

When enabled, PTP 850's marking mechanism modifies each frame's 802.1p UP bit and CFI/DEI bits according to the classifier decision. The CFI/DEI (color) field is modified according to the classifier and policer decision. The color is first determined by a classifier and may be later overwritten by a policer. Green color is represented by a CFI/DEI value of 0, and Yellow color is represented by a CFI/DEI value of 1. Marking is performed on egress frames that are VLAN-tagged.

The marking is performed according to global mapping tables that describe the 802.1p UP bits and the CFI bits (for C-VLAN tags) or DEI bits (for S VLAN tags). The marking bit in the service point egress attributes determines whether the frame is marked as green or according to the calculated color.



Note

The calculated color is sent to the queue manager regardless of whether the marking bit is set.

Regular marking is only performed when:

The outer frame is S-VLAN, and S-VLAN CoS preservation is disabled, or

The outer frame is C-VLAN, and C-VLAN CoS preservation is disabled.

If marking and CoS preservation for the relevant outer VLAN are both disabled, special marking is applied. Special marking means that marking is performed, but only according to the values defined for Green frames in the 802.1Q and 802.1AD marking tables.

When marking is performed, the C-VLAN or S-VLAN 802.1p UP bits are re-marked according to the calculated CoS and color, and the mapping table for C-VLAN or S-VLAN.

11.4.2 Enabling Marking

Marking is enabled and disabled on the service point level. See 3. Ethernet Service Points – Egress Attributes.

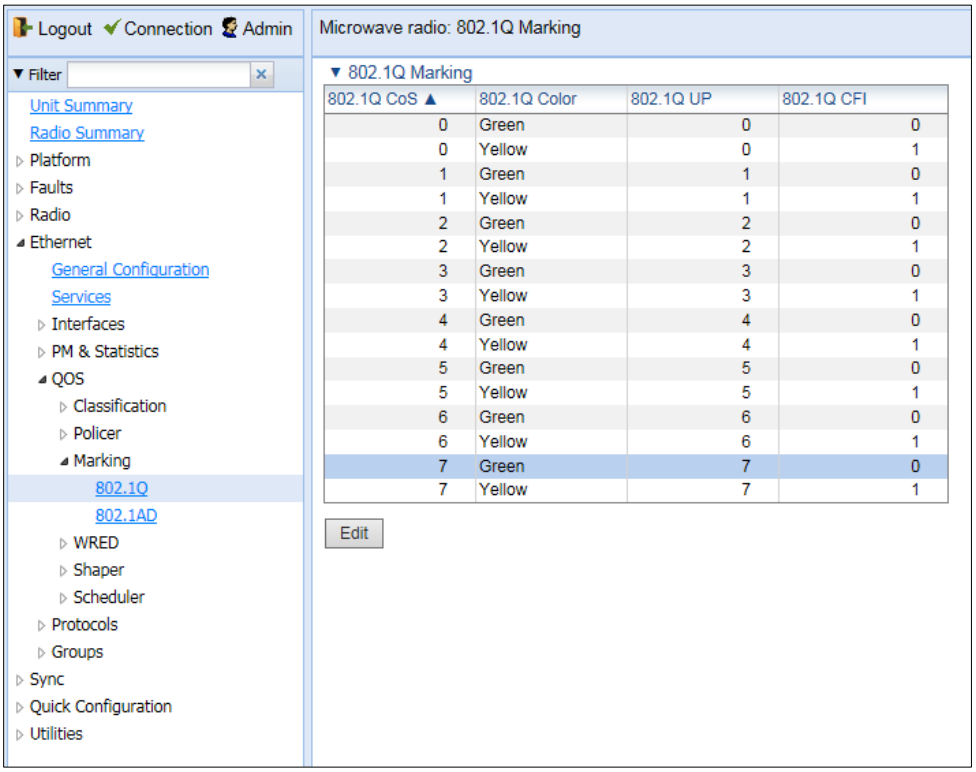
11.4.3 Modifying the 802.1Q Marking Table

The 802.1Q Marking table enables you to modify the CoS to UP and CFI bit mapping that is implemented when marking is enabled.

To modify the 802.1Q Marking table:

1. Select **Ethernet** > **QoS** > **Marking** > **802.1Q**. The 802.1Q Marking page opens. Each row in the 802.1Q Marking page represents a CoS and color combination.

Figure 401 802.1Q Marking Page



2. Select the row you want to modify and click **Edit**. The 802.1Q Marking - Edit page opens.

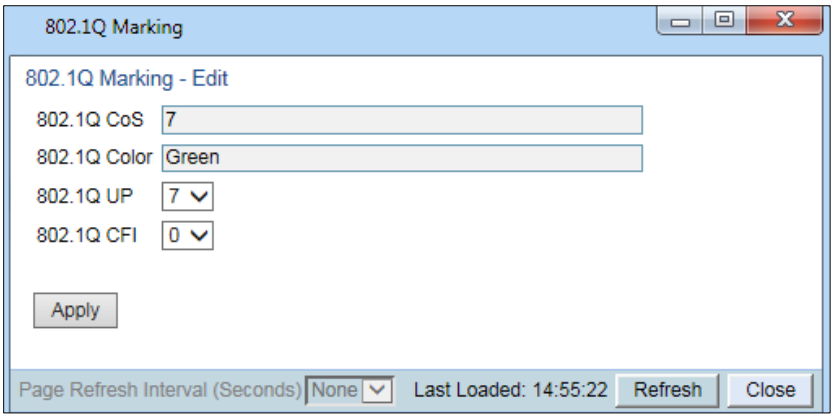


Figure 402 802.1Q Marking - Edit Page

3. Enter the new 802.1Q UP and 802.1Q CFI values.
4. Click **Apply**, then **Close**.

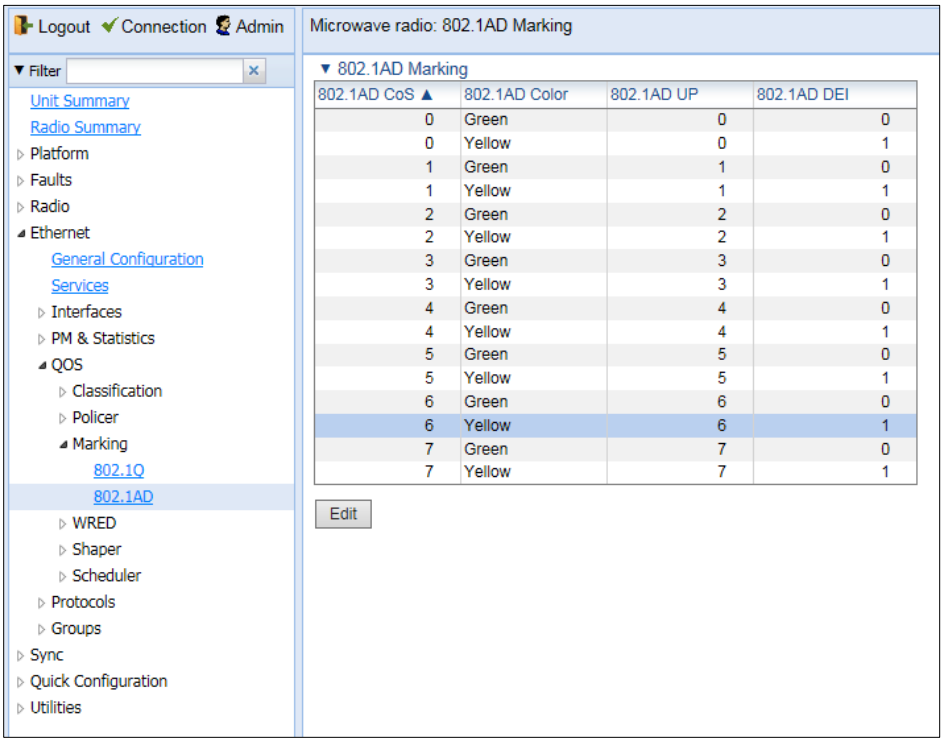
11.4.4 Modifying the 802.1AD Marking Table

The 802.1AD Marking table enables you to modify the CoS to UP and DEI bit mapping that is implemented when marking is enabled.

To modify the 802.1AD Marking table:

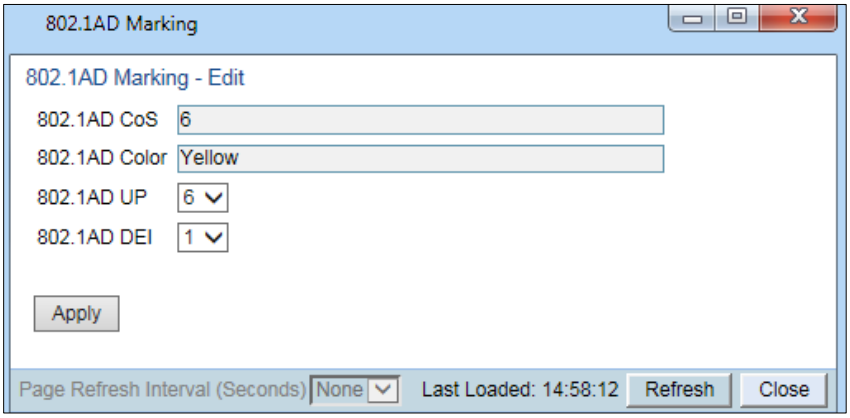
1. Select **Ethernet > QoS > Marking > 802.1AD**. The 802.1AD Marking page opens. Each row in the 802.1AD Marking page represents a CoS and color combination.

Figure 403 802.1AD Marking Page



2. Select the row you want to modify and click **Edit**. The 802.1AD Marking - Edit page opens.

Figure 404 802.1AD Marking - Edit Page



3. Enter the new 802.1AD UP and 802.1AD DEI values.
4. Click **Apply**, then **Close**.

11.5 Configuring WRED

This section includes:

- WRED Overview
- Configuring WRED Profiles
- Assigning WRED Profiles to Queues

11.5.1 WRED Overview

Weighted Random Early Detection (WRED) enables differentiation between higher and lower priority traffic based on CoS. You can define up to 30 WRED profiles. Each profile contains a green traffic curve and a yellow traffic curve. This curve describes the probability of randomly dropping frames as a function of queue occupancy.

The system also includes two pre-defined read-only profiles. These profiles are assigned profile IDs 31 and 32.

Profile number 31 defines a tail-drop curve and is configured with the following values:

- 100% Yellow traffic drop after 64kbytes occupancy.
- 100% Green traffic drop after 128kbytes occupancy.
- Yellow maximum drop is 100%
- Green maximum drop is 100%

Profile number 32 defines a profile in which all will be dropped. It is for internal use and should not be applied to traffic.

A WRED profile can be assigned to each queue. The WRED profile assigned to the queue determines whether or not to drop incoming packets according to the occupancy of the queue. As the queue occupancy grows, the probability of dropping each incoming frame increases as well. As a consequence, statistically more TCP flows will be restrained before traffic congestion occurs.

11.5.2 Configuring WRED Profiles

This section includes:

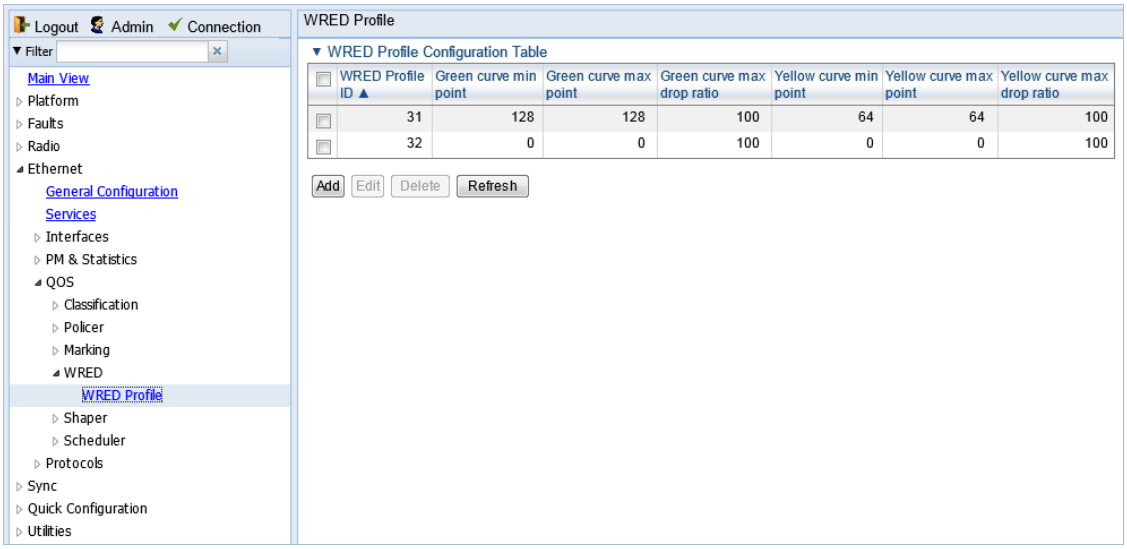
- Adding a WRED Profile
- Editing a WRED Profile
- Deleting a WRED Profile

Adding a WRED Profile

To add a WRED profile:

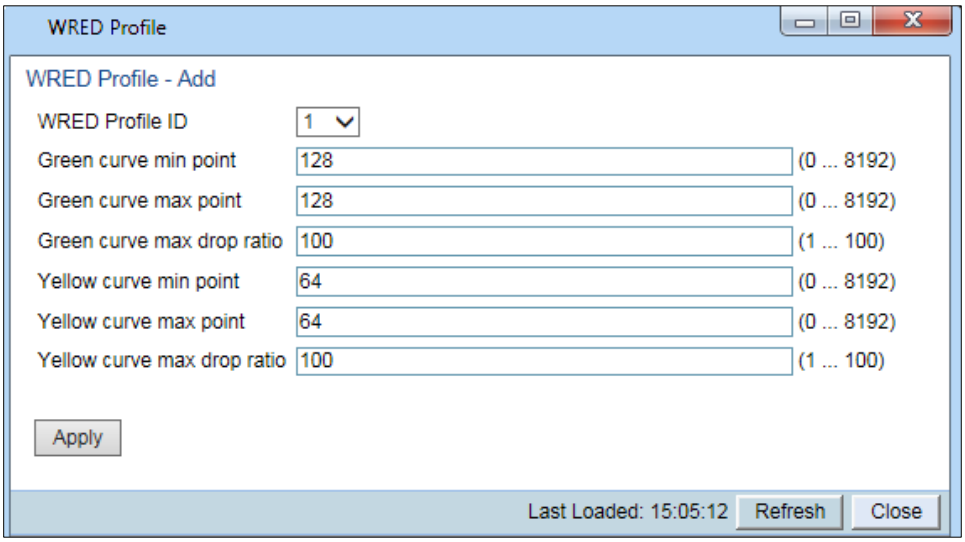
1. Select **Ethernet** > **QoS** > **WRED** > **WRED Profile**. The WRED Profile page opens.

Figure 405 WRED Profile Page



2. Click **ADD**. The WRED Profile - Add page opens, with default values displayed.

Figure 406 WRED Profile - Add Page



3. In the **WRED Profile ID** field, select a unique ID to identify the profile. Permitted values are 1-30.
4. In the **Green curve min point** field, enter the minimum throughput of green packets for queues with this profile, in Kbytes (24-8192). When this value is reached, the system begins dropping green packets in the queue.
5. In the **Green curve max point** field, enter the maximum number of green packets for queues with this profile, in Kbytes (24-8192). When this value is reached, all green packets in the queue are dropped.
6. In the **Green curve max drop ratio** field, enter the maximum percentage (1-100) of dropped green packets for queues with this profile.
7. In the **Yellow curve min point** field, enter the minimum number of yellow packets for queues with this profile, in Kbytes (24-8192). When this value is reached, the system begins dropping yellow packets in the queue.

8. In the **Yellow curve max point** field, enter the maximum number of yellow packets for queues with this profile, in Kbytes (24-8192). After this value is reached, all yellow packets in the queue are dropped.
9. In the **Yellow curve max drop ratio** field, enter the maximum number (1-100) of dropped yellow packets for queues with this profile.
10. Click **Apply**, then **Close**.

Editing a WRED Profile

To edit a WRED profile:

1. Select **Ethernet** > **QoS** > **WRED** > **WRED Profile**. The WRED Profile page opens ().
2. Select the profile you want to edit and click Edit. The WRED Profile – Edit page opens. This page is similar to the WRED Profile – Add page (Figure 406). You can edit any parameter except the **WRED Profile ID**.
3. Modify the profile.
4. Click **Apply**, then **Close**.

Deleting a WRED Profile

You cannot delete a WRED profile that is assigned to a queue. You must first remove the WRED profile from the queue, then delete the WRED profile. See Assigning WRED Profiles to Queues.

To delete a WRED profile, select the profile in the WRED Profile Configuration table (Figure 405) and click **Delete**. The profile is deleted.

To delete multiple WRED profiles:

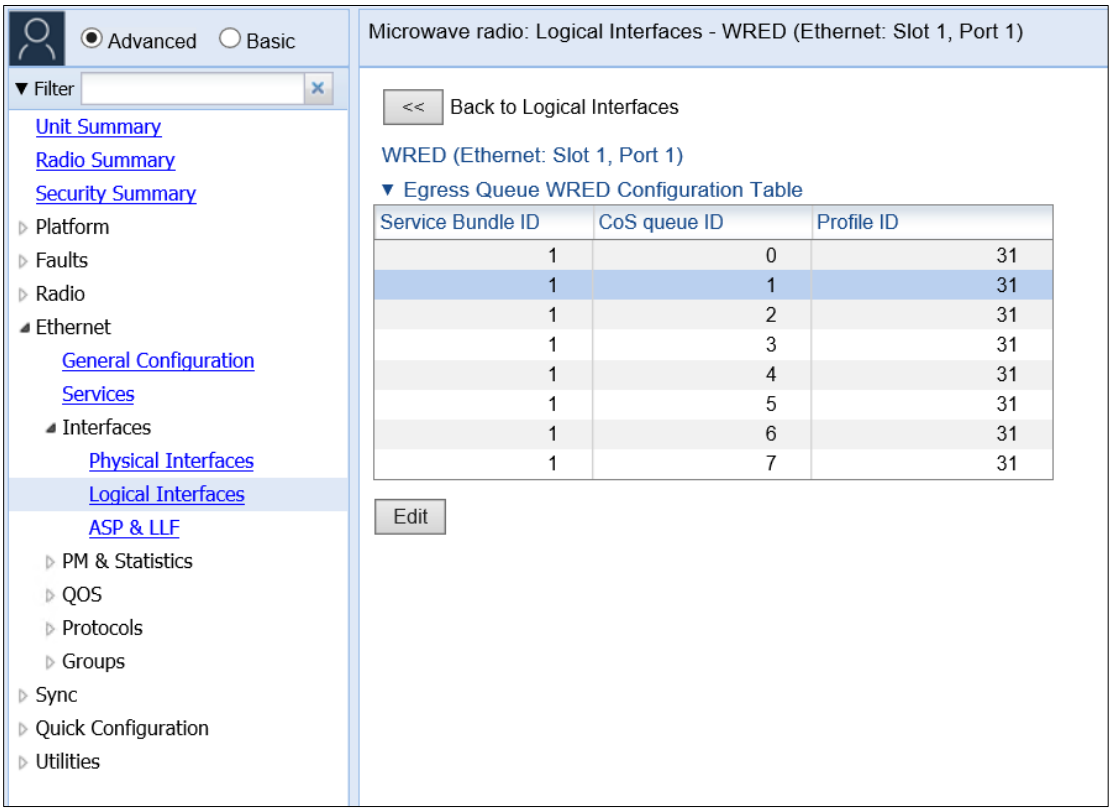
1. Select the profiles in the WRED Profile Configuration table or select all the profiles by selecting the check box in the top row.
2. Click **Delete**. The profiles are deleted.

11.5.3 Assigning WRED Profiles to Queues

To assign a WRED profile to a queue:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 381).
2. Select an interface in the Ethernet Logical Port Configuration table and click **WRED**. The WRED page opens.

Figure 407 Logical Interfaces – WRED Page



3. Select a CoS Queue ID and click **Edit**. The Logical Interfaces – WRED – Edit page opens.

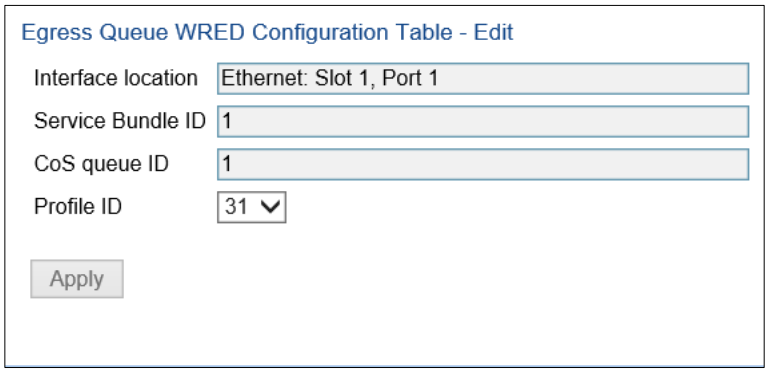


Figure 408: Logical Interfaces – WRED - Edit Page

4. In the **Profile ID** field, select the WRED profile you want to assign to the selected queue.
5. Click **Apply**, then **Close**.

11.6 Configuring Egress Shaping

This section includes:

- Egress Shaping Overview
- Configuring Queue Shaper Profiles
- Configuring Service Bundle Shaper Profiles
- Assigning a Queue Shaper Profile to a Queue
- Assigning a Service Bundle Shaper Profile to a Service Bundle

11.6.1 Egress Shaping Overview

Egress shaping determines the traffic profile for each queue. PTP 850E can perform queue shaping on the queue level, using dual leaky bucket shaping. On the queue level, you can configure up to 32 single leaky bucket shaper profiles. If no profile is attached to the queue, no egress shaping is performed on that queue.

In addition, when H-QoS is enabled on an interface, you can define up to 32 Service Bundle Shaper profiles and assign these profiles to the interface per service bundle. The Serivce Bundle Shaper profiles determine the traffic profile per service bundle for each interface, using dual leaky bucket shaping. This enables you to differentiate the shaping profile per service point and per interface, based on the service bundle assigned to the service point and the Service Bundle Shaping profile assigned to the interface per service bundle.

For further information about H-QoS, see H-QoS Overview.

Note: H-QoS is only supported with PTP 850C. H-QoS with PTP 850E is planned for future release.

11.6.2 Configuring Queue Shaper Profiles

This section includes:

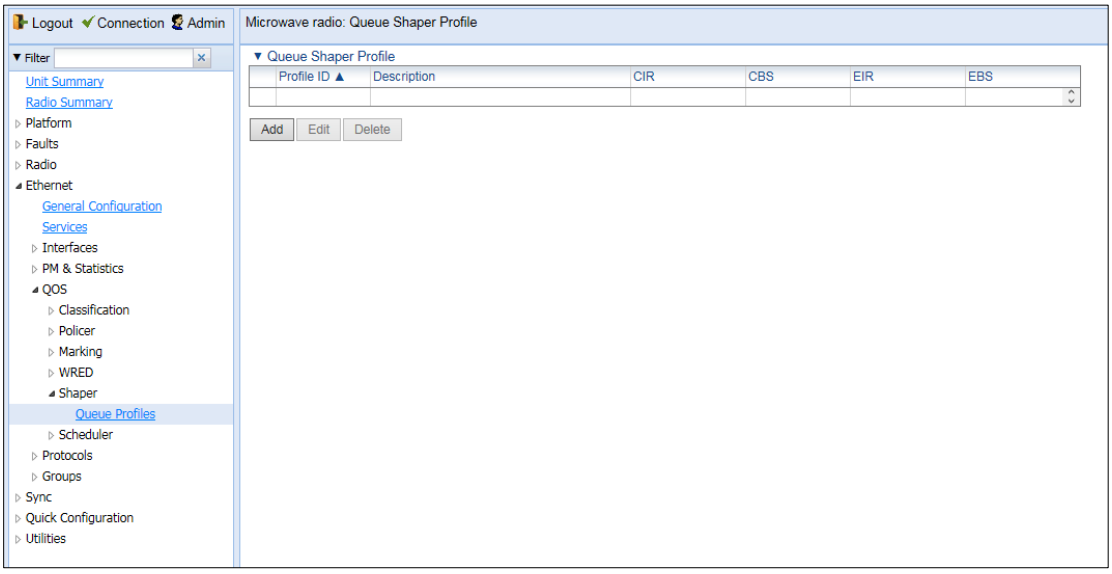
- Adding a Queue Shaper Profile
- Editing a Queue Shaper Profile
- Deleting a Queue Shaper Profile

Adding a Queue Shaper Profile

To add a queue shaper profile:

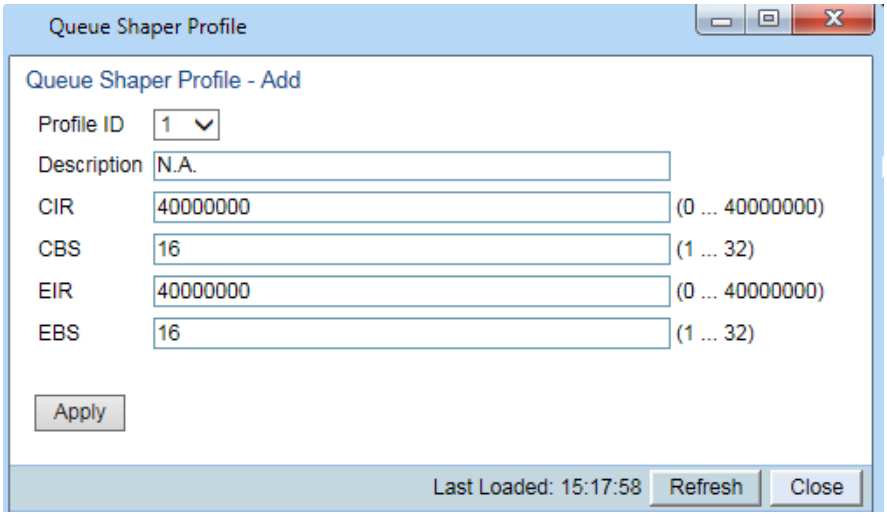
1. Select **Ethernet** > **QoS** > **Shaper** > **Queue Profiles**. The Queue Shaper Profile page opens.

Figure 409 Queue Shaper Profile Page



2. Click **Add**. The Queue Shaper – Add page opens, with default values displayed.

Figure 410 Queue Shaper Profile – Add Page



3. Configure the profile's parameters. See Table 68 Queue Shaper Profile **Parameters** for a description of the queue shaper profile parameters.

4. Click **Apply**, then **Close**.



Note

EIR and EBS are only relevant for policers assigned to logical interfaces.

Table 68 Queue Shaper Profile Parameters

Parameter	Definition
Profile ID	A unique ID for the queue shaper profile. You can choose any unused value from 1 to 32. Once you have added the profile, you cannot change the Profile ID.

Parameter	Definition
Description	A description of the queue shaper profile.
CIR	Enter the Committed Information Rate (CIR) for the shaper, in Kbits per second. Permitted values are 0-40000000 kbps (40 Gbps). If the value is 0, all incoming CIR traffic is dropped. Granularity is 81 kbps. The default value is 40000000 kbps.
CBS	Enter the Committed Burst Rate (CBR) for the shaper, in Kbytes. Permitted values are 1-32 KB. The default value is 16 KB.
EIR	Enter the Excess Information Rate (EIR) for the shaper, in Kbits per second. Permitted values are 0-40000000 kbps (40 Gbps). If the value is 0, all incoming EIR traffic is dropped. Granularity is 162 kbps. The default value is 40000000 kbps.
EBS	Enter the Excess Burst Rate (EBR) for the shaper, in Kbytes. Permitted values are 1-32 KB. The default value is 16 KB.

Editing a Queue Shaper Profile

To edit a queue shaper profile:

1. Select **Ethernet** > **QoS** > **Shaper** > **Queue Profiles**. The Queue Shaper Profile page opens (Figure 409).
2. Select the profile you want to edit and click **Edit**. The Queue Shaper Profile – Edit page opens. This page is similar to the Queue Shaper Profile – Add page (Figure 410). You can edit any parameter except the **Profile ID**.
3. Modify the profile.
4. Click **Apply**, then **Close**.

Deleting a Queue Shaper Profile

You cannot delete a queue shaper profile that is assigned to a queue. You must first remove the profile from the queue, then delete the profile. See Assigning a Queue Shaper Profile to a Queue.

To delete a queue shaper profile, select the profile in the Queue Shaper Profiles Configuration table (Figure 409) and click **Delete**. The profile is deleted.

To delete multiple queue shaper profiles:

1. Select the profiles in the Queue Shaper Profiles Configuration table or select all the profiles by selecting the check box in the top row.

2. Click **Delete**. The profiles are deleted.

Configuring Service Bundle Shaper Profiles

Note: This section is only relevant if H-QoS is enabled on at least one interface. In System Release 11.9, H-QoS is only supported with PTP 850C. For PTP 850E, H-QoS is planned for future release.

This section includes:

- Adding a Service Bundle Shaper Profile
- Editing a Service Bundle Shaper Profile
- Deleting a Service Bundle Shaper Profile

Adding a Service Bundle Shaper Profile

To add a service bundle shaper profile:

1 Select **Ethernet > QoS > Shaper > Service Bundle Profiles**. The Service Bundle Shaper Profile page opens.

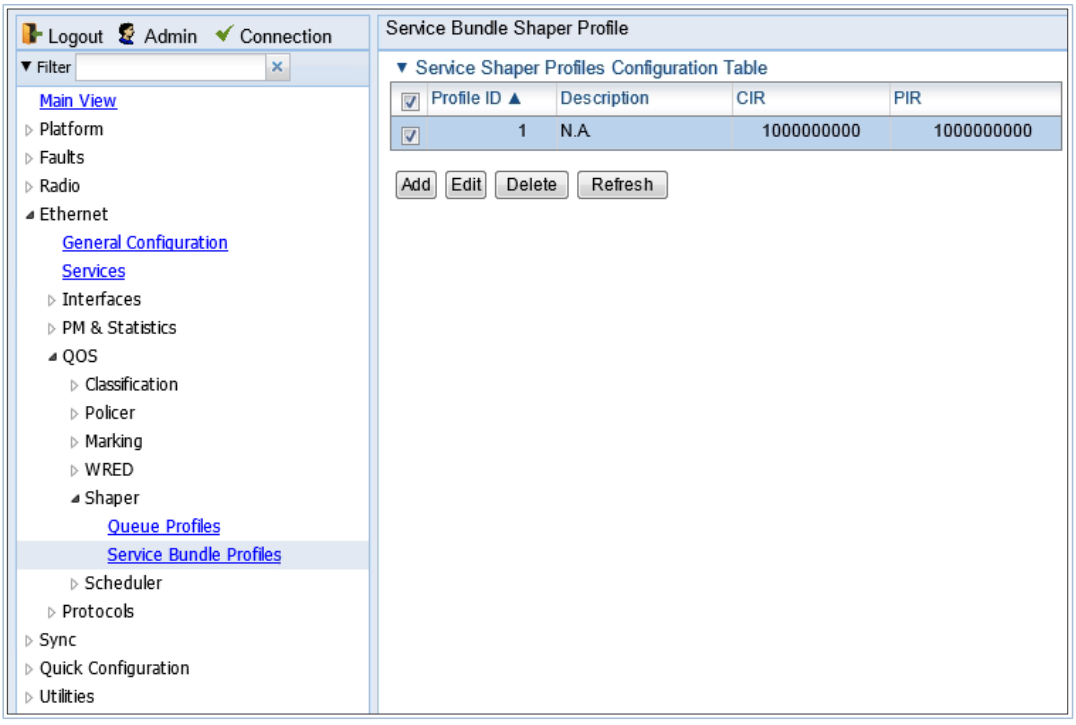


Figure 411 Service Bundle Shaper Profile Page

2 Click **Add**. The Service Bundle Shaper Profile – Add page opens, with default values displayed.

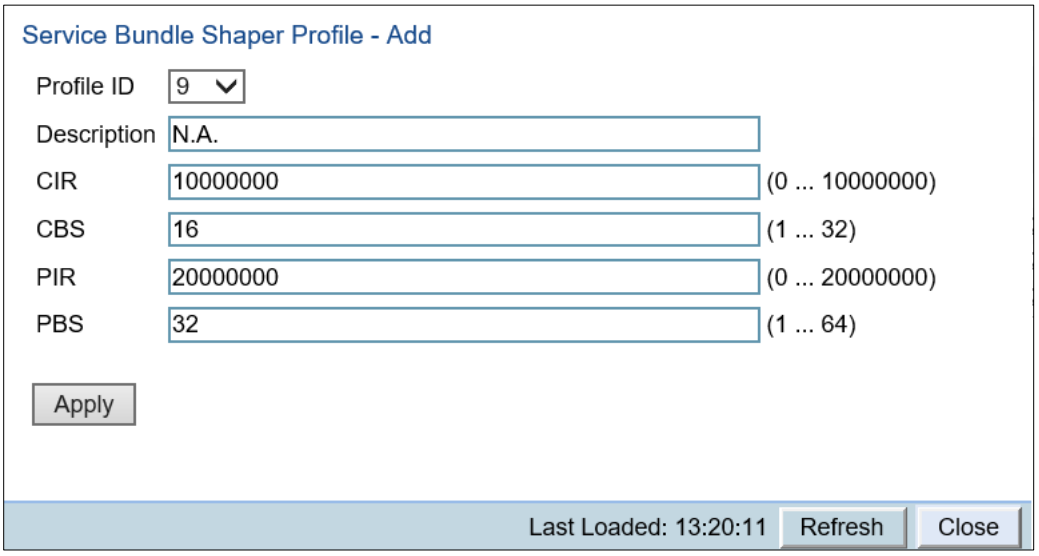


Figure 289: Service Bundle Shaper Profile – Add Page

3 In the **Profile ID** field, select a unique ID to identify the profile. Permitted values are 1-31.

4 Optionally, in the **Description** field, enter a description of the profile.

5 In the **CIR** field, enter the Committed Information Rate (CIR) assigned to the profile, in bits per second. Permitted values are:

- 0 – 32,000,000 bps, with granularity of 16,000.
- 32,000,000 – 1,000,000,000 bps, with granularity of 64,000.

6 In the **PIR** field, enter the Peak Information Rate (PIR) assigned to the profile, in bits per second. Permitted values are:

- 16,000 – 32,000,000 bps, with granularity of 16,000.
- 32,000,000 – 1,000,000,000 bps, with granularity of 64,000.

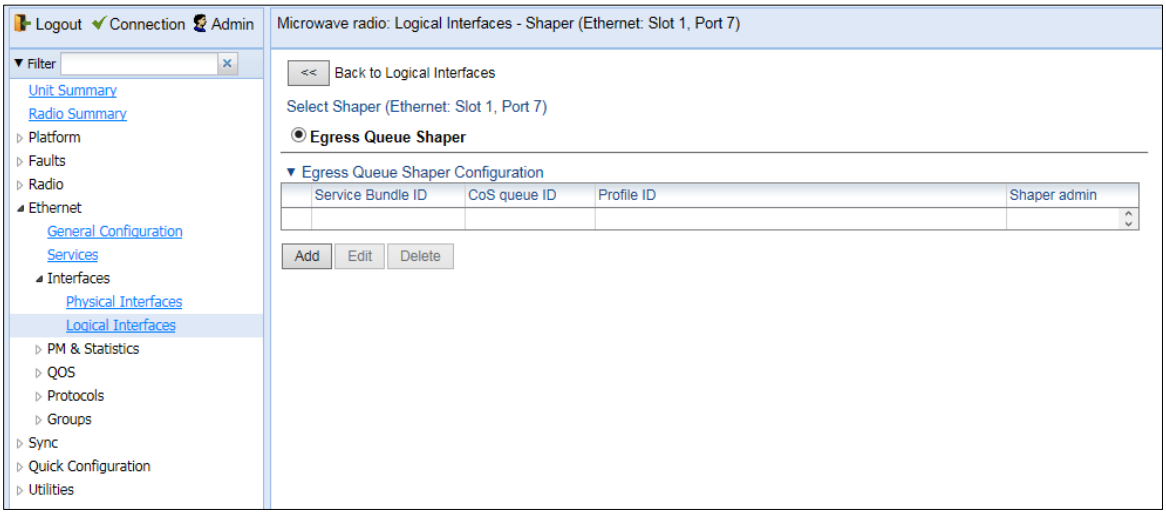
7 Click **Apply**, then **Close**.

11.6.3 Assigning a Queue Shaper Profile to a Queue

To assign a queue shaper profile to a queue:

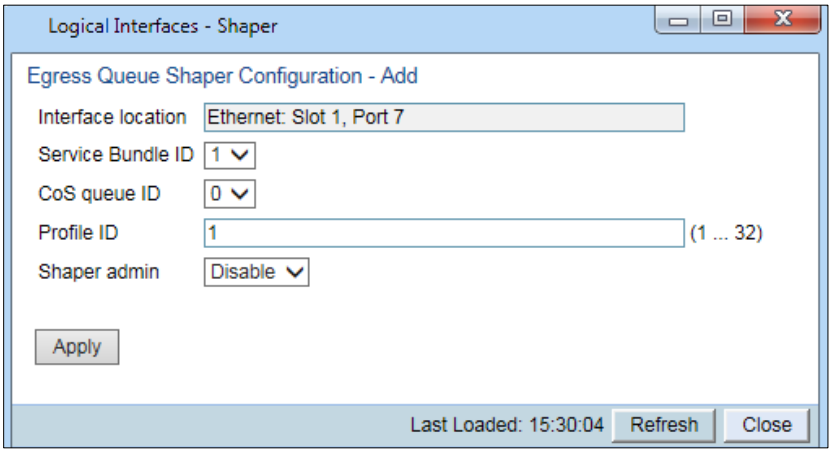
1. Select **Ethernet** > **Interfaces** > **Logical Interfaces**. The Logical Interfaces page opens.
2. Select an interface in the Ethernet Logical Port Configuration table and click **Shaper**. The Logical Interfaces – Shaper page opens, with the Egress Queue Shaper Configuration table open by default. All queue shaper profiles defined in the system are listed in the table.

Figure 412 Logical Interfaces – Shaper – Egress Queue Shaper



3. Click **Add**. The Egress Queue Shaper Configuration – Add page opens.

Figure 413 Logical Interfaces – Egress Queue Shaper Configuration – Add Page



Note

In this release, only one service bundle (Service Bundle ID 1) is supported.

4. In the **CoS queue ID** field, select the CoS queue ID of the queue to which you want to assign the shaper. Queues are numbered according to CoS value, from 0 to 7.
5. In the **Profile ID** field, select from a list of configured queue shaper profiles. See Configuring Queue Shaper Profiles.
6. In the **Shaper Admin** field, select **Enable** to enable egress queue shaping for the selected queue, or **Disable** to disable egress queue shaping for the selected queue.
7. Click **Apply**, then **Close**.

To assign a different queue shaper profile to a queue:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 381).

2. Select an interface in the Ethernet Logical Port Configuration table and click **Shaper**. The Logical Interfaces – Shaper page opens, with the Egress Queue Shaper Configuration table open by default (Figure 412).
3. Select an interface in the Ethernet Logical Port Configuration table and click **Shaper**. The Logical Interfaces – Shaper page opens, with the Egress Queue Shaper Configuration table open by default (Figure 412).
4. Select the row you want to edit and click **Edit**. The Egress Queue Shaper Configuration – Edit page opens. This page is similar to the Egress Queue Shaper Configuration – Add page (Figure 413).
5. To assign a different egress queue shaper profile, select the profile in the **Profile ID** field.
6. To enable or disable egress queue shaping for the selected queue, select **Enable** to enable egress queue shaping for the queue, or **Disable** to disable egress queue shaping for the queue.
7. Click **Apply**, then **Close**.

11.7 Configuring Scheduling

This section includes:

- Scheduling Overview
- Configuring Priority Profiles
- Configuring Queue WFQ Profiles
- Configuring Service Bundle WFQ Profiles
- Assigning a Priority Profile to an Interface
- Assigning a Queue WFQ Profile to an Interface
- Assigning a Service Bundle WFQ Profile to a Service Bundle

11.7.1 Scheduling Overview

Scheduling determines the priority among the queues. PTP 850 provides a unique hierarchical scheduling model that includes four priorities, with Weighted Fair Queuing (WFQ) within each priority, and shaping per port and per queue.

The scheduler scans the queues and determines which queue is ready to transmit. If more than one queue is ready to transmit, the scheduler determines which queue transmits first based on:

Queue Priority – A queue with higher priority is served before lower-priority queues.

Weighted Fair Queuing (WFQ) – If two or more queues have the same priority and are ready to transmit, the scheduler transmits frames from the queues based on a WFQ algorithm that determines the ratio of frames per queue based on a predefined weight assigned to each queue.

11.7.2 Configuring Priority Profiles

Scheduling priority profiles determine the queue priority. Each profile contains eight CoS-based priorities, corresponding to eight queues in an interface to which the profile is assigned. You can configure up to eight priority profiles. A ninth profile, Profile ID 9, is pre-configured. You can configure Green priorities from 4 (highest) to 1 (lowest). An additional four Yellow priority profiles are defined automatically.

This section includes:

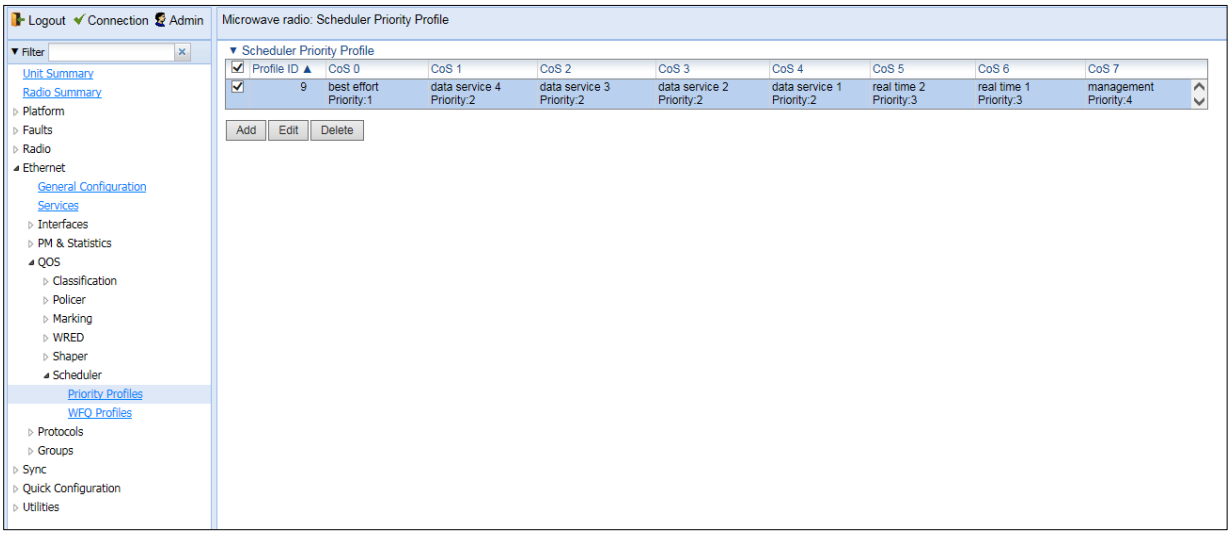
- Adding a Scheduler Priority Profile
- Editing a Service Scheduler Priority Profile
- Deleting a Scheduler Priority Profile

Adding a Scheduler Priority Profile

To add a scheduler priority profile:

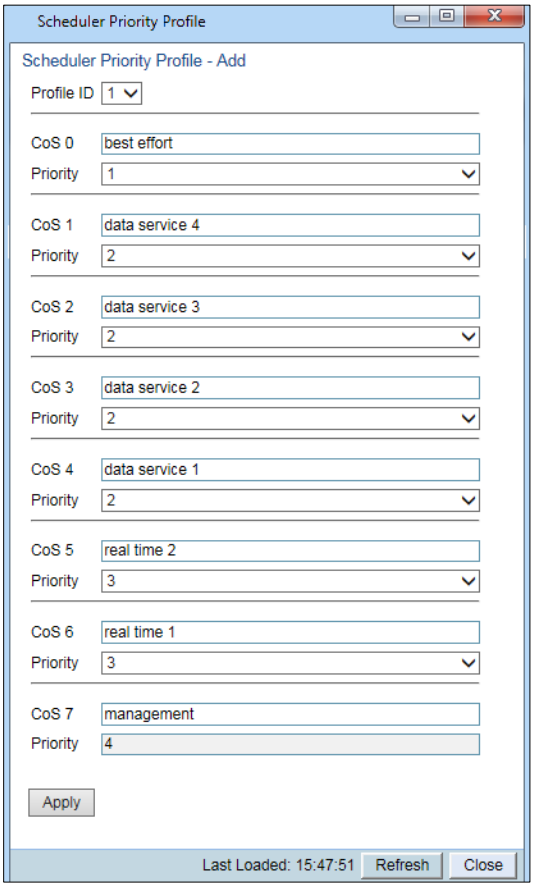
1. Select **Ethernet > QoS > Scheduler > Priority Profiles**. The Scheduler Priority Profile page opens.

Figure 414 Scheduler Priority Profile Page



2. Click **Add**. The Scheduler Priority Profile – Add page opens, with default values displayed.

Figure 415 Scheduler Priority Profile – Add Page



3. In the **Profile ID** field, select a unique Profile ID between 1 and 8.
4. For each CoS value, enter the Green priority, from 4 (highest) to 1 (lowest) (1-4). This priority is applied to Green frames with that CoS egressing a queue to which the profile is assigned.
5. Optionally, you can enter a description of up to 20 characters in the field to the right of each CoS value.
6. Click **Apply**, then **Close**.

Note

The Yellow priority values are assigned automatically by the system.

Editing a Service Scheduler Priority Profile

To edit a scheduler priority profile:

1. Select **Ethernet** > **QoS** > **Scheduler** > **Priority Profiles**. The Scheduler Priority Profile page opens (Figure 414).
2. Select the profile you want to edit and click **Edit**. The Scheduler Priority Profile – Edit page opens. This page is similar to the Scheduler Priority Profile – Add page (Figure 415). You can edit any parameter except the **Profile ID**.
3. Modify the profile.
4. Click **Apply**, then **Close**.

Deleting a Scheduler Priority Profile

To delete a scheduler priority profile, select the profile in the Scheduler Priority Profiles page (Figure 414) and click **Delete**. The profile is deleted.

To delete multiple scheduler priority profiles:

1. Select the profiles in the Scheduler Priority Profiles page or select all the profiles by selecting the check box in the top row.
2. Click **Delete**. The profiles are deleted.

11.7.3 Configuring WFQ Profiles

WFQ profiles determine the relative weight per queue. Each profile contains eight CoS-based weight values, corresponding to eight queues in an interface to which the profile is assigned. You can configure up to five WFQ profiles. A sixth profile, Profile ID 1, is pre-configured.

This section includes:

- WFQ Overview
- Adding a Queue WFQ Profile
- Editing a Queue WFQ Priority Profile
- Deleting a Queue WFQ Profile

11.7.3.1 WFQ Overview

The scheduler serves the queues based on their priority, but when two or more queues have data to transmit and their priority is the same, the scheduler uses Weighted Fair Queuing (WFQ) to determine the weight within each priority. WFQ defines the transmission ratio between the queues.

For each queue WFQ profile, you can determine the relative weights for both CIR and EIR traffic.

The system supports up to six WFQ profiles. Profile ID 1 is a pre-defined read-only profile, and is used as the default profile. Profiles 2 to 6 are user-defined profiles.

The following table provides an example of a WFQ profile.

Table 69 WFQ Profile Example

Profile ID	Queue Weight - CIR	Queue Weight - EIR
0	15	20
1	15	20
2	15	20
3	15	20
4	15	20
5	15	20
6	15	20
7	20	20

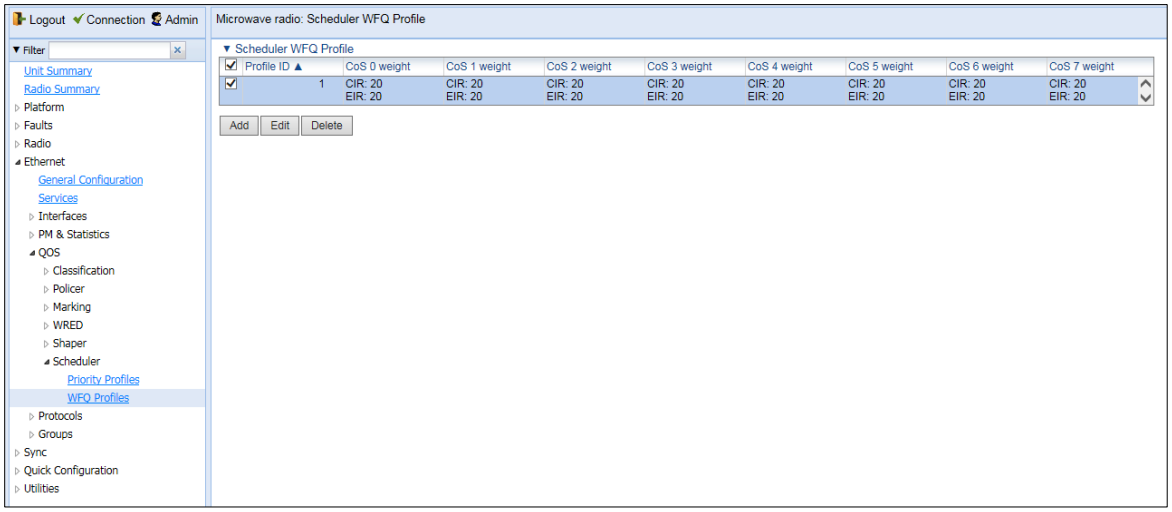
You can attach one of the configured WFQ profiles to each interface. By default, the interface is assigned Profile ID 1, the pre-defined system profile. Profile ID 1 assigns 20 to each CoS for both CIR and EIR traffic.

Adding a queue WFQ Profile

To add a WFQ profile:

1. Select **Ethernet > QoS > Scheduler > Queue WFQ Profiles**. The Scheduler **Queue** WFQ Profile page opens.

Figure 416 Scheduler WFQ Profile Page



2. Click **Add**. The Scheduler WFQ Profile – Add page opens, with default values displayed.

Figure 417 Scheduler WFQ Profile – Add Page



3. In the **Profile ID** field, select a unique Profile ID between 2 and 7. Profile ID 1 is used for a pre-defined WFQ profile.
4. For each CoS value, enter the CIR weight and the EIR weight for that CoS, from 1 to 20.
5. Click **Apply**, then **Close**.

Editing a WFQ Priority Profile

To edit a scheduler WFQ profile:

1. Select **Ethernet** > **QoS** > **Scheduler** > **WFQ Profiles**. The Scheduler WFQ Profile page opens.
2. Select the profile you want to edit and click **Edit**. The Scheduler WFQ Profile – Edit page opens. This page is similar to the Scheduler WFQ Profile – Add page . You can edit any parameter except the **Profile ID**.
3. Modify the profile.
4. Click **Apply**, then **Close**.

Deleting a WFQ Profile

To delete a scheduler WFQ profile, select the profile in the Scheduler WFQ Profiles page and click **Delete**. The profile is deleted.

To delete multiple scheduler WFQ profiles:

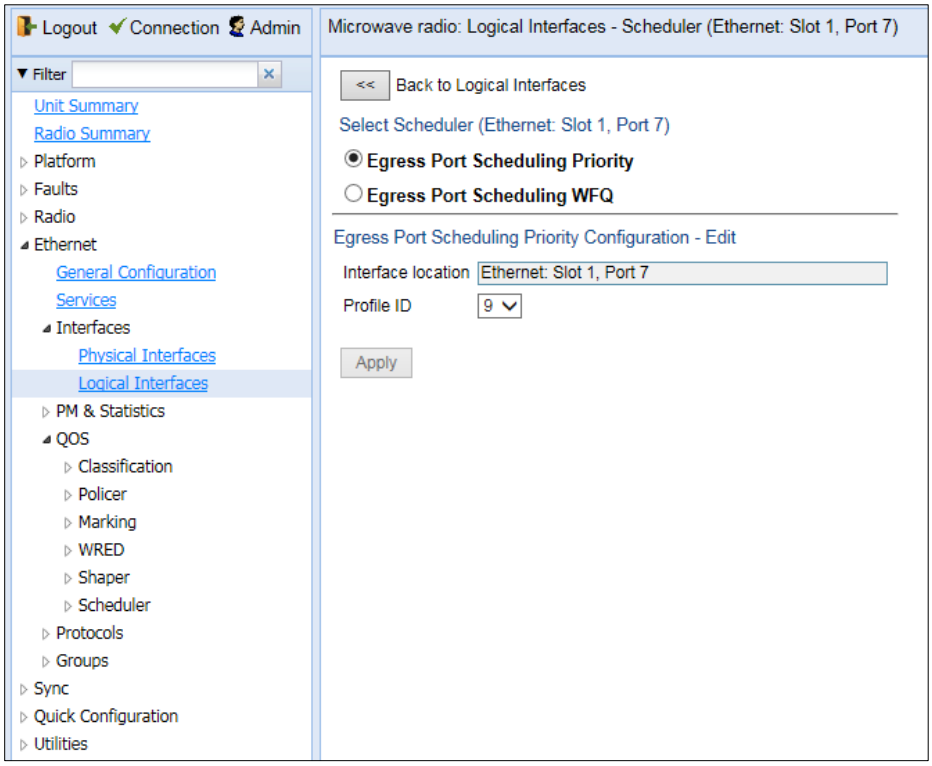
1. Select the profiles in the Scheduler WFQ Profiles page or select all the profiles by selecting the check box in the top row.
2. Click **Delete**. The profiles are deleted.

11.7.4 Assigning a Queue Priority Profile to an Interface

To assign a priority profile to an interface:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens.
2. Select an interface in the Ethernet Logical Port Configuration table and click **Scheduler**. The Logical Interfaces – Scheduler page opens, with the Egress Port Scheduling Priority Configuration – Edit page open by default.

Figure 418 Logical Interfaces – Scheduler – Egress Port Scheduling Priority



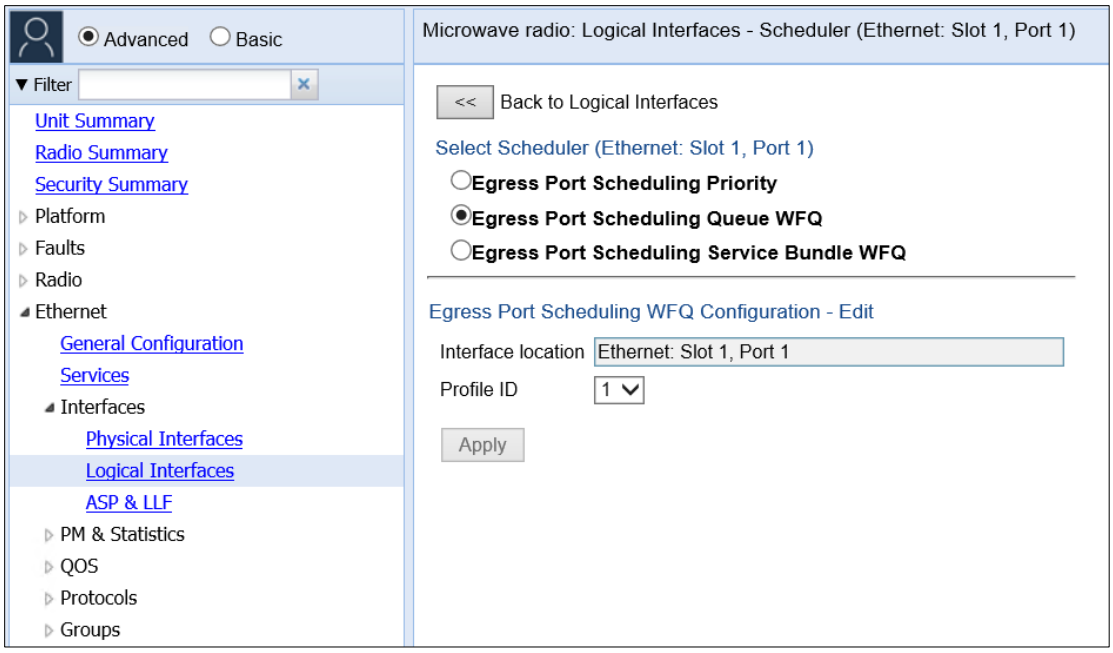
3. In the **Profile ID** field, select from a list of configured scheduling priority profiles.
4. Click **Apply**, then **Close**.

11.7.5 Assigning a Queue WFQ Profile to an Interface

To assign a Queue WFQ profile to an interface:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens.
2. Select an interface in the Ethernet Logical Port Configuration table and click **Scheduler**. The Logical Interfaces – Scheduler page opens, with the Egress Port Scheduling Priority Configuration – Edit page open by default.
3. Select **Egress Port Scheduling** Queue **WFQ**. The Egress Port Scheduling Queue WFQ Configuration – Edit page opens.

Figure 419 Logical Interfaces – Scheduler – Egress Port Scheduling Queue WFQ



4. In the **Profile ID** field, select from a list of configured scheduling priority profiles.
5. Click **Apply**, then **Close**.

11.7.6 Assigning a Service Bundle WFQ Profile to a Service Bundle

To assign a Service Bundle WFQ profile to an interface:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 381).
2. Select an interface in the Ethernet Logical Port Configuration table and click **Scheduler**. The Logical Interfaces – Scheduler page opens, with the Egress Port Scheduling Priority Configuration – Edit page open by default (Figure 418).
3. Select **Egress Port Scheduling Service Bundle WFQ**. The Egress Port Scheduling Service Bundle WFQ Configuration – Edit page opens.

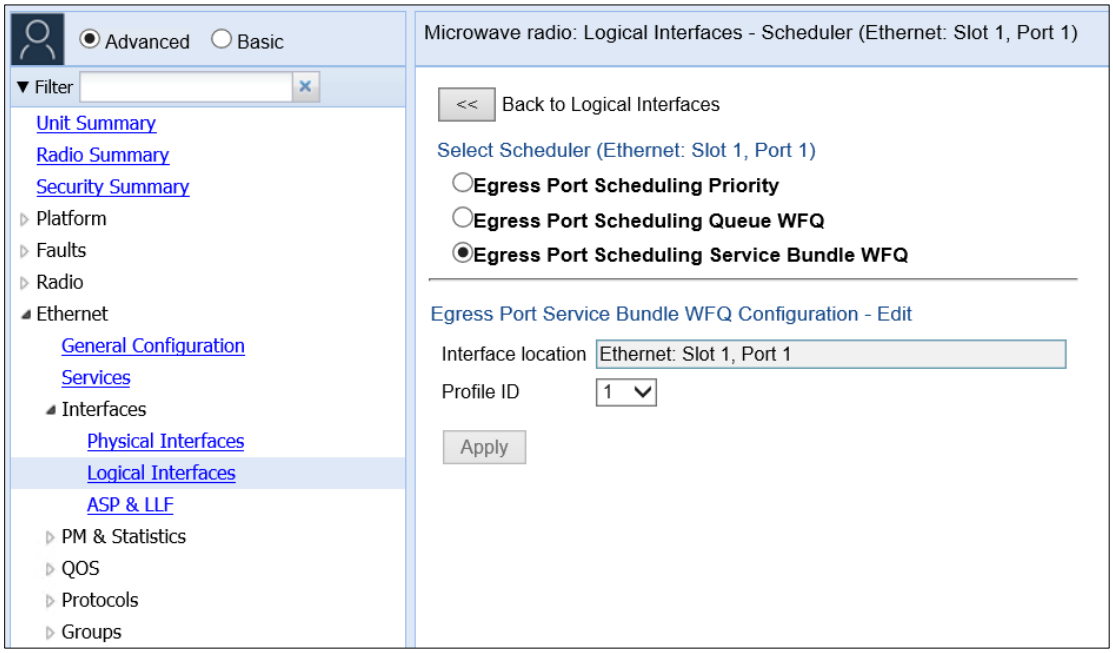


Figure 420: Logical Interfaces – Scheduler – Egress Port Scheduling Service Bundle WFQ

4. In the **Profile ID** field, select from a list of configured scheduling Service Bundle WFQ profiles.
5. Click **Apply**, then **Close**.

11.7.7 Enabling Hierarchical QoS (H-QoS)

This section includes:

- H-QoS Overview
- Configuring H-QoS

11.7.8 H-QoS Overview

Note: H-QoS is only supported with PTP 850C. H-QoS with PTP 850E is planned for future release.

In a standard QoS mechanism, egress data is mapped to a single service bundle on the egress interface. This single service bundle supports up to eight priority queues, which correspond to the CoS of the data. Since all traffic for the interface egresses via these queues, there is no way to distinguish between different services and traffic streams within the same priority.

H-QoS adds the ability to distinguish between different services, creating a hierarchy of egress queues per service *and* CoS. This gives operators the ability to prioritize traffic streams on the basis of logical interface, service bundle, and CoS, creating multiple queues.

H-QoS enables you to use up to six service bundles (1-6). One of these service bundles is assigned to each service point.

Note: In addition to the six configurable service bundles, the system includes Service Bundle 0 (reserved for TDM and not available to the user) and Service Bundle 7 (reserved for management).

When H-QoS is enabled on an interface, you can define up to 32 Service Bundle Shaper profiles and assign these profiles to the interface per service bundle. The Serivce Bundle Shaper profiles determine the traffic profile per service bundle for each interface, using dual leaky bucket shaping. This enables you to differentiate the shaping profile per service point and per interface, based on the service bundle assigned to the service point and the Service Bundle Shaping profile assigned to the interface per service bundle.

In addition, when H-QoS is enabled on an interface, you can define up to 32 Service Bundle WFQ profiles and assign one of these profiles to the interface. The Service Bundle WFQ profile defines the relative weights for both CIR and EIR traffic per service bundle. This enables you to define a unique WFQ scheduling profile on the basis of service bundle, interface, and CoS (via the Queue WFQ profile) and Assigning a Service Bundle WFQ Profile to a Service Bundle.

H-QoS can be enabled on radio and Ethernet interfaces, as well as Link Bonding, Multi-Carrier ABC, and LAG groups.

The management service point uses Service Bundle 7 instead of 1, regardless of whether the QoS mode is Standard or Hierarchical. Therefore, use Service Bundle 7 for reading Egress CoS Statistics and assigning queue shapers for management traffic. Note, however, that the Service Bundle ID is displayed as 1 (for the pre-configured management point), or as configured by the user for additional management service points.

11.7.9 Configuring H-QoS

To enable H-QoS on an interface:

1 Select **Ethernet** > **Interfaces** > **Logical Interfaces**. The Logical Interfaces page opens (Figure 381).
2 Select an interface in the Ethernet Logical Port Configuration table and click **Edit**. The Logical Interfaces – Edit page opens.

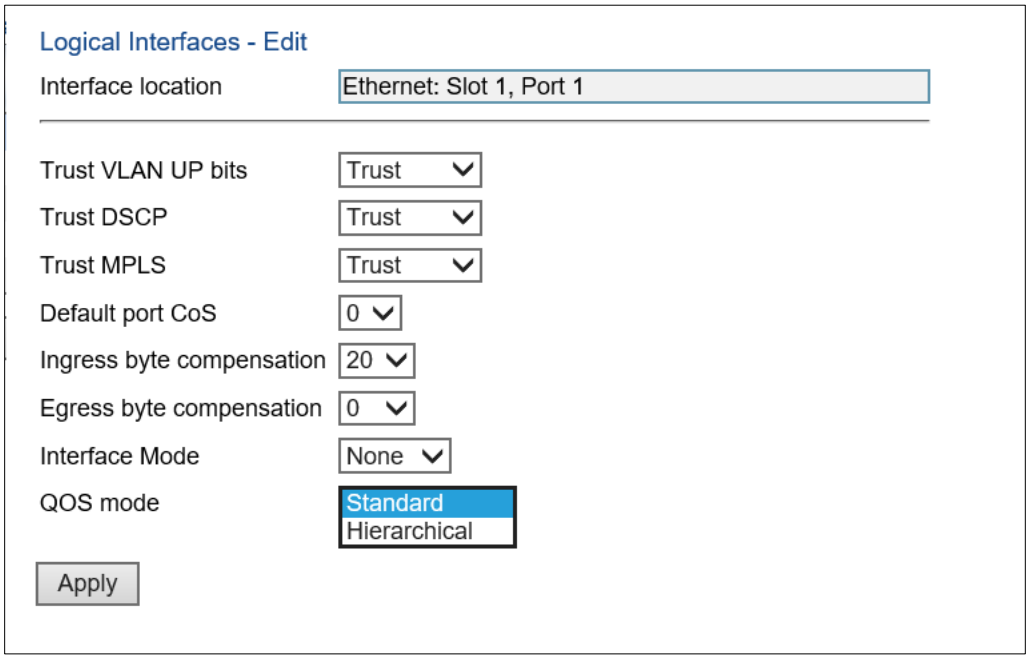


Figure 421: Logical Interfaces Page – Edit (QoS Mode)

3 In the **QOS mode** field, select **Hierarchical** to enable H-QoS on the interface.
4 Click **Apply**.

Note: For radio interfaces only (including Multi-Carrier ABC and Link Bonding groups), you must reboot the unit after changing the **QOS mode**. Until the unit is rebooted, an alarm will be raised on the interface.

This is not necessary for Ethernet or LAG interfaces.

11.8 Configuring and Displaying Queue-Level PMs

PTP 850 devices support advanced traffic PMs per CoS queue and service bundle. For each logical interface, you can configure thresholds for Green and Yellow traffic per queue. You can then display the following PMs for 15-minute and 24-hour intervals, per queue and color:

- Maximum bytes passed per second
- Minimum bytes passed per second
- Average bytes passed per second
- Maximum bytes dropped per second
- Minimum bytes dropped per second

- Average bytes dropped per second
- Maximum packets passed per second
- Minimum packets passed per second
- Average packets passed per second
- Maximum packets dropped per second
- Minimum packets dropped per second
- Average packets dropped per second
- Seconds bytes per second were over the configured threshold per interval

These PMs are available for any type of logical interface, including groups. To activate collection of these PMs, the user must add a PM collection rule on a logical interface and service bundle and set the relevant thresholds per CoS and Color. When the PM is configured on a group, queue traffic PMs are recorded for the group and not for the individual interfaces that belong to the group.

One collection rule is available per interface.

PMs for queue traffic are saved for 30 days, after which they are removed from the database. It is important to note that they are not persistent, which means they are not saved in the event of unit reset.

To configure queue-level PMs:

1 Select **Ethernet** > **PM & Statistics** > **Egress CoS PM** > **Configuration**. The Egress CoS PM Configuration page opens.

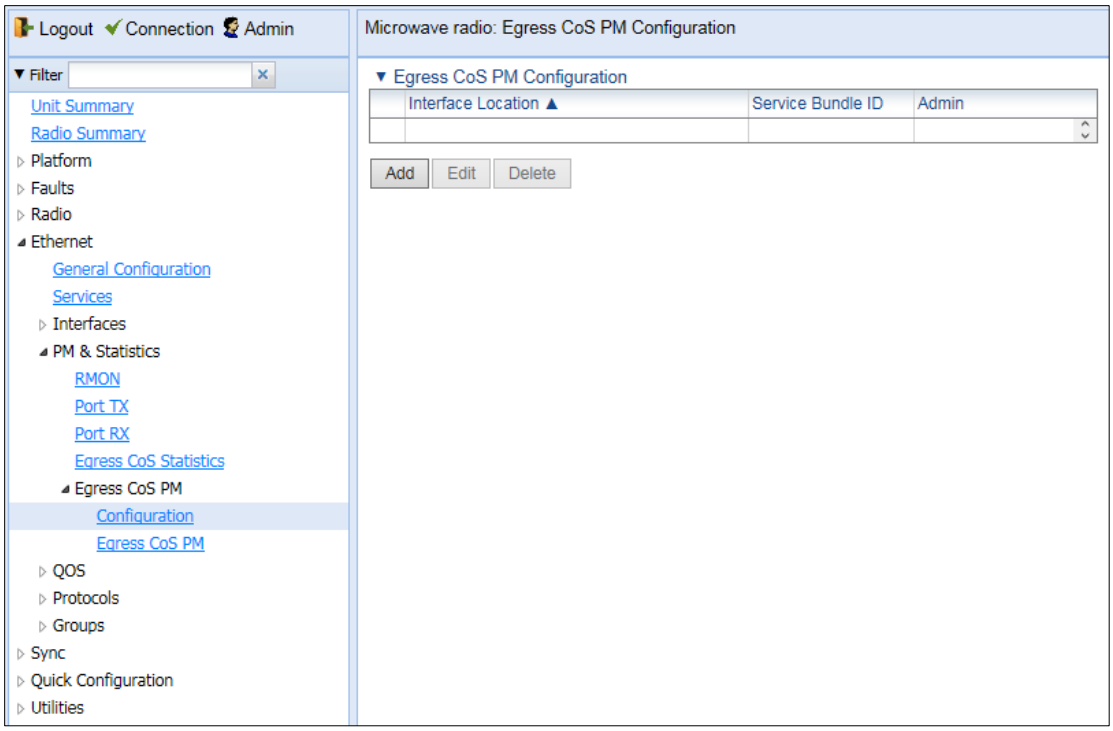


Figure 422 Egress CoS PM Configuration Page

2 Click **Add**. The Egress CoS PM Configuration – Add page opens.

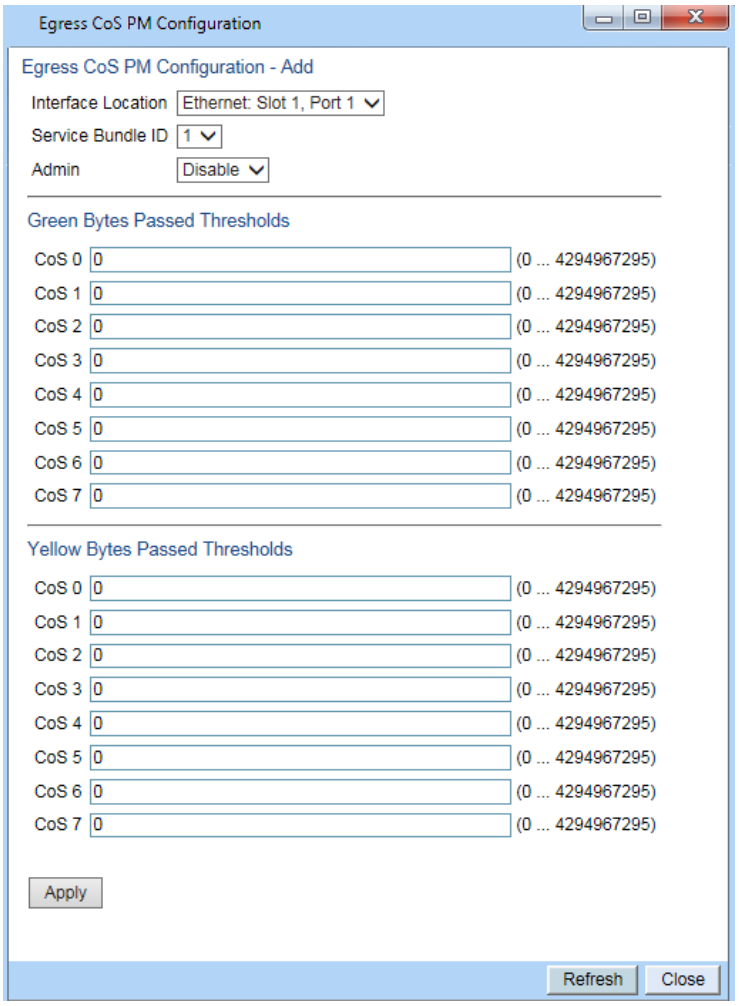


Figure 423 Egress CoS PM Configuration – Add Page

3 In the **Interface Location** field, select the interface for which you want to configure the collection rule.
4 In the **Service Bundle** field, select a service bundle (1-6).
5 In the **Admin** field, select **Enable** to enable the collection rule.
6 Enter the Green and Yellow thresholds for each CoS, in bytes (0-4294967295).
7 Click **Apply**.
8 Repeat these steps to configure collection rules for additional interfaces.

To display queue-level PMs:

1 Select **Ethernet** > **PM & Statistics** > **Egress CoS PM** > **Egress CoS PM**. The Egress CoS PM page opens.

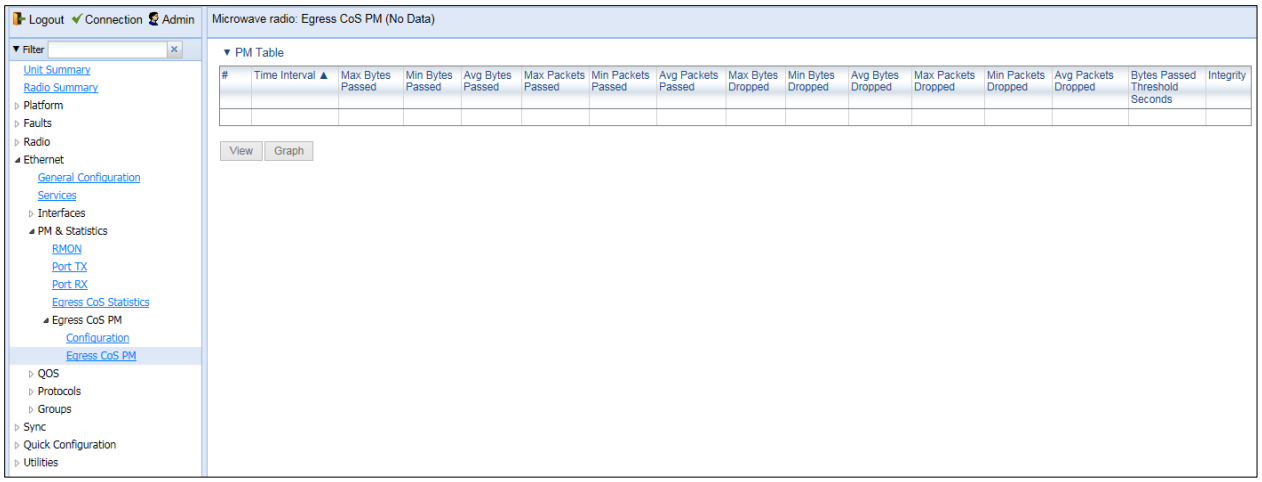


Figure 424 Egress CoS PM Page

The **Integrity** column indicates whether the values received at the time and date of the measured interval are valid. An X in the column indicates that the values are invalid. This can occur for a number of reasons, including but not limited to a disconnected cable, a missing SFP transceivers, muting of a radio interface, and an operational status of **Down**.

12. Ethernet Protocols

This section includes:

- Configuring G.8032
- Configuring MSTP
- Configuring Ethernet Bandwidth Notification (ETH-BN)
- Configuring LLDP

Related Topics:

- Configuring Service OAM (SOAM) Fault Management (FM)

12.1 Configuring G.8032

This section includes:

- G.8032 Overview
- Configuring the Destination MAC Address
- Adding ERPIs
- Configuring the RPL Owner
- Configuring Timers
- Viewing the ERPI Configuration and Status Parameters
- Viewing ERPI State Information
- Initiating a Manual or Forced Switch and Clearing the Switch or Initiating Reversion
- Blocking or Unblocking R-APS Messages on a Service Point
- Viewing ERPI Statistics

G.8032 Overview

Note: P2P services are not affected by G.8032, and continue to traverse ports that are blocked by G.8032. G.8032 cannot be configured on management ports, including management ports used for traffic (PTP 850S).

ERPS, as defined in the G.8032 ITU standard, is currently the most advanced ring protection protocol, providing convergence times of sub-50ms. ERPS prevents loops in an Ethernet ring by guaranteeing that at any time, traffic can flow on all except one link in the ring. This link is called the Ring Protection Link (RPL). Under normal conditions, the RPL is blocked, i.e., not used for traffic. One designated Ethernet Ring Node, the RPL Owner Node, is responsible for blocking traffic at one end of the RPL. When an Ethernet ring failure occurs, the RPL Owner unblocks its end of the RPL, allowing the RPL to be used for traffic. The other Ethernet Ring Node adjacent to the RPL, the RPL Neighbor Node, may also participate in blocking or unblocking its end of the RPL. A number of ERP instances (ERPIs) can be created on the same ring.

For a more detailed description of G.8032, refer to the Technical Description for the product you are using.

Configuring the Destination MAC Address

To configure the destination MAC address for G.8032:

1 Select **Ethernet > Protocols > G.8032 > General Attribute**. The G.8032 General Attribute page opens.

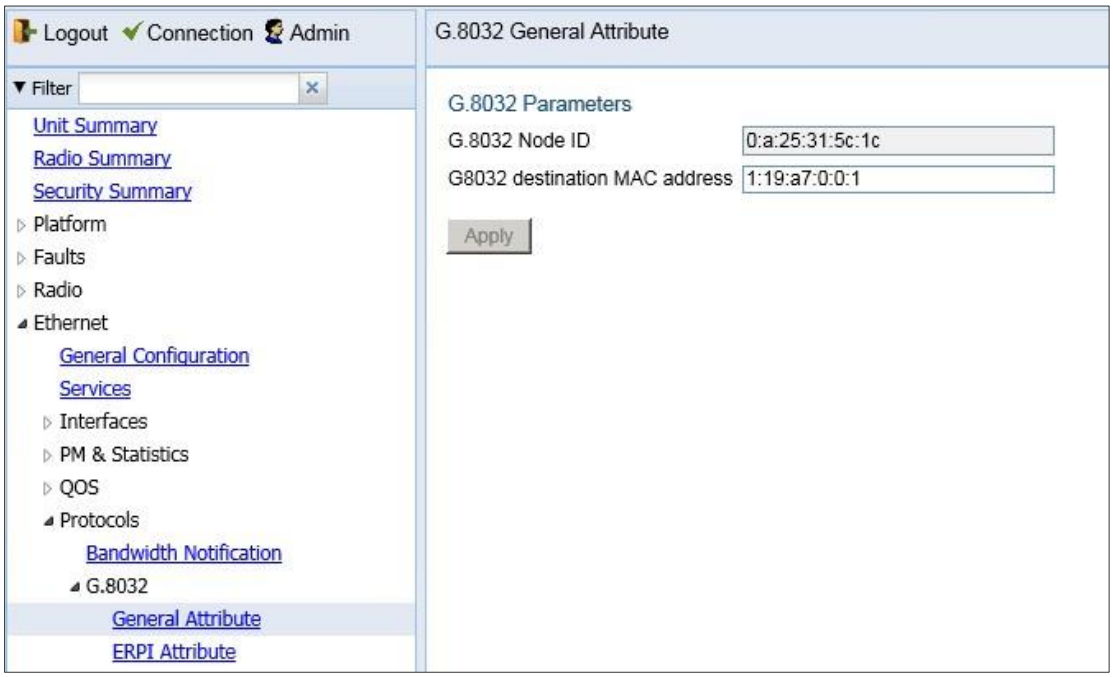


Figure 305: G.8032 General Attribute Page

2 In the **G8032 destination MAC address field**, enter the destination MAC address for PDUs generated by the node.

3 Click **Apply**.

Adding ERPIs

You can configure up to 16 Ethernet Ring Protection instances (ERPIs). Each ERPI is associated with an Ethernet service defined in the system.

To add an ERPI:

1 Select **Ethernet > Protocols > G.8032 > ERPI Attribute**. The G.8032 ERPI Attribute page opens.

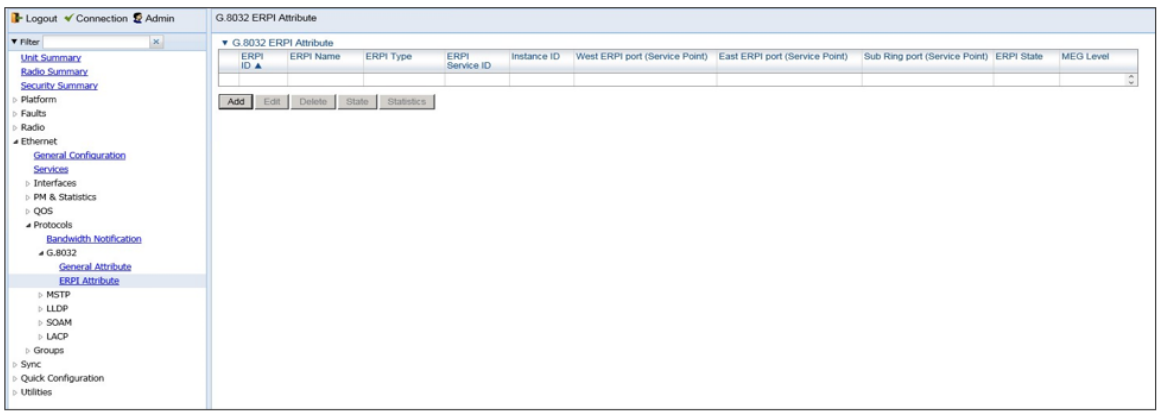


Figure 306: G.8032 ERPI Attribute Page

2 Click **Add**. The Add G8032 ERPI Attribute wizard opens.



Figure 307: G.8032 ERPI Attribute Wizard – Page 1

3 In the **ERPI ID** field, select an available ID. The ERPI ID is a unique ID that identifies the ERPI.

4 Optionally, in the **ERPI Name** field, enter a descriptive name for the ERPI.

5 In the **Type** field, select the type of ERPI, based on the type of ring:

- Ring: A Ring is an Ethernet ring that is connected on two ports (East and West service points) to an interconnection node.
- Sub-ring: A Sub-Ring is an Ethernet ring which is connected to another ring or network through the use of interconnection nodes (East and West service points). On their own, the Sub-Ring links do not form a closed physical loop. A closed loop may be formed by the sub-ring links and the link between interconnection nodes that is controlled by other ring or network.
- Ring with sub-ring: The ERPI includes both a ring, with East and West service points, and a connection to a sub-ring using a Sub-Ring service point.

6 In the **Service ID** field, select the ID of the Ethernet service to which the ERPI belongs.

7 Optionally, in the **MEG Level** field, select the Maintenance Entity Group (MEG) level used for R-APS messages sent in the ERPI (0-7).

8 Click **Next**. The second page of the Add G.8032 ERPI Attribute wizard opens.

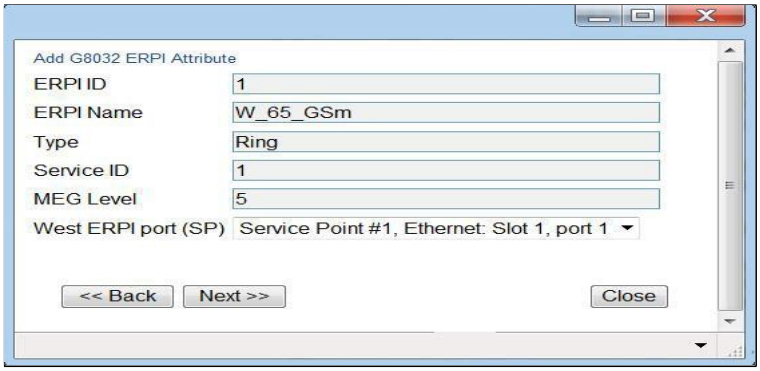


Figure 308: G.8032 ERPI Attribute Wizard – Page 2

9 In the **West ERPI port (SP)** field, select the first endpoint for the ERPI. This can be any service point that has been configured for the service.

Note: Service points on the PTP 850 side of the link must have a single, determinate VLAN. This means the service point type must be dot1q, s-tag, or QinQ. On the customer side, any service point type can be used.

10 Click **Next**. The third page of the Add G.8032 ERPI Attribute wizard opens.

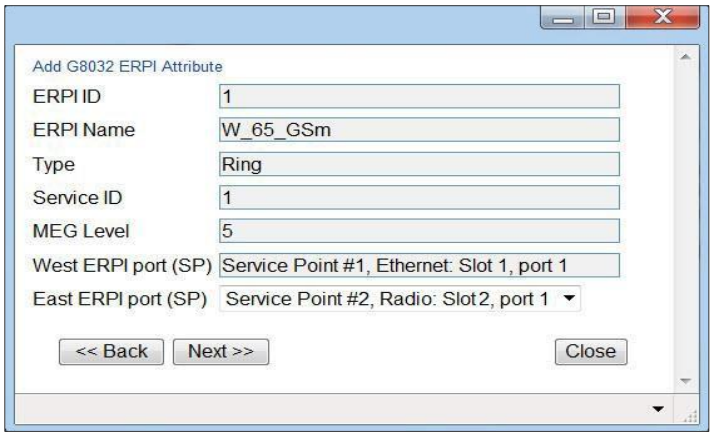


Figure 309: G.8032 ERPI Attribute Wizard – Page 3

11 In the **East ERPI port (SP)** field, select the second endpoint for the ERPI. This can be any service point that has been configured for the service.

12 Click **Next**:

- If the Type is Ring or Sub-ring, the Submit page opens. Go to Step 15.
- If the Type is Ring with sub-ring, the fourth page of the Add G.8032 ERPI Attribute wizard opens.

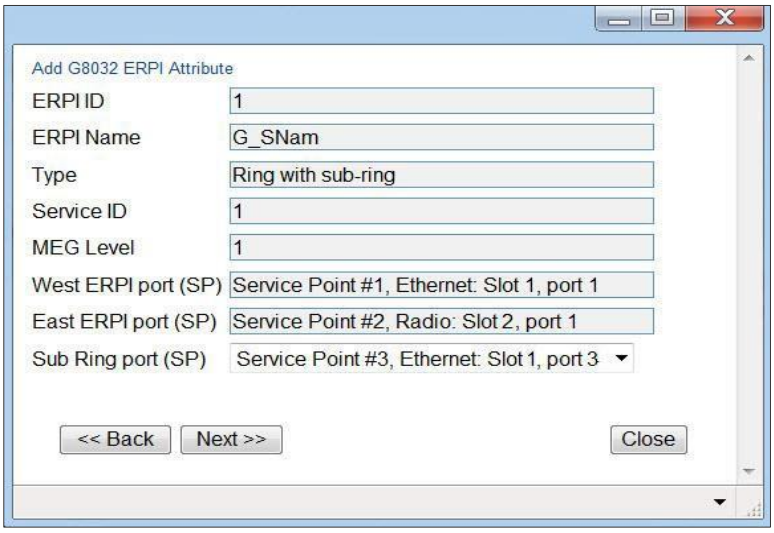


Figure 310: G.8032 ERPI Attribute Wizard – Page 4

13 In the **Sub Ring port (SP)** field, select the service point that connects the Ring with the Sub-Ring. This can be any service point that has been configured for the service.

14 Click **Next**. The Submit page opens.

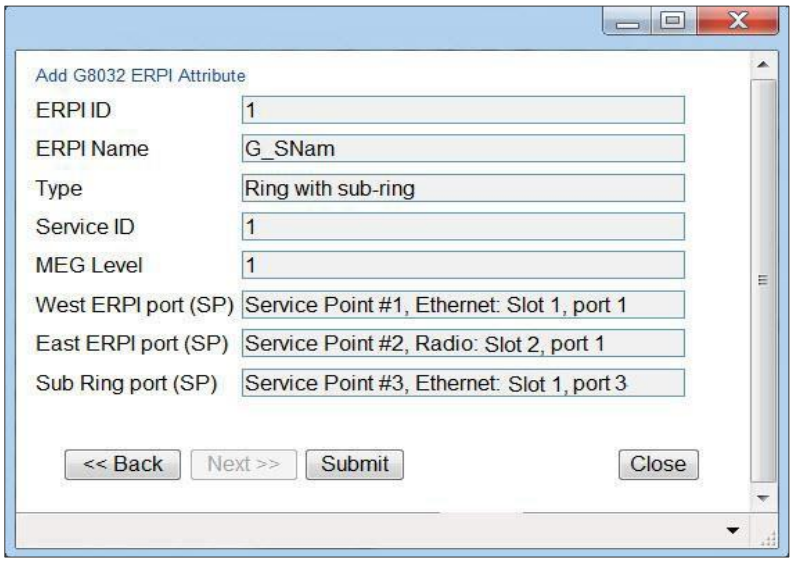


Figure 311: G.8032 ERPI Attribute Wizard – Submit

15 Verify that the parameters of the ERPI are correct and click **Submit**.

Configuring the RPL Owner

The RPL Owner Node is a node in the ERPI that is responsible for blocking traffic at one end of the ERPI. You can select one RPL per ERPI. To designate the RPL Owner Node:

1 Select **Ethernet > Protocols > G.8032 > ERPI Attribute**. The G.8032 ERPI Attribute page opens (*Figure 306*).

2 Select the ERPI and click **Edit**. The ERPI Attribute – Edit page opens.

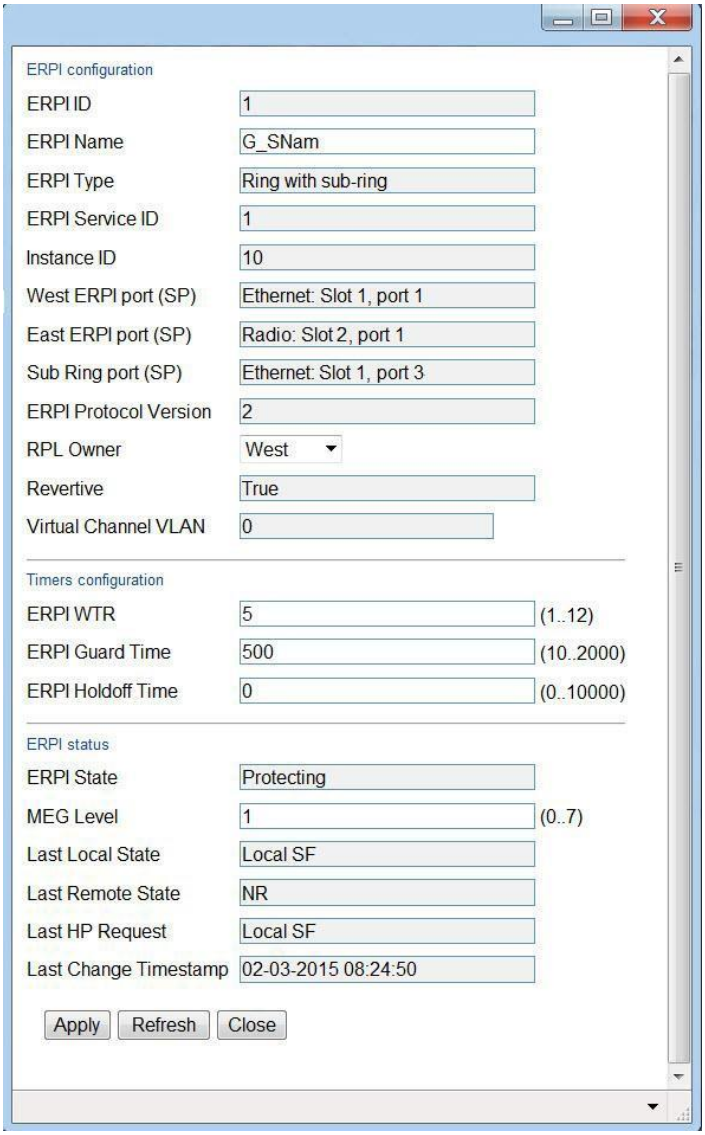


Figure 312: G.8032 ERPI Attribute – Edit Page

3 In the **RPL Owner** field, select the service point you want to configure as RPL Owner.

4 Click **Apply**, then **Close**.

Configuring Timers

You can configure timers per ERPI to control the ERPI's switching and convergence parameters. The following timers are available:

- **Wait to Restore (WTR) Timer** – Defines a minimum time the system waits after signal failure is recovered before reverting to idle state, when the RPL can again be blocked.
- **Guard Time** – The guard time is the minimum time the system waits after recovery from a signal failure before accepting new R-APS messages. The Guard Time should be greater than the maximum expected forwarding delay for which one R-APS message circles around the ring.

- **Hold-Off Time** – Determines the time period from failure detection to response. It is used to coordinate between recovery mechanisms (which mechanism takes place first).

To configure the ERPI timers:

1 Select **Ethernet > Protocols > G.8032 > ERPI Attribute**. The G.8032 ERPI Attribute page opens (*Figure 306*).

2 Select the ERPI and click **Edit**. The ERPI Attribute – Edit page opens (*Figure 312*).

3 In the **ERPI WTR** field, enter the Wait to Restore (WTR) timer (in minutes).

4 In the **ERPI Guard Time** field, enter the ERPI guard time (in msec). You must enter a multiple of 10.

5 In the **ERPI Holdoff Time** field, enter the ERPI hold-off time (in msec). You must enter a multiple of 100.

6 Click Apply, then Close.

8.1.2 Viewing the ERPI Configuration and Status Parameters

The G.8032 ERPI Attribute page (*Figure 306*) displays some of the configuration and status parameters for ERPIs configured in the system.

To display a full list of configuration and status parameters for an ERPI:

1 Select **Ethernet > Protocols > G.8032 > ERPI Attribute**. The G.8032 ERPI Attribute page opens .

2 Select the ERPI and click **Edit**. The ERPI Attribute – Edit page opens.

- Table 63 lists and describes the parameters in the ERPI configuration section of the ERPI Attribute – Edit page.
- Table 64 lists and describes the parameters in the ERPI status section of the ERPI Attribute – Edit page.

Table 63: ERPI Configuration Parameters

Parameter	Definition
ERPI ID	Read-only. A unique ID that identifies the ERPI.
ERPI Name	A descriptive name for the ERPI.
ERPI Type	Read-only. The ERPI type.
ERPI Service ID	Read-only. The ID of the Ethernet service to which the ERPI belongs.
Instance ID	Read-only. The MSTI to which the Ethernet service is mapped. See
West ERPI Port (SP)	Read-only. The interface to which the west ERPI service point belongs.
East ERPI Port (SP)	Read-only. The interface to which the east ERPI service point belongs.
Sub Ring Port (SP)	Read-only. The interface to which the service point that connects the Ring with the Sub-Ring belongs.
ERPI Protocol Version	Read-only. The ERPI (G.8032) protocol version currently being used in the unit.
RPL Owner	The RPL Owner Node is a node in the ERPI that is responsible for blocking traffic at one end of the ERPI. See *Configuring the RPL Owner*.
Revertive	Read-only. Indicates whether the ERPI is currently in revertive mode.
Virtual Channel VLAN	Read-only. The VLAN of the virtual channel. If the value is 0, there is no virtual channel.

Table 64: ERPI Status Parameters

Parameter	Definition
ERPI State	Indicates the current ERPI state. Possible values are: • Initializing • Idle • Pending • Protecting • FS (Forced Switch) • MS (Manual Switch)
MEG Level	The Maintenance Entity Group (MEG) level used for R-APS messages sent in the ERPI.
Last Local State	Describes the current local state input to the ERPI state machine.
Last Remote State	Indicates the last event received from the other end of the link.

Last HP Request	Indicates the last high-priority event.
Last Change	Indicates the time of the last ring state transition.

Viewing ERPI State Information

To view information about an ERPI's state:

1 Select **Ethernet > Protocols > G.8032 > ERPI Attribute**. The G.8032 ERPI Attribute page opens (*Figure 306*).

2 Select the ERPI and click **State**. The ERPI Attribute – State page opens.

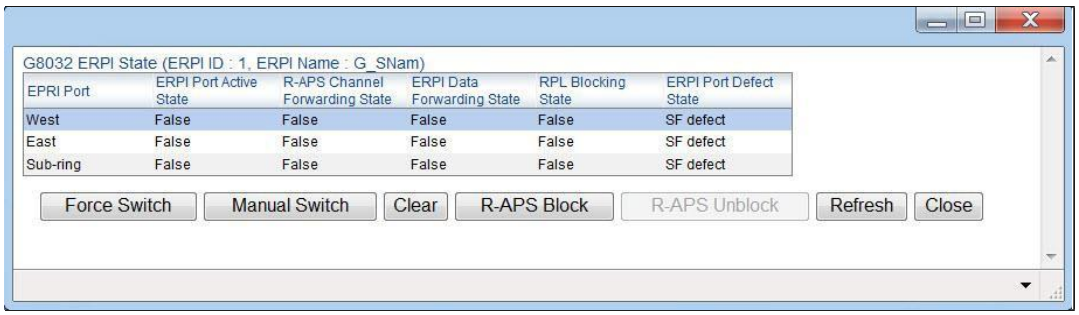


Figure 313: G.8032 ERPI Attribute – State Page

Below table lists and describes the parameters in the ERPI Attribute – State page.

Table 65: ERPI State Parameters

Parameter	Definition
ERPI Port	Identifies whether the row is for the West endpoint, the East endpoint, or a Sub-Ring
ERPI Port Active State	Indicates whether or not the service point is active for traffic forwarding.
R-APS Channel Forwarding State	Indicates whether the service point is forwarding R-APS messages.
ERPI Data Forwarding State	Indicates whether the service point is in unblocked (forwarding) state.
RPL Blocking State	Only relevant if the ERPI to which the service point belongs is the RPL owner. Indicates whether the
ERPI Port Defect State	Indicates whether the service point is in Signal Fail (SF) or Signal Defect (SD) state. Note: Support for Signal Defect state is planned for future release.

Initiating a Manual or Forced Switch and Clearing the Switch or Initiating Reversion

You can initiate a manual or forced switch, clear the switch, and initiate reversion, from the G.8032 ERPI Attribute – State page:

1. Select **Ethernet > Protocols > G.8032 > ERPI Attribute**. The G.8032 ERPI Attribute page opens (*Figure 306*).
2. Select the ERPI and click **State**. The ERPI Attribute – State page opens (*Figure 313*).
3. Select the service point on which you want to perform the operation.
   - To initiate a forced switch, click Force Switch.
   - To initiate a manual switch, click Manual Switch.
   - To clear a forced or manual switch, click Clear. You can also click Clear to trigger convergence prior to the expiration of the relevant timer.

Blocking or Unblocking R-APS Messages on a Service Point

To enable or disable transmission of R-APS messages on a service point:

1. Select **Ethernet > Protocols > G.8032 > ERPI Attribute**. The G.8032 ERPI Attribute page opens (*Figure 306*).
2. Select the ERPI and click **State**. The ERPI Attribute – State page opens (*Figure 313*).
3. Select the service point on which you want to perform the operation.
   - To block R-APS message transmission on the service point, click R-APS Block.
   - To enable R-APS message transmission on the service point, click R-APS Unblock.

Viewing ERPI Statistics

To view statistics about an ERPI:

1. Select **Ethernet > Protocols > G.8032 > ERPI Attribute**. The G.8032 ERPI Attribute page opens (*Figure 306*).
2. Select the ERPI and click **Statistics**. The ERPI Attribute – Statistics page opens.

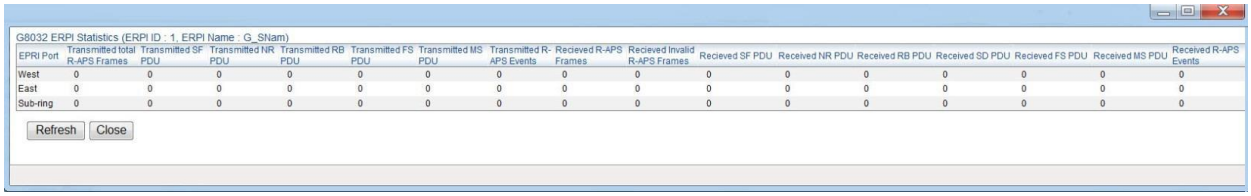


Figure 314: G.8032 ERPI Attribute – Statistics Page

Table 66 lists and describes the statistics shown in the ERPI Attribute – Statistics page.

Table 66: ERPI Statistics

Parameter	Definition
ERPI Port	Identifies whether the row is for the West endpoint, the East endpoint, or a Sub-Ring connection point.
Transmitted Total R-APS	The number of R-APS frames that have been transmitted via the service point.
Transmitted SF PDU	The number of R-APS Signal Fail (SF) frames that have been transmitted via the service point.
Transmitted NR PDU	The number of R-APS No Request (NR) frames that have been transmitted via the service point.
Transmitted RB PDU	The number of R-APS RPL Blocked (RB) frames that have been transmitted via the service point.
Transmitted FS PDU	The number of R-APS Force Switched (FS) frames that have been transmitted via the service point.
Transmitted MS PDU	The number of R-APS Manual Switched (MS) frames that have been transmitted via the service point.
Transmitted R-APS	Reserved for future use.
Received R-APS Frames	The number of R-APS frames that have been received via the service point.
Received Invalid R-APS	The number of R-APS frames with an invalid format that have been received via the service point.
Received SF PDU	The number of R-APS Signal Fail (SF) frames that have been received via the service point.
Received NR PDU	The number of R-APS No Request (NR) frames that have been received via the service point.
Received RB PDU	The number of R-APS RPL Blocked (RB) frames that have been received via the service point.
Received SD PDU	The number of R-APS Signal Degrade (SD) frames that have been received via the service point.
Received FS PDU	The number of R-APS Forced Switch (FS) frames that have been received via the service point.
Received MS PDU	The number of R-APS Manual Switch (MS) frames that have been received via the service point.
Received R-APS	Reserved for future use.

12.2 Configuring MSTP

This section includes:

- MSTP Overview
- Mapping Ethernet Services to MSTP instances (MSTIs)
- Configuring the MSTP Bridge Parameters
- Configuring the MSTP Port Parameters

MSTP Overview

Note: P2P services are not affected by MSTP, and continue to traverse ports

that are blocked by MSTP. MSTP cannot be configured on management ports, including

management ports used for traffic (PTP 850S).

MSTP, as defined in IEEE 802.1q, provides full connectivity for frames assigned to any given VLAN throughout a bridged LAN consisting of arbitrarily interconnected bridges.

With MSTP, an independent multiple spanning tree instance (MSTI) is configured for each group of services, and only one path is made available (unblocked) per spanning tree instance. This prevents network loops and provides load balancing capability. It also enables operators to differentiate among Ethernet services by mapping them to different, specific MSTIs. The maximum number of MSTIs is configurable, from 2 to 16.

MSTP is an extension of, and is backwards compatible with, Rapid Spanning Tree Protocol (RSTP).

PTP 820F, PTP 820G, and PTP 820GX support MSTP according to the following IEEE standards:

- 802.1q
- 802.1ad amendment (Q-in-Q)
- 802.1ah (TE instance)

For a more detailed description of MSTP support, refer to the *Technical Description* for the product you are using.

Mapping Ethernet Services to MSTP instances (MSTIs)

Ethernet services can be mapped to MSTP instances (MSTIs) in the Instances per Service Mapping section of the Ethernet General Configuration page. All mapping of Ethernet services to MSTP instances (MSTIs) should be performed before enabling MSTP.

To map Ethernet services to MSTP instances (MSTIs):

1 Select **Ethernet > General Configuration**. The Ethernet General Configuration page opens (*Figure 226*).

2 In the Instance per Service Mapping table, select the Service ID of the service you want to map.

3 Click **Edit**. The Instance per Service Mapping – Edit page opens.

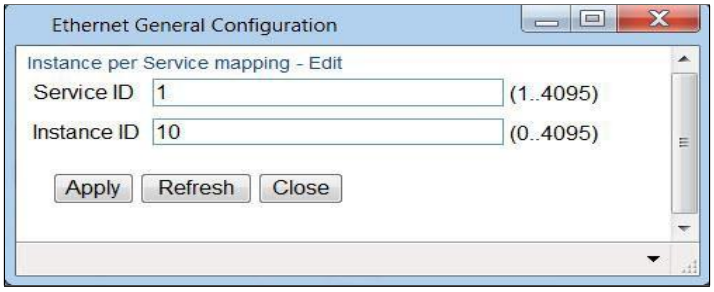


Figure 315: Instance Per Service Mapping – Edit Page

4 In the **Instance ID** field, enter a number between 0 and 16, or 4095. A service mapped to MSTI 4095 is never blocked by any protocol.

5 Click **Apply**.

By default, all Ethernet services are mapped to MSTI 0, which represents the CIST (Common Instance Spanning Tree).

Configuring the MSTP Bridge Parameters

This section includes:

- Enabling MSTP and Configuring the MSTP Bridge General Attributes
- Viewing and Configuring the MSTP Bridge Configuration ID
- Viewing and Configuring the MSTP Bridge Spanning Tree
- Viewing and Configuring the MSTP Bridge CIST Parameters
- Viewing and Configuring the MSTP Bridge MSTI Parameters
- Viewing the MSTP VLAN Parameters

Enabling MSTP and Configuring the MSTP Bridge General Attributes

To configure the MSTP bridge general attributes:

1 Select **Ethernet > Protocols > MSTP > Bridge > General Attributes**. The MSTP Bridge General Attributes page opens.

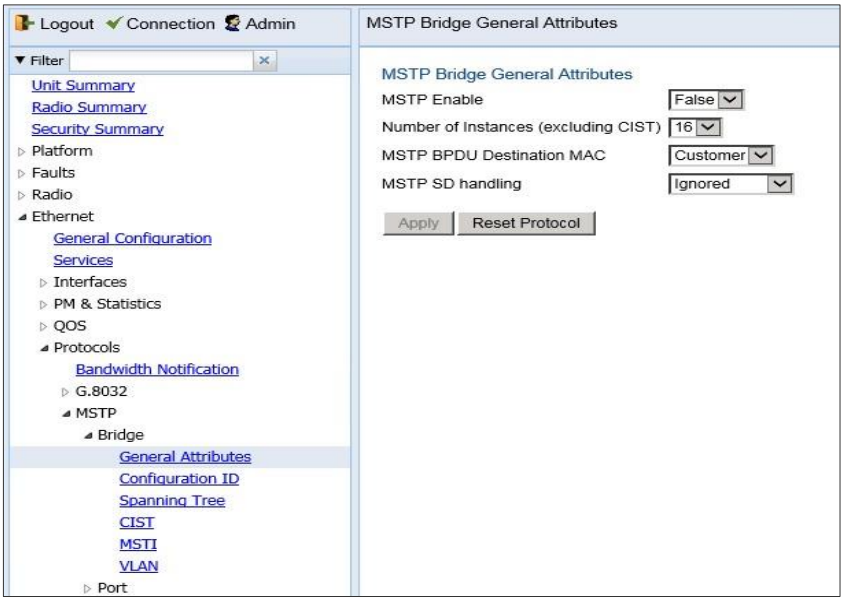


Figure 316: MSTP Bridge General Attributes Page

2 In the **MSTP Enable** field, select **True** to enable MSTP on the unit. To disable MSTP, select **False**.

- Enabling MSTP starts the protocol and sets all ports in all MSTP instances to Blocking state. Convergence upon enabling the protocol generally takes less than two seconds.
- Disabling MSTP stops the MSTP protocol from running and sets all ports in all MSTP instances to Forwarding state.

3 In the **Number of Instances (excluding CIST)** field, select the number of Multiple Spanning Tree instances (MSTIs). Possible values are 1-16. This number does not include the Common and Internal Spanning Tree (CIST).

4 In the **MSTP BPDU Destination MAC** field, select the destination MAC address of BPDUs generated in the unit. Options are:

- Customer – The destination MAC address of BPDUs is 0x0180-C200-0000. Provider BPDUs are either tunneled or discarded.
- Provider – The destination MAC address of BPDUs is 0x0180-C200-0008. Customer BPDUs are either tunneled or discarded.

5 In the **MSTP SD Handling** field, select how MSTP handles Signal Degrade (SD) failures. Options are:

- Ignored – Signal Degrade (SD) failures are ignored in MSTP.
- Same as SF – SD failures trigger a topology change.

6 Click **Apply**.

To reset the MSTP stack, click **Reset Protocol**.

Viewing and Configuring the MSTP Bridge Configuration ID

To configure the Configuration Name and Revision Level:

1 Select **Ethernet > Protocols > MSTP > Bridge > Configuration ID**. The MSTP Bridge Configuration ID page opens.

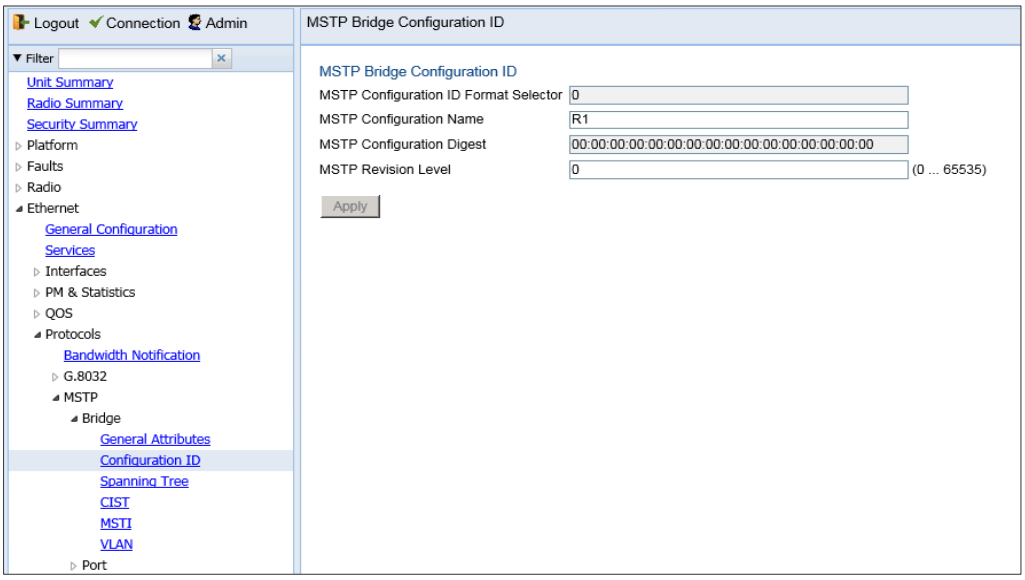


Figure 317: MSTP Bridge Configuration ID Page

2 Modify the configurable parameters.

3 Click **Apply**.

Table 67 lists and describes the parameters in the MSTP Bridge Configuration ID page.

Table 67: MSTP Bridge Configuration ID Parameters

Parameter	Definition
MSTP Configuratio	Read-only. Indicates the format specified in 802.1Q.
MSTP Configuration Name	Enter a valid configuration name. **Note:** Changing the Configuration Name when MSTP is enabled causes the MSTP stack to reset.
MSTP Configuration	Read-only. Displays the MSTP Configuration Digest.
MSTP Revision Level	Enter a valid MSTP revision level. **Note:** Changing the Revision Level when MSTP is enabled causes the MSTP stack to reset.

Viewing and Configuring the MSTP Bridge Spanning Tree

To configure the bridge-level spanning tree parameters:

1 Select **Ethernet > Protocols > MSTP > Bridge > Spanning Tree**. The MSTP Bridge Spanning Tree page opens.

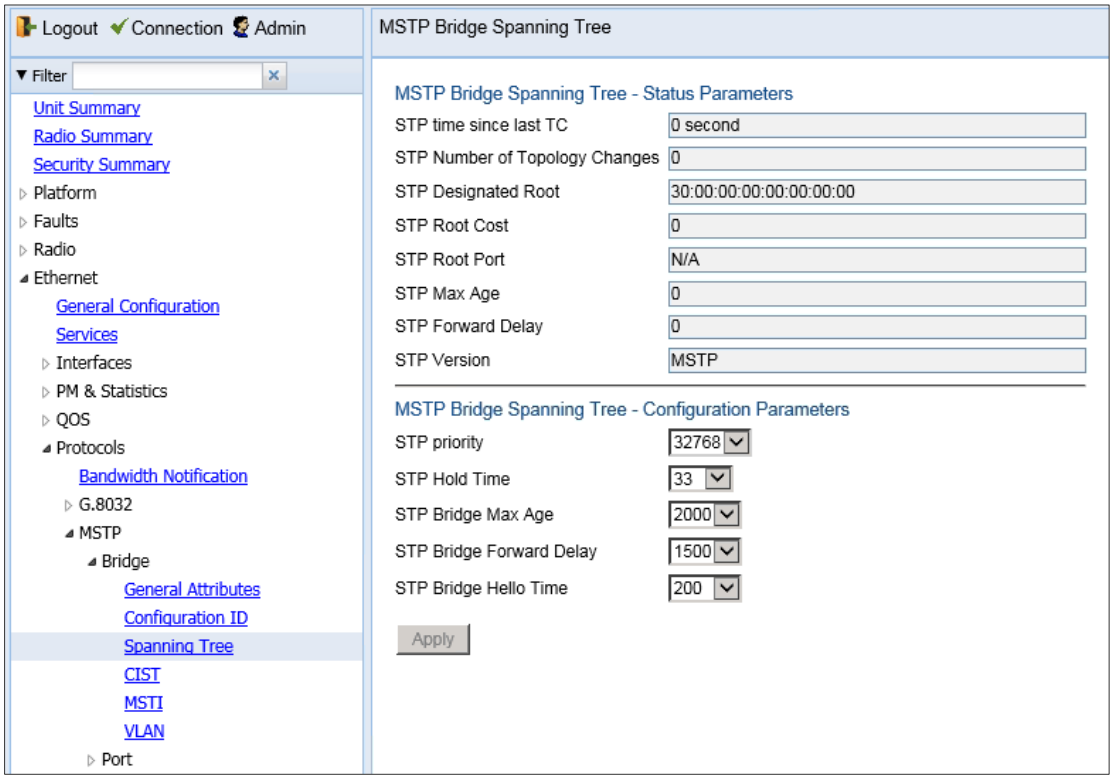


Figure 318: MSTP Bridge Spanning Tree Page

2 Modify the configurable parameters, described in *Table 69*.

3 Click **Apply**.

Table 68 lists and describes the status parameters in the MSTP Bridge Spanning Tree page.

Table 68: MSTP Bridge Spanning Tree Status Parameters

Parameter	Definition
STP Time Since Last TC	The time that has elapsed (in cs) since the last time the bridge entity detected a topology change.
STP Number of Topology Changes	The total number of topology changes that have been detected by this bridge since the management entity was last reset or initialized. **Note:** Discontinuities in the value of this counter can occur upon reinitialization of the management system.
STP Designated Root	The Bridge ID of the spanning tree root, as determined by MSTP in this node. This value is used as the Root ID in all configuration BPDUs originated by this node.
STP Root Cost	The cost of the path to the root as seen from this bridge.
STP Root Port	The port number of the port that offers the lowest cost path from this bridge to the external root bridge

STP Max Age	The maximum age (in cs) of MSTP information learned from the network on any port before the information is discarded. **Note:** This field displays the value actually being used by the bridge, in contrast to the STP Bridge Max Age parameter described below, which is user-configurable and which represents the value that this and all other
STP Forward Delay	The speed at which ports change their spanning state when moving towards the Forwarding state. This value determines how long the port stays in Listening state and Learning state. This value is also used when a topology change has been detected and is underway for purposes of aging all dynamic entries in the filtering database. **Note:** This field displays the value actually being used by the bridge, in contrast to the STP Bridge Forward Delay parameter described below, which is user-configurable and which represents the value that this and all other bridges use if and when this bridge
STP Version	The STP version the bridge is currently running (MSTP).

Table 69: MSTP Bridge Spanning Tree Configuration Parameters

Parameter	Definition
STP Priority	Select a value as the writeable portion of the Bridge ID. This value constitutes the first two octets of the Bridge ID. Possible values are 0-61440, in steps of 4096
STP Hold Time	Select a value (in cs) as the interval length during which no more than two configuration bridge PDUs will be transmitted by this node. Possible values are 10-100.
STP Bridge Max Age	Select a value (in cs) that all bridges will use, when this bridge is the root, as the maximum age of MSTP information learned from the network on any port before the information is discarded.
STP Bridge Forward Delay	Select a value (in cs) that all bridges will use, when this bridge is the root, as the speed at which ports change their spanning state when moving towards the Forwarding state. This value determines how long the port stays in Listening state and Learning state. This value is also used when a topology change has been detected and is underway for purposes of aging all dynamic entries in the filtering database. Options are 400-3000 cs.
STP Bridge Hello Time	Select the value (in cs) that all bridges will use, when this bridge is the root, as the Hello Time. The Hello Time determines how often the switch broadcasts its hello message to other switches, and is the same for all MSTIs. Options are 100-1000 cs.

Viewing and Configuring the MSTP Bridge CIST Parameters

To configure the maximum hops parameter for the Common and Internal Spanning Tree (CIST) and view CIST status information:

1 Select **Ethernet > Protocols > MSTP > Bridge > CIST**. The MSTP Bridge CIST page opens.

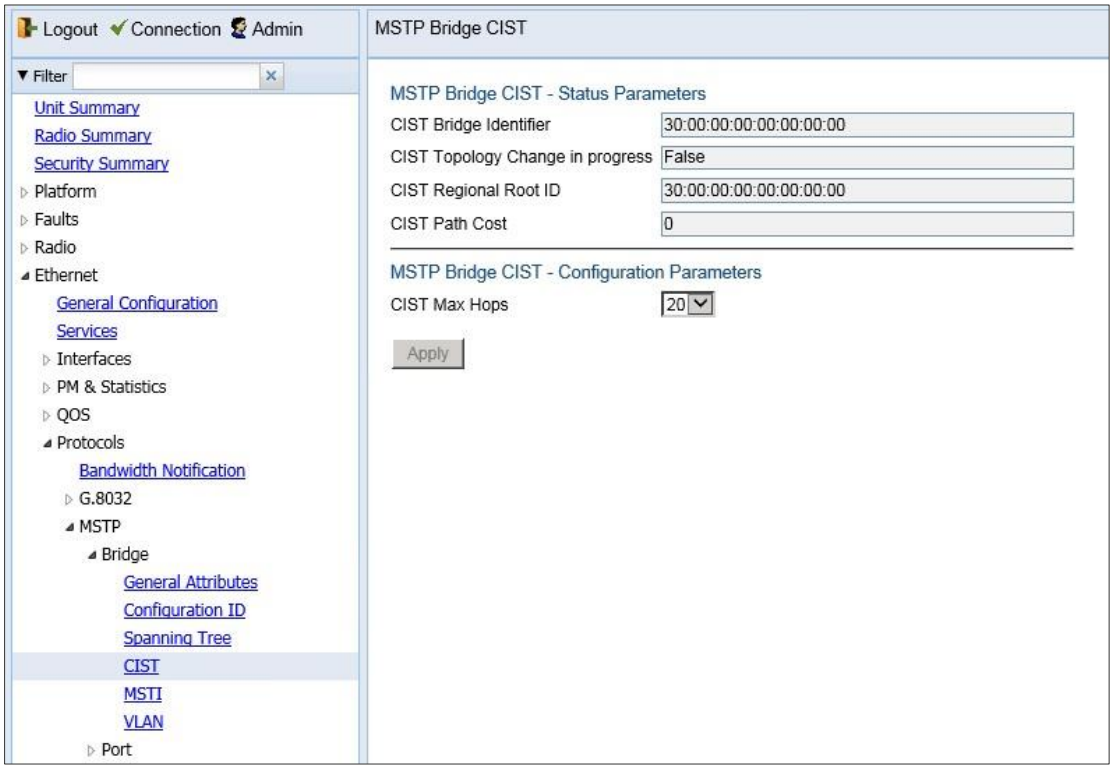


Figure 319: MSTP Bridge CIST Page

2 In the **CIST Max Hops** field, select the value that all bridges will use, when this bridge is the root, as the maximum number of hops allowed for a BPDU within a region before it is discarded. Options are 6-40.

3 Click **Apply**.

Table 70 lists and describes the status parameters in the MSTP Bridge CIST page.

Table 70: MSTP Bridge CIST Status Parameters

Parameter	Definition
CIST Bridge	The Bridge ID of the CIST.
CIST Topology Change in	Indicates whether a topology change is currently in progress for any port that is part of the CIST.
CIST Regional Root	The Bridge ID of the current CIST regional root.
CIST Path Cost	The CIST path cost from the transmitting bridge to the CIST regional root. If the transmitting bridge is the CIST regional root, the value of this parameter may be 0.

Viewing and Configuring the MSTP Bridge MSTI Parameters

To view the parameters of each MSTI in the system, and to configure the MSTI bridge priority for each MSTI:

1 Select **Ethernet > Protocols > MSTP > Bridge > MSTI**. The MSTP Bridge MSTI page opens.

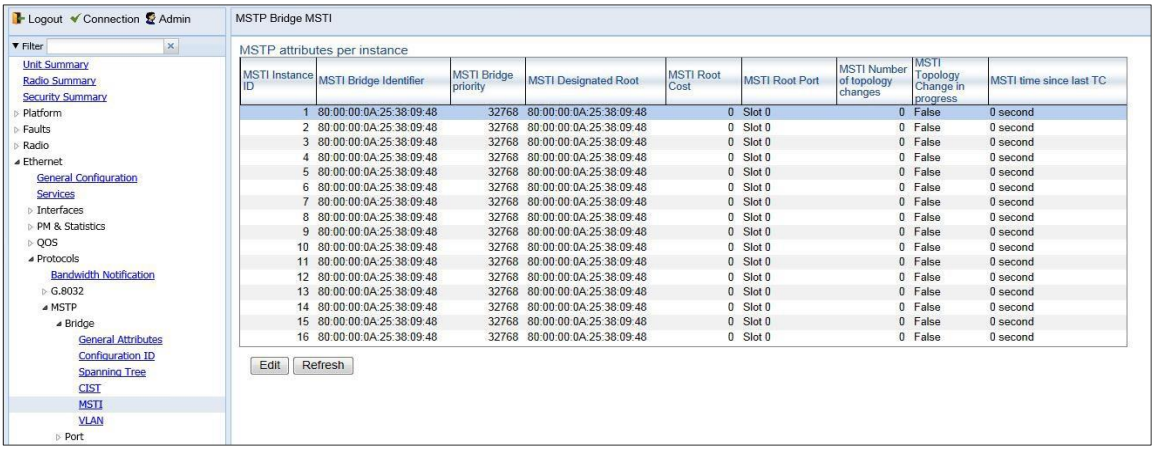


Figure 320: MSTP Bridge MSTI Page

2 To view all the bridge parameters of an MSTI and/or configure its bridge priority, select the MSTI and click **Edit**.

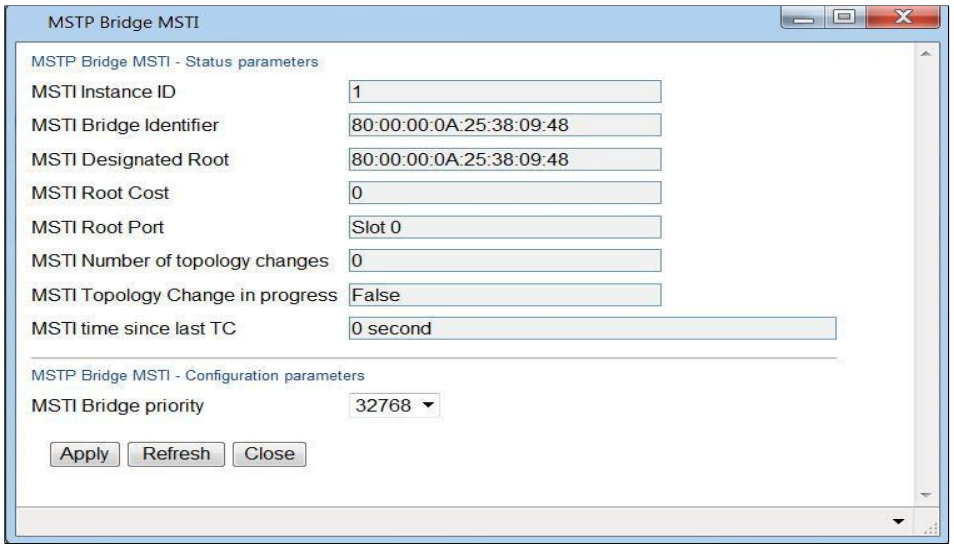


Figure 321: MSTP Bridge MSTI – Edit Page

3 To view all the bridge parameters of an MSTI and/or configure its bridge priority, select the MSTI and click **Edit**.

4 In the **MSTI Bridge Priority** field, enter the MSTI writeable portion of the Bridge ID. Possible values are 0-61440, in steps of 4096.

5 Click **Apply**, then **Close**.

Table 71 lists and describes the status parameters in the MSTP Bridge MSTI page.

Table 71: MSTP Bridge MSTI Status Parameters

Parameter	Definition
MSTI Instance ID	The MSTI ID.
MSTI Bridge	The Bridge ID for the MSTI.
MSTI Designated	The Bridge ID of the root bridge for the MSTI.
MSTI Root Cost	The path cost from the transmitting bridge to the root bridge for the MSTI.
MSTI Root Port	The root port for the MSTI.
MSTI Number of Topology Changes	The number of topology changes that the bridge has detected in the MSTI since the last time the management entity was reset or initialized.
MSTI Topology Change in	Indicates whether a topology change is currently in progress on any port in the MSTI.
MSTI Time Since Last TC	The number of centi-seconds that have elapsed since the last time the bridge identified a topology change for a

Viewing the MSTP VLAN Parameters

Each Ethernet service is mapped to an MSTI. By default, all services (VLAN ID) are assigned to MSTI 0 (CIST). See *Mapping Ethernet Services to MSTP instances (MSTIs)*.

To view the VLAN ID to MSTI mapping table:

1 Select **Ethernet > Protocols > MSTP > Bridge > VLAN**. The MSTP Bridge VLAN page opens.

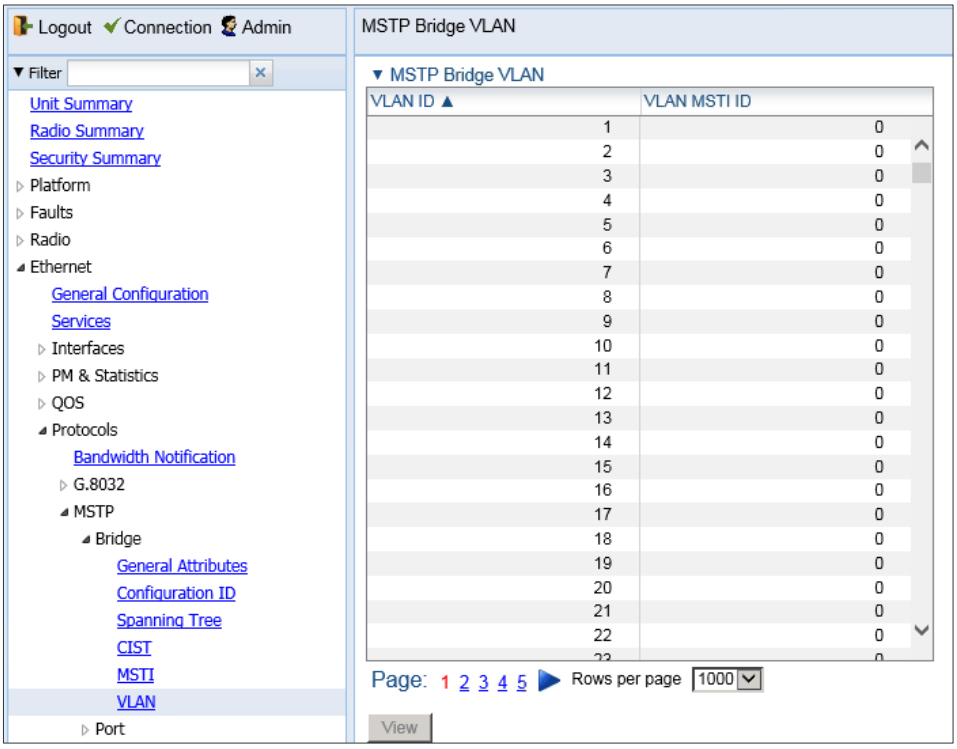


Figure 322: MSTP Bridge VLAN Page

Configuring the MSTP Port Parameters

This section includes:

- Viewing and Configuring the MSTP Port Spanning Tree
- Viewing and Configuring the MSTP Port CIST Parameters
- Viewing and Configuring the MSTP Port MSTI Parameters
- Viewing and Resetting the BPDU Counters

Viewing and Configuring the MSTP Port Spanning Tree

To view the port-level spanning tree parameters and configure the STP port priority:

1 Select **Ethernet > Protocols > MSTP > Port > Spanning Tree**. The MSTP Port Spanning Tree page opens.

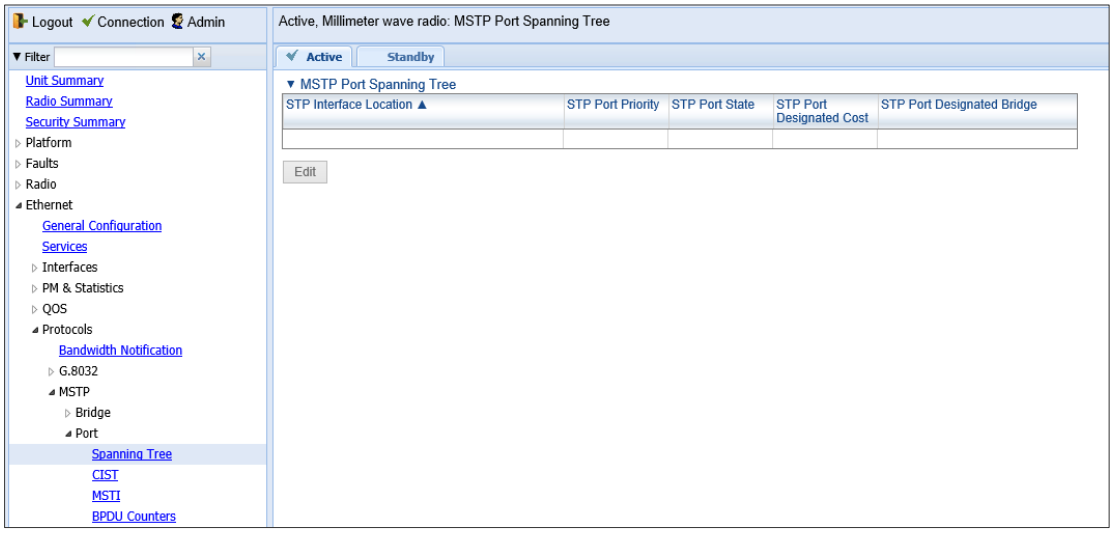


Figure 323: MSTP Port Spanning Tree Page

2 Select an interface and click **Edit**. The MSTP Port Spanning Tree – Edit page opens.

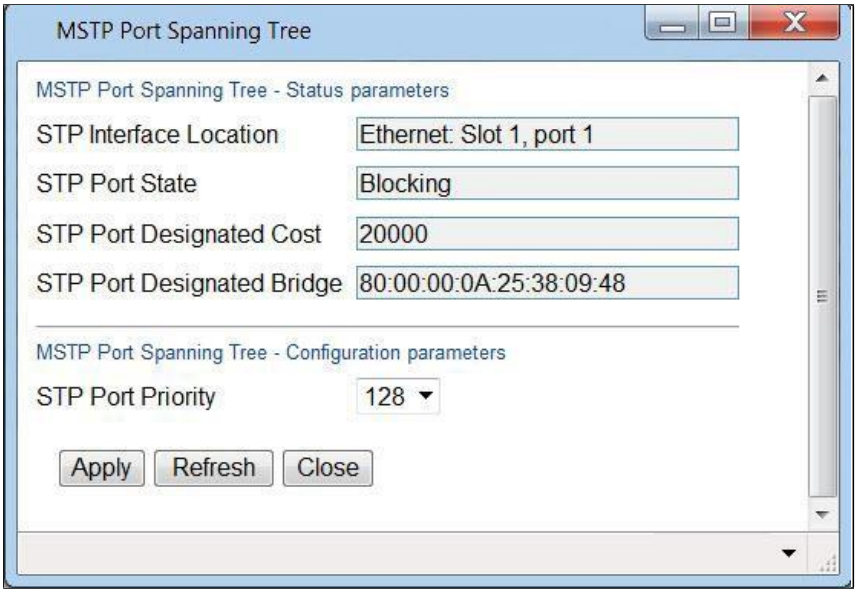


Figure 324: MSTP Port Spanning Tree – Edit Page

3 In the **STP Port Priority** field, select the CIST port priority of the interface. You can select values from 0-240, in multiples of 16.

4 Click Apply, then Close.

Table 72 lists and describes the status parameters in the MSTP Port Spanning Tree page.

Table 72: MSTP Port Spanning Tree Status Parameters

Parameter	Definition
STP Interface	The slot number and port number of the port.
STP Port State	The port's current state, as defined by application of STP. The port's state controls the action the port takes upon receipt of a frame. Possible values are: • **Forwarding** – The port sends and receives traffic normally. • **Blocking** – The port does not send or receive traffic, but does receive BPDUs. • **Learning** – The port receives traffic but does not forward the traffic. The port learns the source MAC addresses of incoming frames. • **Listening** – The port monitors BPDUs, but does not forward traffic and does not learn the source
STP Port Designated	The CIST Path Cost of the segment connected to this port. This value is compared to the root path cost in received
STP Port Designated	The CIST Bridge ID of the bridge that this port considers to be the designated bridge for this port's segment.

Viewing and Configuring the MSTP Port CIST Parameters

To view and configure CIST port parameters:

1 Select **Ethernet > Protocols > MSTP > Port > CIST**. The MSTP Port CIST page opens.

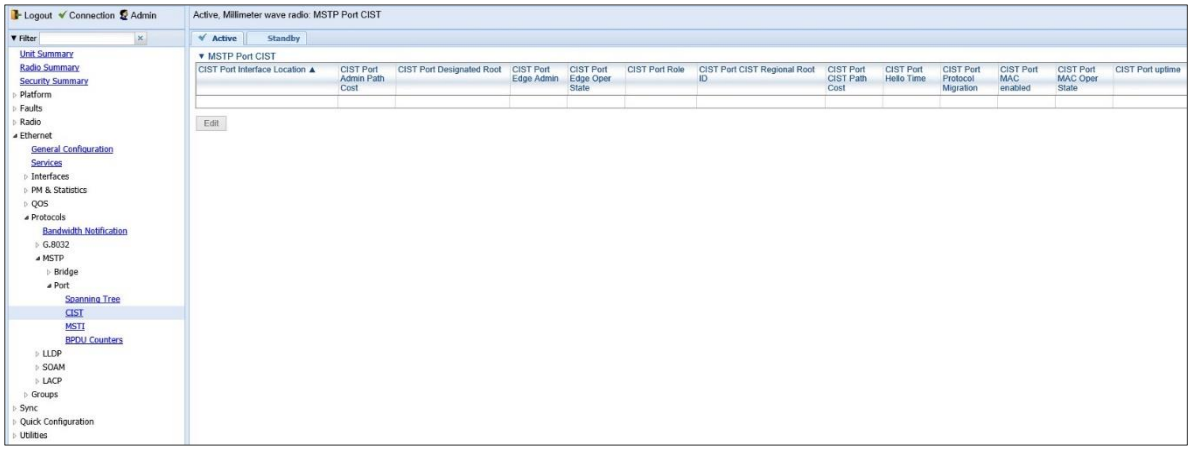


Figure 325: MSTP Port CIST Page

2 Select an interface and click **Edit**. The MSTP Port CIST – Edit page opens.

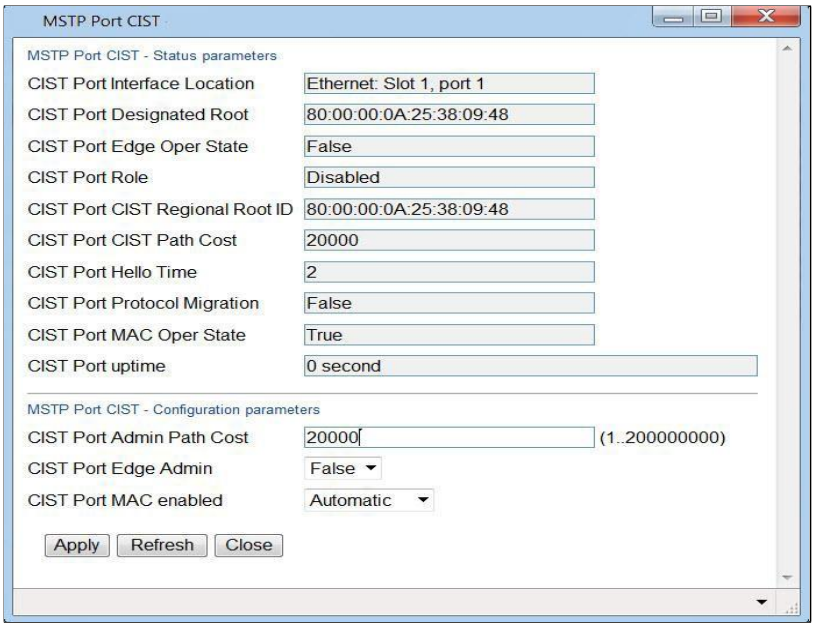


Figure 326: MSTP Port CIST – Edit Page

3 In the **CIST Port Admin Path Cost** field, enter an assigned value for the contribution of this port to the path cost of paths towards the spanning tree root.

4 In the **CIST Port Edge Admin** field, select the port's administrative edge port parameter, for the CIST.

5 In the **CIST MAC enabled** field, select the port's MAC Enabled parameter. A value of **True** indicates that administratively, the MAC is set as if it were connected to a point-to-point LAN. Options are:

- Force True – The MAC is treated as if it is connected to a point-to-point LAN, regardless of any indications to the contrary that are generated by the MAC entity.
- Force False –The MAC is treated as if it is connected to a non-point-to- point LAN, regardless of any indications to the contrary that are generated by the MAC entity.
- Automatic – The MAC Enabled parameter is set to True if the MAC is connected to a point-to-point or full-duplex LAN. The MAC Enabled parameter is set to False if the MAC is connected to a non-point-to-point and half-duplex LAN.

6 Click **Apply**, then **Close**.

Table 73 lists and describes the status parameters in the MSTP Port Spanning Tree page.

Table 73: MSTP Port CIST Status Parameters

Parameter	Definition
CIST Port Interface	The slot number and port number of the port.
CIST Port Designated	The CIST Regional Root ID component of the port's Port Priority vector for the CIST
CIST Port Edge Oper State	Indicates whether or not the port is operating as an Edge port. Possible values are: • **True** – The port is operating as an Edge port, which means it does not process the BPDUs that it receives. • **False** – The port is operating as a non-Edge port, which means it processes the BPDUs that it receives. If CIST Port Edge Admin is set to **True**, the system
CIST Port Role	The port's current role in the CIST. Transient port roles may be: • **Blocking** – The port does not send or receive traffic, but does receive BPDUs. • **Learning** – The port receives traffic but does not forward the traffic. The port learns the source MAC addresses of incoming frames. • **Listening** – The port monitors BPDUs, but does not forward traffic and does not learn the source MAC addresses of incoming frames. Final port roles may be: • **Disabled** – The port is in Operational - Down state and is not included in the MSTP calculation. • **Designated** – The port is in Operational - Up state and has been designated to forward traffic. • **Root** – The port is forwarding traffic towards the root
CIST Port CIST Regional	The Bridge ID of the current CIST Regional Root.
CIST Port CIST Path Cost	The CIST path cost from the transmitting bridge to the CIST regional root. If the transmitting bridge is the CIST regional root, the value of this parameter will be 0.
CIST Port Hello	The port's Hello Time timer parameter value, for the CIST (in cs).

CIST Port Protocol Migration	The current value of the mcheck variable for the port.
CIST Port MAC	The current state of the port's MAC operational parameter. True indicates the MAC is operational.
CIST Port Uptime	The number of seconds that have elapsed since the port was last reset or initialized.

Viewing and Configuring the MSTP Port MSTI Parameters

To view and configure MSTI port parameters:

1 Select **Ethernet > Protocols > MSTP > Port > MSTI**. The MSTP Port MSTI page opens.

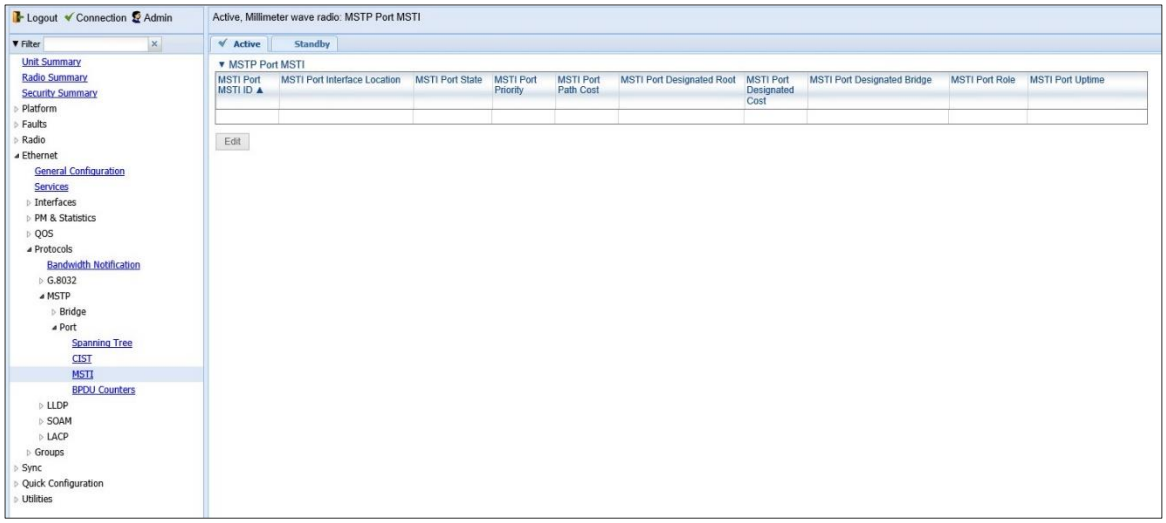


Figure 327: MSTP Port MSTI Page

2 To view the parameters for a specific MSTI-port combination in a separate window and modify several of the parameters, select the row with the MSTI- port combination you want to view and/or modify and click **Edit**. The MSTP Port MSTI – Edit page opens.

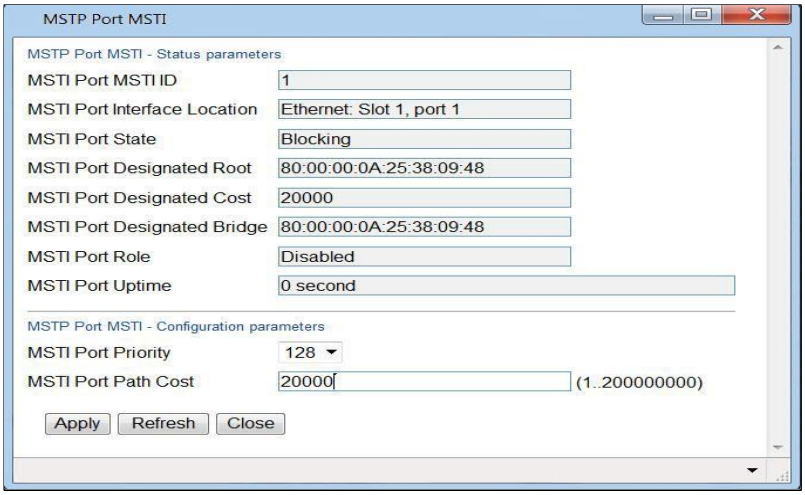


Figure 328: MSTP Port MSTI – Edit Page

3 In the **MSTI Port Priority** field, select the port's Priority parameter value for the MSTI, i.e., the priority field for the Port ID for the MSTI. You can select values from 0-240, in multiples of 16.

4 In the **MSTI Port Path Cost** field, select the port's Path Cost parameter value for the MSTI.

5 Click **Apply**, then **Close**.

Table 74 lists and describes the status parameters in the MSTP MSTI Tree page.

Table 74: MSTP Port MSTI Status Parameters

Parameter	Definition
MSTI Port MSTI ID	The MSTI ID.
MSTI Port Interface	The slot number and port number of the port.
MSTI Port	The port's current state for the MSTI. Possible values are: • **Forwarding** – The port sends and receives traffic normally. • **Blocking** – The port does not send or receive traffic, but does receive BPDUs. • **Learning** – The port receives traffic but does not forward the traffic. The port learns the source MAC addresses of incoming frames. • **Listening** – The port monitors BPDUs, but does not forward traffic and does not learn the source MAC addresses of incoming frames. • **Disabled** – The port is disabled (not by MSTP).
MSTI Port Designated	The Regional Root ID component of the port's Port Priority vector for the MSTI.
MSTI Port Designated	The Internal Root Path Cost component of the port's MSTI port priority vector, for the MSTI.
MSTI Port Designated	The Designated Bridge ID component of the port's MSTI port priority vector.

MSTI Port Role	The port's current role in the MSTI. Transient port roles may be: • **Blocking** – The port does not send or receive traffic, but does receive BPDUs. • **Learning** – The port receives traffic but does not forward the traffic. The port learns the source MAC addresses of incoming frames. • **Listening** – The port monitors BPDUs, but does not forward traffic and does not learn the source MAC addresses of incoming frames. Final port roles may be: • **Disabled** – The port is in Operational - Down state and is not included in the MSTP calculation. • **Designated** – The port is in Operational - Up state and has been designated to forward traffic. • **Root** – The port is forwarding traffic towards the root bridge. • **Alternate** – The port is not forwarding traffic (blocked) but can become a Designated port after MSTP calculation. **Master** – The port is forwarding traffic towards the CIST root bridge.
MSTI Port Uptime	The port's uptime parameter value for the MSTI. This is the number of seconds that have elapsed since the port was last reset or initialized.

Viewing and Resetting the BPDU Counters

To view and reset the BPDU counters:

1 Select **Ethernet > Protocols > MSTP > Port > BPDU Counters**. The MSTP Port BPDU Counters page opens.

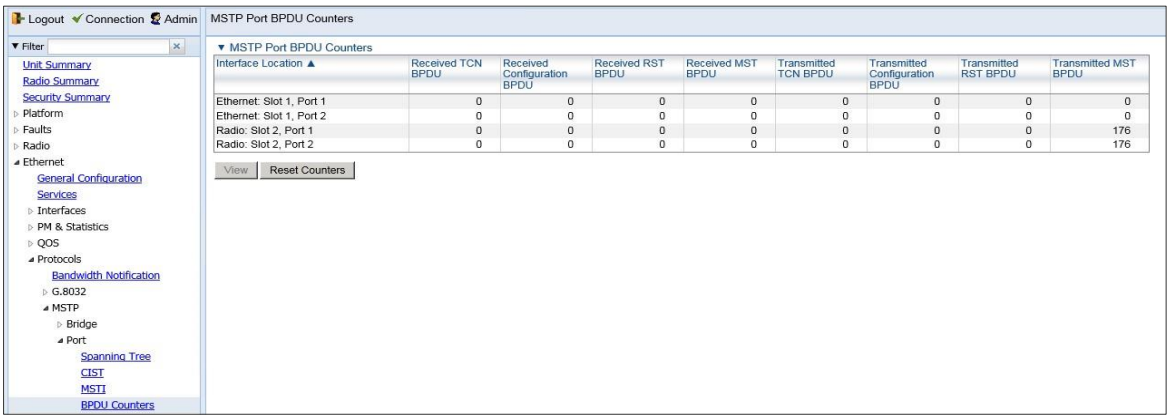


Figure 329: MSTP Port BDPU Counters Page

- To reset the counters, click Reset Counters.
- To display the counters for a specific interface in a separate page, select the interface and click View.

Table 75 describes the available MSTP BPDU counters.

Table 75: MSTP BPDU Counters

Parameter	Definition
Interface Location	The location of the port.
Received TCN	The number of Topology Change Notifications (TCNs) received since the last counter reset.
Received Configuration BPDU	The number of configuration BPDUs received since the last counter reset.
Received RST BPDU	The number of Rapid Spanning Tree (RST) BPDUs received since
Received MST BPDU	The number of Multiple Spanning Tree (MST) BPDUs received since the last counter reset.
Transmitted TCN BPDU	The number of Topology Change Notifications (TCNs) transmitted since the last counter reset.
Transmitted Configuration	The number of configuration BPDUs transmitted since the last counter reset.
Transmitted RST BPDU	The number of Rapid Spanning Tree (RST) BPDUs transmitted since the last counter reset.
Transmitted MST BPDU	The number of Multiple Spanning Tree (MST) BPDUs transmitted since the last counter reset.

12.3 Configuring Ethernet Bandwidth Notification (ETH-BN)

This section includes:

- ETH-BN Overview
- Adding an ETH-BN entity
- Editing an ETH-BN Entity
- Deleting an ETH-BN Entity
- Viewing the Statistics for an ETH-BN Entity

12.3.1 ETH-BN Overview

Ethernet Bandwidth Notification (ETH-BN) is defined by the Y.1731 OAM standard. The purpose of ETH-BN is to inform the L2 or L3 customer switch of the capacity of the radio link in transmit direction. This enables the switch to respond to fluctuations in the radio link by, for example, reconfiguring the shaper on the egress port facing the radio link or rerouting traffic to other egress ports.

Once ETH-BN is enabled, the radio unit reports bandwidth information to upstream third-party switches. The ETH-BN entity creates a logical relationship between a radio interface, called the Monitored Interface, and an Ethernet interface, called the Control Interface. When bandwidth degrades from the nominal value in the Monitored Interface, messages relaying the actual bandwidth values (BNM frames) are periodically sent over the Control Interface. Once the bandwidth returns to its nominal level, BNM messages are no longer sent. Optionally, the device can be configured to send BNM frames even when bandwidth is at its nominal level.



Note

Only single interfaces, not groups, can be used as the Monitored Interface and the Control Interface.

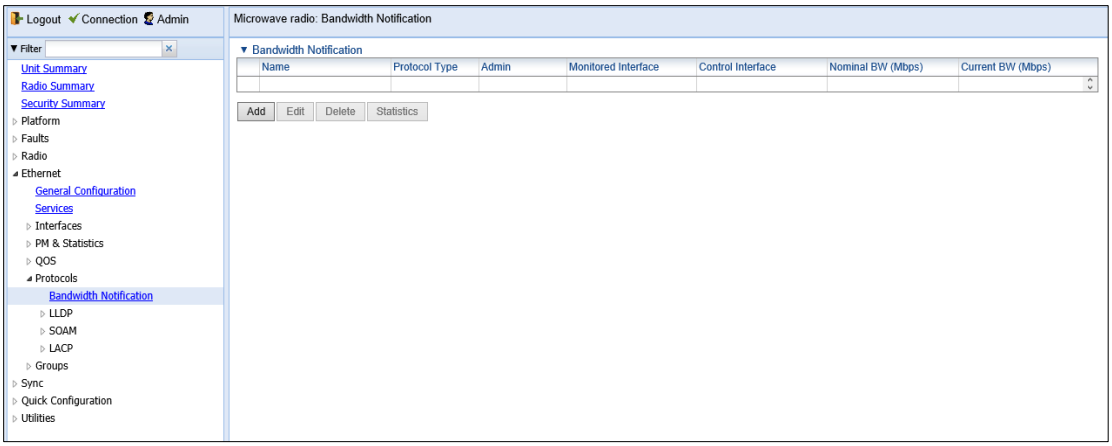
The same radio interface can be configured as a Monitored Interface for multiple EBN instances. However, an Ethernet interface can only be configured as a Control Interface for a single EBN instance.

12.3.2 Adding an ETH-BN entity

To add an ETH-BN entity:

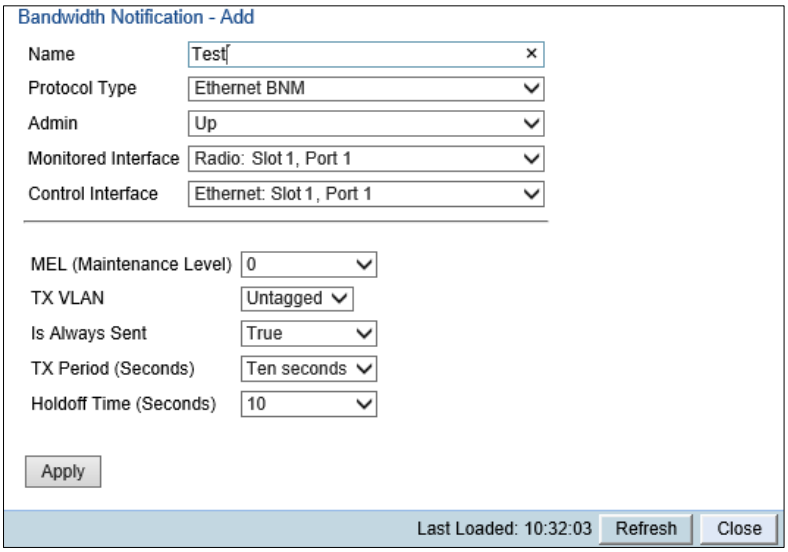
1. Select **Ethernet** > **Protocols** > **Bandwidth Notification**. The Bandwidth Notification page opens.

Figure 425 Bandwidth Notification Page



2. Click **Add**. The Bandwidth Notification - Add page opens.

Figure 426 Bandwidth Notification – Add Page



3. In the Name field, enter a name for the ETH-BN entity.
4. In the Protocol Type field, select Ethernet BNM.
5. In the Admin field, select Up to enable ETH-BN monitoring or Down to disable ETH-BN monitoring.
6. In the Monitored Interface field, select the Monitored Interface. This is the interface which is constantly monitored for its bandwidth value.
7. In the Control Interface field, select the Control Interface. This is the interface to which messages are transmitted when bandwidth in the monitored interface degrades below the nominal value.
8. In the **MEL** field, select the CFM Maintenance Level in the messages (0-7).



Note

If CFM MEPs are being used, the MEL must be set to a value greater than the MEG level of the MEP. Otherwise, the BNM frames will be dropped.

If CFM MEPs are not being used, the MEL for ETH-BN must be set to a value greater than 0. Otherwise, the BNM frames will be dropped.

9. In the **Tx VLAN** field, specify the VLAN on which messages are transmitted. Options are:
   - Untagged.
   - 1 – 4090.



Note

The CoS of the VLAN is automatically set to 7.

10. In the **Is Always Sent** field, specify whether periodic BNM frames should be sent even when there is no bandwidth degradation in the monitored interface:
    - **True** – BNM frames are always sent, even when the bandwidth is at its nominal value.
    - **False** – BNM frames are only sent when the current bandwidth is lower than the nominal bandwidth (default value).
11. In the **Tx Period** field, specify how often messages are transmitted when **Is Always Sent** is set to **True** or, if not, when bandwidth is below the nominal value. Options are:
    - One second
    - Ten seconds (default)
    - Sixty seconds

Note: If the **Holdoff Time** is set to 0, then if the bandwidth drops below the nominal value, a BNM frame is transmitted immediately.

12. In the **Holdoff Time** field, specify the amount of time (in seconds) the system waits when bandwidth degradation occurs, before transmitting a message. If the bandwidth is below the nominal value when the holdoff period ends, the system starts transmitting messages. Options are 0-10. The default value is 0.



Note

If the bandwidth fluctuates before the Holdoff Time expires, and is lower than the nominal bandwidth when the Holdoff Time expires, the first BNM frame sent when the timer expires gives the lowest bandwidth that was recorded while the timer was running. Subsequent BNM frames are sent with the actual current bandwidth.

13. Click **Apply**, then **Close**.

Table 70 ETH-BN Status Parameters

Parameter	Definition

Nominal BW	The maximum radio TX bitrate achievable with the current radio configuration.
Current BW	The current radio TX bitrate.

12.3.3 Editing an ETH-BN Entity

To edit an ETH-BN entity:

1. Select **Ethernet** > **Protocols** > **Bandwidth Notification**. The Bandwidth Notification page opens.
2. Select the ETH-BN entity in the Bandwidth Notification page.
3. Click Edit. The Bandwidth Notification - Edit page opens.
   The Edit page is similar to the Bandwidth Notification – Add page . However, the **Control interface** and **Monitored interface** parameters are read-only, and additional read-only parameters display the **Nominal BW**, and the **Current BW**.
4. Edit the ETH-BN attributes, as described in Adding an ETH-BN entity.
5. Click Apply, then **Close**.

12.3.4 Deleting an ETH-BN Entity

To delete an ETH-BN entity:

1. Select **Ethernet** > **Protocols** > **Bandwidth Notification**. The Bandwidth Notification page opens.
2. Select the ETH-BN entity in the Bandwidth Notification page.
3. Click **Delete**. The ETH-BN entity is removed.

12.3.5 Viewing the Statistics for an ETH-BN Entity

To view the statistics for an ETH-BN entity:

1. Select **Ethernet** > **Protocols** > **Bandwidth Notification**. The Bandwidth Notification page opens.
2. Select the ETH-BN entity in the Bandwidth Notification page.
3. Click Statistics. The Bandwidth Notification - Statistics page opens.

Figure 427 Bandwidth Notification - Statistics Page (ETH-BN)

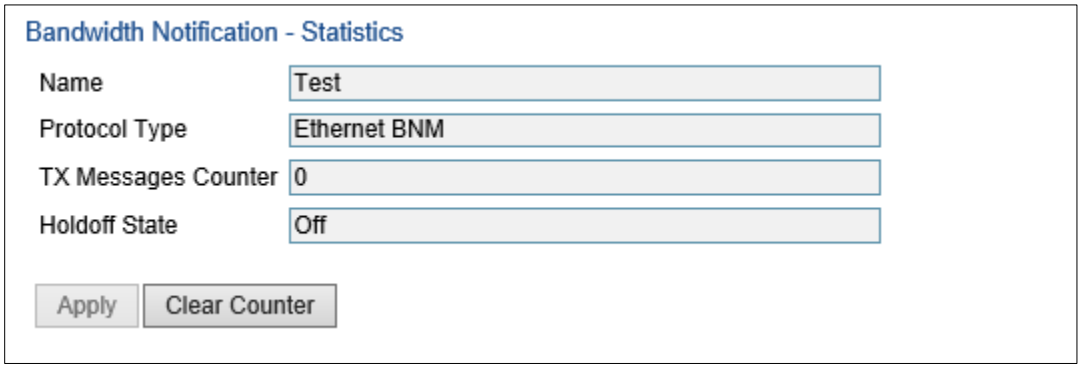


Table 71 ETH-BN Entity Statistics Parameters

Parameter	Definition
Name	The name of the ETH-BN entity.
Protocol Type	Ethernet BNM.
Tx Messages Counter	The number of bandwidth messages transmitted since the counter was last reset.
Holdoff State	The Holdoff state of the monitored link. Options are: • **Off** – Holdoff time measurement has not been started. • **Counting** – Holdoff time measurement has started but the timeout has not elapsed yet. • **On** – Holdoff measurement time has ended and the current bandwidth is still below the nominal value.

12.4 Configuring LLDP

This section includes:

- LLDP Overview
- Displaying Peer Status
- Configuring the General LLDP Parameters
- Configuring the LLDP Port Parameters
- Displaying the Unit's Management Parameters
- Displaying Peer Unit's Management Parameters
- Displaying the Local Unit's Parameters
- Displaying LLDP Statistics

12.4.1 LLDP Overview

Link Layer Discovery Protocol (LLDP) is a vendor-neutral layer 2 protocol that can be used by a network element attached to a specific LAN segment to advertise its identity and capabilities and to receive identity and capacity information from physically adjacent layer 2 peers. LLDP is a part of the IEEE 802.1AB – 2005 standard that enables automatic network connectivity discovery by means of a port identity information exchange between each port and its peer. Each port periodically sends and also expects to receive frames called Link Layer Discovery Protocol Data Units (LLDPDU). LLDPDUs contain information in TLV format about port identity, such as MAC address and IP address.

LLDP is used to send notifications to the NMS, based on data of the local unit and data gathered from peer systems. These notifications enable the NMS to build an accurate network topology.

Displaying Peer Status

To display a summary of the important LLDP management information regarding the unit's nearest neighbor (peer):

1 Select **Ethernet > Protocols > LLDP > Remote Management**. The LLDP Remote Management page opens.

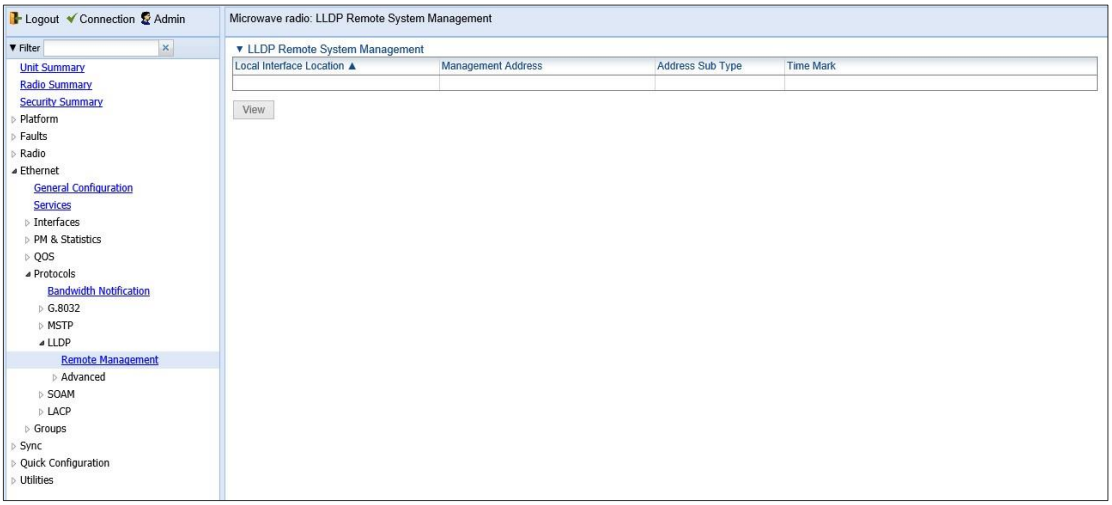


Figure 428 LLDP Remote System Management Page

Below tatble describes the LLDP remote system management parameters. These parameters are read-only.

Table 72 LLDP Remote System Management Parameters

Parameter	Definition
Local Interface	The location of the local interface.
Management Address	The octet string used to identify the management address component associated
Address Sub Type	The type of management address identifier encoding used in the associated LLDP Agent Remote
Time Mark	The time the entry was created.

Configuring the General LLDP Parameters

This section explains how to define the general LLDP parameters for the unit. For instructions on defining port-specific parameters, see Configuring the LLDP Port Parameters.



Note

The management IP address advertised by the local element depends on the IP protocol (IPv4 or IPv6) configured for the unit. See Defining the IP Protocol Version for Initiating Communications.

To display and configure the general LLDP parameters for the unit:

1 Select **Ethernet > Protocols > LLDP > Advanced > Configuration > Parameters**. The LLDP Configuration Parameters page opens.

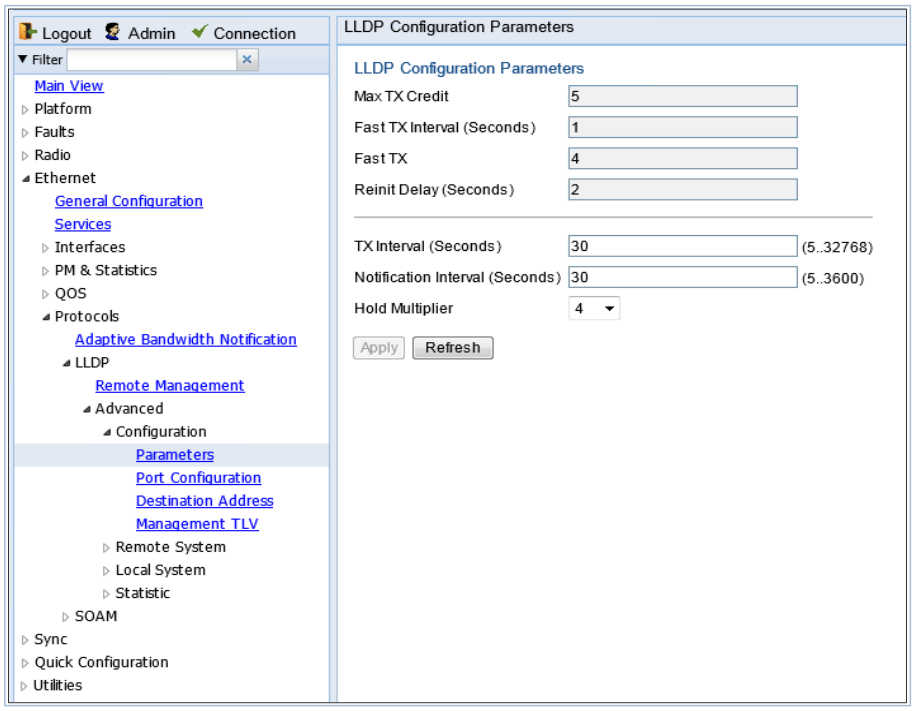


Figure 429 LLDP Configuration Parameters Page

2 Modify the configurable parameters, described in *Table 64*.

3 Click **Apply**.

Below table lists and describes the status parameters in the LLDP Configuration Parameters page.

Table 73 LLDP Read-Only Configuration Parameters

Parameter	Definition
Max TX Credit	Displays the maximum number of consecutive LLDPDUs that can be transmitted at any one time. In this release, the Max TX Credit is set at
Fast TX Interval (Seconds	Displays, in seconds, the interval at which LLDP frames are transmitted during fast transmission periods, such as when the unit detects a new peer. In this release, the Fast TX Interval is set at 1.
Fast TX	The initial value used to initialize the variable which determines the number of transmissions that are made during fast transmission periods. In this release, the Fast TX No. is set at 4.
Reinit Delay (Seconds)	Defines the minimum time, in seconds, the system waits after the LLDP Admin status becomes Disabled until it will process a request to reinitialize LLDP. For instructions on disabling or enabling LLDP on a port, see *Configuring the LLDP Port Parameters*. In this release, the Reinit Delay is set at 2.
TX Interv	Defines the interval, in seconds, at which LLDP frames are transmitted. You can select a value from 5 to 32768. The default value is 30.

Notification Interval	Defines the interval, in seconds, between transmission of LLDP notifications during normal transmission periods. You can select a value from 5 to 3600. The default value is 10.
Hold Multiplier	Defines the time-to-live (TTL) multiplier. The TTL determines the length of time LLDP frames are retained by the receiving device. The TTL is determined by multiplying the TX Interval by the Hold Multiplier. You can select a value from 2 to 10. The default value is 4.

Configuring the LLDP Port Parameters

To enable LLDP per port and determine how LLDP operates and which TLVs are sent for each port:

1 Select **Ethernet > Protocols > LLDP > Advanced > Configuration > Port Configuration**. The LLDP Port Configuration page opens.

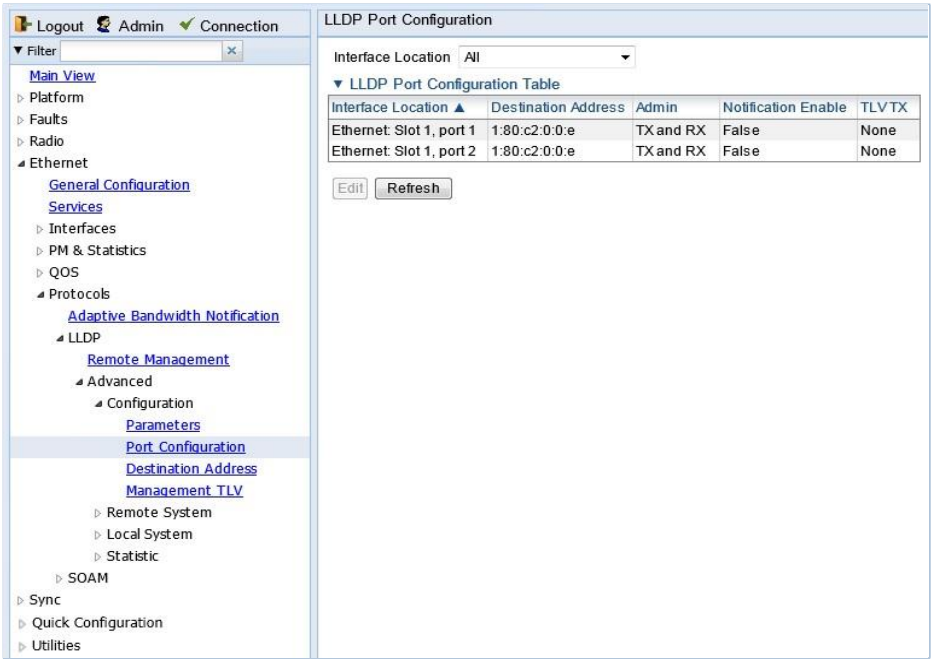


Figure 430 LLDP Port Configuration Page

2 Select an interface and click **Edit**. The LLDP Port Configuration - Edit page opens.

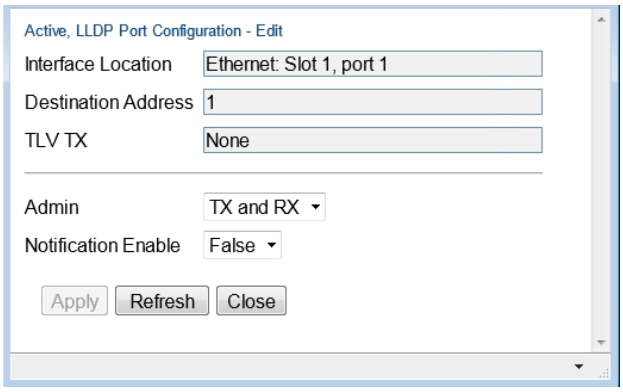


Figure 431 LLDP Port Configuration - Edit Page

3 In the **Admin** field, select from the following options to define how the LLDP protocol operates for this port:

- **TX Only** – LLDP agent transmits LLDP frames on this port but does not update information about its peer.
- **RX Only** – LLDP agent receives but does not transmit LLDP frames on this port.
- **TX and RX** – LLDP agent transmits and receives LLDP frames on this port (default value).
- **Disabled** – LLDP agent does not transmit or receive LLDP frames on this port.

4 In the **Notification Enable** field, select from the following options to define, on a per agent basis, whether or not notifications from the agent to the NMS are enabled:

- **True** – The agent sends a Topology Change trap to the NMS whenever the system information received from the peer changes.
- **False** – Notifications to the NMS are disabled (default value).

5 Click **Apply**, then **Close**.

Table 74 LLDP Port Configuration Status Parameters

Parameter	Definition
Interface	Identifies the port.
Destination	The destination address of the LLDP agent associated with this port.
TLV TX	Indicates which of the unit's capabilities is transmitted by the LLDP agent for the port: • **PortDesc** – The LLDP agent transmits Port Description TLVs. • **SysName** – The LLDP agent transmits System Name TLVs. • **SysDesc** – The LLDP agent transmits System Description TLVs. • **SysCap** – The LLDP agent transmits System Capabilities TLVs.

Displaying the Unit's Management Parameters

To display the unit's destination LLDP MAC address:

1 Select **Ethernet > Protocols > LLDP > Advanced > Configuration > Destination Address**. The LLDP Destination Address Table page opens.

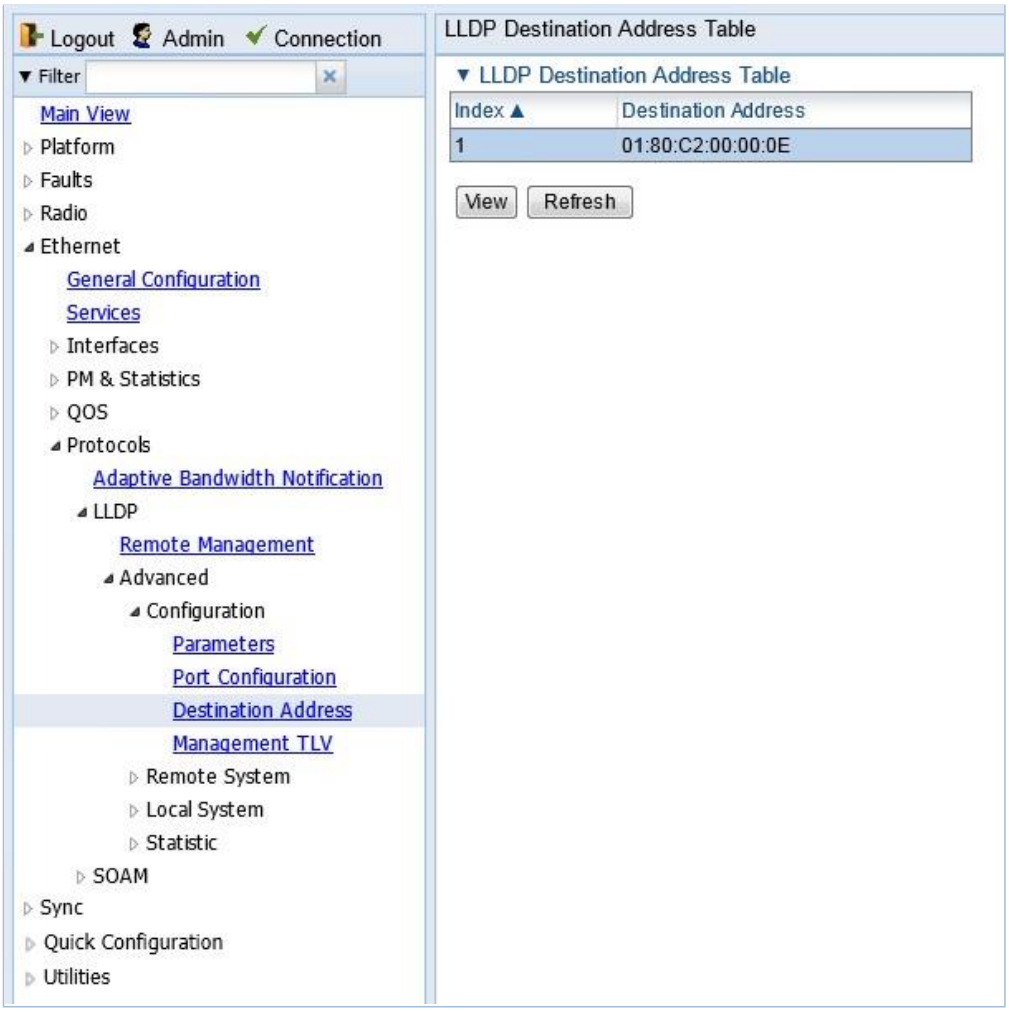


Figure 432 LLDP Destination Address Table Page

To displays the MAC address associated with the unit for purposes of LLDP transmissions:

1 Select **Ethernet > Protocols > LLDP > Advanced > Configuration > Management TLV**. The LLDP Management TLV Configuration page opens.

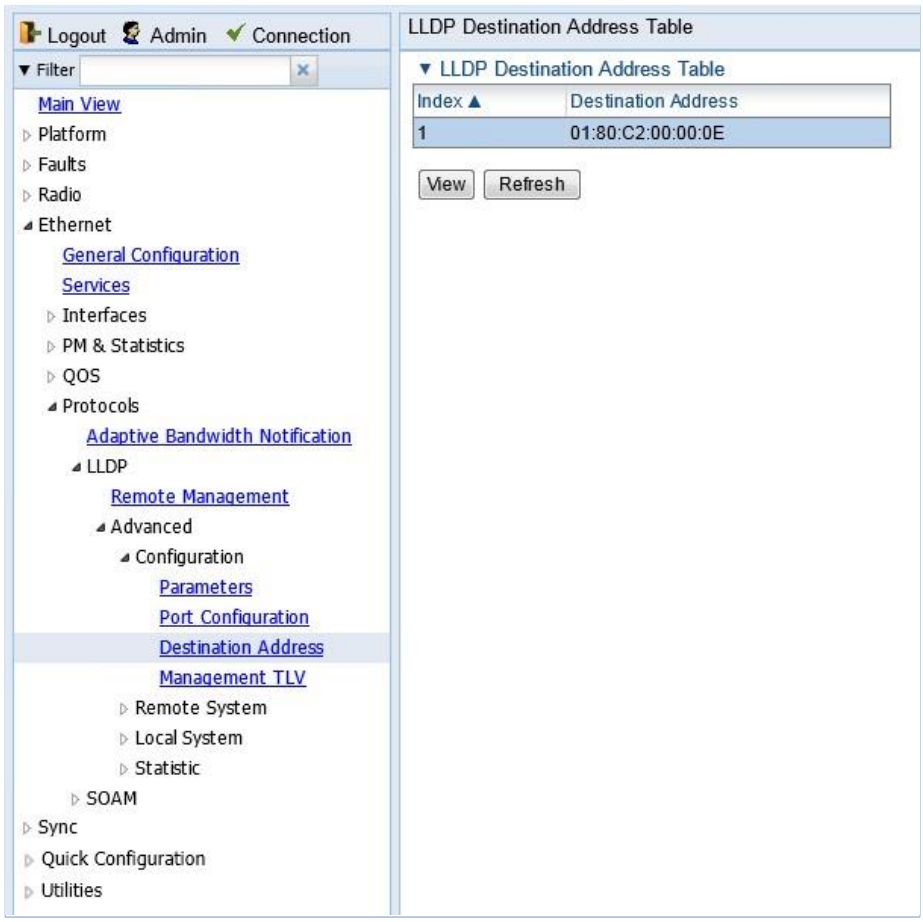


Figure 433 LLDP Management TLV Configuration Page

Below table lists and describes the status parameters in the LLDP Management TLV Configuration page.

Table 75 LLDP Management TLV Parameters

Parameter	Definition
Interface Location	Identifies the port.
Destination Address	Defines the MAC address associated with the port for purposes of LLDP transmissions.
Management	The unit's IP address.
Address Subtype	Defines the type of the management address identifier encoding used for the Management Address.
Tx Enable	Indicates whether the unit's Management Address is transmitted with LLDPDUs. In this release, the Management Address is always

Displaying Peer Unit's Management Parameters

To display LLDP management information about the unit's nearest neighbor (peer):

1 Select **Ethernet > Protocols > LLDP > Advanced > Remote System > Management**. The LLDP Remote System Management page opens.

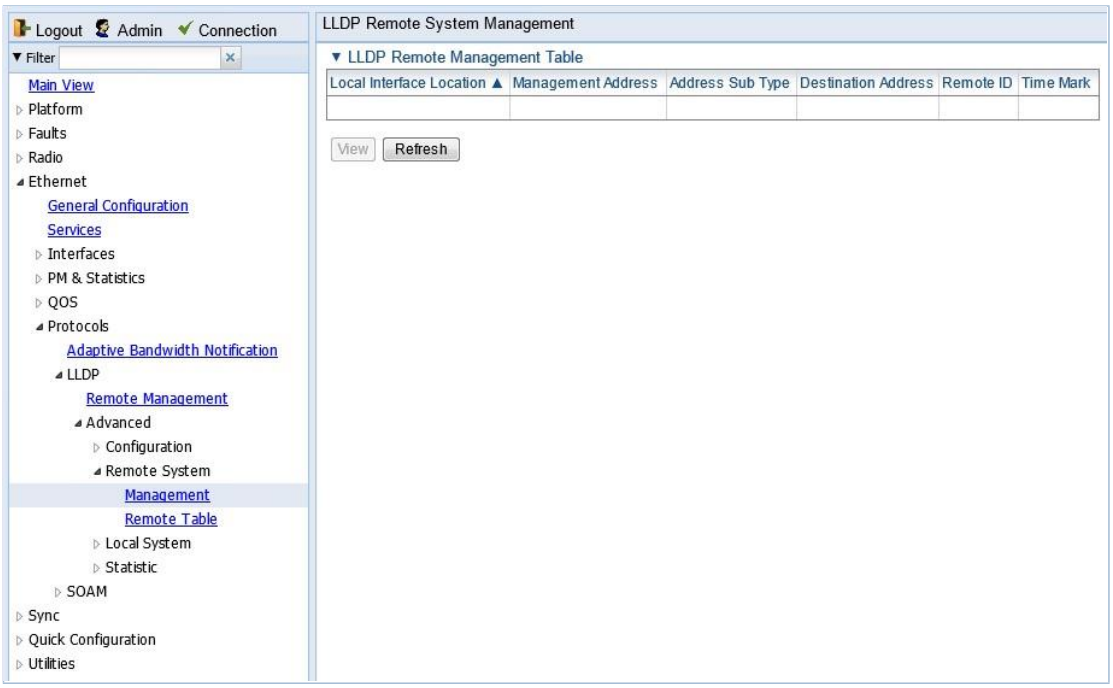


Figure 434 LLDP Remote System Management Page

Below table describes the LLDP remote system management parameters. These parameters are read-only.

Table 76 LLDP Remote System Management Parameters

Parameter	Definition
Local Interface	The location of the local interface.
Management Address	The octet string used to identify the management address component associated with the remote system.
Address Sub Type	The type of management address identifier encoding used in the associated LLDP Agent Remote Management Address.
Destination	The peer LLDP agent's destination MAC Address.
Remote ID	An arbitrary local integer value used by this agent to identify a particular connection instance, unique only for the indicated remote system.
Time Mark	The time the entry was created.

To display unit parameter information received via LLDP from the unit's nearest neighbor (peer):

1 Select **Ethernet > Protocols > LLDP > Advanced > Remote System > Remote Table**. The LLDP Remote System Table page opens.

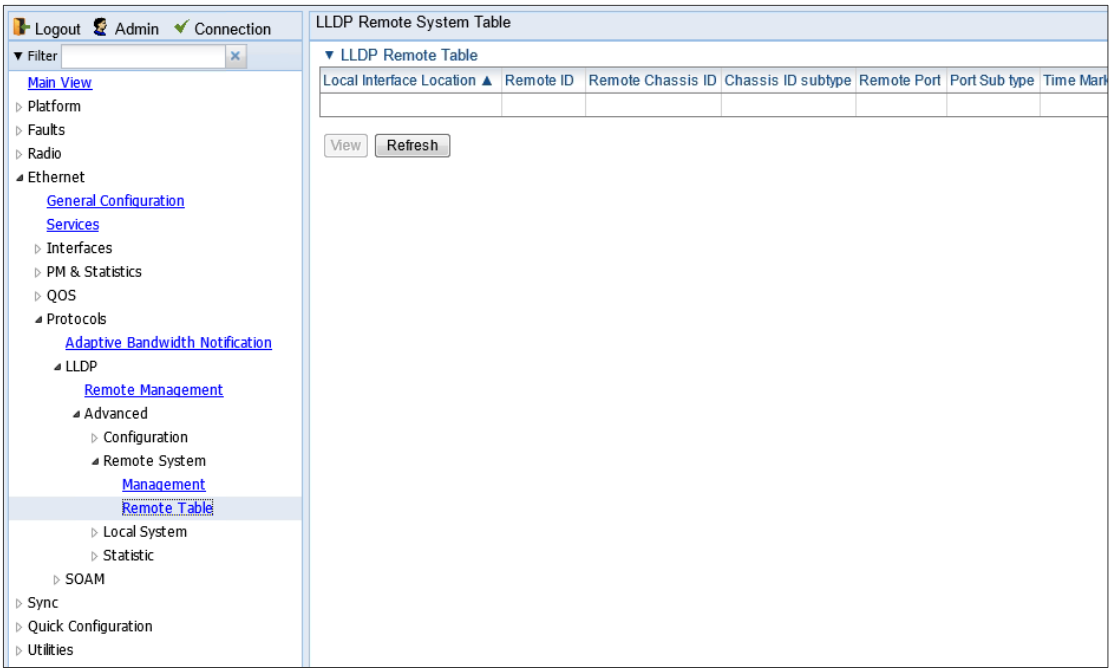


Figure 435 LLDP Local System Parameters Page

Below table describes the parameters in the LLDP Local System Parameters page. These parameters are read-only.

Table 77 LLDP Local System Parameters

Parameter	Definition
System Name	The system name included in TLVs transmitted by the LLDP agent, as defined in the **Name** field of the Unit Parameters page. See *Configuring Unit Parameters*.
System Description	The system description included in TLVs transmitted by the LLDP agent, as defined in the **Description** field of the Unit Parameters page. See *Configuring Unit Parameters*.
Chassis ID	The MAC Address of the local unit.
Chassis ID SubType	The type of encoding used to identify the local unit. In this release, this parameter is always set to MAC Address.

Capabilities Supporte	A bitmap value used to identify which system capabilities are supported on the local system, as included in TLVs transmitted by the LLDP agent. The bitmap is defined by the following parameters: 0 – other 1 – repeater 2 – bridge 3 – wlanAccessPoint 4 – router 5 – telephone 6 – docsisCableDevice 7 – stationOnly 8 – cVLANComponent 9 – sVLANComponent
Capabilities Enabled	A bitmap value used to identify which system capabilities are enabled on the local system, as included in TLVs transmitted by the LLDP agent. The bitmap is defined by the following parameters: 0 – other 1 – repeater 2 – bridge 3 – wlanAccessPoint 4 – router 5 – telephone 6 – docsisCableDevice 7 – stationOnly 8 – cVLANComponent 9 – sVLANComponent

To display the unit's port parameters, as transmitted by the LLDP agents:

1 Select **Ethernet > Protocols > LLDP > Advanced > Local System > Port**. The LLDP Local System Port page opens.

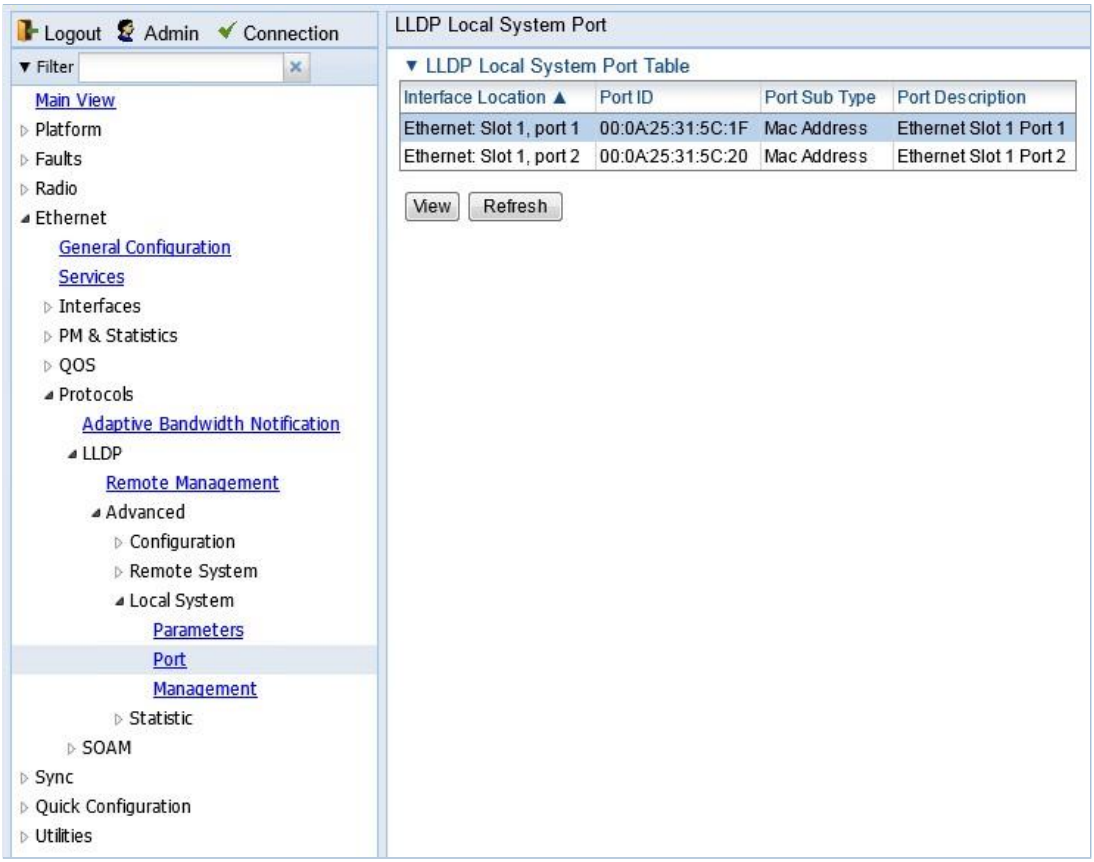


Figure 436 LLDP Local System Port Page

Below table describes the parameters in the LLDP Local System Port page. These parameters are read-only.

Table 78 LLDP Local System Port Parameters

Parameter	Definition
Interface	Identifies the port.
Port ID	The port's MAC address.
Port Sub Type	The type of encoding used to identify the port in LLDP transmissions. In this release, this parameter is always set to MAC Address.
Port	A description of the port.

To display the unit's management parameters, as transmitted by the LLDP agents:

1 Select **Ethernet > Protocols > LLDP > Advanced > Local System > Management**. The LLDP Local System Management page opens.

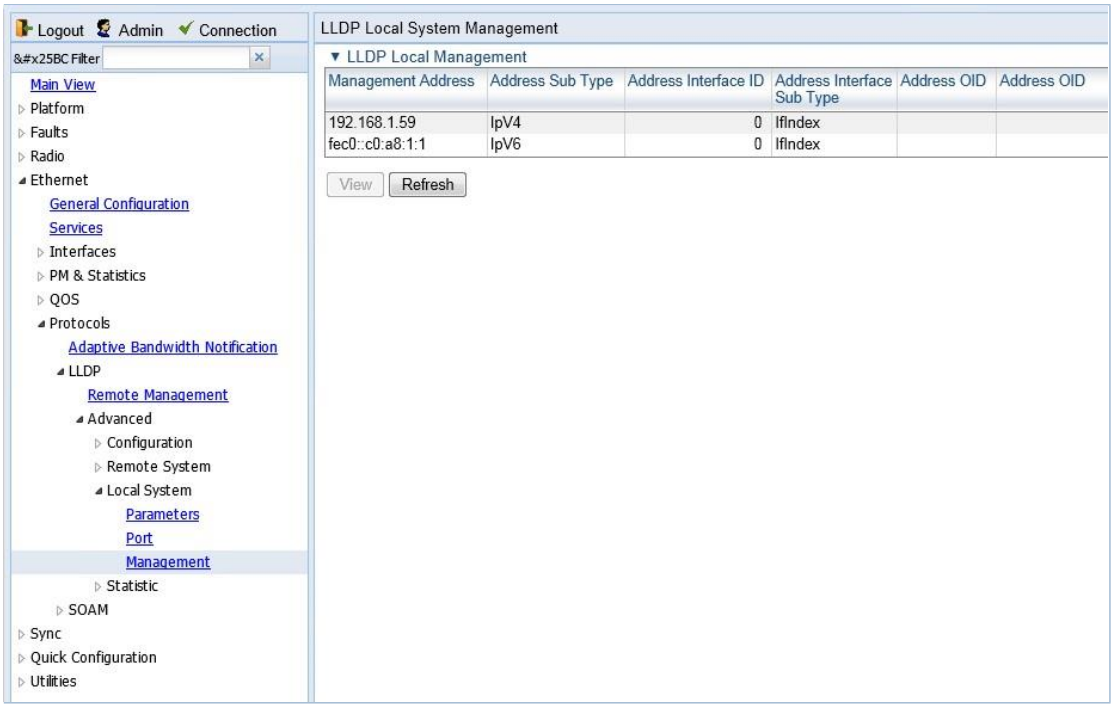


Figure 437 LLDP Local System Management Page

2 To display all the parameters, select a row and click View.

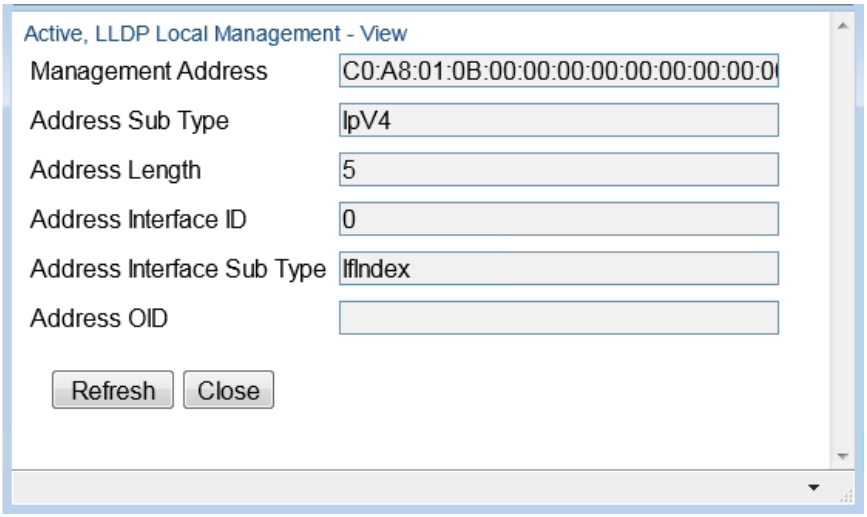


Figure 438 LLDP Local System Management – View Page

Below table describes the parameters in the LLDP Local System Management page. These parameters are read-only.

Table 79 LLDP Local System Management Parameters

Parameter	Definition
Management Address	The local unit's IP address.
Address Sub Type	The format of the local unit's IP Address.
Address Length	Reserved for future use.
Address Interface ID	Reserved for future use.
Address Interface Sub Type	Reserved for future use.
Address OID	Reserved for future use.

Displaying LLDP Statistics

To display statistics about changes reported via LLDP by the remote unit:

1 Select **Ethernet > Protocols > LLDP > Advanced > Statistic > General**. The LLDP Statistic page opens.

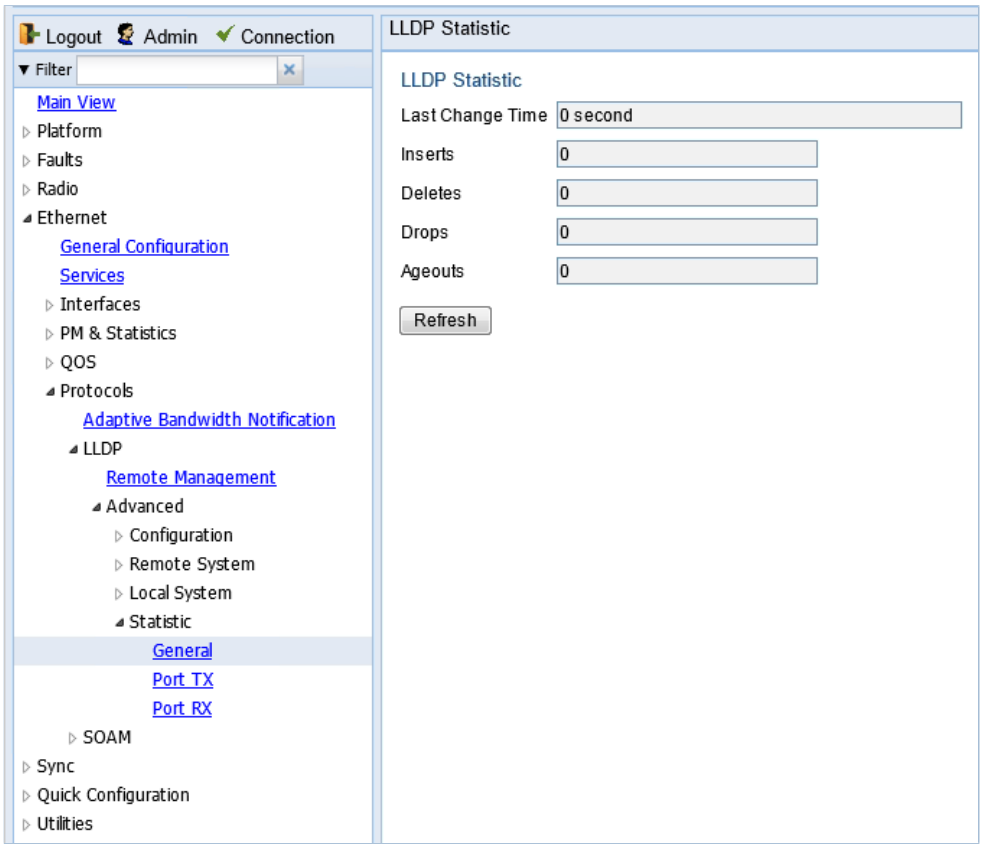


Figure 439 LLDP Statistic Page

Table 80 LLDP Statistics

Parameter	Definition
Last Change Time	The time of the most recent change in the remote unit, as reported via LLDP.
Inserts	The number of times the information from the remote system has changed.
Deletes	The number of times the information from the remote system has been deleted.
Drops	Reserved for future use.
Ageouts	The number of times the information from the remote system has been deleted from the local unit's database because the information's TTL has expired. The **RX Ageouts** counter in the Port RX page is similar to this counter, but is for specific ports rather than the entire unit.

To display statistics about LLDP transmissions and transmission errors:

1 Select **Ethernet > Protocols > LLDP > Advanced > Statistic > Port TX**. The LLDP Port TX Statistic page opens.

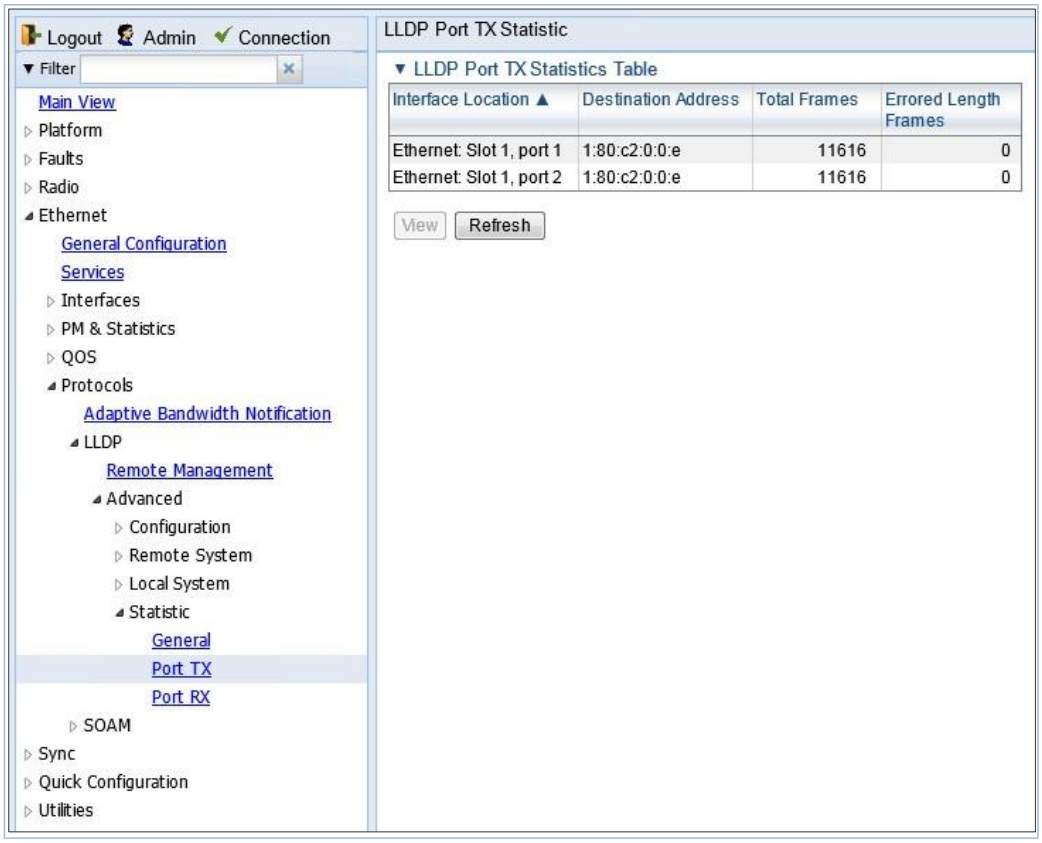


Figure 440 LLDP Port TX Statistics Page

Table 81 LLDP Port TX Statistics

Parameter	Definition
Interface	The index value used to identify the port in LLDP transmissions.
Destination	The LLDP MAC address associated with this entry.
Total Frames	The number of LLDP frames transmitted by the LLDP agent on this port to the destination MAC address.
Errored Length Frames	The number of LLDPDU Length Errors recorded for this port and destination MAC address. If the set of TLVs that is selected in the LLDP local system MIB by network management would result in an LLDPDU that violates LLDPDU length restrictions, then the No. of Length Error statistic is incremented by 1, and an LLDPDU is sent containing the mandatory TLVs plus as many of the optional TLVs in the set as will fit in the remaining LLDPDU length.

To display statistics about LLDP frames received by the unit:

1 Select **Ethernet > Protocols > LLDP > Advanced > Statistic > Port RX**. The LLDP Port TX Statistic

page opens.

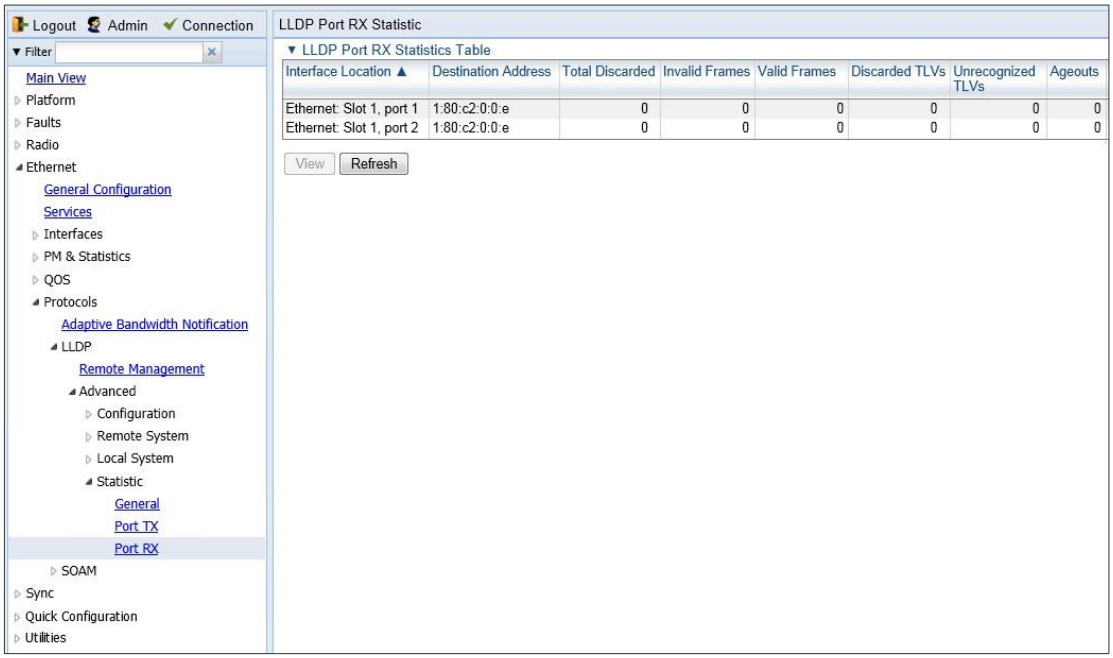


Figure 441 LLDP Port RX Statistics Page

Table 82 LLDP Port RX Statistics

Parameter	Definition
Interface	The index value used to identify the port in LLDP transmissions.
Destination	The LLDP MAC address associated with this entry.
Total Discarded	The number of LLDP frames received by the LLDP agent on this port, and then discarded for any reason. This counter can provide an indication that LLDP header formatting problems may exist with the local LLDP agent in the sending system or that LLDPDU validation problems may exist with the local LLDP agent in the receiving system.
Invalid Frames	The number of invalid LLDP frames received by the LLDP agent on this port while the agent is enabled.
Valid Frames	The number of valid LLDP frames received by the LLDP agent on this port.
Discarded TLVs	The number of LLDP TLVs discarded for any reason by the LLDP agent on this
Unrecognized	The number of LLDP TLVs received on the given port that are not recognized

Ageouts	The number of age-outs that occurred on the port. An age-out is the number of times the complete set of information advertised by the remote system has been deleted from the unit's database because the information timeliness interval has expired. This counter is similar to the LLDP No. of Ageouts counter in the LLDP Statistic page, except that it is per port rather than for the entire unit. This counter is set to zero during agent initialization. This counter is incremented only once when the complete set of information is invalidated (aged out) from all related tables on a particular port. Partial ageing is not

13. Synchronization

This section includes:

- Configuring the Sync Source
- Configuring the Outgoing Clock and SSM Messages
- Configuring 1588 Transparent Clock
- Configuring 1588 Boundary Clock
- Disabling 1588 PTP

13.1 Configuring the Sync Source



Note

To configure a sync source on which the sync source Quality parameter must be set according to ANSI specifications and you must change the ETSI/ANSI mode to ANSI before configuring the sync source. See Changing the ETSI/ANSI Mode (CLI).

Frequency signals can be taken by the system from Ethernet and radio interfaces.

The reference frequency may also be conveyed to external equipment through different interfaces. For instructions how to configure the outgoing clock, see Configuring the Outgoing Clock and SSM Messages.

Frequency is distributed by configuring the following parameters in each node:

System Synchronization Sources – These are the interfaces from which the frequency is taken and distributed to other interfaces. Up to 16 sources can be configured in each node. A revertive timer can be configured. For each interface, you must configure:

- **Priority (1-16)** – No two synchronization sources can have the same priority.
- **Quality** – The quality level applied to the selected synchronization source. This enables the system to select the source with the highest quality as the current synchronization source.

Each unit determines the current active clock reference source interface:

- The interface with the highest available quality is selected.
- From among interfaces with identical quality, the interface with the highest priority is selected.

Note

You can configure a revertive timer for the PTP 850 unit. When the revertive timer is configured, the unit will not switch to another synchronization source unless that source has been stable for at least the number of seconds defined in the revertive timer. This helps to prevent a situation in which numerous switchovers occur when a synchronization source reports a higher quality for a brief time interval, followed by a degradation of the source's quality. By default, the revertive timer is set to 0, which means that it is disabled. Configuration of the revertive timer must be performed via CLI. See Configuring the Revertive Timer (CLI).

When configuring the Sync source, the Sync mode must be set to its default setting of automatic. To display the current Sync mode, enter the following CLI command in root view:

Root > platform sync mode show

If the Sync mode is set to pipe, you must set it to automatic by entering the following CLI command in root view:

Root > platform sync mode set automatic

When configuring an Ethernet interface as a Sync source, the Media Type of the interface must be RJ45 or SFP, not Auto-Type.

13.1.1 Viewing the Sync Source Status

To view the current sync source and its quality:

1 Select **Sync > Sync Source**. The Sync Source page opens.

Figure 442 Sync Source Page

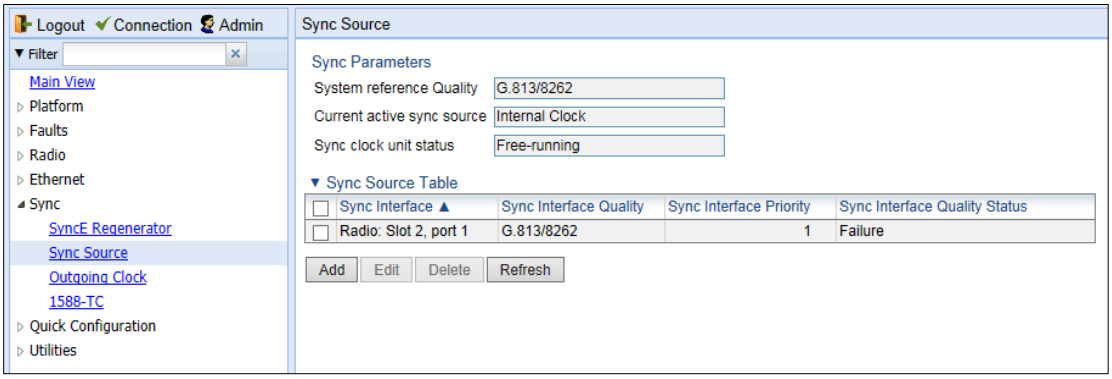


Table 83 Sync Source Parameters

Parameter	Definition
System Reference Quality	The quality of the current synchronization source interface. A value of **DNU** indicates that no synchronization source interfaces are currently defined.

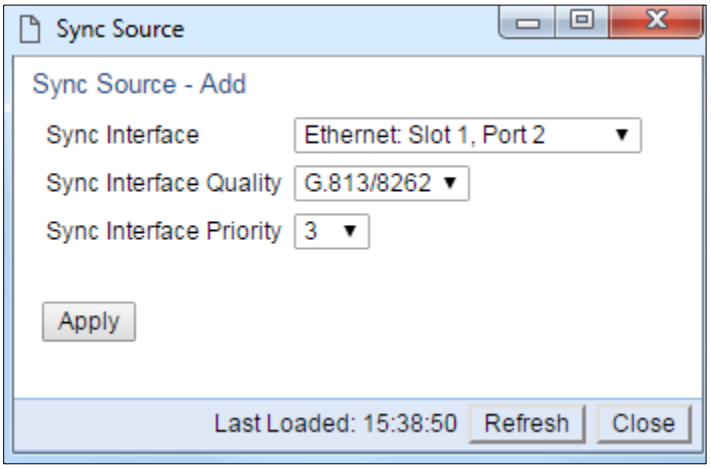
Parameter	Definition
Current Active Sync Source	The currently active system synchronization source interface.
Sync Clock Unit Status	The status of the unit's Sync E mechanism.
Sync Interface	Displays the interface that is configured as a synchronization source.
Sync Interface Quality	Displays the quality level assigned to this synchronization source. This enables the system to select the source with the highest quality as the current synchronization source. If the **Sync Interface Quality** is set to **Automatic**, the quality is determined by the received SSMs. If no valid SSM messages are received or in case of interface failure (such as LOS, LOC, LOF), the quality becomes "Failure." SSM must be enabled on the remote interface in order for the interface to receive SSM messages. For instructions how to enable SSM, see Configuring the Outgoing Clock and SSM Messages.
Sync Interface Priority	Displays the priority assigned to this synchronization source.
Sync Interface Quality Status	Displays the current actual synchronization quality of the interface.

13.1.2 Adding a Sync Source

To add a synchronization source:

1 In the Sync Source page (Figure 442), click **Add**. The Sync Source – Add page opens.

Figure 443 Sync Source – Add Page



2 In the **Sync Interface** field, select the interface you want to define as a synchronization source. You can select from the following interface types:

Ethernet interfaces

Radio interface



Note

In order to select an Ethernet interface, you must first specify the media type for this interface. See Configuring Ethernet Interfaces.

3 In the **Sync Interface Quality** field, select the quality level applied to the selected synchronization source. This enables the system to select the source with the highest quality as the current synchronization source.

If the **Sync Interface Quality** is set to **Automatic**, the quality is determined by the received SSMs. If no valid SSM messages are received or in case of interface failure (such as LOS, LOC, LOF), the quality becomes **Failure**. SSM must be enabled on the remote interface in order for the interface to receive SSM messages. For instructions how to enable SSM, see Configuring the Outgoing Clock and SSM Messages.

If the **Sync Interface Quality** is set to a fixed value, then the quality status becomes **Failure** upon interface failure (such as LOS, LOC, LOF).

4 In the **Sync Interface Priority** field, select the priority of this synchronization source relative to other synchronization sources configured in the unit (1-16). You cannot assign the same priority to more than one synchronization source. Once a priority value has been assigned, it no longer appears in the **Sync Interface Priority** dropdown list.

5 Click **Apply**, then **Close**.

13.1.3 Editing a Sync Source

To edit a synchronization source:

1 In the Sync Source page (Figure 442), click **Edit**. The Sync Source – Edit page opens.

2 Edit the parameters, as defined above. You can edit all the parameters except **Sync Interface**, which is read-only.

3 Click **Apply**, then **Close**.

13.1.4 Deleting a Sync Source

To delete a synchronization source:

1 Select the synchronization source in the Sync Source page (Figure 442).

2 Click **Delete**. The synchronization source is deleted.

13.2 Configuring the Outgoing Clock and SSM Messages



Note

> Under certain circumstances in which an adequate clock signal is unavailable, an interface may go from locked state to holdover state. Normally, when an interface is in holdover state, it uses stored data to determine its outgoing clock. However, you can set the unit to apply a default quality of DNU (Do Not Use) to any interface in holdover state via the CLI. For instructions, see Changing the Default Quality (CLI).

In the Outgoing Clock page, you can view and configure the following synchronization settings per interface:

The interface's clock source (outgoing clock).

For radio interfaces, the synchronization radio channel (used for interoperability).

SSM message administration.

In order to provide topological resiliency for synchronization transfer, PTP 850E implements the passing of SSM messages over the radio interfaces. SSM timing in PTP 850E complies with ITU-T G.781.

In addition, the SSM mechanism provides reference source resiliency, since a network may have more than one source clock. The following are the principles of operation:

At all times, each source interface has a “quality status” which is determined as follows:

If quality is configured as fixed, then the quality status becomes “failure” upon interface failure (such as LOS, LOC, LOF).

If quality is automatic, then the quality is determined by the received SSMs. If no valid SSM messages are received or in case of interface failure (such as LOS, LOC, LOF), the quality becomes "failure.

Each unit holds a parameter which indicates the quality of its reference clock. This is the quality of the current synchronization source interface.

The reference source quality is transmitted through SSM messages to all relevant radio interfaces.

In order to prevent loops, an SSM with quality “Do Not Use” is sent from the active source interface (both radio and Ethernet)

In order for an interface to transmit SSM messages, SSM must be enabled on the interface. By default, SSM is disabled on all interfaces.

When configuring the outgoing clock and SSM administration, the Sync mode must be set to its default setting of automatic. To display the current Sync mode, enter the following CLI command in root view:

```
root> platform sync mode show
```

If the Sync mode is set to pipe, you must set it to automatic by entering the following CLI command in root view:

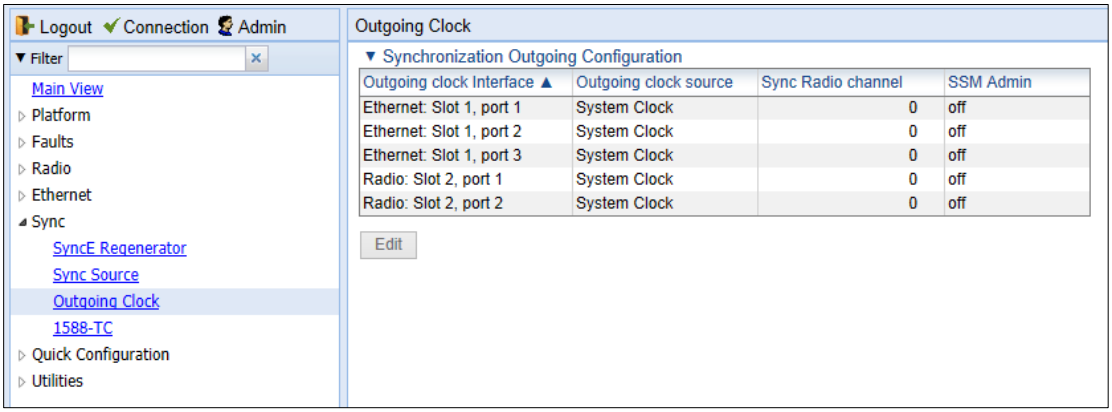
```
root> platform sync mode set automatic
```

To configure the outgoing clock on an Ethernet interface, the Media Type of the interface must be RJ45 or SFP, not Auto-Type. To view and configure the Media Type of an Ethernet interface, see Configuring Ethernet Interfaces.

To view and configure the synchronization parameters of the unit’s interfaces:

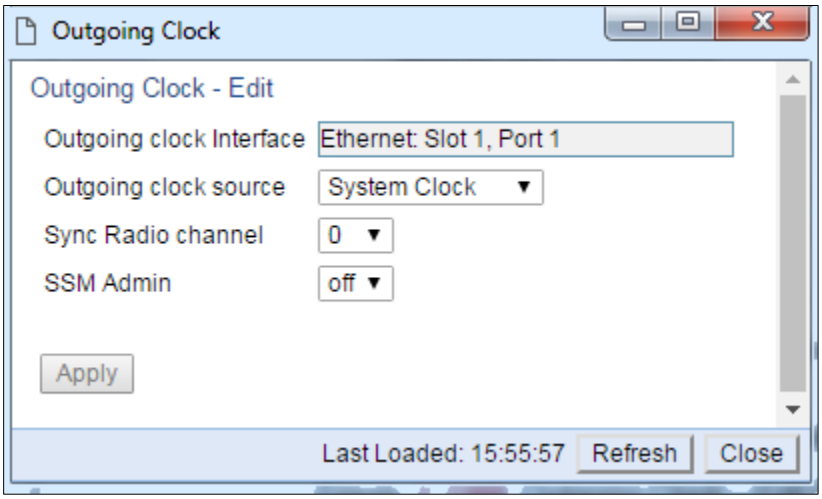
1 Select **Sync > Outgoing Clock**. The Outgoing Clock page opens.

Figure 444 Outgoing Clock Page



2 Select the interface you want to configure and click **Edit**. The Outgoing Clock – Edit page opens.

Figure 445 Outgoing Clock – Edit Page



3 In the **Outgoing clock source** field, select the interface's synchronization source. Options are:

Local Clock – The interface uses its internal clock as its synchronization source.

System Clock – Default value. The interface uses the system clock as its synchronization source.

Source Interface – Reserved for future use.

Time Loop – Reserved for future use.

4 In **Sync Radio Channel** field, use the default value of 0.

5 In the **SSM Admin** field, select **On** or **Off** to enable or disable SSM for the interface. By default, SSM is disabled on all interfaces.

13.3 Configuring 1588 Transparent Clock

PTP 850E uses 1588v2-compliant Transparent Clock to counter the effects of delay variation. Transparent Clock measures and adjusts for delay variation, enabling the PTP 850E to guarantee ultra-low PDV.

A Transparent Clock node resides between a master and a slave node, and updates the timestamps of PTP packets passing from the master to the slave to compensate for delay, enabling the terminating clock in the slave node to remove the delay accrued in the Transparent Clock node. The Transparent Clock node is itself neither a master nor a slave node, but rather, serves as a bridge between master and slave nodes.

Note the following:

- 1588 TC is not supported when Master-Slave communication is using the IPv6 transport layer.



Note

It is recommended to ensure that the PTP service uses the same type of equipment and physical connection (SFP or RJ-45) on both sides of the radio link. This makes Transparent Clock timestamping more accurate.

Make sure to enable Transparent Clock on the remote side of the link before enabling it on the local side.

To configure Transparent Clock:

1 Add the port receiving synchronization from the customer side as a Sync source, with Sync Interface Priority 1. See *Adding a Sync Source*.

2 Add a radio interface as a Sync source, with lower priority than the port receiving synchronization from the customer side. See *Adding a Sync Source*.

3 On the remote side of the radio link, add the radio interface facing the local device as a Sync source, with Sync Interface Priority 1. See *Adding a Sync Source*.

4 On the remote side of the radio link, if there is an Ethernet port conveying synchronization, add this port as a Sync source, with lower priority than the radio interface. See *Adding a Sync Source*.

5 Verify that the Sync Interface Quality Status of the first Sync source is not Failure. See Viewing the Sync Source Status.

6 Select **Sync > 1588 > General Configuration**. The 1588 – General Configuration page opens.

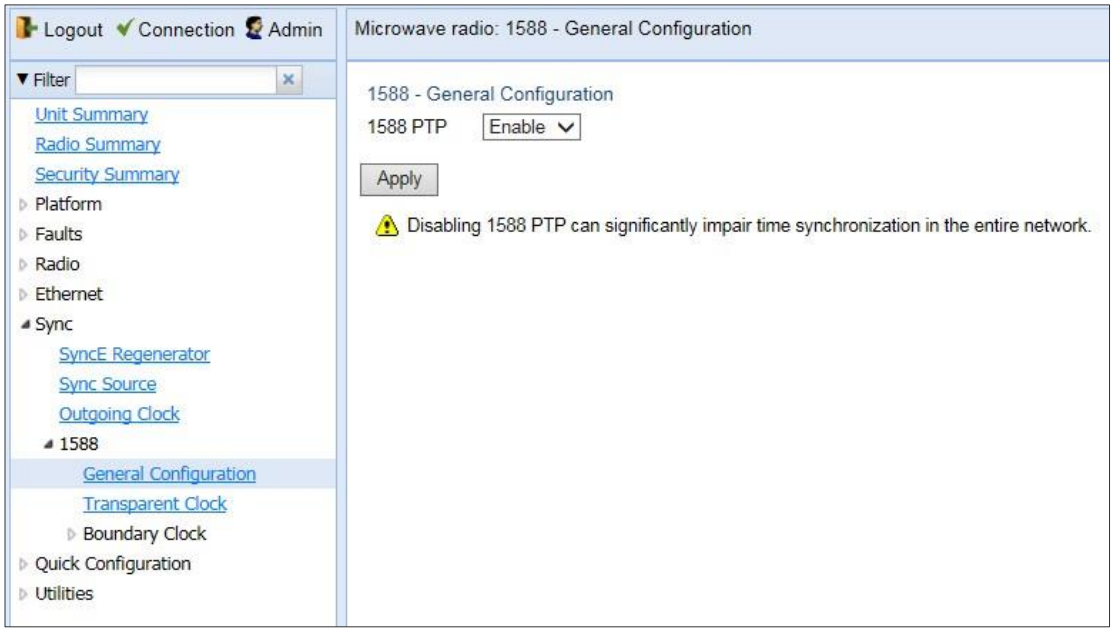


Figure 168: 1588 General Configuration Page

7 In the **1588 PTP** field, select **Enable**.

8 Click **Apply**.

9 Select **Sync > 1588 > Transparent Clock**. The 1588 Transparent Clock page opens.

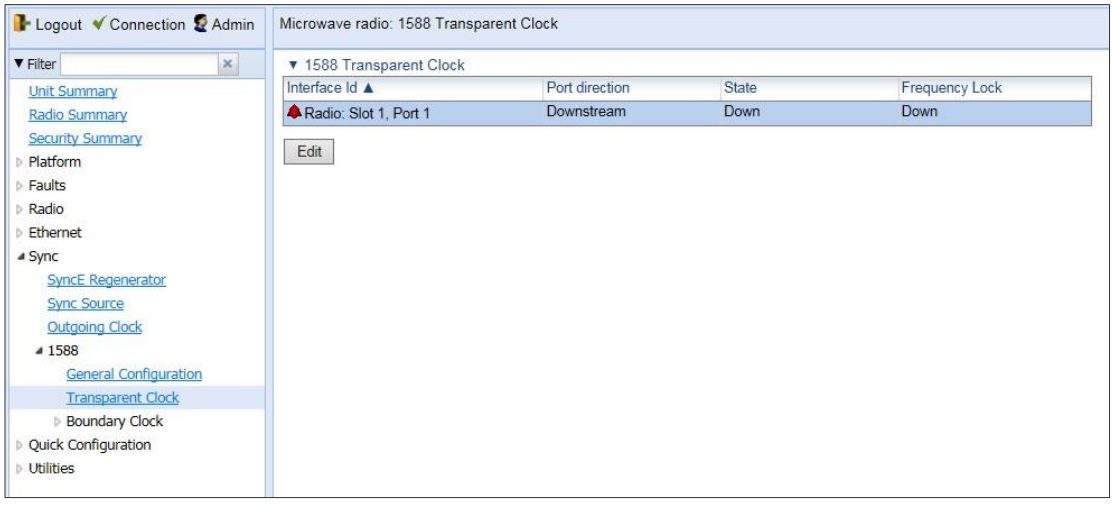


Figure 169: 1588 Transparent Clock Page

10 Select the radio interface and click **Edit**. The 1588 Transparent Clock – Edit page opens.

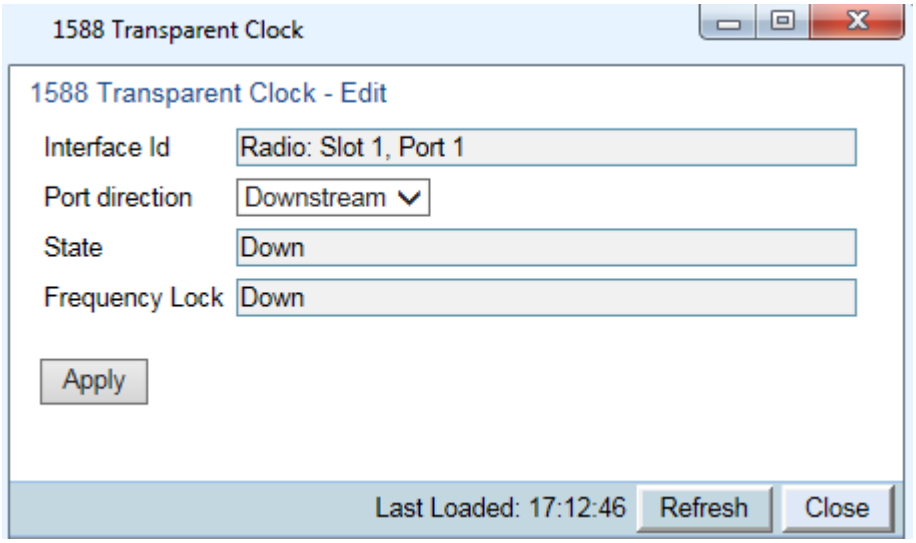


Figure 446 1588 Transparent Clock – Edit Page

11 In the **Port direction** field, select **Upstream** or **Downstream**. This field must be set to different values on the two sides of the link, so that if you set the local side to **Upstream**, you must set the remote side to **Downstream**, and vice versa. Otherwise than that, it does not matter how you set this field.

12 Click **Apply**, then **Close**.

13 1588 packets should be mapped to CoS 7. By default, 1588 packets are *not* mapped to any CoS. To map 1588 packets to CoS 7, you must *disable* CoS preservation for 1588 packets. This must be performed via CLI, using the following command:

```
root> ethernet generalcfg ptp-tc cos-preserve set admin disable
```

14 To map 1588 packets to CoS 7, enter the following command:

```
root> ethernet generalcfg ptp-tc cos-preserve cos value 7
```

After you enter these commands, 1588 packets will automatically be mapped to CoS 7.

Note

If necessary, you can use the ethernet generalcfg ptp-tc cos-preserve cos value command to map a different CoS value (0-7) to 1588 packets, but it is recommended to map 1588 packets to CoS 7.

To disable Transparent Clock synchronization:

1 Select **Sync > 1588 > General Configuration**. The 1588 – General Configuration page opens (*Figure 168*).

2 In the **1588 PTP** field, select **Disable**.

3 Click **Apply**.



Note

Disabling 1588 PTP can drastically affect time synchronization performance in the entire network.

13.4 Configuring 1588 Boundary Clock

Boundary Clock complies with ITU-T Telecom Profile G.8275.1. This enables PTP 850E, with Boundary Clock, to meet the rigorous synchronization requirements of 5G networks.

The Boundary Clock in PTP 850E supports up to 16 1588 slave clock devices.

The Boundary Clock terminates the PTP flow it receives on the slave port, recovers the time and phase, and regenerates the PTP flow on the master ports.

The Boundary Clock node selects the best synchronization source available in the domain and regenerates PTP towards the slave clocks. This reduces the processing load from grandmaster clocks and increases the scalability of the synchronization network, while rigorously maintaining timing accuracy.

The PTP 850E Boundary Clock mechanism requires the use of untagged Ethernet multicast PTP packets as specified in G.8275.1.



Note

Boundary Clock and Transparent Clock can be used together in the same PTP 850E node.

Note that in release 11.1:

- 1588 BC can only be used in a chain or star topology. It cannot be used in a ring topology.
- 1588 BC is not supported when Master-Slave communication is using the IPv6 transport layer.

13.4.1 Enabling Boundary Clock



Note

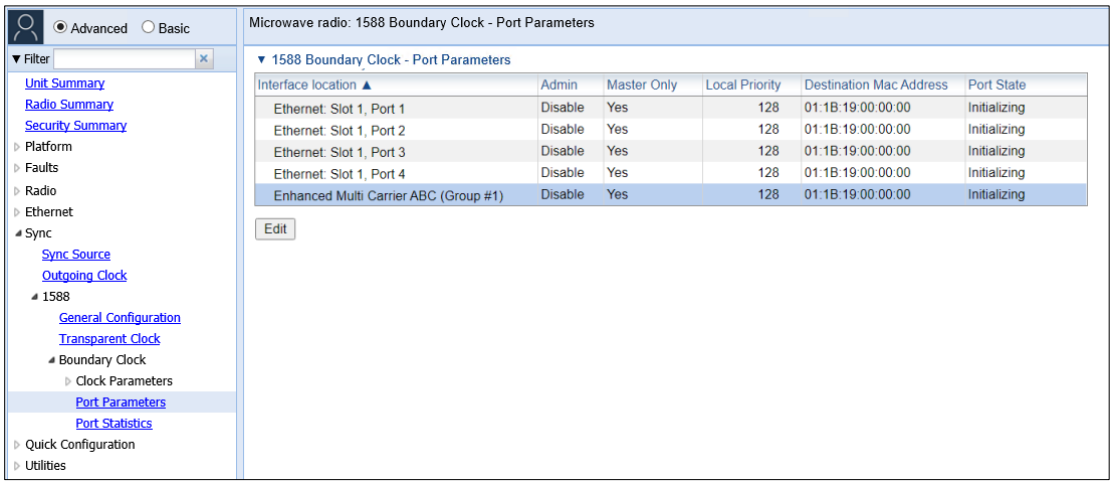
Before configuring Boundary Clock, you must configure Transparent Clock. See Configuring 1588 Transparent Clock.

To enable Boundary Clock:

1. Select Sync > 1588 > General Configuration. The 1588 – General Configuration page opens (Figure 191).
2. In the **1588 PTP** field, select **Enable**.
3. Click Apply.

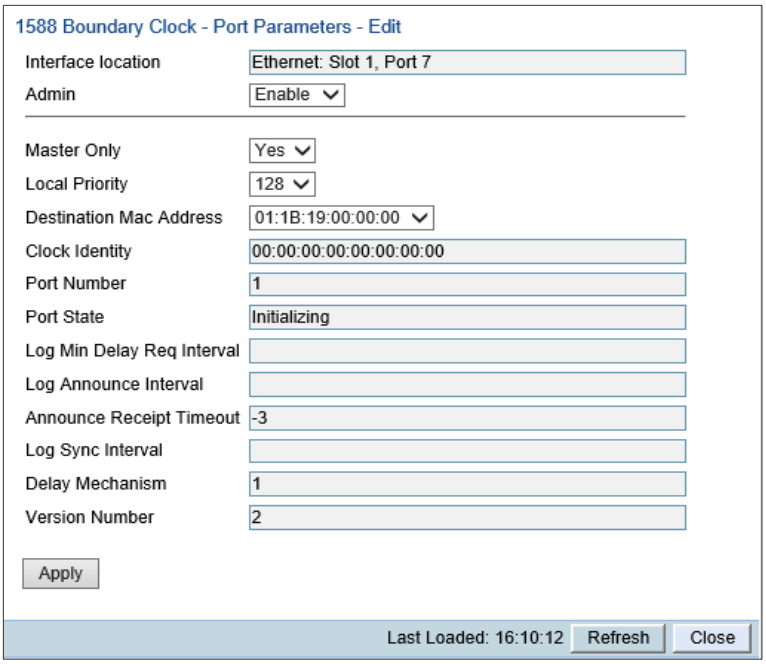
4. Select **Sync > 1588 > Boundary Clock > Port Parameters**. The 1588 Boundary Clock – Port Parameters page opens. You can configure up to 16 interfaces per unit to be part of the Boundary Clock node. These interfaces can be radio and Ethernet interfaces, but not TDM interfaces or groups (e.g., LAG or Multi- Carrier ABC groups).

Figure 447 1588 Boundary Clock – Port Parameters Page



5. Select an interface and click **Edit**. The 1588 Boundary Clock – Port Parameters – Edit page opens.

Figure 448 1588 Boundary Clock – Port Parameters – Edit Page



6. In the **Admin** field, select **Enable**.
7. In the **Master Only** field, select from the following options:

- Yes – The port can only be used as the master port, which means the port acts as a PTP synchronization source for other nodes.
- No – The port can be used as either a master port or the slave port. The slave port receives PTP synchronization input from an external grandmaster clock. The Best Master Clock Algorithm (BMCA) determines the port's role, based on its determination of which is the best available grandmaster clock. Only one slave port can exist in a single PTP 850E node at any one time.

8. Optionally, in the **Local Priority** field, select a value between 1-255. The default value is 128. The Local Priority value is taken into account when two identical announce messages are received by at least two different ports. In such a case, the Boundary Clock mechanism selects the slave port based on the best (lowest) Local Priority.
9. In the **Destination Mac Address** field, select a MAC address for multicast re-transmission of PTP packets. Options are:
    - 01-1B-19-00-00-00 – General group address. An 802.1Q VLAN Bridge would forward the frame unchanged.
    - 01-80-C2-00-00-0E – Individual LAN Scope group address. An 802.1Q VLAN Bridge would drop the frame.
10. Click **Apply**.
11. Repeat these steps to add up to 16 interfaces to the unit's Boundary Clock node.
12. To map PTP packets into the Boundary Clock node, a service point must be created on each interface in the Boundary Clock node. This service point must be defined to gather untagged packets. See Adding a Service Point.
13. Add a port receiving synchronization from the customer side as a Sync source, with Sync Interface Priority 1.
14. Add a radio interface as a Sync source, with lower priority than the port receiving synchronization from the customer side.

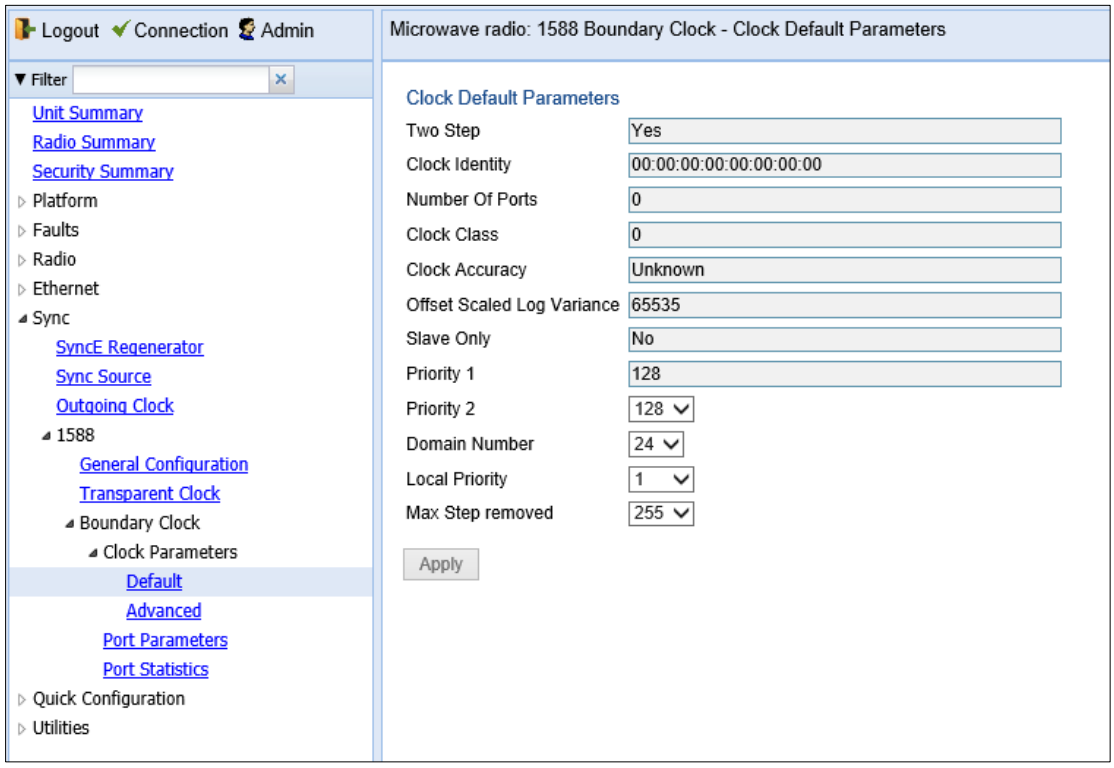
15. On the remote side of the radio link, add the radio interface facing the local device as a Sync source, with Sync Interface Priority 1.
16. On the remote side of the radio link, if there is an Ethernet port conveying synchronization, add this port as a Sync source, with lower priority than the radio interface.
17. Verify that the Sync Interface Quality Status of the first Sync source is not Failure.

13.4.2 Displaying and Setting the Boundary Clock Default Parameters

To display and set the Boundary Clock default parameters:

1. Select **Sync** > **1588** > **Boundary Clock** > **Clock Parameters** > **Default**. The 1588 Boundary Clock – Clock Default Parameters page opens.

Figure 449 1588 Boundary Clock – Clock Default Parameters Page



2. In the **Priority 2** field, you can select a value between 0 and 255. The default value is 128. The Priority 2 value is one of the factors used by the BMCA to determine the grandmaster. The PTP 850E's Boundary Clock node advertises this value when it is not locked on an external grandmaster.
3. In the Domain **Number** field, you can select a value between 24 and 43. The default value is 24.
4. In the **Local Priority** field, you can select a value between 1 and 255. The default value is 128. The Local Priority value is taken into account when two identical announce messages are received by at least two different ports. In such a case, the Boundary Clock mechanism selects the slave port based on the best (lowest) Local Priority.

5. In the **Max Step removed** field, you can select the maximum number of PTP clocks traversed from the grandmaster to the slave clock in the local PTP 850E Boundary Clock node. The value range is 1-255. The default value is 255. If the defined number is exceeded, packets from this grandmaster candidate are discarded and the grandmaster will not be eligible for use by the Boundary Clock node.
6. To implement your changes, click **Apply**.

Figure 450 Boundary Clock Default Parameters

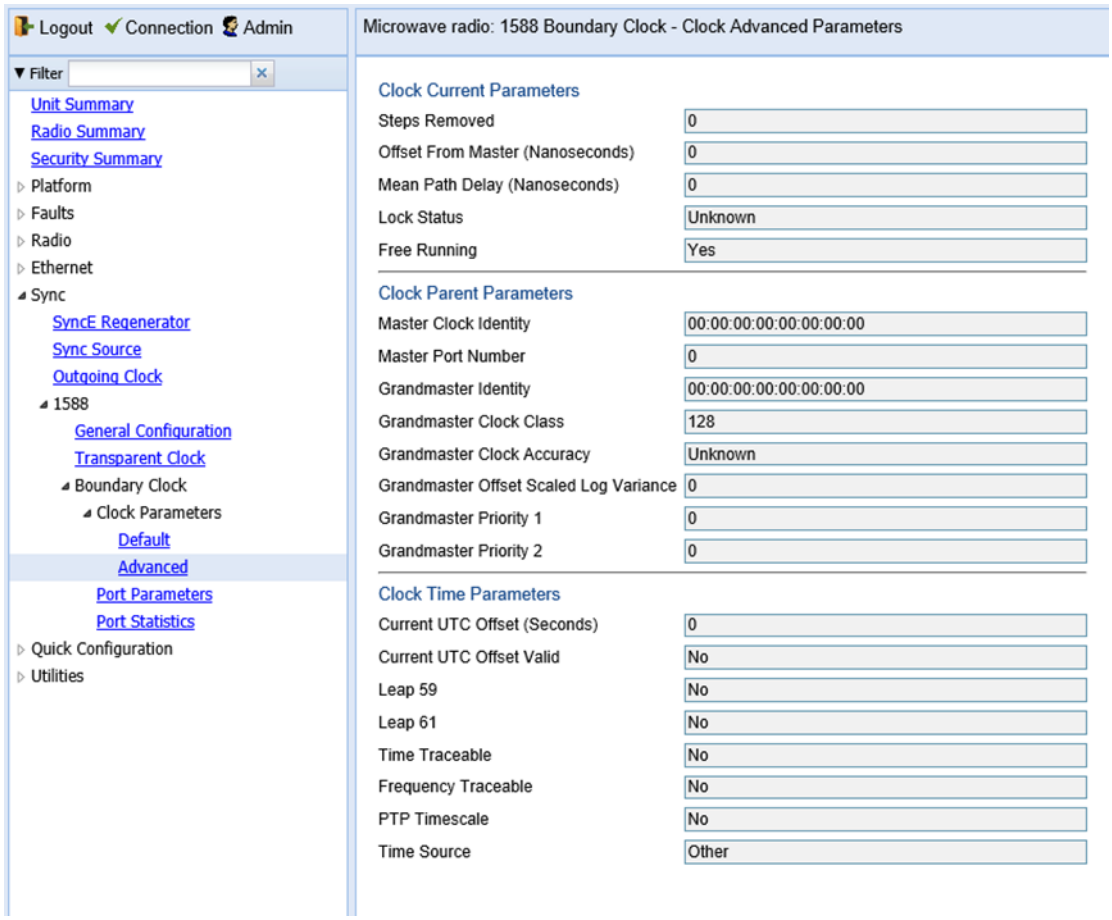
Parameter	Definition
Two Step	Indicates whether the Boundary Clock node is operating in two-step mode. In PTP 850E, this is always set to Yes.
Clock Identity	Identifies the system clock.
Number of Ports	Displays the number of ports on the unit on which Boundary Clock is enabled. The maximum is 16 per PTP 850E unit.
Clock Class	One of the elements of the clock quality, as defined in IEEE-1588.
Clock Accuracy	One of the elements of the clock quality, as defined in IEEE-1588.
Offset Scaled Log Variance	One of the elements of the clock quality, as defined in IEEE-1588.
Slave Only	Indicates whether the Boundary Clock node is operating in slave mode only. In PTP 850E, this is always set to No.
Priority 1	Always displays 128.

13.4.3 Displaying the Boundary Clock Advanced Parameters

To display and set the Boundary Clock advanced parameters:

1. Select **Sync > 1588 > Boundary Clock > Clock Parameters > Advanced**. The 1588 Boundary Clock – Clock Advanced Parameters page opens.

Figure 451 1588 Boundary Clock – Clock Advanced Parameters Page



All of the advanced Boundary Clock parameters are read-only. Beow table lists and describes the Boundary Clock advanced parameters.

Table 84 Boundary Clock Advanced Parameters

Parameter	Definition
Steps Removed	The number of PTP clocks traversed from the grandmaster to the slave clock in the local PTP 850E Boundary Clock node. You can define a maximum number of steps in the Clock Default Parameters page. See Displaying and Setting the Boundary Clock Default Parameters.
Offset from Master (Nanoseconds)	The time difference between the master clock and the local slave clock (in ns).
Mean Path Delay (Nanoseconds)	The mean propagation time for the link between the master and the local slave (in ns).
Lock Status	Provides 1588 Boundary Clock stack lock status information.
Free Running	APR stack manual freerun state.
Master Clock Identity	The clock identity of the current master clock.
Master Port Number	The clock identity of the current master port.

Parameter	Definition
Grandmaster Identity	The clock identity of the current grandmaster.
Grandmaster Clock Class	The clock class of the current grandmaster. The clock class is one of the elements of the clock quality, as defined in IEEE-1588.
Grandmaster Clock Accuracy	The clock accuracy of the current grandmaster. The clock accuracy is one of the elements of the clock quality, as defined in IEEE-1588.
Grandmaster Offset Scaled Log Variance	The offset scaled log variance of the current grandmaster. The offset scaled log variance is one of the elements of the clock quality, as defined in IEEE-1588.
Grandmaster Priority 1	The Priority 1 value of the current grandmaster.
Grandmaster Priority 2	The Priority 2 value of the current grandmaster.
Current UTC Offset (Seconds)	The current UTC offset value (in seconds).
Current UTC Offset Valid	Indicates whether the current UTC offset value is valid.
Leap 59	Indicates that the last minute of the current UTC day contains 59 seconds.
Leap 61	Indicates that the last minute of the current UTC day contains 61 seconds.
Time Traceable	Traceability to the primary time reference.
Frequency Traceable	Traceability to the primary frequency reference.
PTP Timescale	Indicates whether the clock time scale of the grandmaster clock is PTP.
Time Source	The source of the time used by the grandmaster clock.

13.4.4 Displaying the Boundary Clock Port Parameters

To display the Boundary Clock port parameters:

1. Select Sync > 1588 > Boundary Clock > Port Parameters. The 1588 Boundary Clock – Port Parameters page opens (Figure 194).
2. Select the port you want to configure and click Edit. The 1588 Boundary Clock – Port Parameters – Edit page opens (*Figure 195*).

   For an explanation of the configurable fields, see Enabling Boundary Clock. Below lists and describes the read-only Boundary Clock port parameters.

Table 85 Boundary Clock Port Parameters

Parameter	Definition
Clock Identity	The PTP 850E unit's clock identity. The same value is used for every port that belongs to the Boundary Clock node.

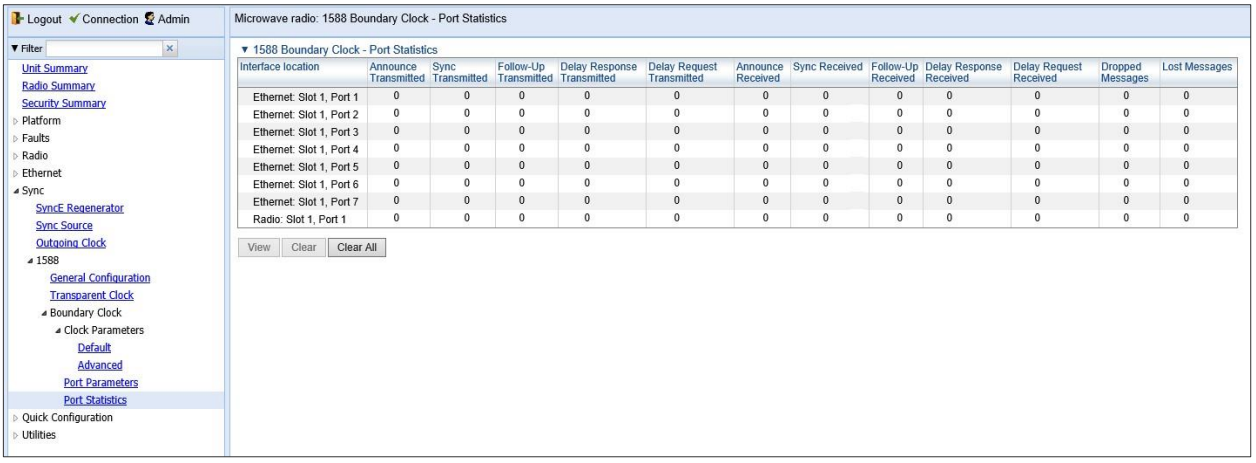
Parameter	Definition
Port Number	Displays the number of the port according to the activation sequence of every port.
Port State	Indicates whether the port is currently acting as Master (distributing PTP to other nodes) or Slave (receiving PTP from a grandmaster).
Log Min Delay Req Interval	The minimum allowed interval between Delay Request messages.
Log Announce Interval	The interval between Announce messages.
Announce Receipt Timeout	The maximum allowed number of intervals without receiving any Announce messages.
Log Sync Interval	Interval between sync messages.
Delay Mechanism	Always displays 1.
Version Number	Always displays 2.

13.4.5 Displaying the Boundary Clock Port Statistics

To display the Boundary Clock port statistics:

1. Select **Sync > 1588 > Boundary Clock > Port Statistics**. The 1588 Boundary Clock – Port Statistics page opens.

Figure 452 1588 Boundary Clock – Port Statistics Page



- To display the statistics for a specific port in a separate page, click **View**.
- To clear the statistics for a specific port, select the port's row and click **Clear**.
- To clear the statistics for all Boundary Clock ports, click **Clear All**.

Table 86 Boundary Clock Port Statistics

Parameter	Definition

Announce Transmitted	The number of Announce messages that have been transmitted from the port.
Sync Transmitted	The number of Sync messages that have been transmitted from the port.
Follow-Up Transmitted	The number of Follow-Up messages that have been transmitted from the port.
Delay Response Transmitted	The number of Delay Response messages that have been transmitted from the port.
Delay Request Transmitted	The number of Delay Request messages that have been transmitted from the port.
Announce Received	The number of Announce messages that have been received by the port.
Sync Received	The number of Sync messages that have been received by the port.
Follow-Up Received	The number of Follow-Up messages that have been received by the port.
Delay Response Received	The number of Delay Response messages that have been received by the port.
Delay Request Received	The number of Delay Request messages that have been received by the port.
Dropped Messages	The number of dropped messages.
Lost Messages	The number of lost messages.

13.4.6 Disabling 1588 PTP

To disable 1588 PTP synchronization:

1. Select **Sync > 1588 > Boundary Clock > Port Parameters**. The 1588 Boundary Clock – Port Parameters page opens (*Figure 194*).
2. Select an interface and click **Edit**. The 1588 Boundary Clock – Port Parameters
3. In the **Admin** field, select **Disable**.



Note

It is important to disable Boundary Clock on the interfaces before disabling 1588 PTP.

4. Select **Sync > 1588 > General Configuration**. The 1588 – General Configuration page.
5. In the **1588 PTP** field, select **Disable**.
6. Click **Apply**.



Note

Disabling 1588 PTP disables both Transparent Clock and Boundary Clock, and can drastically affect time synchronization performance in the entire network.

14. Access Management and Security

This section includes:

- Quick Security Configuration
- Configuring the General Access Control Parameters
- Configuring the Session Timeout
- Configuring Users
- Configuring RADIUS
- Configuring TACACS+
- Viewing Remote Access User Connectivity and Permissions
- Configuring X.509 CSR Certificates
- Enabling HTTPS
- Downloading and Installing an RSA Key
- Enabling Telnet Access
- Configuring Access Control Lists
- Uploading the Security Log
- Uploading the Configuration Log
- Configuring SSO Web Login with Microsoft Entra ID

Note: PTP 850 devices support SDN, with NETCONF/YANG capabilities. This enables PTP 850 devices to be managed via SDN using Cambium's SDN controller, SDN Master. NETCONF must be enabled via CLI. See Enabling NETCONF (CLI).

You can terminate all active sessions via a CLI command. See Terminating all Active Sessions (CLI).

Related topics:

- Changing Your Password
- Operating in FIPS Mode
- Configuring AES-256 Payload Encryption

14.1 Quick Security Configuration

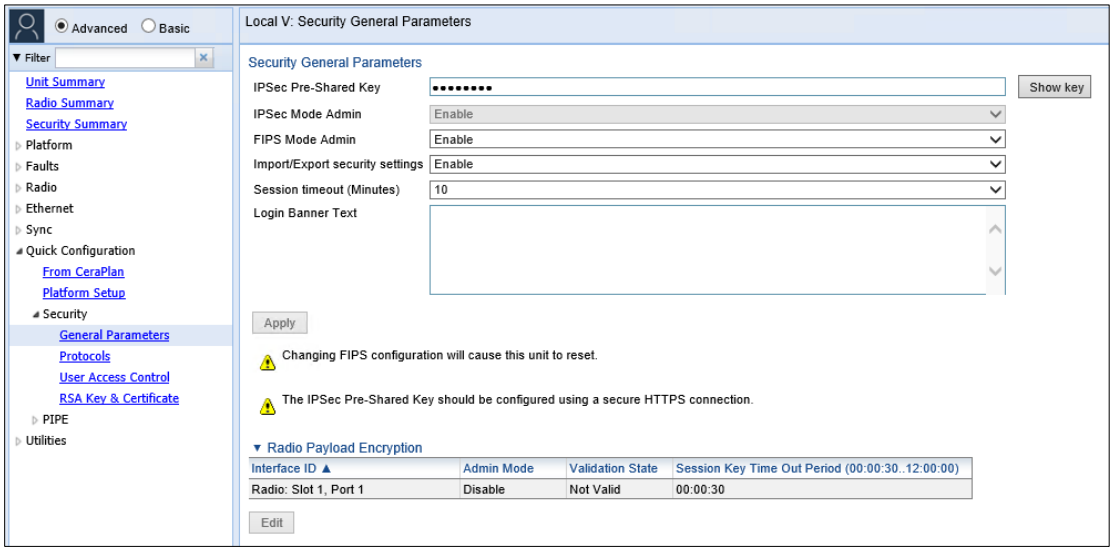
The Web EMS provides a set of Quick Configuration pages that enable you to quickly configure the unit's access and security parameters. This section describes these pages, with cross references to the sections in which each parameter is described in depth.

14.1.1 Quick Security Configuration – General Parameters Page

To configure the FIPS Admin, import and export security settings, session timeout, a login banner, and AES-256 payload encryption:

1 Select **Quick Configuration** > **Security** > **General Parameters**. The Quick Configuration Security General Parameters page opens.

Figure 453 Quick Configuration Security General Parameters Page



Note

The FIPS Mode Admin field is not relevant for PTP 850E.

2 The **IPSec Pre-Shared Key and IPSec Mode Admin** fields only appear for units with unit redundancy. For instructions, s**ee** Encrypting the Protection Link.

3 In the **FIPS Mode Admin** field, you can enable or disable FIPS mode. For details, see Operating in FIPS Mode.

The **Import/Export security settings** field determines whether security configurations are included in configuration backup files. If you select **Enable**, security configurations will *not* be included in backup files.

4 In the **Session timeout** field, you can configure a session timeout, in minutes, from 1 to 60 minutes. The default session timeout is 10 minutes. For details,

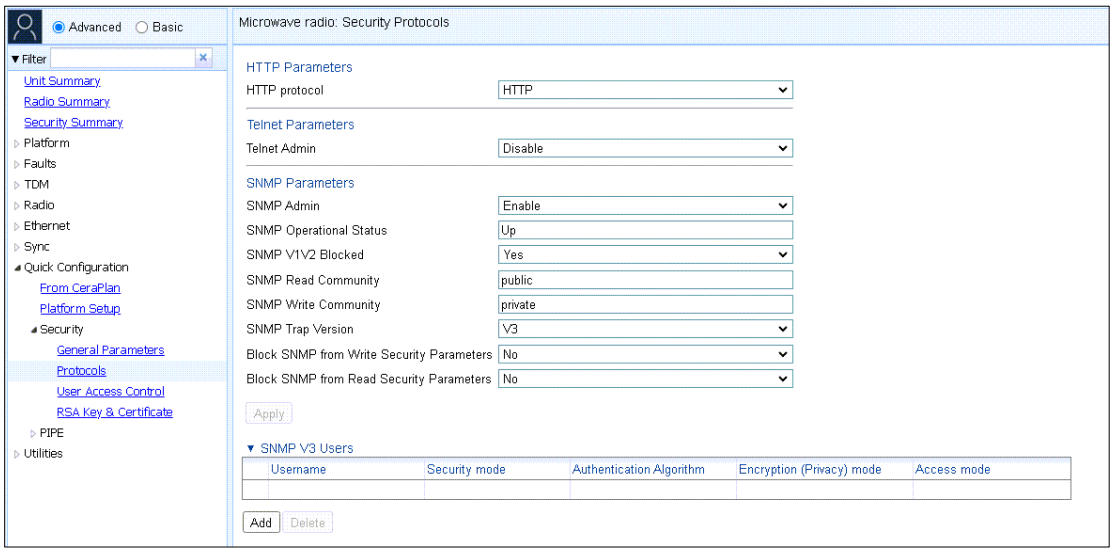
5 In the **Login Banner Text** field, you can define a login banner of up to 2,000 bytes. This banner will appear every time a user establishes a connection with the Web EMS. The banner appears before the login prompt, so that users will always see the login banner and must manually close the banner before logging in to the Web EMS. For details, see Defining a Login Banner.

14.1.2 Quick Security Configuration – Protocols Page

To configure the HTTP type, Telnet blocking, and SNMP parameters:

1. Select **Quick Configuration** > **Security** > **Protocols**. The Quick Configuration Security Protocols page opens.

Figure 454 Quick Configuration Security Protocols Page



2. In the **HTTP protocol** field, you can determine the web interface protocol for accessing the unit (HTTP or HTTPS). By default, the web interface protocol is HTTP. For details, see Enabling HTTPS.

> **Note**
>
> After changing the HTTP protocol, management is lost. To restore management, simply refresh the page.

3. In the **Telnet Admin** field, you can block or enable telnet access to the unit. By default, telnet access is enabled. For details, see Blocking Telnet Access.
4. In the **SNMP Parameters** area, you can configure the unit's SNMP parameters. For details.
   In addition, you can configure the following parameters only in the Quick Configuration Security Protocols page:
   I. In the **Block SNMP from Write Security Parameters** field, select **Yes** if you want to block SNMP from writing security parameters.
   II. In the **Block SNMP from Read Security Parameters** field, select **Yes** if you want to block SNMP from reading security parameters.
5. When you are finished editing the parameters described above, click **Apply**.
6. In the **SNMP V3 Users** are, you can click **Add** to add SNMP V3 users. For details.

14.1.3 Quick Security Configuration – Access Control Page

To configure parameters relating to users and login parameters:

1. Select **Quick Configuration** > **Security** > **Access Control**. The Quick Configuration Security Protocols page opens.

Figure 455 Quick Configuration Security Access Control Page



2. In the **Login & Password Management** area, you can configure enhanced security requirements for user passwords and for logging into the unit. For details.
3. When you are finished editing the login and password parameters, click **Apply**.
4. In the **User Accounts** area, you can configure individual users:

    I. To add a user, click **Add**.
    II. To edit an existing user, select the user in the User Accounts table and click **Edit**.

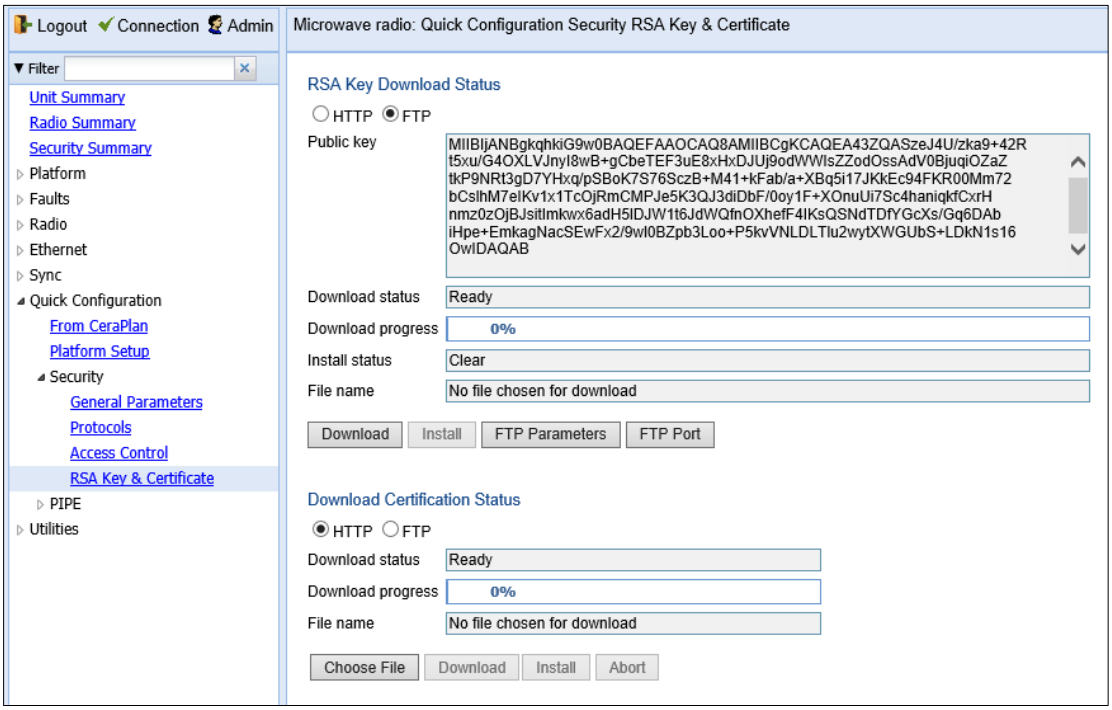
    For details.
5. To configure user profiles, click **Access Control User Profiles**. For details, see Configuring User Profiles.

14.1.4 Quick Security Configuration – RSA Key & Certificate Page

To download and install an RSA key and/or a Certificate Signing Request (CSR) file:

1. Select **Quick Configuration** > **Security** > **RSA Key & Certificate**. The Quick Configuration Security RSA Key & Certificate page opens.

Figure 456 Quick Configuration Security RSA Key & Certificate Page



2. In the **RSA Key Download Status** area, you can download and install an RSA key. For details, see Downloading and Installing an RSA Key.
3. In the **Download Certification Status** area, you can download and install a CSR file. For details, see Configuring X.509 CSR Certificates.

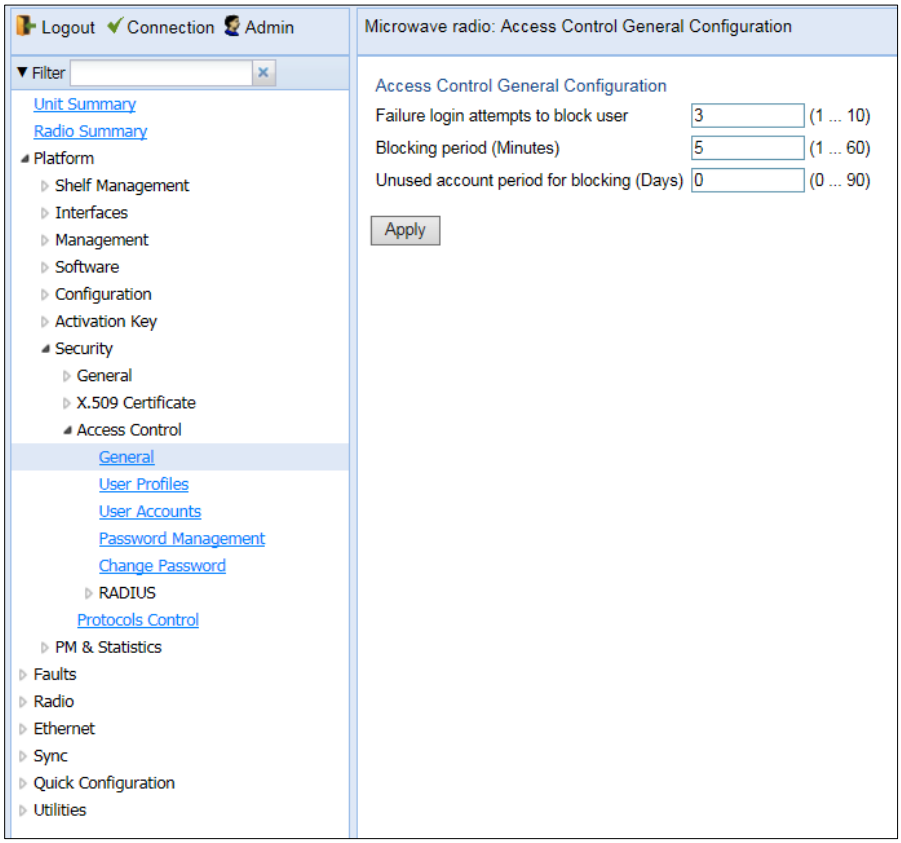
14.2 Configuring the General Access Control Parameters

To avoid unauthorized login to the system, PTP 850 automatically blocks users upon a configurable number of failed login attempts. You can also configure PTP 850 to block users that have not logged into the unit for a defined number of days.

To configure the blocking criteria:

1. Select **Platform > Security > Access Control > General**. The Access Control General Configuration page opens.

Figure 457 Access Control General Configuration Page

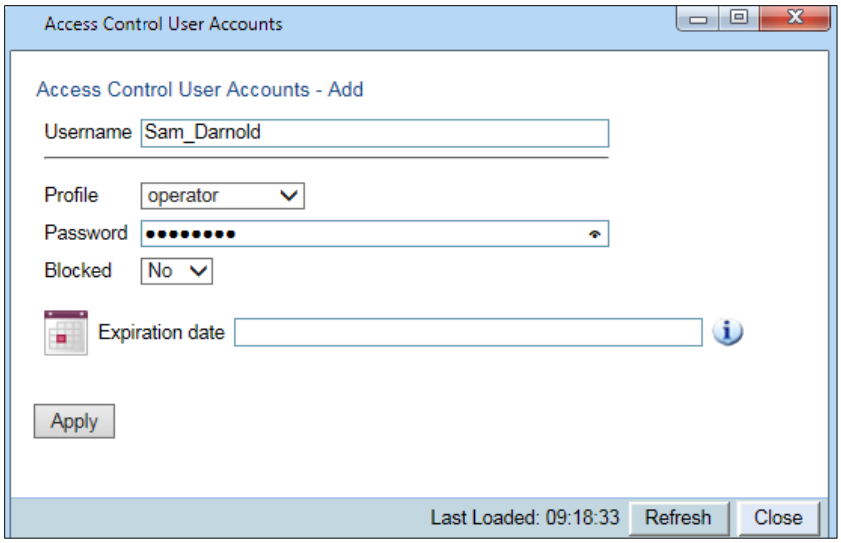


2. In the **Failure login attempts to block user** field, select the number of failed login attempts that will trigger blocking. If a user attempts to login to the system with incorrect credentials this number of times consecutively, the user will temporarily be prevented from logging into the system for the time period defined in the **Blocking period** field. Valid values are 1-10. The default value is 3.
3. In the **Blocking period (Minutes)** field, enter the length of time, in minutes, that a user is prevented from logging into the system after the defined number of failed login attempts. Valid values are 1-60. The default value is 5.
4. In the **Unused account period for blocking (Days)** field, you can configure a number of days after which a user is prevented from logging into the system if the user has not logged in for the configured number of days. Valid values are 0, or 30-90. If you enter 0, this feature is disabled. The default value is 0.
5. Click **Apply**.

Once a user is blocked, you can unblock the user from the User Accounts page. To unblock a user:

1. Select **Platform > Security > Access Control > User Accounts**. The Access Control User Accounts page opens (Figure 463).
2. Select the user and click **Edit**. The Access Control User Accounts - Edit page opens.

Figure 458 Access Control User Accounts - Edit Page



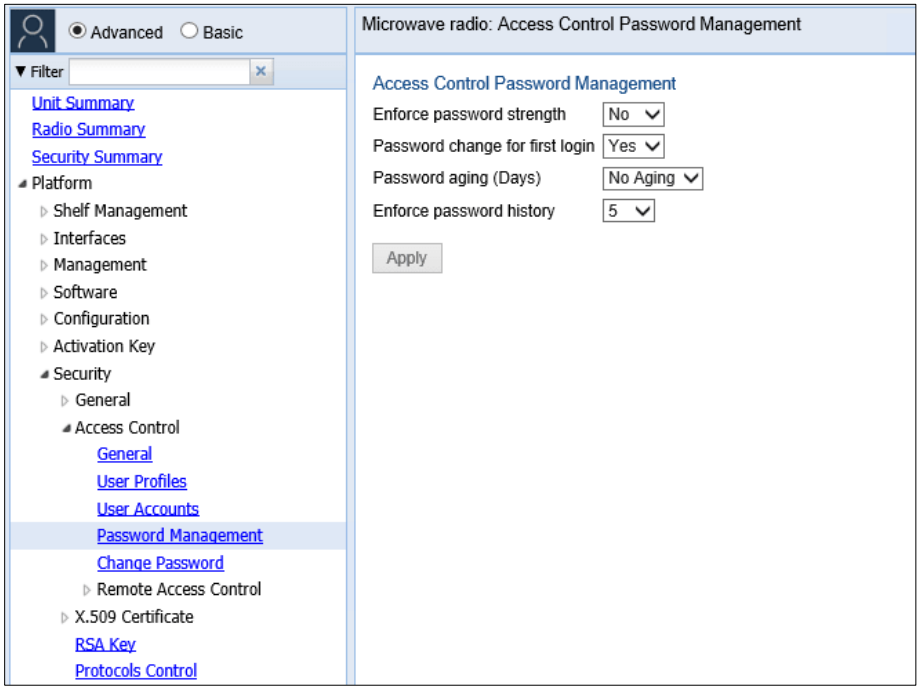
3. In the **Blocked** field, select **No**.
4. Click **Apply**, then **Close**.

14.3 Configuring the Password Security Parameters

To configure enhanced security requirements for user passwords:

1. Select **Platform** > **Security** > **Access Control** > **Password Management**. The Access Control Password Management page opens.

Figure 459 Access Control Password Management Page



2. In the **Enforce password strength** field, select **Yes** or **No**. When **Yes** is selected:

Password length must be at least eight characters.

Password must include characters of at least three of the following character types: lower case letters, upper case letters, digits, and special characters. For purposes of meeting this requirement, upper case letters at the beginning of the password and digits at the end of the password are not counted.

The last five passwords you used cannot be reused.

3. In the **Password change for first login** field, select **Yes** or **No**. When **Yes** is selected, the system requires the user to change his or her password the first time the user logs in.
4. In the **Password aging (Days)** field, select the number of days that user passwords will remain valid from the first time the user logs into the system. You can enter 20-90, or **No Aging**. If you select **No Aging**, password aging is disabled and passwords remain valid indefinitely.
5. In the **Enforce Password history** field, select the number of previous passwords that cannot be reused. For example, if you select 5, the last five passwords the user configured cannot be reused. If you select 0, there is no limitation on reusing old passwords.
6. Click **Apply**.

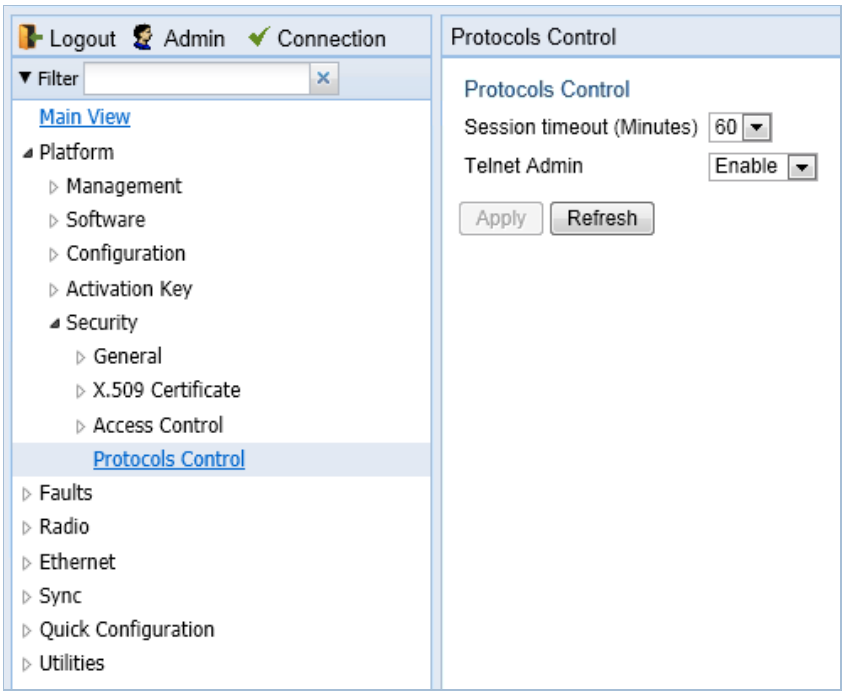
14.4 Configuring the Session Timeout

By default, there is a 10 minute session timeout. If you do not perform any activity on the system for the period of time defined as the session timeout, the user session times out and you will have to log in to the system again.

To modify the session timeout:

1. Select **Platform** > **Security** > **Protocols Control**. The Protocols Control page opens.

Figure 460 Protocols Control Page



2. In the **Session timeout (Minutes)** field, select a session timeout, in minutes, from 1 to 60.



Note

For information about the **Telnet Admin** field, see Blocking Telnet Access.

3. Click **Apply**.

14.5 Configuring Users

This section includes:

- User Configuration Overview
- Configuring User Profiles
- Adding User Accounts

Related topics:

- Changing Your Password

14.5.1 User Configuration Overview

User configuration is based on the Role-Based Access Control (RBAC) model. According to the RBAC model, permissions to perform certain operations are assigned to specific roles. Users are assigned to particular roles, and through those role assignments acquire the permissions to perform particular system functions.

In the PTP 850 GUI, these roles are called user profiles. Up to 50 user profiles can be configured. Each profile contains a set of privilege levels per functionality group, and defines the management protocols (access channels) that can be used to access the system by users to whom the user profile is assigned.

The system parameters are divided into the following functional groups:

- Security
- Management
- Radio
- TDM
- Ethernet
- Synchronization

A user profile defines the permitted access level per functionality group. For each functionality group, the access level is defined separately for read and write operations. The following access levels can be assigned:

- **None** – No access to this functional group.
- **Normal** – The user has access to parameters that require basic knowledge about the functional group.

- **Advanced** – The user has access to parameters that require advanced knowledge about the functional group, as well as parameters that have a significant impact on the system as a whole, such as restoring the configuration to factory default settings.

14.5.2 Configuring User Profiles

User profiles enable you to define system access levels. Each user must be assigned a user profile. Each user profile contains a detailed set of read and write permission levels per functionality group.

The system includes a number of pre-defined user profiles. You can edit these profiles, and add user profiles. Together, the system supports up to 50 user profiles.

For devices with Unit Redundancy, user profiles are copied dynamically to the Standby unit, without the need to perform a Copy-to-Mate operation. This includes both new user profiles and changes to existing user profiles.

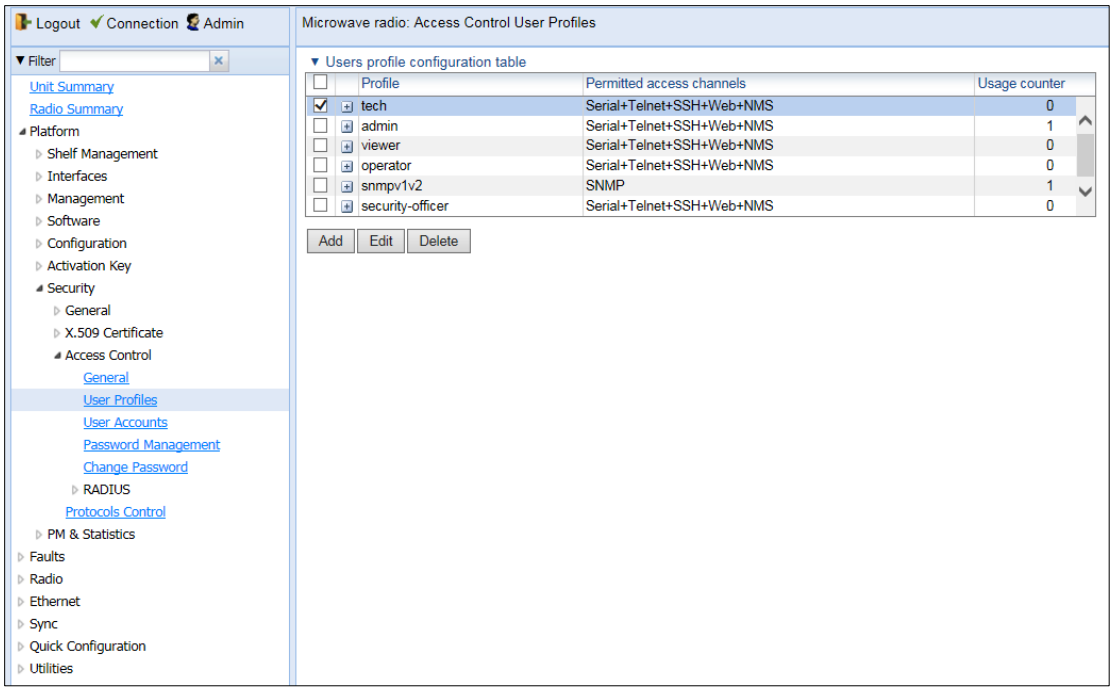
Note that it may take up to a minute for new user profile or user account and changes to existing user profiles and accounts to be copied to the Standby unit. Therefore, if an unexpected switchover takes place less than one minute after adding or modifying a user profile or account:

- Check that the user profile or account is configured in the new Active unit. If it is not, reconfigure the user profile or account and make sure at least one minute passes before another switchover occurs.
- If the user profile or account is configured in the new Active unit, check that you can successfully log into the unit with that user. If you cannot, delete the user profile or account and re-configure it in the new Active unit.

To add a user profile:

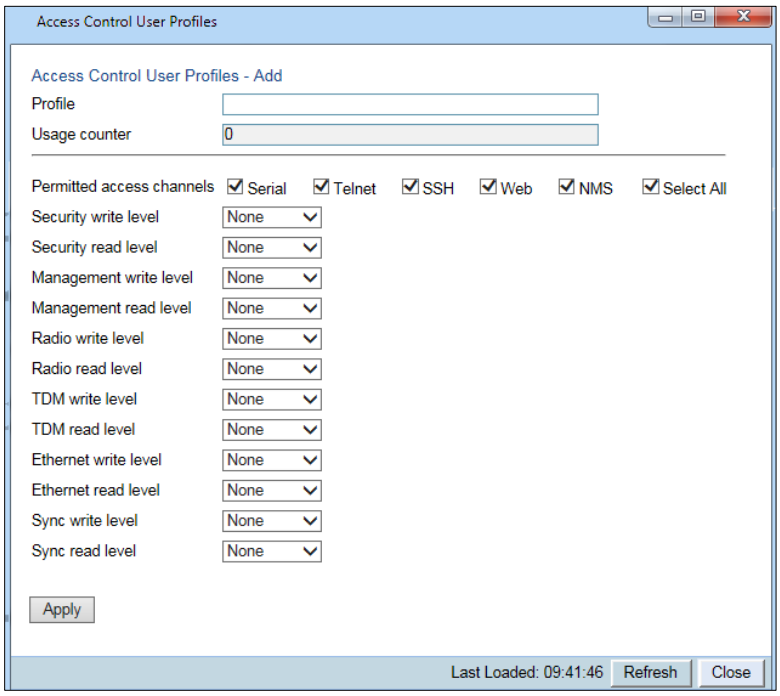
1. Select **Platform > Security > Access Control > User Profiles**. The Access Control User Profiles page opens.

Figure 461 Access Control User Profiles Page



2. Click **Add**. The Access Control User Profiles - Add page opens.

Figure 462 Access Control User Profiles - Add Page



3. In the **Profile** field, enter a name for the profile. The profile name can include up to 49 characters. Once you have created the user profile, you cannot change its name.

Note

The **Usage counter** field displays the number of users to whom the user profile is assigned.

4. In the **Permitted access channels** row, select the access channels the user will be permitted to use to access the system.
5. For each functionality group, select one of these options for write level and read level. All users with this profile will be assigned these access levels:
   - **None**
   - **Normal**
   - **Advanced**
6. Click **Apply**, then **Close**.

To view a user profile, click + next to the profile you want to view.

To edit a user profile, select the profile and click **Edit**. You can edit all of the profile parameters except the profile name.

To delete a user profile, select the profile and click **Delete**.

Note

You cannot delete a user profile if the profile is assigned to any users.

14.5.3 Adding User Accounts

You can configure up to 2,000 users. Each user has a user name, password, and user profile. The user profile defines a set of read and write permission levels per functionality group.

For devices with Unit Redundancy, user accounts are copied dynamically to the standby unit, without the need to perform a Copy-to-Mate operation. This includes both new user accounts and changes to existing user accounts.

Note that it may take up to a minute for new user account and changes to existing user accounts to be copied to the Standby unit. Therefore, if an unexpected switchover takes place less than one minute after adding or modifying a user account:

- Check that the user account is configured in the new Active unit. If it is not, reconfigure the user account and make sure at least one minute passes before another switchover occurs.
- If the user account is configured in the new Active unit, check that you can successfully log into the unit with that user. If you cannot, delete the user account and re-configure it in the new Active unit.

To add a new user:

1 Select **Platform** > **Security** > **User Access Control** > **User Accounts**. The Access Control User Accounts page opens.

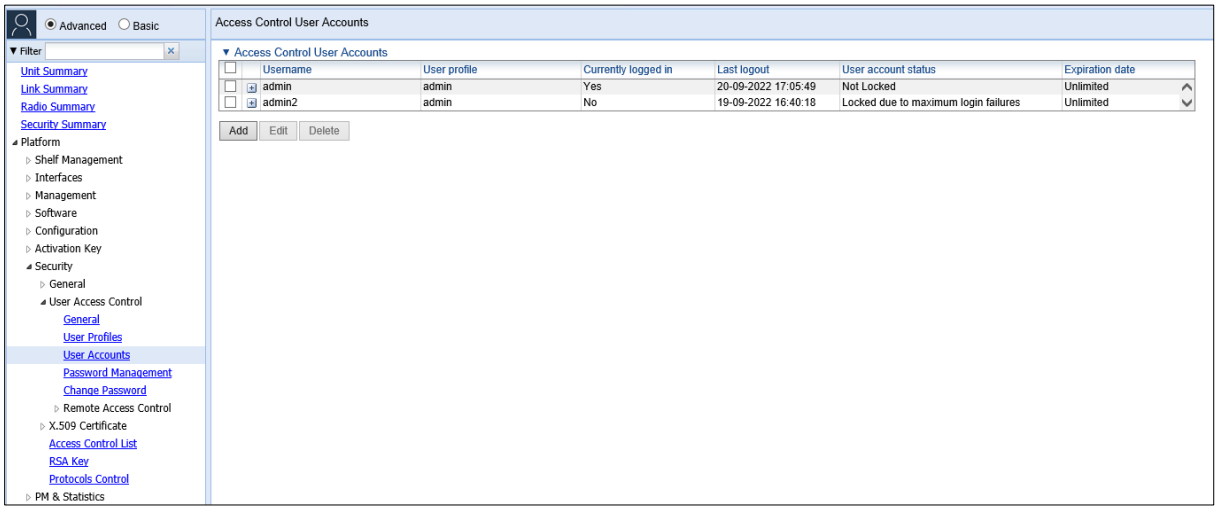


Figure 463: Access Control User Accounts Page

2 Click **Add**. The Access Control User Accounts - Add page opens.

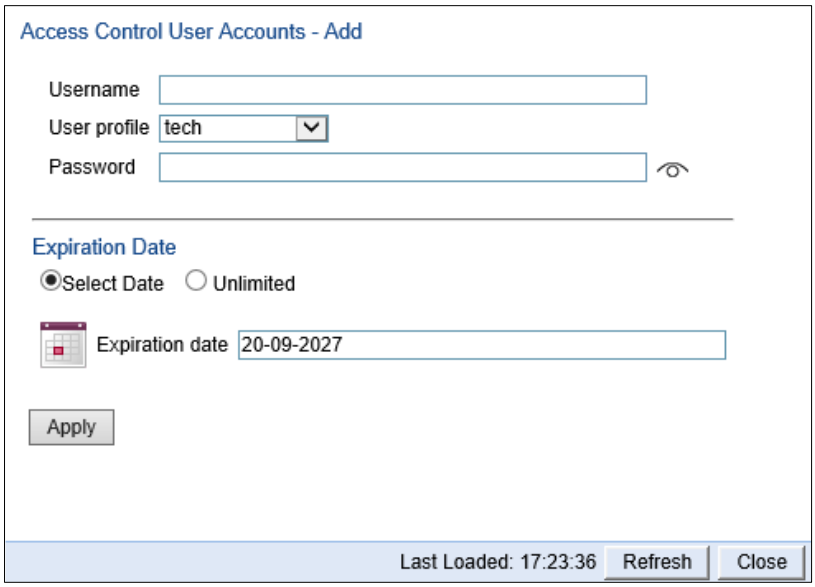


Figure 464: Access Control User Accounts - Add Page

3 In the **Username** field, enter a user name for the user. The user name can be up to 32 characters. User names cannot include special characters.

4 In the **User Profile** field, select a User Profile. The User Profile defines the user's access levels for functionality groups in the system.

5 In the **Password** field, enter a password for the user. If **Enforce Password Strength** is activated, the password must meet the following criteria:

- Password length must be at least eight characters.
- Password must include characters of at least three of the following character types: lower case letters, upper case letters, digits, and special characters.
- No character can be repeated three times, e.g., aaa, ###, 333.
- No more than two consecutive characters can be used, e.g., ABC, DEF, 123.
- The user name string cannot appear in the password, either in order or in reverse order. For example, if the user name is "admin", neither of the following passwords are allowed: *%Asreadmin!df23* and *%Asrenimda!df23*.

6 In the **Expiration date** field, select from the following options:

- To configure an expiration date for the user, select **Select Date**, then click the calendar icon and select a date, or enter a date in the format dd-mm-yyyy. The latest date that can be configured is 30-12-2037.
- To configure the user with no expiration date, select **Unlimited**.

In addition to the configurable parameters described above, the Access Control User Accounts page displays the following information for each user:

- **Currently Logged In** – Indicates whether the user is currently logged into the system (Yes/No).
- **Last Logout** – The date and time the user most recently logged out of the system.

To edit a user's account details, select the user and click **Edit**. You can edit all of the user account parameters except the **User name** and **password**.

To add a user, click **Add**.

To delete a user, select the user and click **Delete**.

14.5.4 Editing and Blocking Users

To block a user, or edit the Profile or Expiration Date:

1 Select **Platform** > **Security** > **User Access Control** > **User Accounts**. The Access Control User Accounts page opens.
2 Select the user and click **Edit**. The Access Control User Accounts - Edit page opens.

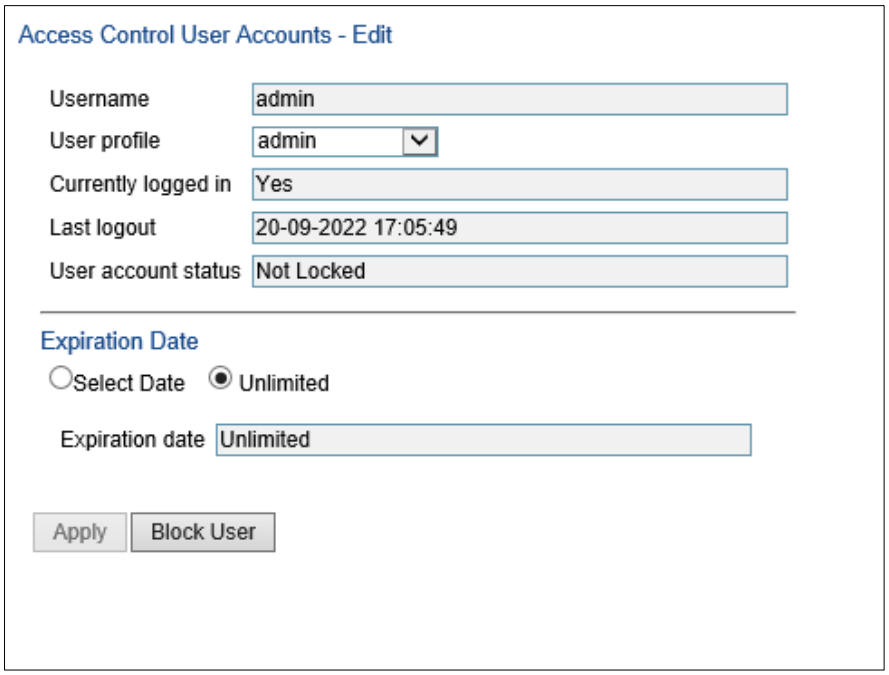


Figure 465: Access Control User Accounts - Edit Page

3 To block a user, click **Block User**. You can use this option to block a user temporarily, without deleting the user from the system. If you block a user while the user is logged into the system, the user will be automatically logged out of the system within 30 seconds.
When you block a user, the User account status is set to **Locked due to configuration**, and an **Unblock User** button appears in place of the **Block User** button. To unblock the user, click **Unblock User**.

Note: Users can also be blocked by the system automatically for attempting to login to the system with incorrect credentials a user-configurable consecutive number of times. A user that is blocked as a result of consecutive login failures cannot be manually unblocked and must wait for the configured Blocking Period to expire.

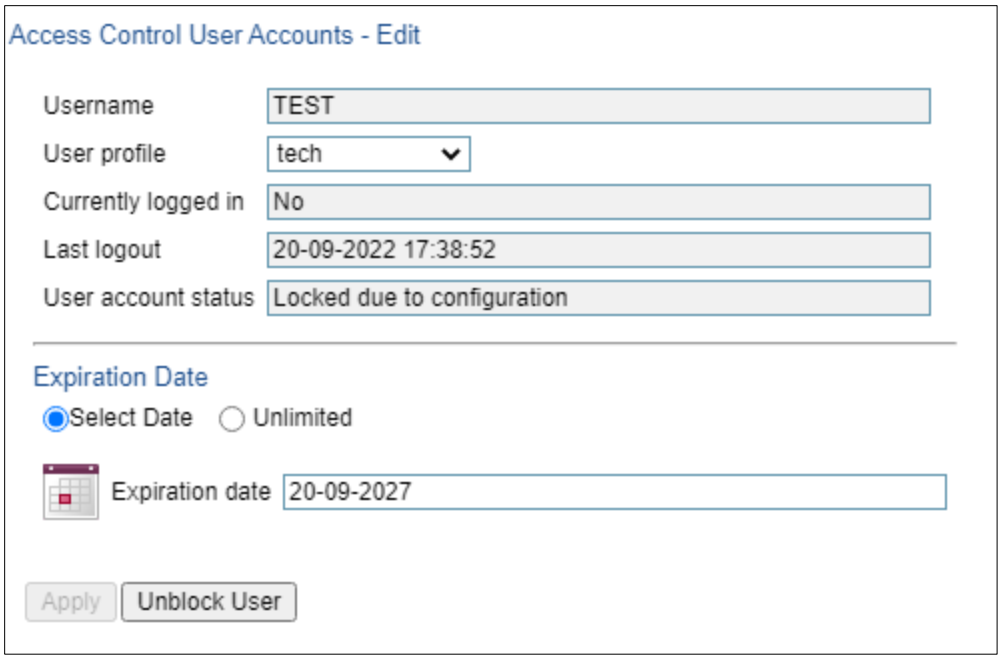


Figure 466: Access Control User Accounts - Edit Page (User Blocked)

4 Click **Apply**, then **Close**.

14.6 Configuring RADIUS

This section includes:

- RADIUS Overview
- Activating RADIUS Authentication
- Configuring the RADIUS Server Attributes
- Configuring a RADIUS Server

14.6.1 RADIUS Overview

The RADIUS protocol provides centralized user management services. PTP 850E supports RADIUS server and provides a RADIUS client for authentication and authorization. When RADIUS is enabled, a user attempting to log into the system from any access channel (CLI, WEB, NMS) is not authenticated locally. Instead, the user's credentials are sent to a centralized standard RADIUS server which indicates to the PTP 850E whether the user is known, and which privilege is to be given to the user.

The following RADIUS servers are supported:

- FreeRADIUS
- RADIUS on Windows Server (IAS)
    - Windows Server 2008

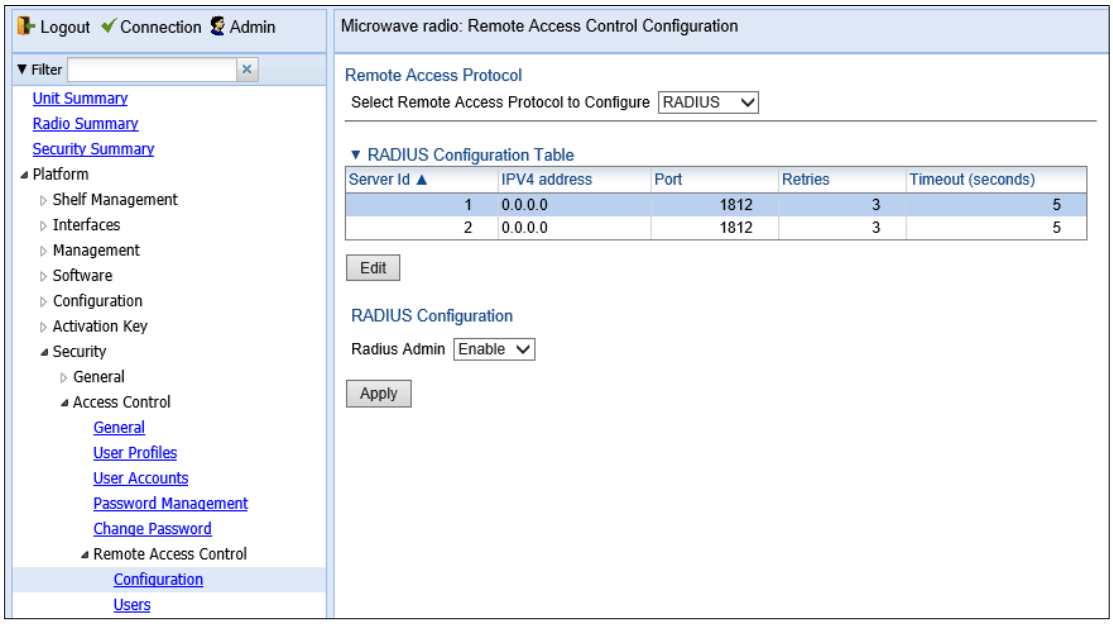
You can define up to two Radius servers. If you define two, one serves as the primary server and the other as the secondary server.

14.6.2 Activating RADIUS Authentication

To activate RADIUS authentication:

1. Select **Platform > Security > Access Control > Remote Access Control > Configuration**. The Remote Access Control Configuration page opens.

Figure 467 Remote Access Control Configuration Page (RADIUS)



2. In the **Select Remote Access Protocol to Configure** field, select **RADIUS**.
3. Configure the RADIUS server attributes. See Configuring the RADIUS Server Attributes.
4. In the **RADIUS Admin** field, select **Enable**.
5. Click **Apply**.



Note

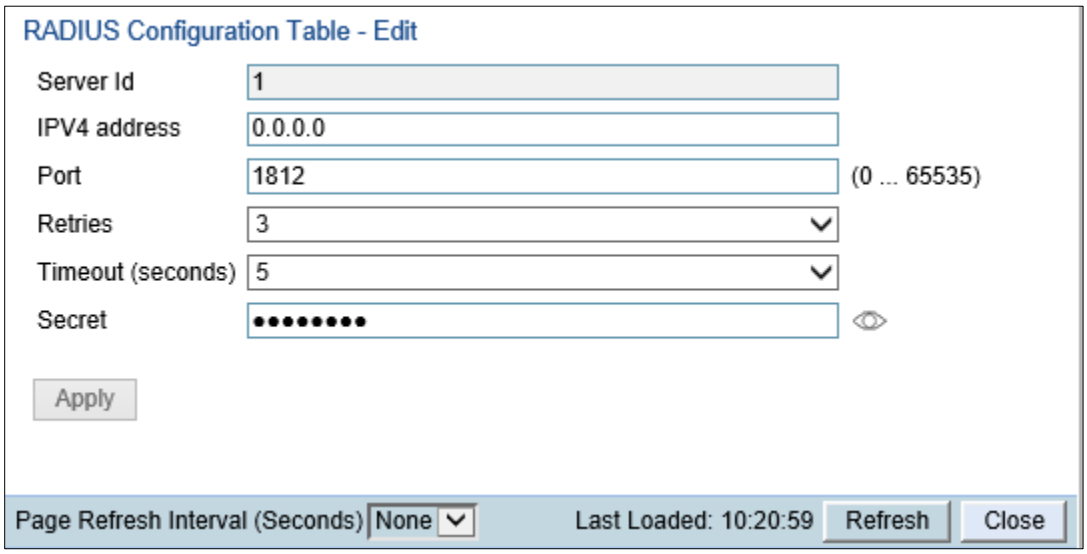
When the Protocol is changed, all active sessions are terminated when you click Apply.

14.6.3 Configuring the RADIUS Server Attributes

To configure the RADIUS server attributes:

1. Select **Platform > Security > Access Control > Remote Access Control > Configuration**. The Remote Access Control Configuration page opens. Verify that **RADIUS** is selected in the **Protocol** field.
2. In the Radius Configuration table, select the line that corresponds to the RADIUS server you want to configure:
   - Select **Server ID 1** to configure the Primary Radius server.
   - Select **Server ID 2** to configure the Secondary Radius server.
3. Click **Edit**. The Radius Configuration – Edit page opens.

Figure 468 Radius Configuration – Edit Page



4. In the **IPV4 address** field, enter the IP address of the RADIUS server.
5. In the **Port** field, enter the port of the RADIUS server.
6. In the **Retries** field, enter the number of times the unit will try to communicate with the RADIUS server before declaring the server to be unreachable.
7. In the **Timeout** field, enter the timeout (in seconds) that the agent will wait in each communication with the selected RADIUS server before retrying if no response is received.
8. In the **Secret** field, enter the shared secret of the RADIUS server. The string must be between 22-128 characters long.
    1 Click **Apply**, then **Close**.

In addition to the configurable parameters described above, the Remote Access Control Configuration page displays the following information for each RADIUS server:

- Server **Id** – The server ID of the Radius server:
    - 1 – The primary Radius server.
    - 2 – The secondary Radius server.

14.6.4 Configuring a RADIUS Server

If you want to use the PTP 850 RADIUS feature, you must first install a RADIUS server and configure it to work with the PTP 850 device.

The following subsections describe how to configure a Win2008 RADIUS server and a Linux FreeRADIUS server to work with an PTP 850. For the sake of simplicity, the subsections describe how to create three users: an Advanced user with Advanced read/write permissions, a Normal user with regular read/write permissions, and a Viewer user with no read/write permissions.



Note

These RADIUS servers are third-party software. The instructions provided in this section are illustrative only and are provided for the convenience of PTP 850E users. For exact and up-to-date instructions, we urge you to rely on the documentation provided with the RADIUS server you are using. Cambium is not responsible for syntax changes or variations in different GNU distributions.

Configuring a Win 2008 RADIUS Server

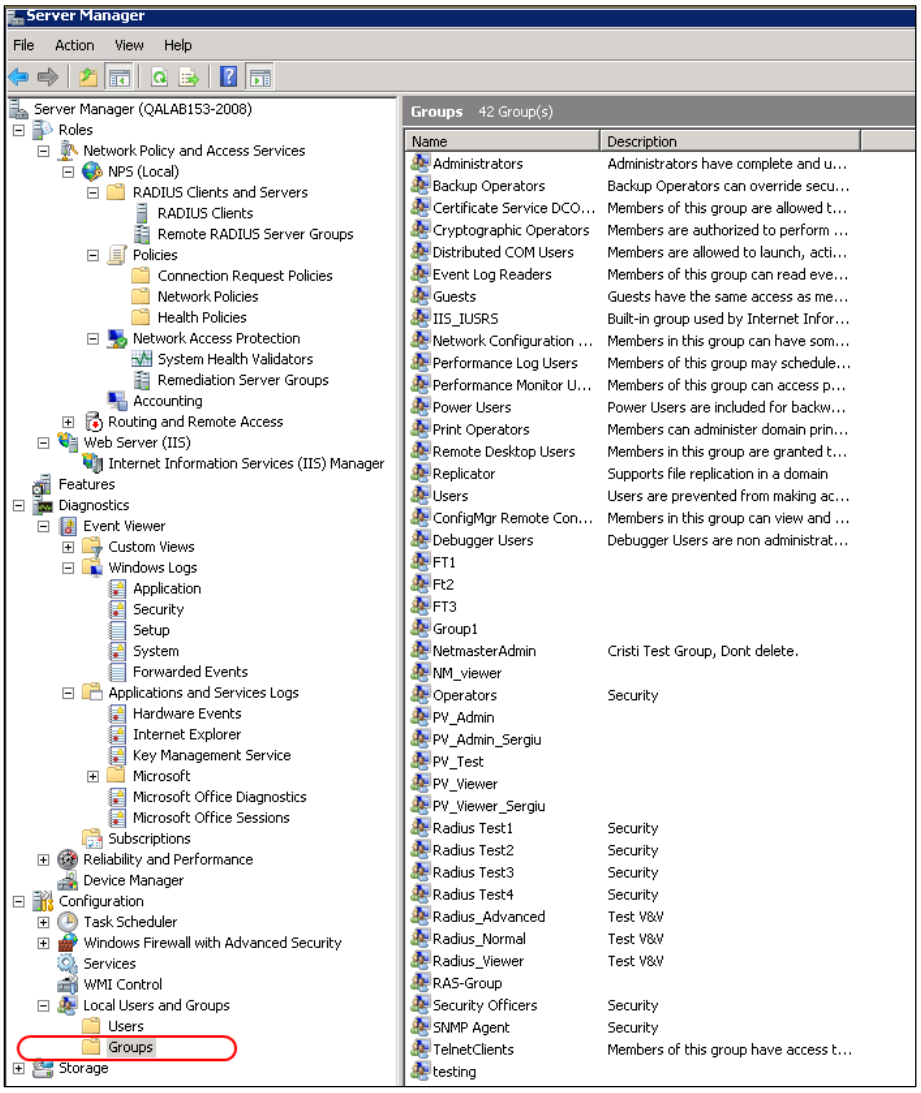
The following sub-sections describe how to configure a Win 2008 RADIUS Server to work with an PTP 850 device.

Step 1 – Creating Groups and Users

To create groups and users:

1. Create three user groups, as follows:
   I. In the Server Manager, navigate to **Configuration** > **Local Users and Groups**.
   II. Right click **Groups** and create the following three user groups:
   - Radius_Advanced
   - Radius_Normal
   - Radius_Viewer

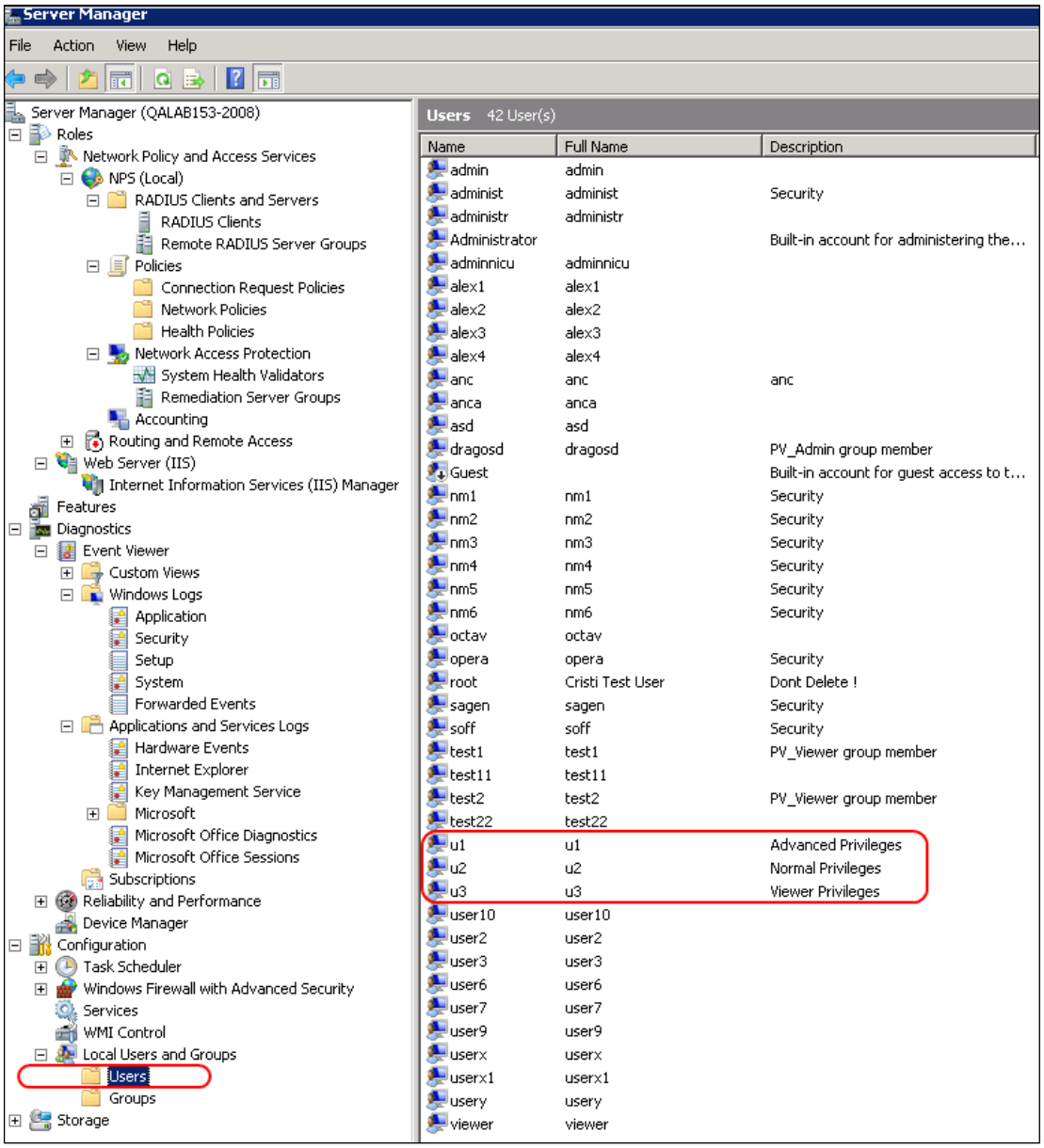
Figure 469 Server Manager – Creating User Groups



2. Create three users:

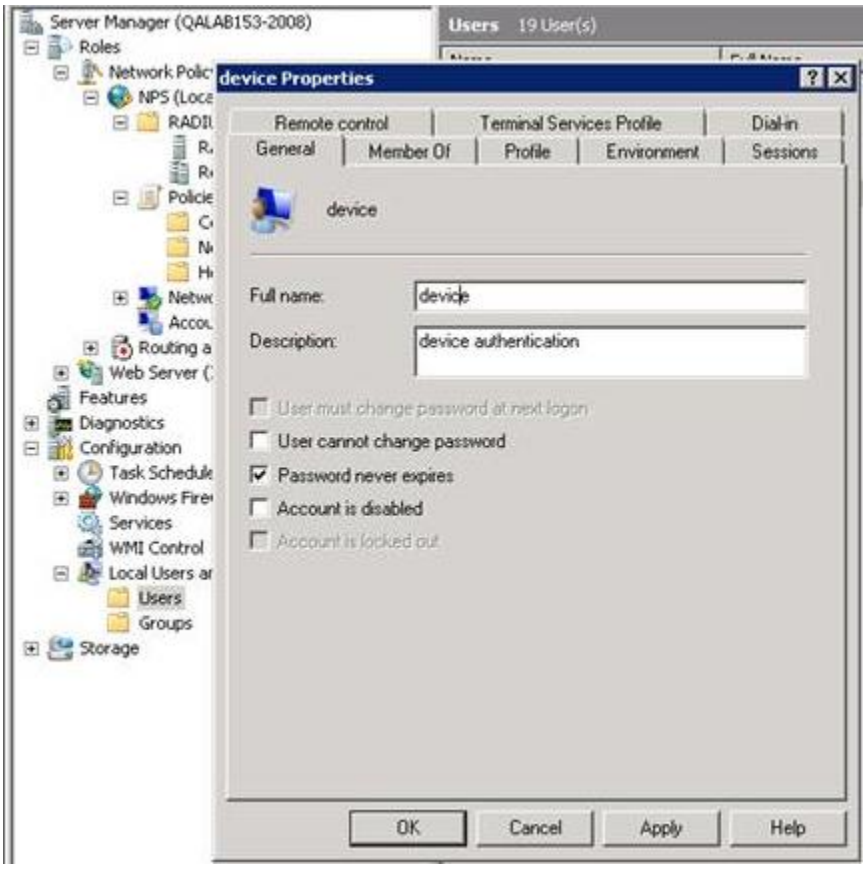
- u1
- u2
- u3

Figure 470 Server Manager – Creating Users



3. In the Device Properties – General tab, make sure to select **Password never expires**. If you leave the default setting (**User must change password at next logon**), authentication may fail.

Figure 471 Server Manager – User Password Settings



4. Attach each user to a group, as follows:

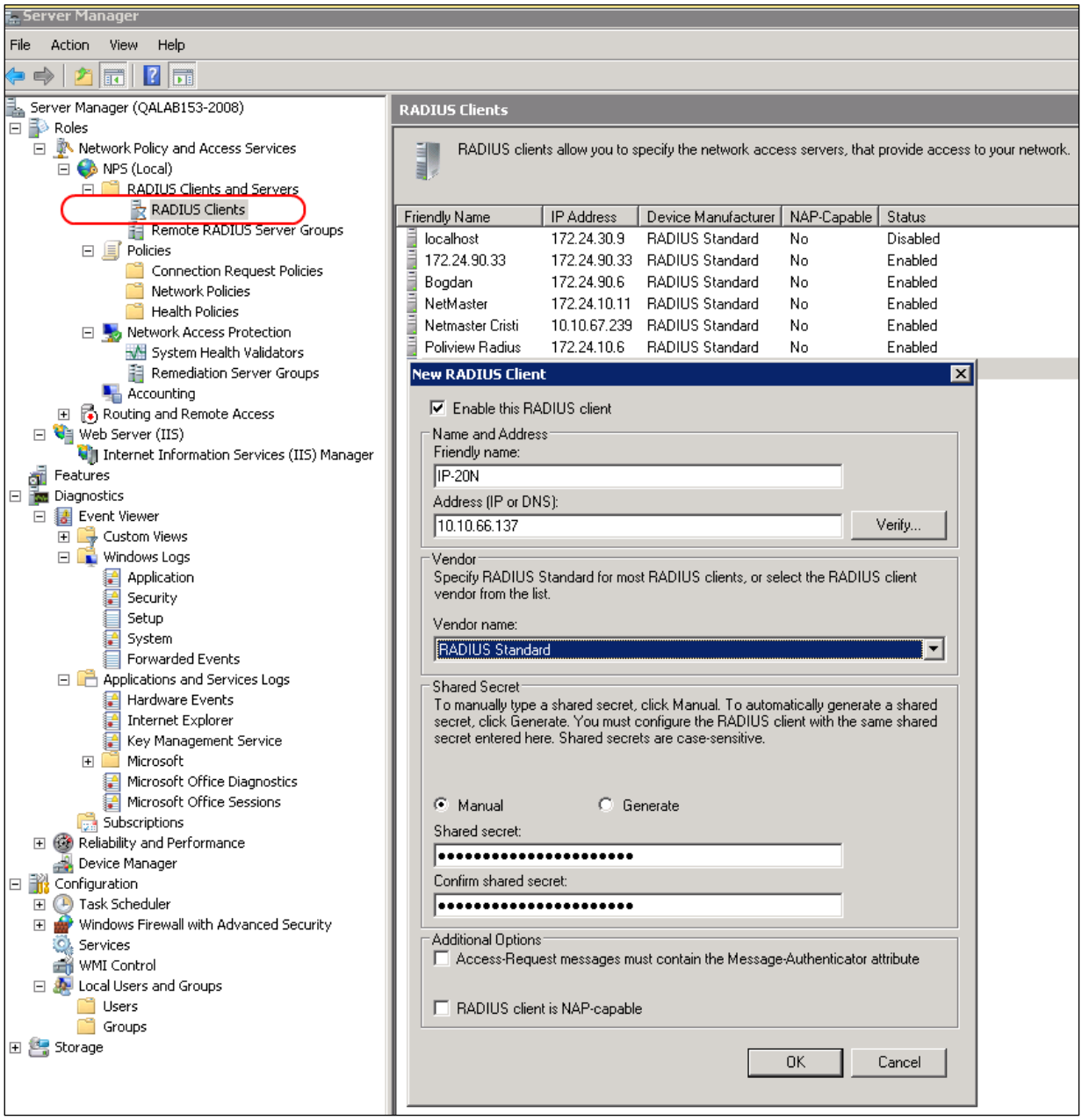
    - Attach u1 to Radius_Advanced
    - Attach u2 to Radius_Normal
    - Attach u3 to Radius_Viewer

Step 2 – Creating a RADIUS Client

Define the PTP 850 device as a RADIUS client, as follows:

1. In the Server Manager, navigate to Roles > Network Policy and Access Services > NPS (Local) > RADIUS Clients and Servers > RADIUS Clients.
2. Right-click **RADIUS Clients**, and select **New RADIUS Client**. The New RADIUS Client window appears.

Figure 472 Server Manager – Creating a RADIUS Client



3. In the New RADIUS Client window:

   I. Select the Enable this RADIUS client check box.
   II. Enter a descriptive **Friendly name** for the device, such as PTP 850.
   III. Enter the device IP **Address**.
   IV. Select RADIUS Standard as the Vendor name.
   V. In the **Shared Secret** section, select **Manual**, and enter a **Shared secret**, then enter it again in **Confirm shared secret**. Note down the secret because you will need to enter the same value in the **Secret** field of the Radius Configuration – Edit page.

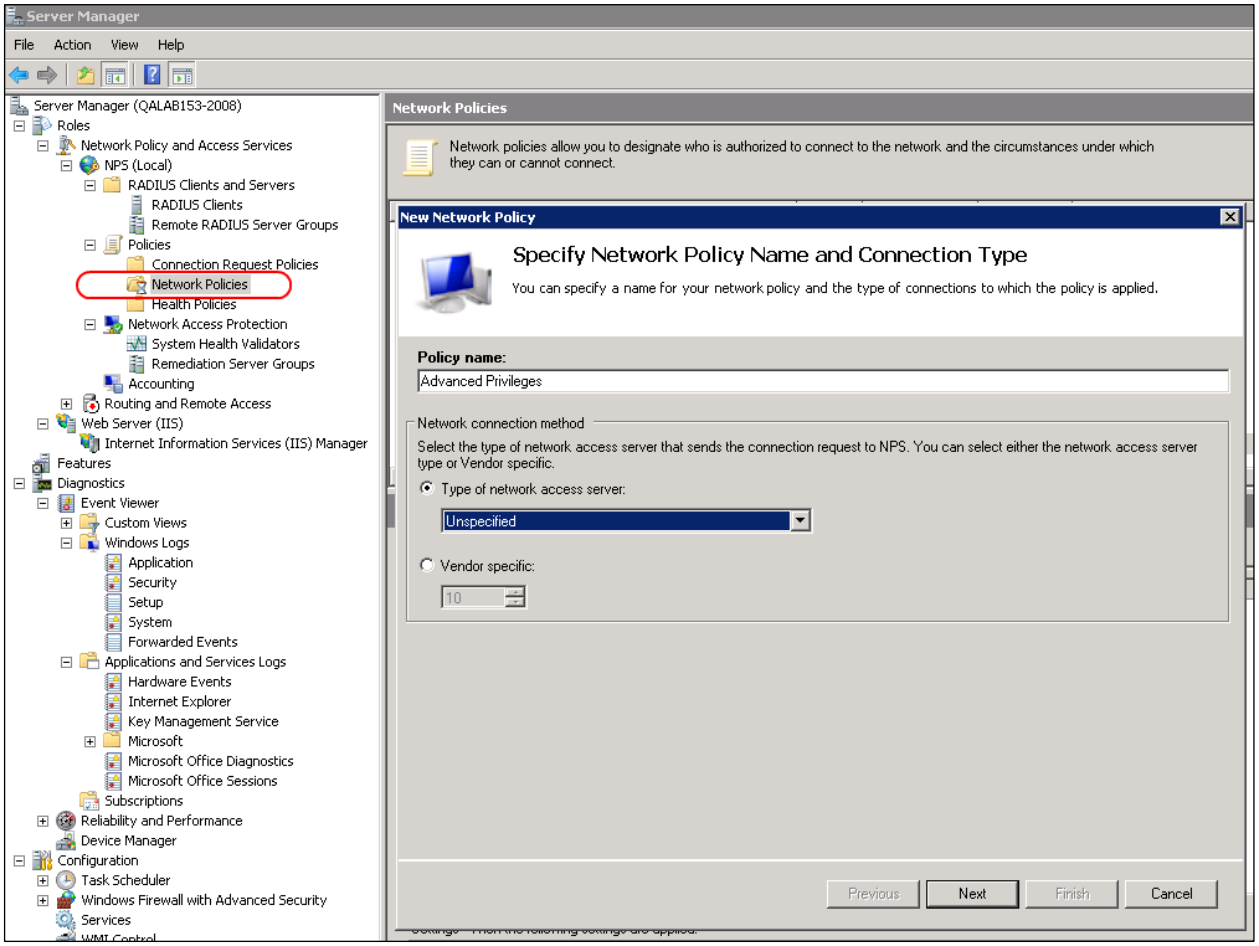
Step 3 – Creating a Network Policy

Create a network policy for each of the three groups you created: Radius_Advanced, Radius_Normal, Radius_Viewer. That is, follow the instructions in this section, for each of the three groups.

To create a network policy:

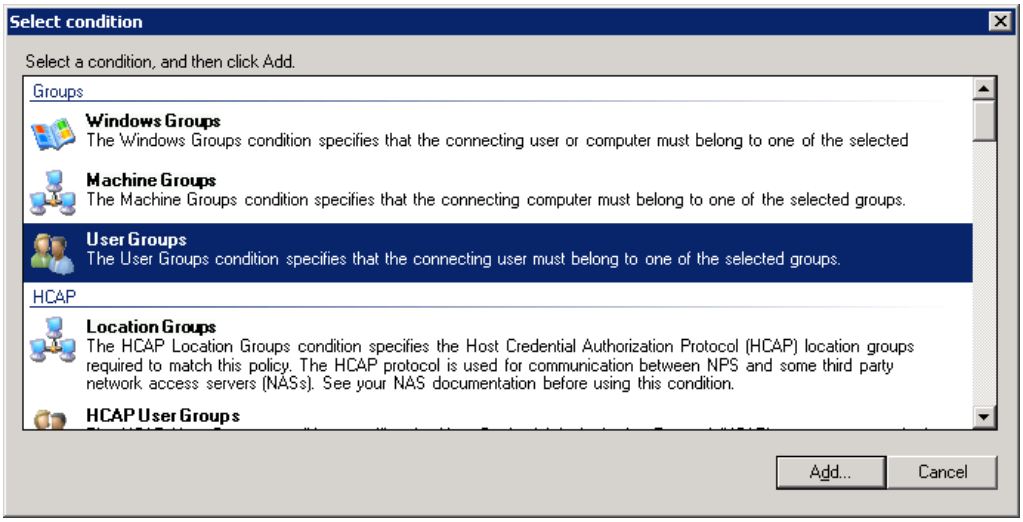
1. In the Server Manager, navigate to Roles > Network Policy and Access Service > NPS (Local) > Policies > Network Policies.
2. Right-click **Network Policies**, and select **New**. The New Network Policy wizard appears.
3. In the specify Network Policy Name and Connection Type, give the policy a descriptive name, indicating whether it is a policy for the Advanced, the Normal or the Viewer group.

Figure 473 Create Network Policy – Specify Name and Connection Type



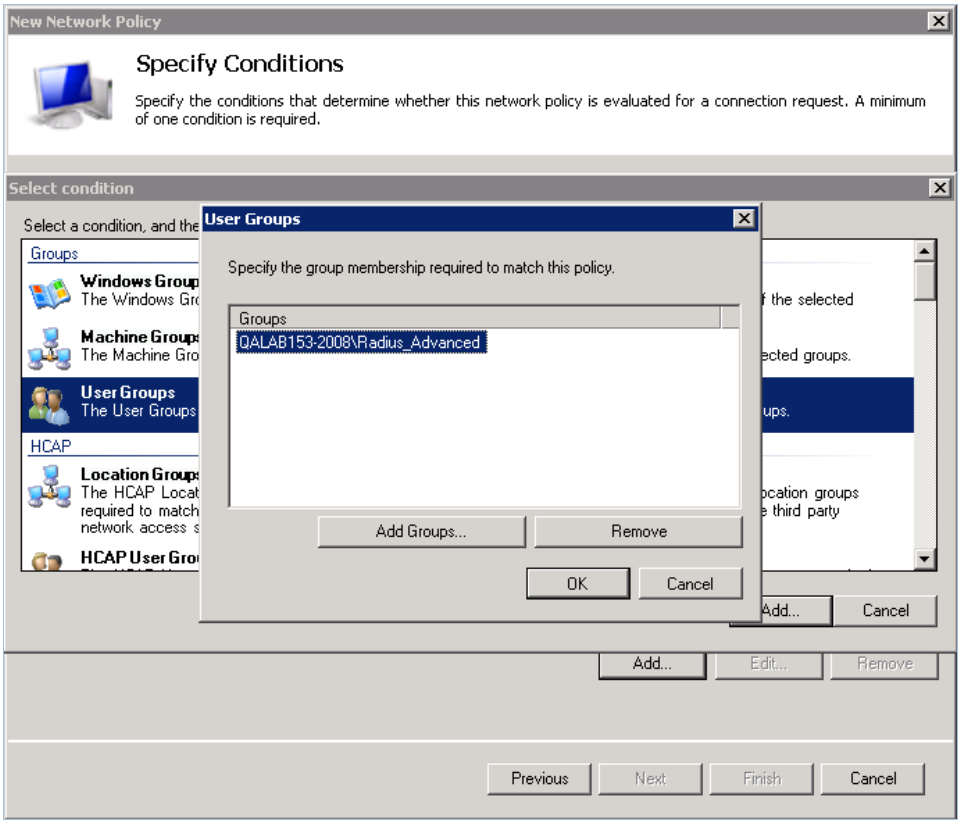
4. Click **Next**.
5. In the Specify Conditions window, click **Add.**
6. In the Select Condition window that appears, select the **User Groups** condition and click **Add**.

Figure 474 Create Network Policy – Select Condition



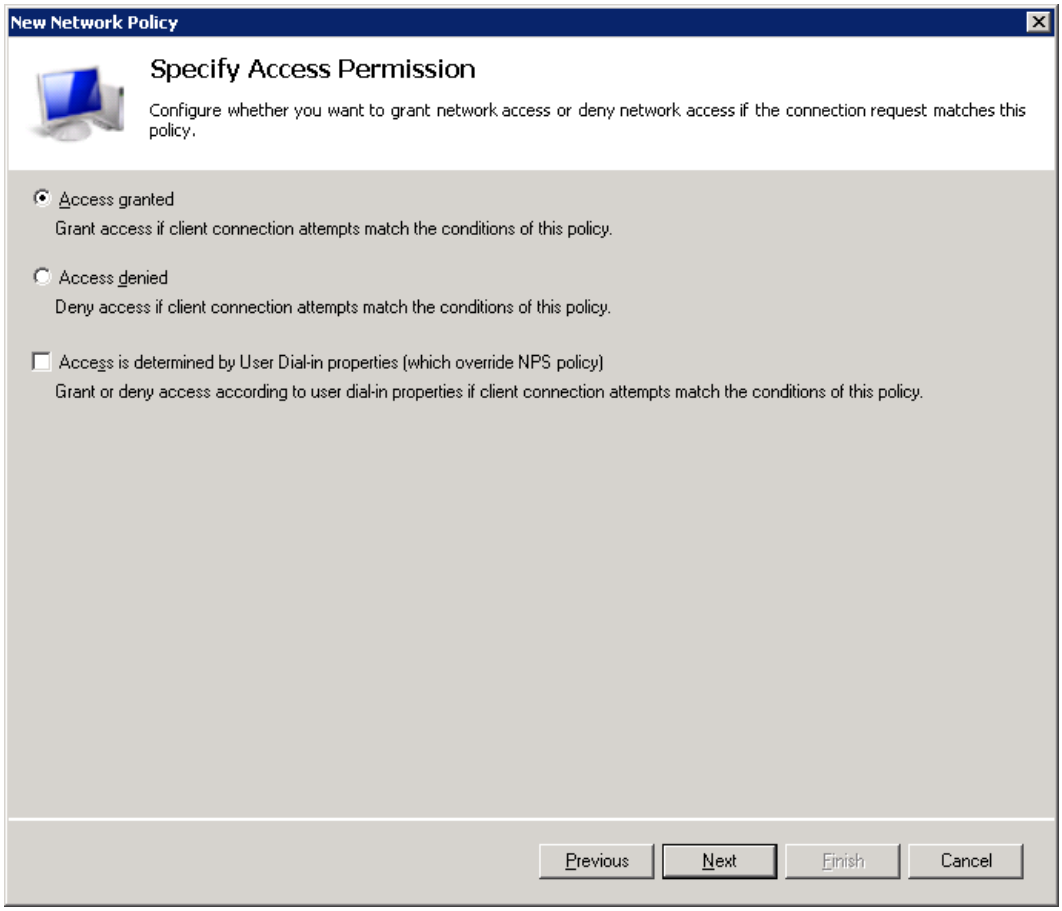
7. In the User Groups window that appears, click **Add Groups**.
8. In the Select Group window that appears, click **Advanced**.
9. In the Select Group window that appears, click **Find Now** to list all groups, and then select the appropriate group from the list: Radius_Advanced, Radius_Normal, or Radius_Viewer.
10. Click **OK**.

Figure 475 Create Network Policy – User Group added to Policy's Conditions



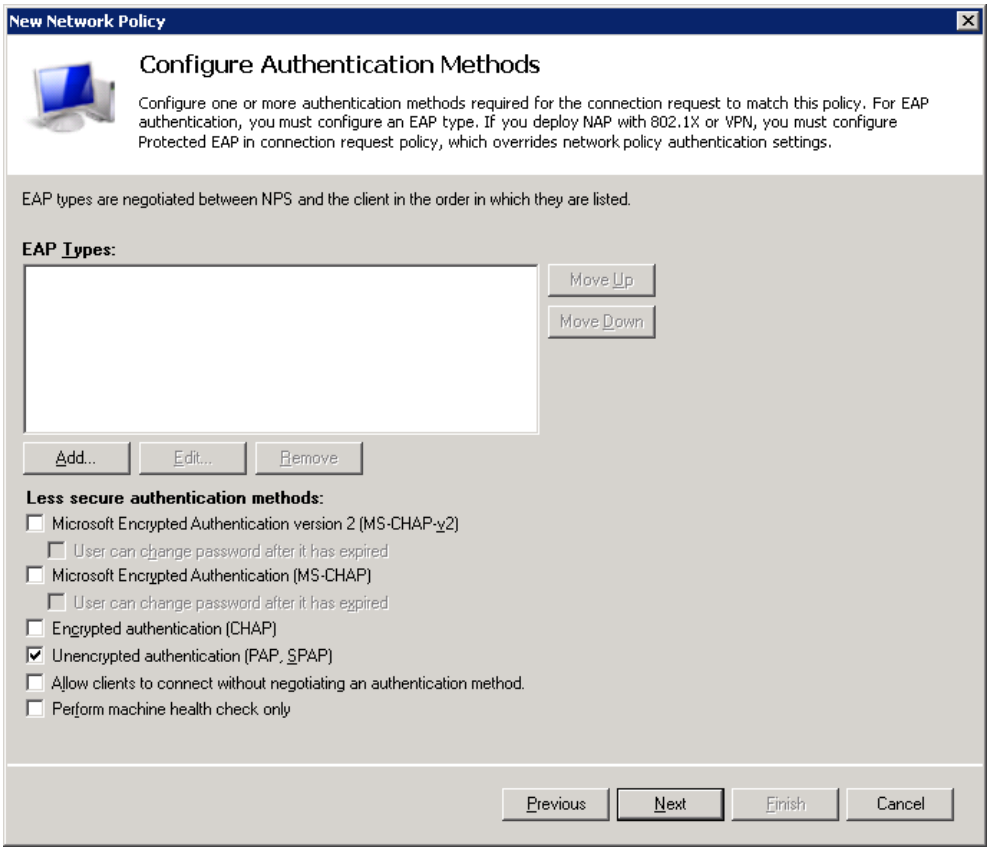
11. Click **OK** to save settings.
12. Click **Next**.
13. In the Specify Access Permission window that appears, select the **Access Granted** option.

Figure 476 Create Network Policy – Specifying Access Permission



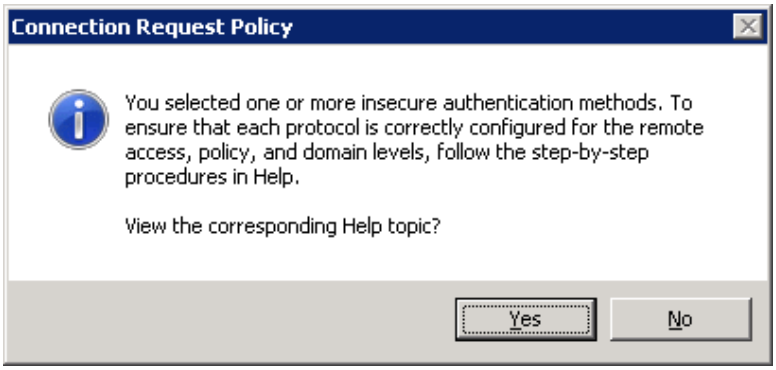
14. Click **Next**.
15. In the Configure Authentication Methods window that appears, make sure only the **Unencrypted Authentication (PAP, SPAP)** option is selected.

Figure 477 Create Network Policy – Configuring Authentication Methods



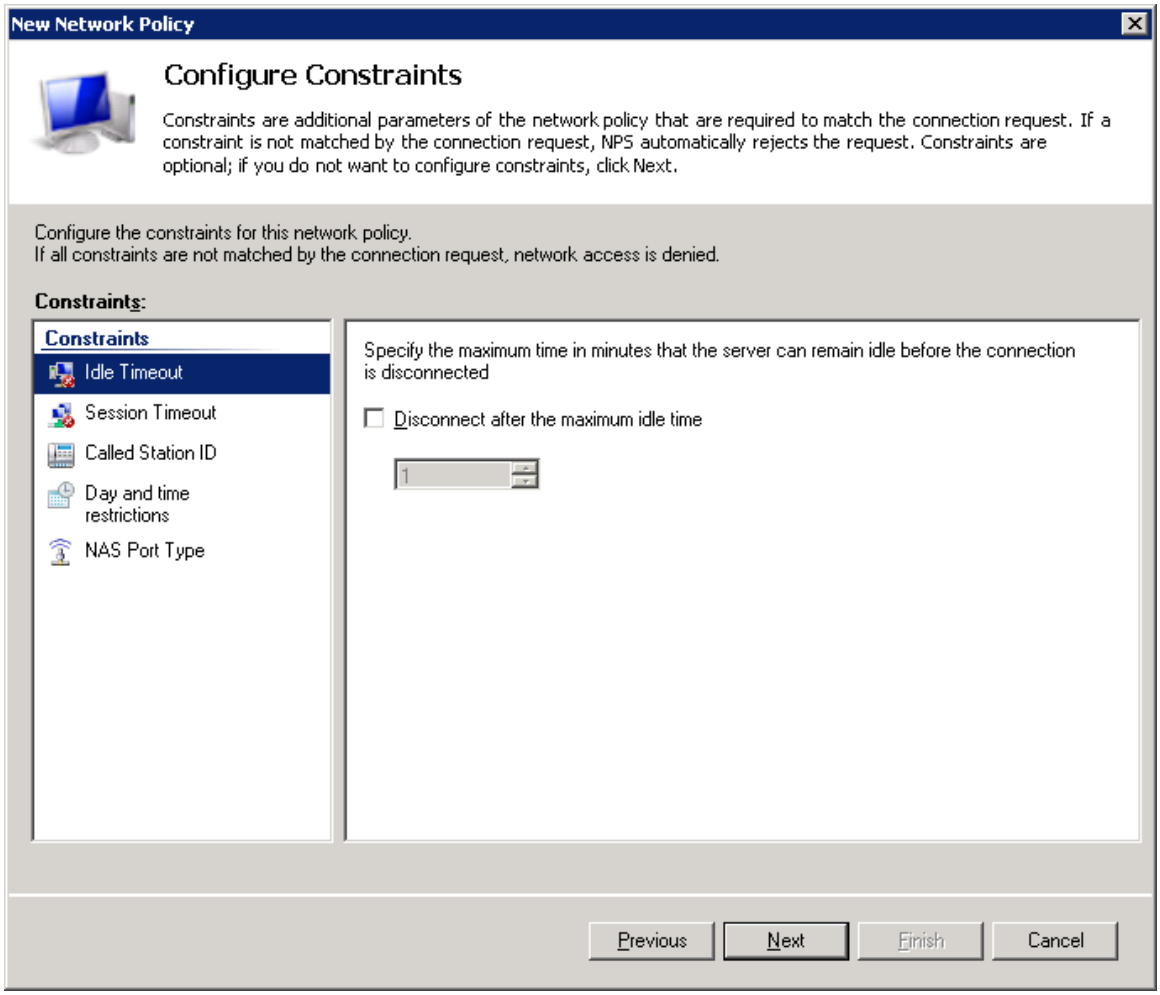
16. In the query window that appears, click **No**.

Figure 478 Create Network Policy – Insecure Authentication Method Query



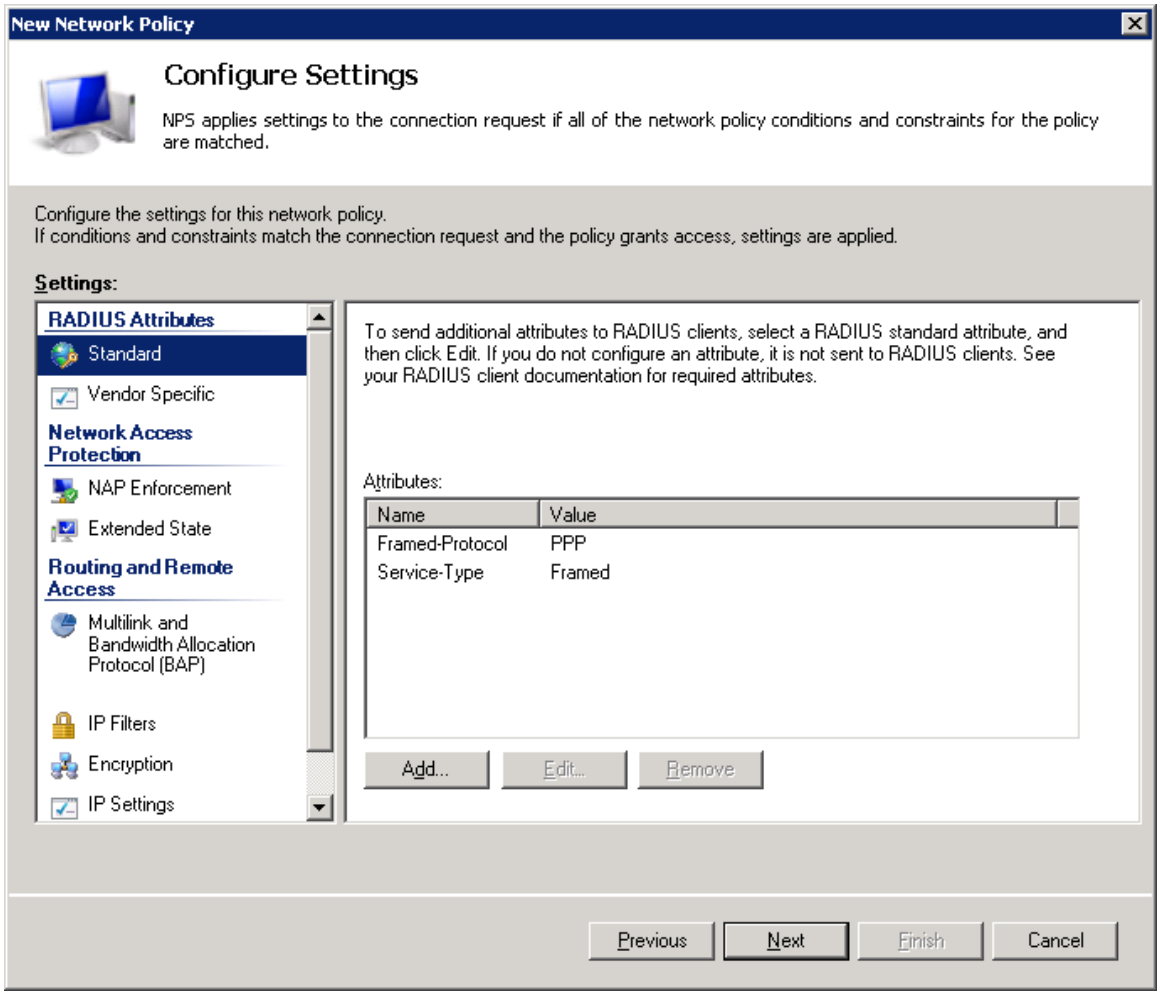
17. In the Configure Constraints window that appears, click **Next**

Figure 479 Create Network Policy – Configuring Constraints



18. In the Configure Settings window that appears:
    I. Remove all **Standard** RADIUS attributes. Make sure the Attributes table is empty.

Figure 480 Create Network Policy – Configuring Settings

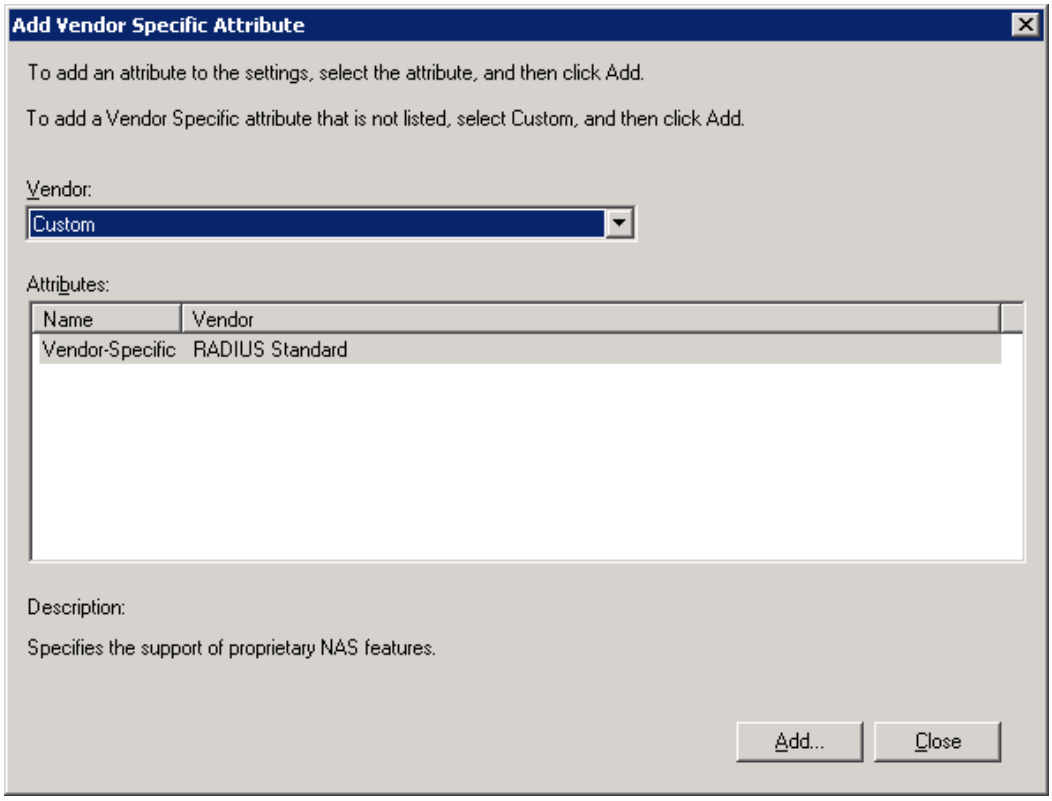


II. Select the **Vendor Specific** checkbox and click **Add** under the Attributes table.

19. In the Add Vendor Specific Attribute window that appears:

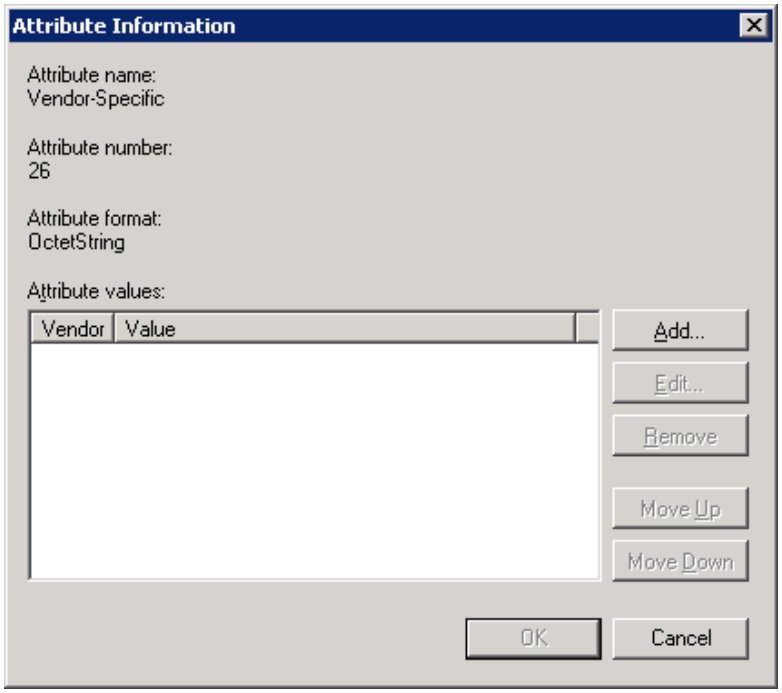
I. Select **Custom** in the **Vendor** drop down field.
II. Click Add.

Figure 481 Create Network Policy – Adding Vendor Specific Attributes



20. In the Attribute Information window that appears, click **Add**.

Figure 482 Create Network Policy – Selecting to Add Attribute Information

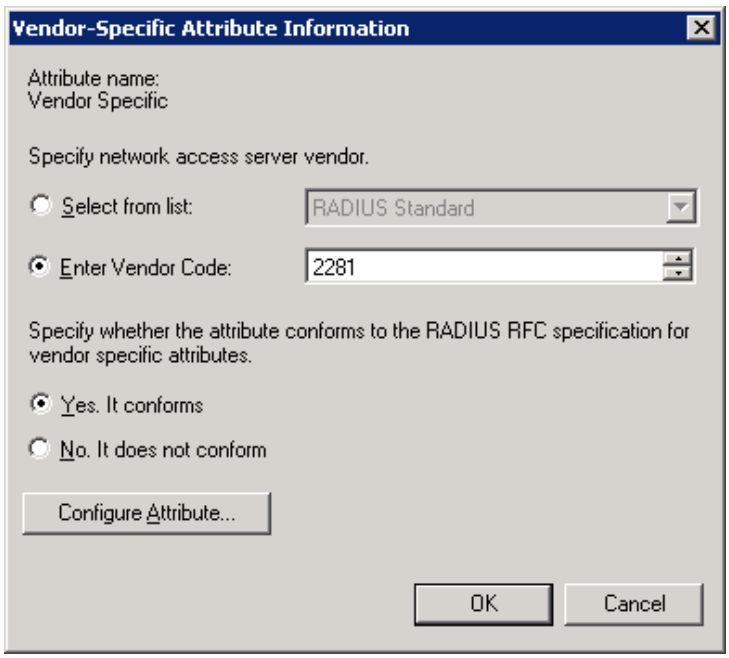


21. In the Vendor-Specific Attribute Information window that appears:

    i Select **Enter Vendor Code**.

ii Enter **2281** in the **Enter Vendor Code** field.
iii Select the option **Yes. It conforms**.
iv Click **Configure Attribute**.

Figure 483 Create Network Policy – Specifying the Vendor



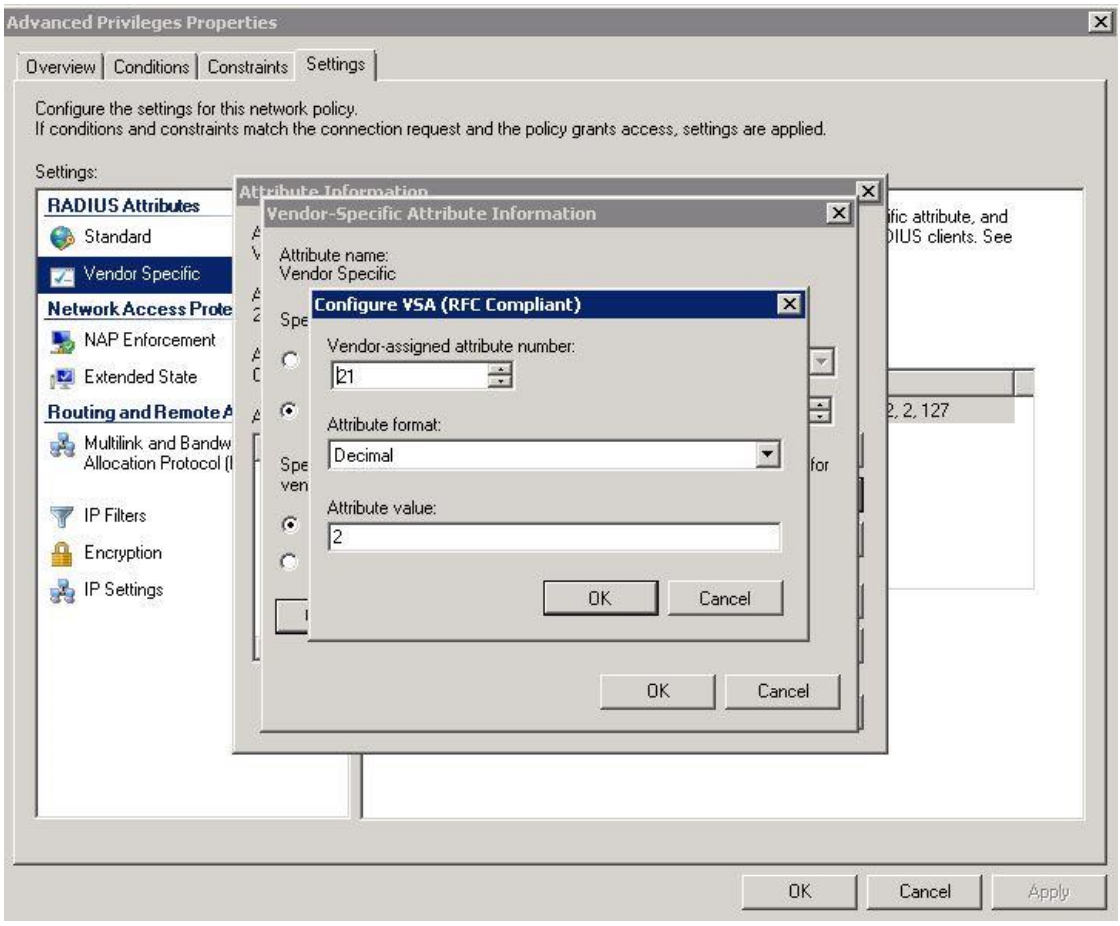
22. In the Configure VSA (RFC Compliant) window that appears, configure 13 attributes as follows:

i For **Vendor-assigned attribute number** from 21 till 32, select **Decimal** in the **Attribute format** field. These twelve attributes define the Read access level (None, Regular, or Advanced), and the Write access level (None, Regular, or Advanced) for each of the six functional groups (Ethernet, Management, Radio, Security, Sync, TDM). Therefore, in the **Attribute value** field enter the value corresponding to the access level you wish to permit to members of the group whose policy you are configuring, where:

- **2** = Advanced
- **1** = Regular
- **0** = None

Thus for example, enter 2 for all twelve attributes if you are configuring a policy for the Radius_Advanced group. This gives Advanced read permissions and Advanced write permissions, for all six functional groups, to the members of the Radius_Advanced group.

Figure 484 Create Network Policy – Configuring Vendor-Specific Attribute Information



ii For **Vendor-assigned attribute number** 50, select **Decimal** in the **Attribute format** field. The **Attribute value** of this attribute defines the access channel(s) permitted to members of the group whose policy you are configuring. The **Attribute value** is the sum of the values corresponding to the access channels you wish to permit, where the value for each access channel is:

- none=0
- serial=1
- telnet=2
- ssh=4
- web=8
- nms=16
- snmp=32
- snmpV3=64

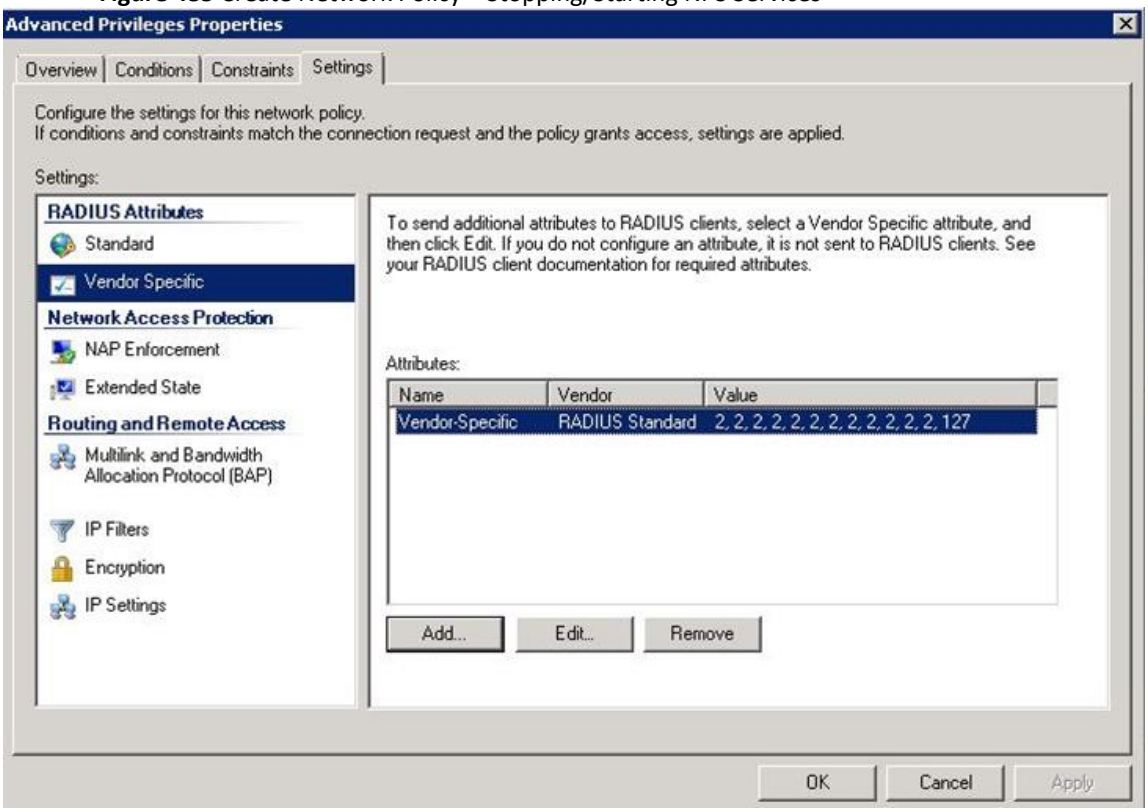
Thus for example, enter **127** to allow access from all channels: Serial + Telnet + SSH + Web + NMS + SNMP +SNMPv3;
Or enter **24** to allow access only from NMS + SNMP channels.

iii Click **OK**.

23. Click **OK**.

The following figure shows the Attributes table for the Radius_Advanced group, where access to the device is allowed from all channels.

Figure 485 Create Network Policy – Stopping/Starting NPS Services



Configuring a Linux FreeRADIUS Server

The following sub-sections describe how to configure a Linux FreeRADIUS server to work with an PTP 850E device.

To so do, you will need to modify the following files:

- `/etc/raddb/users`
- `/etc/raddb/clients.conf`
- `/usr/share/freeradius/dictionary.Cambium`
- `/etc/raddb/dictionary`

Step 1 – Creating Users

This step describes how to create the following three users:

- `u1 – with advanced read/write privileges, password 1111`
- `u2 – with normal read/write privileges, password 2222`
- `u3 – with no read/write privileges, password 3333`

To create these RADIUS users:

1. Add the users in the `/etc/raddb/users` file, using any editor you like, according to the following example:

```
# user1 - advanced privileges
u1   auth-type := local, Cleartext-Password := "1111"
    security-ro = advanced,
    security-wo = advanced,
    mng-ro = advanced,
    mng-wo = advanced,
    radio-ro = advanced,
    radio-wo = advanced,
    tdm-ro = advanced,
    tdm-wo = advanced,
    eth-ro = advanced,
    eth-wo = advanced,
    sync-ro = advanced,
    sync-wo = advanced,
    access_channel = u1accesschannel,
    fall-through = yes
# user2 - regular privileges
u2   auth-type := local, Cleartext-Password := "2222"
    security-ro = regular,
    security-wo = regular,
    mng-ro = regular,
    mng-wo = regular,
    radio-ro = regular,
    radio-wo = regular,
    tdm-ro = regular,
    tdm-wo = regular,
    eth-ro = regular,
    eth-wo = regular,
    sync-ro = regular,
    sync-wo = regular,
    access_channel = u2accesschannel,
    fall-through = yes
# user3 - no privilege (viewer)
u3   auth-type := local, Cleartext-Password := "3333"
```

```
    security-ro = none,
    security-wo = none,
    mng-ro = none,
    mng-wo = none,
    radio-ro = none,
    radio-wo = none,
    tdm-ro = none,
    tdm-wo = none,
    eth-ro = none,
    eth-wo = none,
    sync-ro = none,
    sync-wo = none,
    access_channel = u3accesschannel,
    fall-through = yes
```

1 Save the changes in the `/etc/raddb/users` file.

Step 2 – Defining the Permitted Access Channels

The `access_channel` of each user we configured in the `/etc/raddb/users` file, defines the channels through which that user is allowed to access the unit.

This is done by summing the values corresponding to the allowed channels, where the values are:

```
###   none          0
###   serial         1
###   telnet         2
###   ssh           4
###   web           8
###   nms           16
###   snmp          32
###   snmpV3         64
```

For example:

- The value 127 denotes permission to access the device from all channels: Serial + Telnet + SSH + Web + NMS + SNMP +SNMPv3
- The value 24 indicates permission to access the device only from the Web + NMS channels.

To define each user's access channels:

1 In the `usr/share/freeradius/dictionary.Cambium` file, configure the values of the access channels according to the following example:

```
###  access channel for u1
user:serial+telnet+ssh+web+nms+snmp+snmpV4
```

```
VALUE   ACCESS_CHANNEL      u1accesschannel      127
```

2 Save the changes to the `usr/share/freeradius/dictionary.Cambium` file.

Step 3 – Specifying the RADIUS client

This step describes how to define a device as a RADIUS client. The RADIUS server accepts attempts to connect to a device only if that is device is defined as a RADIUS client.

To define a device as a RADIUS client:

1. In the `/etc/raddb/clients.conf` file, add the device according to the following example.

   - The example shows how to add an PTP 850E device with IP address 192.168.1.118:

     ```
     # PTP 850E
     client 192.168.1.118 {
         secret      = default_not_applicable
         shortname    = Cambium-PTP 850E
     }
     ```

   - Keep in mind:
     - The secret must be between 22 and 128 characters long. Note down the secret because you will need to enter the same value in the Secret field of the Radius Configuration – Edit page.
     - The shortname is not mandatory, but should be added, and should be different for each RADIUS client.

2. Save the changes to the `/etc/raddb/clients.conf` file.

Step 4 – Adding a call to the Cambium Dictionary File

To add a call to the Cambium dictionary file:

1. Add the following at the end of the `/etc/raddb/dictionary` file, using any editor you like:

   ```
   #include the dictionary.Cambium file
   $INCLUDE dictionary.Cambium
   ```

2. Save the changes in the `/etc/raddb/dictionary` file.



Note

Make sure to use absolute path mode if the target file is located in a different directory. For example: *$INCLUDE ../share/freeradius/dictionary.Cambium)*

Step 5 – Restarting the RADIUS server

After configuring all of the above, restart the RADIUS process.

To restart the RADIUS process:

1 Stop the process by entering:

```
killall -9 radiusd
```

2 Start the process running in the background by entering:

```
radius -X &
```



Note

To check the logs each time a user connects to the server, enter:
radius –X &.

14.7 Configuring TACACS+

This section includes:

- TACACS+ Overview
- Activating TACACS+ Authentication and Authorization
- Configuring the TACACS+ Server Attributes
- Configuring a TACACS+ Server

14.7.1 TACACS+ Overview

The TACACS+ protocol provides centralized user management services. TACACS+ separates the functions of Authentication, Authorization, and Accounting (AAA). It enables arbitrary length and content authentication exchanges, in order to support future authentication mechanisms. It is extensible to provide for site customization and future development features, and uses TCP to ensure reliable communication.

PTP 850 supports TACACS+ with authentication, authorization, and accounting. Using TACACS+, the PTP 850 device acts as the client, working with a TACACS+ server to authenticate and authorize users.

Note: PTP 850 supports session-based TACACS+ authorization, but not command-based.

When TACACS+ is enabled, a user attempting to log into the system from any access channel (CLI, WEB, NMS) is not authenticated locally. Instead, the user's credentials are sent to a centralized standard TACACS+ server which indicates to the PTP 850 device whether the user is known, and which privilege is to be given to the user. You must ensure that the user credentials defined in the TACACS+ servers are identical to the user credentials defined for the device. If they are not identical, the user will be unable to access the device locally in the event that all the defined TACACS+ servers are unavailable.

When a user successfully logs in or logs out of the device via TACACS+, the device sends an accounting packet to the TACACS+ server packet which contains the following information:

- User Name
- User IP Address
- Time and Date of Connection
- Connection port on the device

Note: This information is also written to the device's Security Log.

Cambium's TACACS+ solution is compliant with any standard TACACS+ server. Testing has been performed, and interoperability confirmed, with the following TACACS+ servers:

- Cisco ISE - Version 2.6.0.156
- Tacacs.net - Version 1.2
- tac_plus version F4.0.4.27a

You can define up to four TACACS+ servers. When a user attempts to log into the device, the device attempts to contact the first user-defined TACACS+ server to authenticate the user. If no response is received from the server within the user-defined timeout period (1-60 seconds), the device tries again to contact the server up to the user-configured number of retries (1-5). Then, if no response is received from the server, the device attempts to contact the second user-defined TACACS+ server.

If no response is received from any of the servers, the device performs user authentication locally, provided the user name and password are identical in the TACACS+ server and on the device. If the user name or password are not identical, the user will not be able to log in locally. After several unsuccessful attempts, the user will be blocked for the defined blocking period. See Configuring the General Access Control Parameters.

To change passwords on the TACACS+ servers and locally, an admin user must perform the following steps:

1 Change the passwords on the TACACS+ servers.
2 Connect to the device via TACACS+.
3 Disable TACACS+ on the device.
4 Change the passwords on the device.
5 Re-enable TACACS+ on the device.

14.7.2 Activating TACACS+ Authentication and Authorization

Before activating TACACS+, make sure to configure the TACACS+ servers and the TACACS+ server attributes. See:

- Configuring the TACACS+ Server Attributes
- Configuring a TACACS+ Server

The TACACS+ server configuration must be complete before you activate TACACS+ because as soon as you activate TACACS+ by clicking **Apply** at the end of this procedure, all active sessions are terminated and you must log in again via TACACS+.

To activate TACACS+ authentication:

1 Select **Platform > Security > User Access Control > Remote Access Control > Configuration**. The Remote Access Control Configuration page opens.

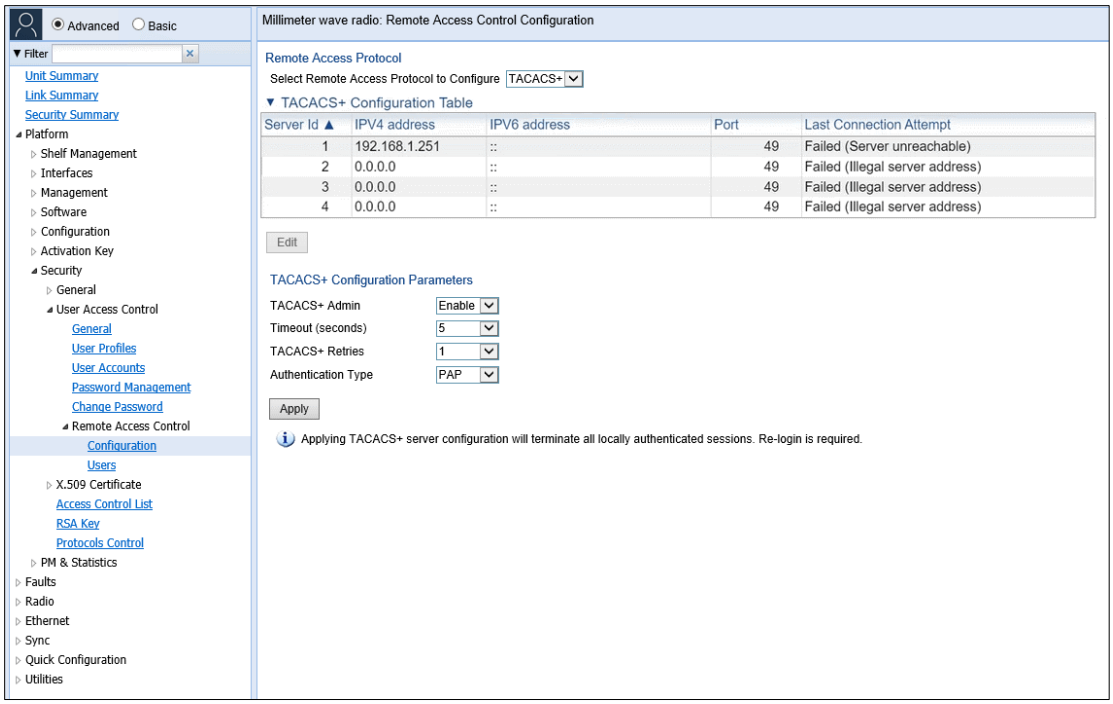


Figure 486: Remote Access Control Configuration Page (TACACS+)

2 In the **Select Remote Access Protocol to Configure** field, select **TACACS+**.
3 Configure the TACACS+ server attributes. See Configuring the TACACS+ Server Attributes.
4 In the **TACACS+ Admin** field, select **Enable**.
5 In the **Timeout** field, define a timeout of 1-60 seconds. The timeout determines how long to wait for a response from the TACACS+ server until the connection attempt times out. When a connection attempt times out, the device attempts to contact the next configured TACACS+ server.
6 In the **TACACS+ Retries** field, define the number of retries (1-5). This is the number of times the device will attempt to contact each server before moving on to the next server on the list. The default value is 1.
7 In the **Authentication Type** field, select from the following supported protocols:

- ASCII
- PAP (default)
- CHAP

8 Click **Apply**.

Note: When the Protocol is changed, all active sessions are terminated when you click **Apply**. Users must log in again via TACACS+.

14.7.3 Configuring the TACACS+ Server Attributes

To configure the TACACS+ server attributes:

1 Select **Platform > Security > User Access Control > Remote Access Control > Configuration**. The Remote Access Control Configuration page opens (Figure 486).

2 In the TACACS+ Configuration table, select the line that corresponds to the TACACS+ server you want to configure. When the device attempts to authenticate a user, the device attempts to contact the first server in the list (Server ID 1). If no response is received from the server within the user-defined timeout period:

- If the **TACACS+ Retries** field is set to 1, the device attempts to contact the second server in the list, then the third, then the fourth. If no response is received from any of the servers, the device performs user authentication locally.
- If the **TACACS+ Retries** field is set to a number greater than 1, the device attempts to contact the first server again, up to the configured number of retries. The device then repeats the process for the second server in the list, then the third, then the fourth. If no response is received from any of the servers, the device performs user authentication locally.

3 Click **Edit**. The TACACS+ Configuration Table – Edit page opens.

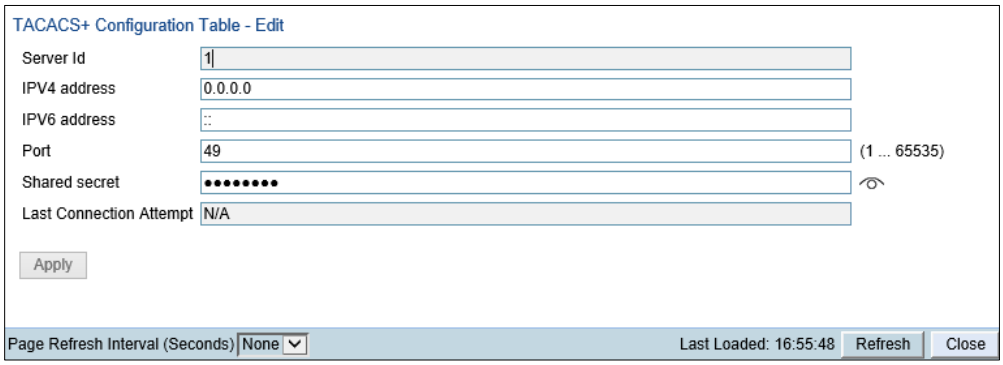


Figure 487: TACACS+ Configuration – Edit Page

4 In either the **IPV4 address** field or the **IPV6 address** field, enter the IP address of the TACACS+ server in IPV4 or IPV6 format.

Note: You cannot enter both an IPv4 and an IPv6 address, but you cannot leave either field blank. If you enter an IPv4 address, enter :: in the **IPV6 address** field. If you enter an IPv6 address, enter 0.0.0.0 in the **IPV4 address** field.

5 In the **Port** field, enter the port of the TACACS+ server. The default value is 49.

6 In the **Shared Secret** field, enter the shared secret of the TACACS+ server. The string must be between 6-63 characters long.

Note: This field should not be left empty unless necessary for debugging.

7 Click **Apply**, then **Close**.

In addition to the configurable parameters described above, the TACACS+ Configuration Table in the Remote Access Control Configuration page displays the following information for each TACACS+ server:

- **Server Id** – The server ID of the server (1-4).
- **Last Connection Attempt** – The connectivity status of the TACACS+ server in the last attempted connection:
  - **Succeeded** – The last connection attempt succeeded.
  - **Failed** – The last connection attempt failed. In the event of failure, this column displays the reason for the failure:
    - **Server unreachable** – This includes failure to reach the server for any reason, including an erroneous server address.
    - **Secret mismatch or server issue** – The shared secret configured on the device does not match the shared secret of the TACACS+ server.
    - **Illegal server address** – This includes instances in which the server address is set to its default (0.0.0.0) or another illegal IP address.

14.7.4 Configuring a TACACS+ Server

To work with TACACS+, you must configure at least one and up to four TACACS+ servers. For instructions, refer to the documentation for the server type you are using.

Use the following guidelines to ensure that the TACACS+ server will interoperate properly with the PTP 850 device.

- The TACACS+ server must be able to accept authentication modes ASCII, PAP, and CHAP.
- It is recommended to configure the privilege levels as follows, regardless of which type of TACACS+ server you are using:
  - service=microwave
  - protocol=ip
  - priv-lvl=0/1/15

    These privilege levels are mapped to local users as follows:
    - privilege level 0 = viewer
    - privilege level 1 = tech
  - privilege level 15 = admin
- Configure RBAC roles as follows. These roles are vendor-specific attributes. <value> can be replaced with *none*, *normal*, or *advanced*:

- service=microwave
- protocol=ip
- security_read=<value>
- security_write=<value>
- mng_read=<value>
- mng_write=<value>
- radio_read=<value>
- radio_write=<value>
- tdm_read=<value>
- tdm_write=<value>
- eth_read= <value>
- eth_write=<value>
- sync_read=<value>
- sync_write=<value>
- access_control=all_channels / web+ssh+telnet+serial+nms (any combination of these channels, separated by "+". For example: web+ssh. For privileges on all channels, use all_channels, which is the same as web+ssh+telnet+serial+nms.

Note: If a user logs in using a channel that is not included in the user's account (e.g., the user authenticates using the Web but access_control=ssh is configured in the server for the user's account), the user will log in successfully but no information will be displayed and the user will be unable to perform any actions on the unit.

- Privilege level overwrite has specific attributes and combines privilege levels and RBAC roles. Overwrite privilege levels can be configured as follows:

- Overwrite for privilege level 0:
  - service=microwave
  - protocol=ip
  - priv-lvl=0/1/15
  - security_read=advanced
  - security_write=advanced
- Overwrite for privilege level 1:
  - service=microwave
  - protocol=ip
  - priv-lvl=0/1/15
  - radio_read=none
  - radio_write=none
- Overwrite for privilege level 15:
  - service=microwave
  - protocol=ip
  - priv-lvl=0/1/15
  - security_read=normal
  - security_write=normal

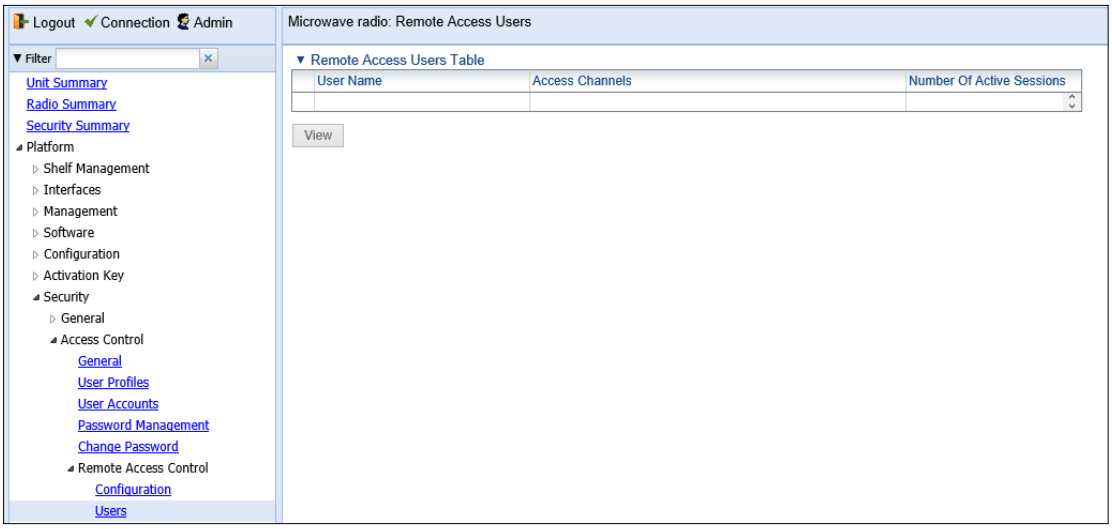
14.8 Viewing Remote Access User Connectivity and Permissions

You can view remote access user connectivity and permissions information for all RADIUS users currently connected.

To view remote access users:

1. Select **Platform** > **Security** > **Access Control** > **Remote Access Control** > **Users**. The Remote Access Users page opens.

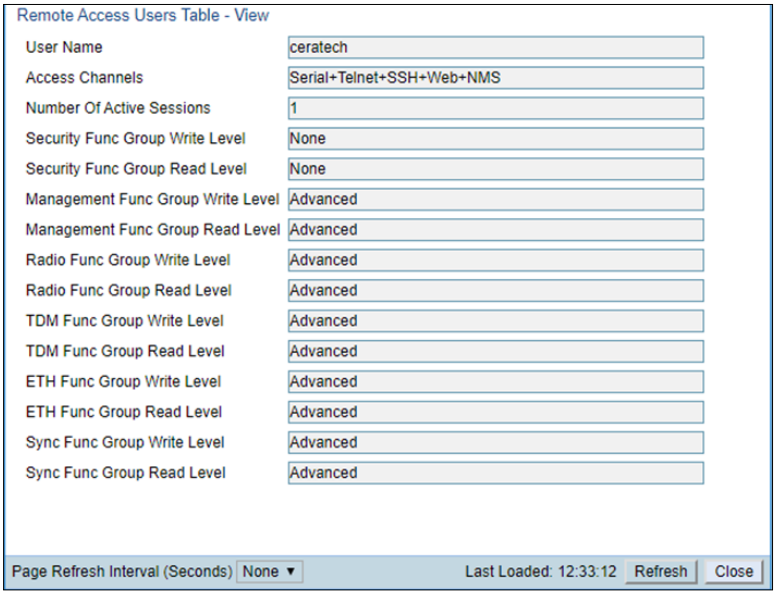
Figure 488 Remote Access Users Page



- The **User ID** column displays the user's name.
- The **Access Channels** column displays the access channels the user is allowed to use to access the unit.
- The **User Instances** column displays the number of open sessions the user currently has.

To view the user's authorized access levels, select the user and click **View**. The Remote Access Users Table – View page opens.

Figure 489 Remote Access Users Table - View



For each of the six functional groups (**Security**, **Management**, **Radio**, **TDM**, **Eth**, **Sync**), the page displays the Read access level (**None**, **Regular**, or **Advanced**), and the Write access level (**None**, **Regular**, or **Advanced**).

14.9 Configuring X.509 CSR Certificates

The web interface protocol for accessing PTP 850 can be configured to HTTP (default) or HTTPS. It cannot be set to both at the same time.

Before setting the protocol to HTTPS, you must:

1. Create and upload a CSR file. See Generating a Certificate Signing Request (CSR) File.
2. Download the certificate to the PTP 850 and install the certificate. See Downloading a Certificate.
3. Enable HTTPS. This must be performed via CLI. See Enabling HTTPS (CLI).

When uploading a CSR and downloading a certificate, the PTP 850 functions as an SFTP client. You must install SFTP server software on the PC or laptop you are using to perform the upload or download. For details, see Installing and Configuring an FTP or SFTP Server.



Note

For these operations, SFTP must be used.

14.9.1 Generating a Certificate Signing Request (CSR) File



Note

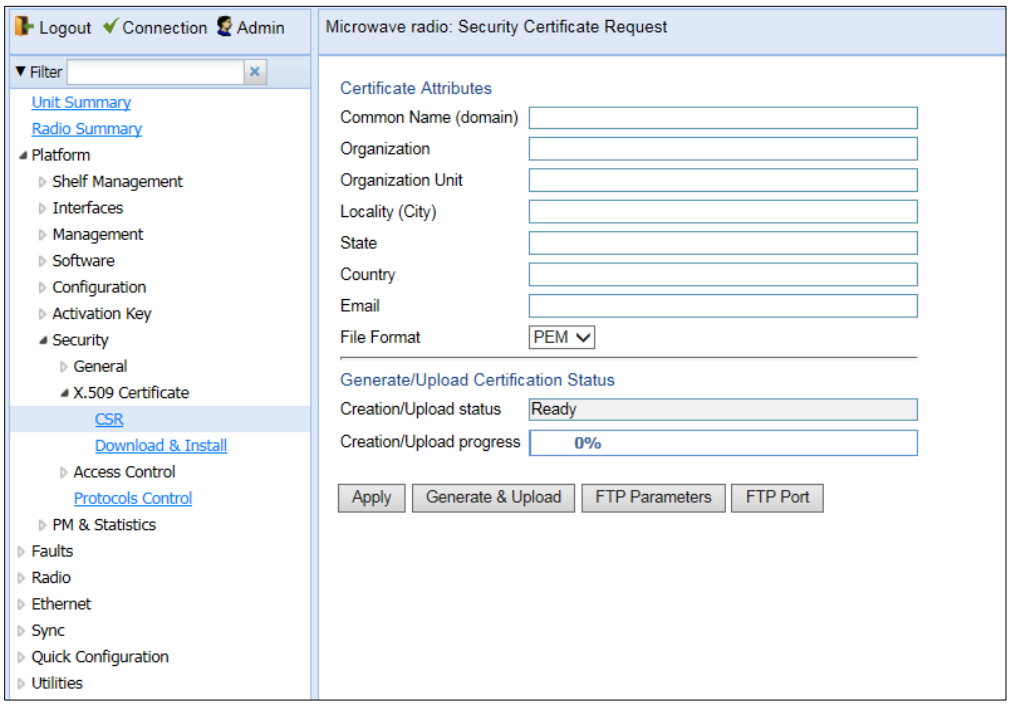
If you need a customized public RSA key, you must download and

install the RSA key first, before generating a CSR file. Otherwise, the CSR file will include the current public RSA key. See Downloading and Installing an RSA Key.

To generate a Certificate Signing Request (CSR) file:

1. Select **Platform** > **Security** > **X.509 Certificate** > **CSR**. The Security Certificate Request page opens.

Figure 490 Security Certificate Request Page



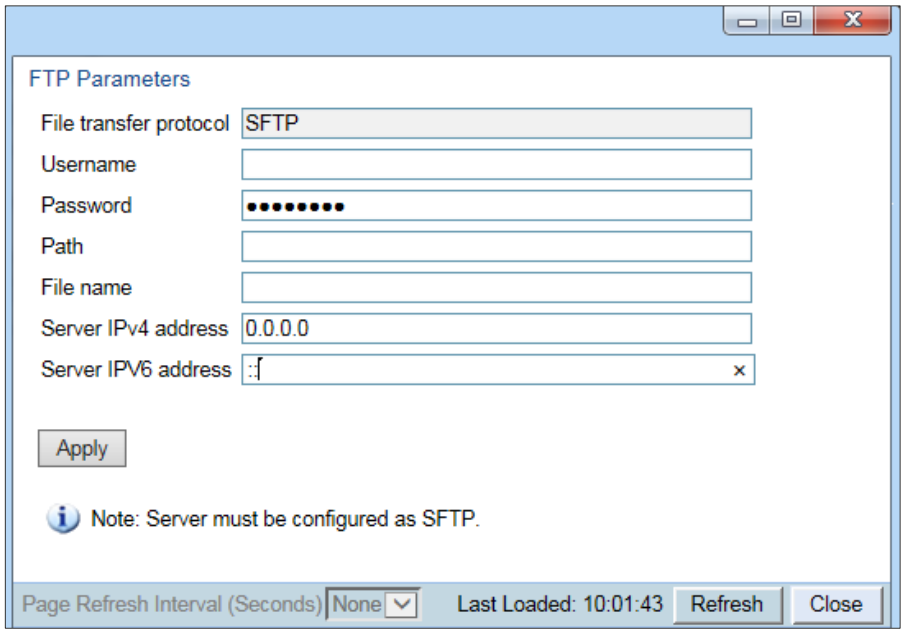
2. In the **Common Name** field, enter the fully–qualified domain name for your web server. You must enter the exact domain name.
3. In the **Organization** field, enter the exact legal name of your organization. Do not abbreviate.
4. In the **Organization Unit** field, enter the division of the organization that handles the certificate.
5. In the **Locality** field, enter the city in which the organization is legally located.
6. In the **State** field, enter the state, province, or region in which the organization is located. Do not abbreviate.
7. In the **Country** field, enter the two-letter ISO abbreviation for your country (e.g., US).
8. In the **Email** field, enter an e-mail address that can be used to contact your organization.
9. In the **File Format** field, select the **PEM** file format. Note that the **DER** file format is planned for future release.

Note

In this version, only PEM is supported.

10. Click **Apply** to save your settings.
11. Click **FTP Parameters** to display the FTP Parameters page.

Figure 491 FTP Parameters Page (Security Certificate Request)



12. In the **Username** field, enter the user name you configured in the SFTP server.
13. In the **Password** field, enter the password you configured in the SFTP server. If you did not configure a password for your SFTP user, simply leave this field blank.
14. In the **Path** field, enter the directory path to which you are uploading the CSR. Enter the path relative to the SFTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
15. In the **File name** field, enter the name you want to give to the exported CSR.
16. If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the SFTP server in the **Server IPV4 address** field. See Defining the IP Protocol Version for Initiating Communications.
17. If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the SFTP server in the **Server IPv6 address** field. See Defining the IP Protocol Version for Initiating Communications.
18. Click **Apply**, then Close, to save the FTP parameters and return to the Security Log Upload page.
19. Click **Generate & Upload**. The file is generated and uploaded.

The **CSR Status** field displays the status of any pending CSR generation and upload. Possible values are:

Ready – The default value, which appears when CSR generation and upload is in progress.

File-in-transfer – The upload operation is in progress.

Success – The file has been successfully uploaded.

Failure – The file was not successfully uploaded.

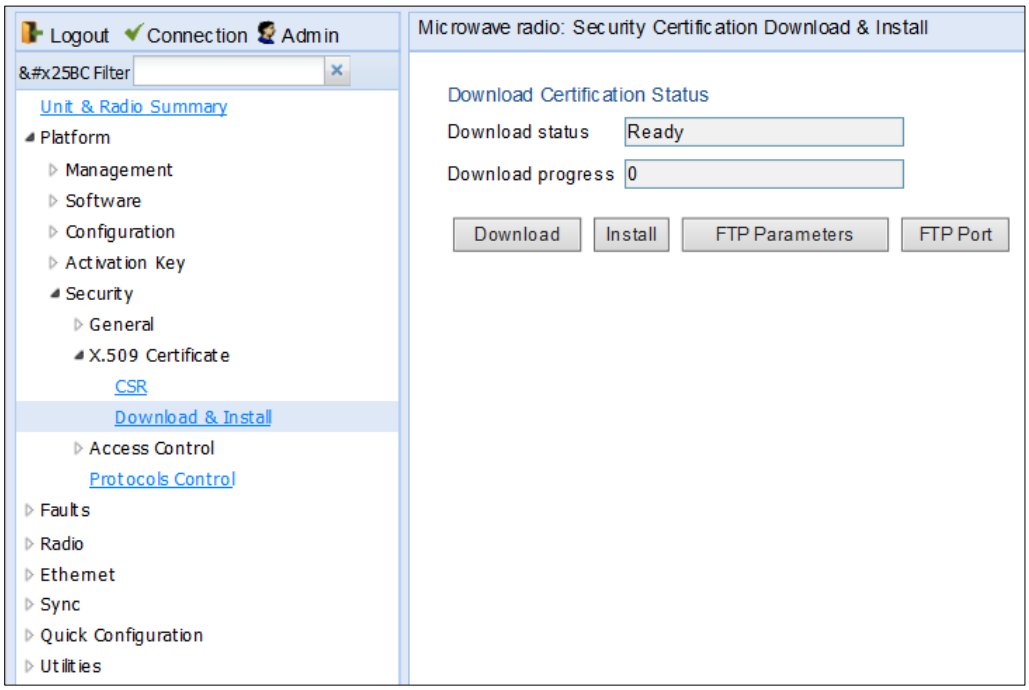
The **CSR Percentage** field displays the progress of any current CSR upload operation.

14.9.2 Downloading a Certificate

To download a certificate:

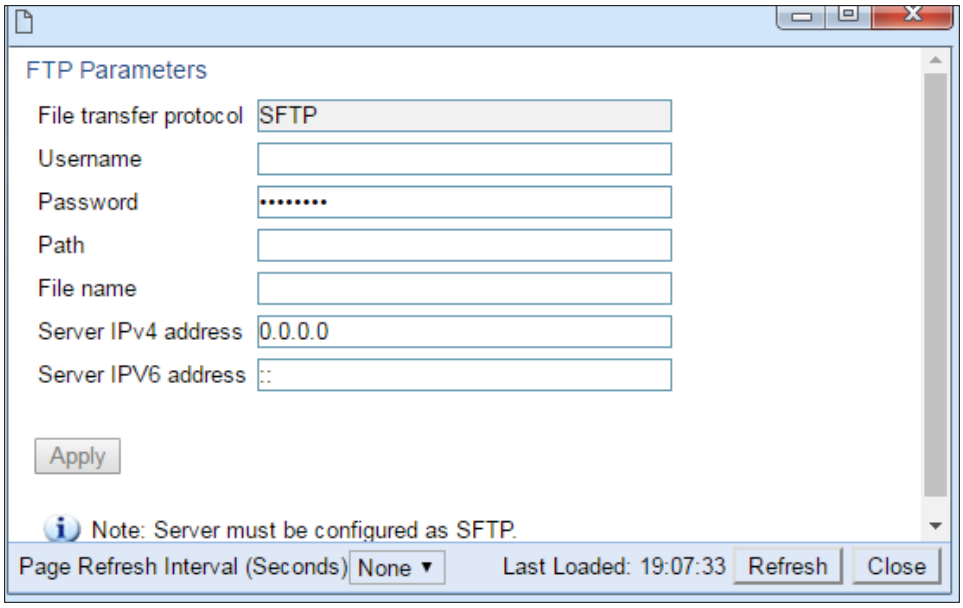
1. Select **Platform > Security > X.509 Certificate > Download & Install**. The Security Certification Download and Install page opens.

Figure 492 Security Certification Download and Install Page



2. Click **FTP Parameters** to display the FTP Parameters page

Figure 493 FTP Parameters Page (Security Certification Download & Install)



3. In the **User name for logging** field, enter the user name you configured in the SFTP server.
4. In the **User password to server** field, enter the password you configured in the SFTP server. If you did not configure a password for your SFTP user, simply leave this field blank.
5. In the **Path** field, enter the directory path from which you are uploading the certificate. Enter the path relative to the SFTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
6. In the **File Name** field, enter the certificate's file name in the SFTP server.
7. If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the SFTP server in the **Server IPV4 address** field. See Defining the IP Protocol Version for Initiating Communications.
8. If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the SFTP server in the **Server IPv6 address** field. See Defining the IP Protocol Version for Initiating Communications.
9. Click **Apply** to save your settings.
10. Click **Download**. The certificate is downloaded.
11. Click **Install**. The certificate is installed on the PTP 850.

14.10 Enabling HTTPS

By default, HTTP is used by PTP 850E as its web interface protocol.

To enable HTTPS instead of HTTP:

1 Select **Platform** > **Security** > **Protocols Control**. The Protocols Control page opens.
2 In the **HTTP protocol** field, select **HTTPS**.
3 Click **Apply**.



Note

Make sure you have installed a valid certificate in the PTP 850E before changing the web interface protocol to HTTPS. Failure to do this may prevent users from accessing the Web EMS.

14.11 Downloading and Installing an RSA Key

PTP 850 devices support RSA keys for communication using HTTPS and SSH protocol. The PTP 850 device comes with randomly generated default private and public RSA keys. However, you can replace the private key with a customer-defined private key. The corresponding RSA public key will be generated based on this private key. The file must be in PEM format. Supported RSA private key sizes are 2048, 4096, and 8192.

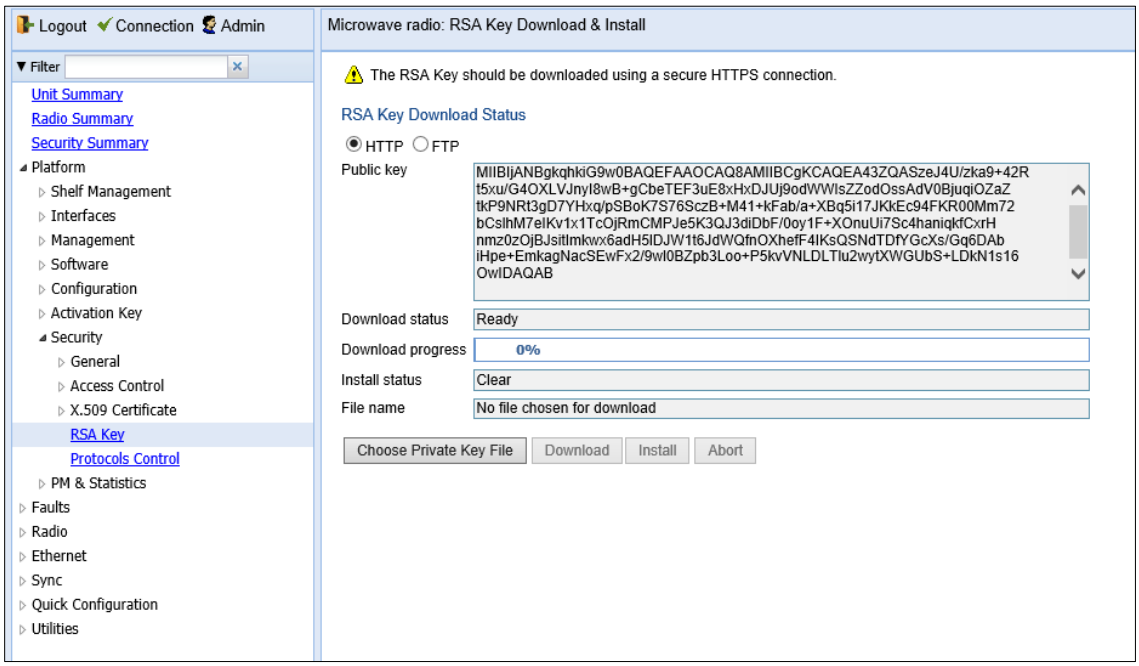
The following is an example of a valid RSA private key file:

-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC+7jRmt27yF4xD
h5Pc8w4ikvXUu32BI0eOyELmeUBnEeIHbCOXD3upi8+ZnH51Q+8hzgoSqXgEYFgZ
MoF/sXCrO2yf62UJ5ohj3zadhx/7585zoGwHtYz1S62hsa4+cdAl/i1Vbc6CoUBh5642
XYje+Q+q1XJtObed884eaQcXUFLIBipYKvVx2kuelymansE91WJU+UjFIc3aiQG8qsSg
W5Ar6wet0pXkP2Vdemo//QAXXjcTqqMBuizrlhlcvi+OKYFI9kSh21ZqSgjvK3cfAssCJ
BIY5d6t6bVkX9p2gjo/IPnErjAv7W6IZoemotb5KAeSHeR1sYTw17/xlpM7AgMBAAECg
gEAAwliLKQMOq4kh/UXD/OPAIPDXyp1jjaTw8dBm811OG5wttzXGrxJ+OIFX5Rn79Db
HnbayCiJL8tMe2dx5yhY+hA247roX3ua0w57cuPxnp21izc+S0fC7H/TTM1jpRCbATpa
ruTRMlitinZshJGA73Lsod3v36GEXxm/6dHnz/drCs2F4NdHWpjMAAG/1CiBwut8jNkJ
Uwa78lvk3JF+XRoZ0txN2mlybQxxzjuNXqZbNO6H3Ua2u1iYyD+McfgOWCCUfSnstG
RhFg0OsQuqj6d74qKVQWaukEH91SVZHEoqX6DgpKy4INZBxORZmITNmadwNhw5
O7rvFxZ205u4gQKBgQDT5bXvc0Ok+Ypm2xnIbu2GFjxNYwYhR3TvHPy14NIO5Q9l/
uDqwrSL1igzaIr6EbZyLu8cDXa4aybrzCyBfPeG89Qq+a6J3JR/RwJndLyjV4h5CT8Zy4
O/wjgTrP3Rhq7LAbWgLjSarafLgruHTcnOifhkK7MK7Fr+xi2IJfOKQQKBgQDmq1eYNzl
MPlATESlsfbkcL49jSsu70kYg0g5loI6+bVPo9K7mopICtWC/fwdNlUAfO+vr/231YUfSo
7YNEDNNRoT/NwvqqtAYxZaIUdIQxhMywF9jjYBBuq6+f/7+dwDfNBtMb2q7hceTdk6
yZ8/MehCkvSwOBmP+lq0FwTmmewKBgQClxmj31G1ve+rTXUZmkKly7OJwiLAbCRR
qnXr3r9Om43151i2QfJNTc1AwKVzTI1ftLNrUT5Q541qnzyxigaoFYmzy0jPCI1d128/9sE
6EW87hImLDg3ynYQMOlaDRc1T8bXHyxzNQb9t+U+DykeD4POifNbD1MsRd3h1xDn/i
AQKBgHmKpukJkCNgYgjp7g3AYR084izLaHZa4aDBjc0v4QQtzxzccJwN5SmQMJ42
bL6wecz7YeBEAshcrd+La42Oj7mUAtgHRTwtLOEgm6TQmANGmy8OtjRahs4bc5/IC
ZNDWS5C4m9v9aIBYFuO5wCSOqffWY20L9Zj/6RR+HEj0yCpAoGAHwrbRqPVZtZpt
FuNsCq130dtmqI7HFQAIqrc5DwP7YSsznE6biHfLUw891xu0vmevALrCaoeOMaidugo
hgiorSJO4qk7l3XN3pUJhPYqbhtdCVnBI2Fm9pr3V/SHGvrl1NW92cXObeQ2UEBiKP
OyQKfOBIbac707u0HqaTu+/ts=
-----END PRIVATE KEY-----

To download and install a private RSA key:

1. Select **Platform** > **Security** > **RSA Key**. The RSA Key Download & Install page opens.

Figure 494 RSA Key Download & Install Page (HTTP Selected)



2. Select **HTTP** to download the file via HTTP/HTTPS or **FTP** to download the file via SFTP.



Note

It is strongly recommended not to use HTTP to download RSA key files

14.11.1.1 Downloading an RSA Key via HTTP or HTTPS

To download and install a private RSA key file using HTTP or HTTPS:

1 Select **HTTP**.
2 Click **Choose Private Key File**.
3 Browse to and select the file.
4 Click **Download**. The download begins. You can view the status of the download in the **Download Status** field.
5 Once the download has been completed, click **Install** to install the RSA key file. You can view the status of the installation in the **Install Status** field.



Note

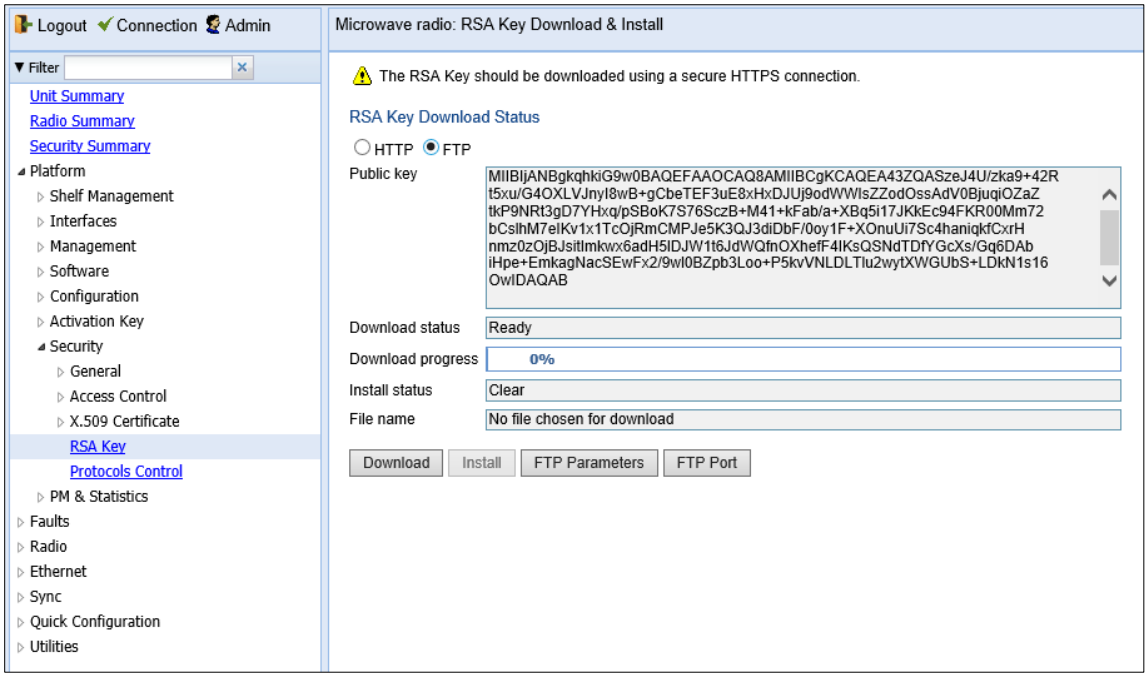
To discontinue the download process, click Abort.

14.11.1.2 Downloading an RSA Key via SFTP

To download and install a private RSA key file using SFTP:

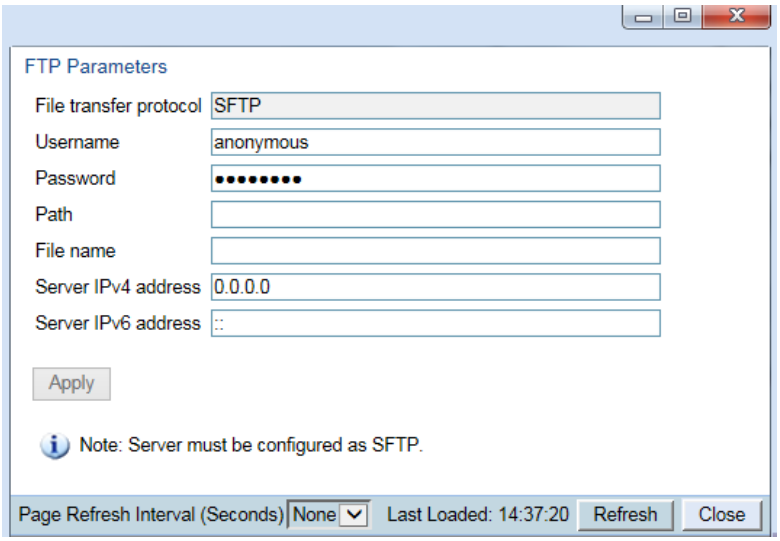
1. Install and configure SFTP server software on the PC or laptop you are using to perform the software upgrade. See Installing and Configuring an FTP or SFTP Server.
2. In the RSA Key Download & Install page, select **FTP**.

Figure 495 RSA Key Download & Install Page (FTP Selected)



3. Click **FTP Parameters** to display the FTP Parameters page.

Figure 496 FTP Parameters Page



4. The **File Transfer Protocol** field is read-only and displays **SFTP**. RSA key files cannot be downloaded to an PTP 850 device using FTP.
5. In the **Username** field, enter the user name you configured in the SFTP server.
6. In the **Password** field, enter the password you configured in the SFTP server. If you did not configure a password for your SFTP user, simply leave this field blank.

7. In the **Path** field, enter the directory path from which you are downloading the file. Enter the path relative to the SFTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//"..
8. If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the SFTP server in the **Server IPv4 address** field.
9. If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the SFTP server in the **Server IPv6 address** field.
10. Click **Apply** to save your settings.
11. In the RSA Key Download & Install page, click **Download**. The download begins. You can view the status of the download in the **Download Status** field.
12. Once the download has been completed, click **Install** to install the RSA key file. You can view the status of the installation in the **Install Status** field.



Note

To discontinue the download process, click Abort.

Table 87 RSA File Download & Install Status Parameters

Parameter	Definition
Download Status	The status of any pending RSA file download. Possible values are: e default value, which appears when no download ss. – The download is in progress. The download was aborted by user command. If an error occurs during the download, an appropriate error message is displayed in this field. When the download is complete, one of the following status indications appears: File downloaded and verified successfully. e download failed or verification failed. When the system is reset, the Download Status returns to Ready.
Download Progress	Displays the progress of the current download.
Install Status	The status of any pending installation. Possible values are:

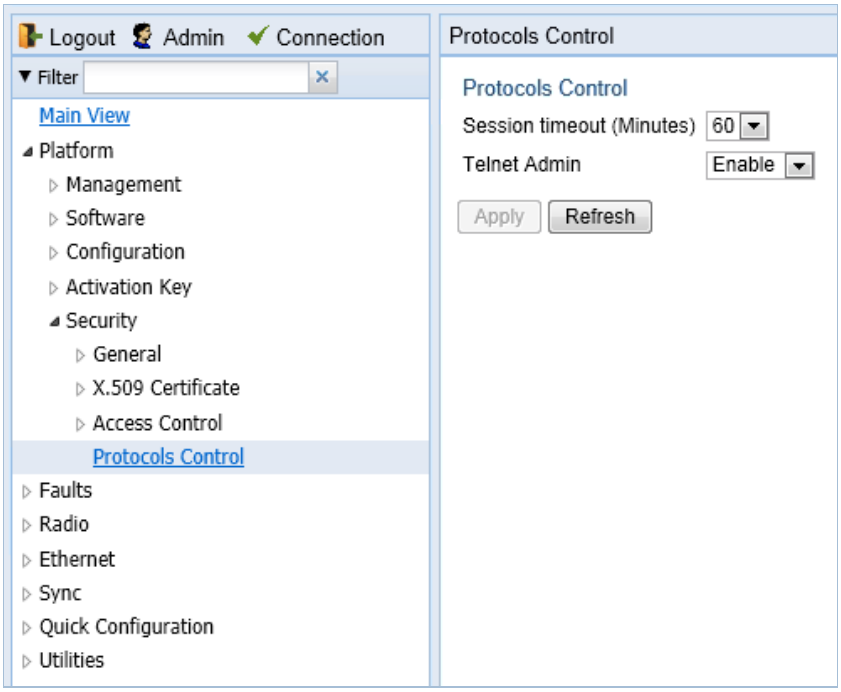
14.12 Blocking Telnet Access

You can block telnet access to the unit. By default, telnet access is not blocked.

To block telnet access:

1 Select **Platform** > **Security** > **Protocols Control**. The Protocols Control page opens.
2 In the **Telnet Admin** field, select **Disable** to block telnet access. By default, telnet access is enabled (**Enable**).
3 Click **Apply**.
4 Select **Platform** > **Security** > **Protocols Control**. The Protocols Control page opens.

Figure 497 Protocols Control Page



5 In the **Telnet Admin** field, select **Disable** to block telnet access. By default, telnet access is enabled (**Enable**).
6 Click **Apply**.

14.13 Configuring Access Control Lists

You can create rules to limit management traffic, i.e., traffic destined to the logical management interface. This includes both in-band and out-of-band management traffic. These rules are added to an access control list. The device maintains separate access control lists for IPv4 addresses and IPv6 addresses. You can configure up to 40 rules for each list.

Access control rules can be based on the following criteria:

- Source IP address
- Network subnet prefix length
- Protocol type

- Destination port

Each rule is either an “accept” rule or a “drop” rule. By using combinations of accept and drop rules, you can ensure that only certain traffic is permitted to ingress the management interface. You must be careful to configure the correct priority for the rules to ensure that traffic is limited as you intend.

Traffic received by the management interface is checked against the access control list in the order of priority configured by the user, from highest priority to lowest priority. Once a matching rule is found, the rule is applied to accept or drop the packet, and the checking stops for that packet.

For example, to allow only packets from subnet 192.168.1/24 to ingress the management interface, you must configure the following rules:

- Accept packets from any source address in the subnet of 192.168.1.0, prefix 24, any protocol, any destination port. The priority for this rule *must be* higher than the priority for the next rule blocking traffic (e.g. 3).
- Drop packets from source address 0.0.0.0, prefix 0, any protocol, any destination port. The priority for this rule *must be* lower than the priority for the previous rule accepting packets (e.g., 4).

To configure access control rules:

1 Select **Platform > Security > Access Control List**. The Access Control List Configuration page opens.

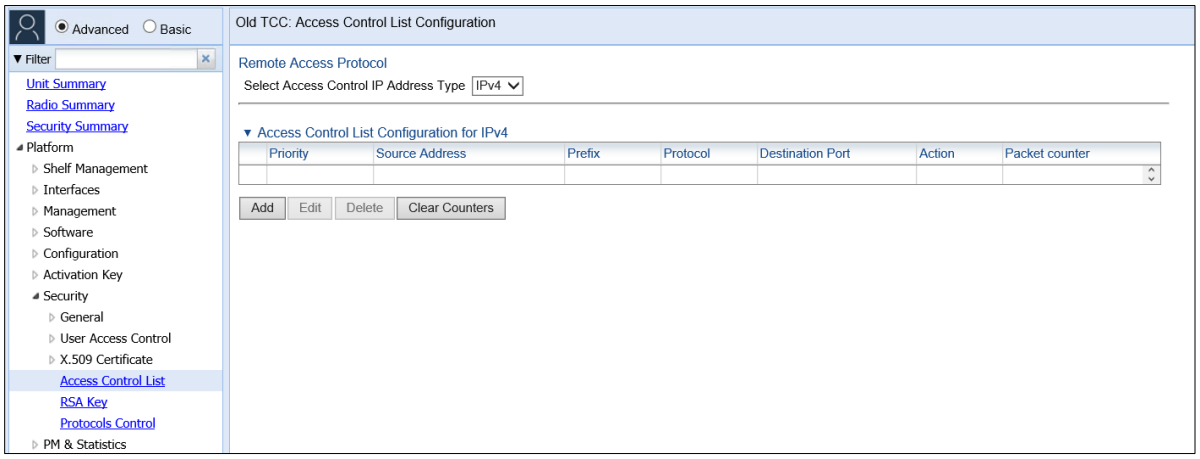


Figure 498: Access Control List Configuration Page

2 In the **Select Access Control IP Address Type** field, select **IPv4** or **IPv6**.
3 Click **Add**. The Access Control List Configuration – Add page opens.

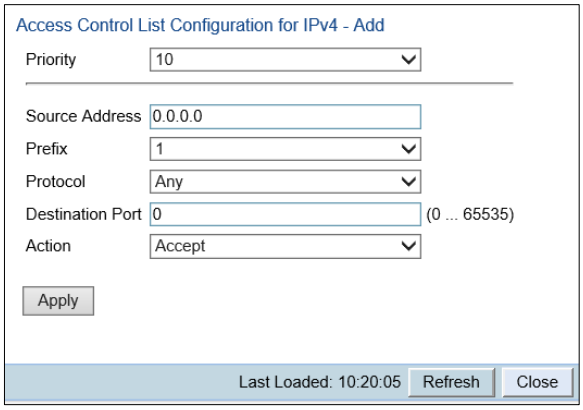


Figure 499: Access Control List Configuration for IPv4 - Add

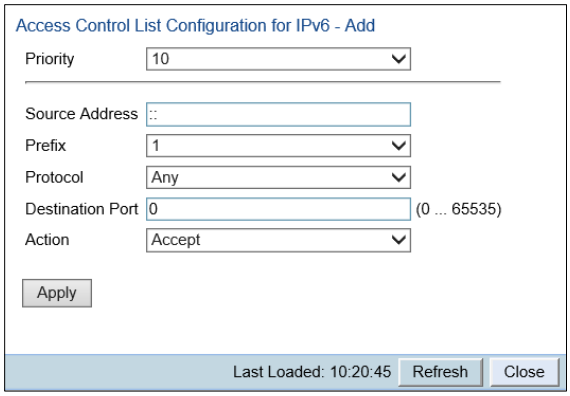


Figure 500: Access Control List Configuration for IPv6 - A

4 In the **Priority** field, select a priority for the rule (1-4000). The lower the number, the higher the priority will be for the rule. For example, a rule with Priority = 1 has the highest priority. Every rule must have a unique **Priority** value. The default value is 10.

Note: It is recommended to assign priorities in multiples of 10 (e.g., 10, 20, 30).

5 In the **Source Address** field, enter the source IP address to which the rule will be applied. If the **Source Address** is set to 0.0.0.0 (IPv4) or 0::0 (IPv6), the rule will be applied to all IP addresses, and the **Prefix** field (below) will have no meaning.

6 In the **Prefix** field, select the network subnet prefix to be validated by the rule. Options are:

- IPv4: 1-32 (default = 1)
- IPv6: 1-128 (default = 1)

7 In the **Protocol** field, select a protocol type to which the rule will be applied, or select **Any** to apply the rule to all protocol types. Options are:

- **Any**
- **TCP**
- **UDP**
- **ICMP** (for IPv6, this appears as **ICMPv6**)

8 In the **Destination Port** field, enter the destination port to which the rule will be applied (0 – 65535). To apply the rule to all ports, enter 0.

9 In the **Action** field, select one of the following options:

- **Accept – Traffic to which the rule applies is accepted.**
- **Drop – Traffic to which the rule applies is dropped.**

10 Click **Apply**. The rule is applied immediately, but is only saved temporarily, and a five-minute failsafe timer begins, as shown in Figure 501. To confirm the rule, click **Keep Changes**. To reject the changes, click **Revert**. If you do not click **Keep Changes** or **Revert** within the timeout period, the rule is discarded. Note that rules that have not yet been confirmed are not included in backup configuration files, and are not copied to mate if you perform a copy-to-mate operation before confirming the rule.

Note: The purpose of the failsafe timer is to ensure that if you accidently enter a rule that causes management connectivity to be lost, the rule will be discarded and management restored in five minutes, with no user intervention required. A single timer runs for both IPv4 and IPv6, starting with the first rule configured for either IPv4 or IPv6.

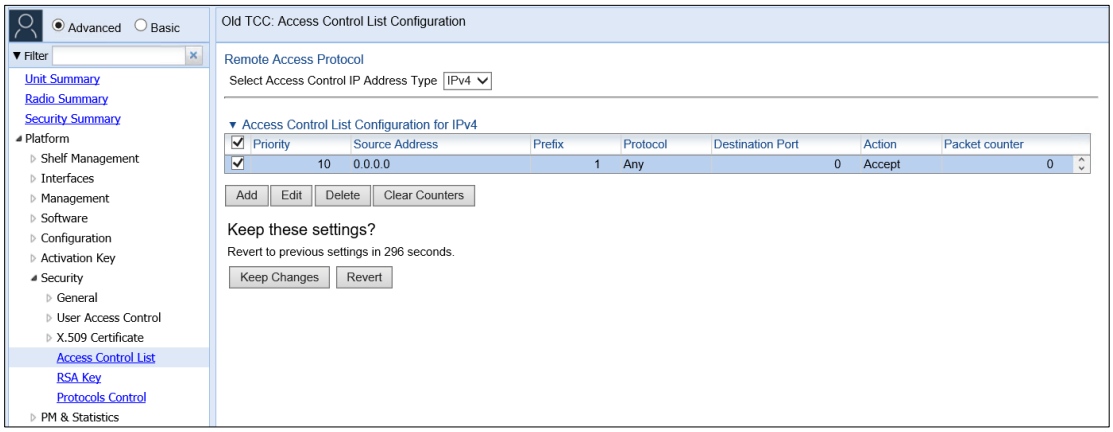


Figure 501: Access Control List Configuration Page – Failsafe Timer

To edit a rule, select the rule in the Access Control List Configuration page and click **Edit**. An Edit page opens, similar to the Access Control List Configuration –Add page. You can edit any of the rule's parameters except the **Priority**.

For each rule, the Access Control List Configuration page displays the number of matching packets that have been received by the management interface in the **Packet counter** column. To clear the counters for all rules, click **Clear Counters**.

Note: Clicking **Clear Counters** only clears the counters for the currently displayed IP type. For example, if you click Clear Counters while displaying IPv4 rules, counters will be cleared for all IPv4 rules but not for IPv6 rules, and vice versa.

14.14 Uploading the Security Log

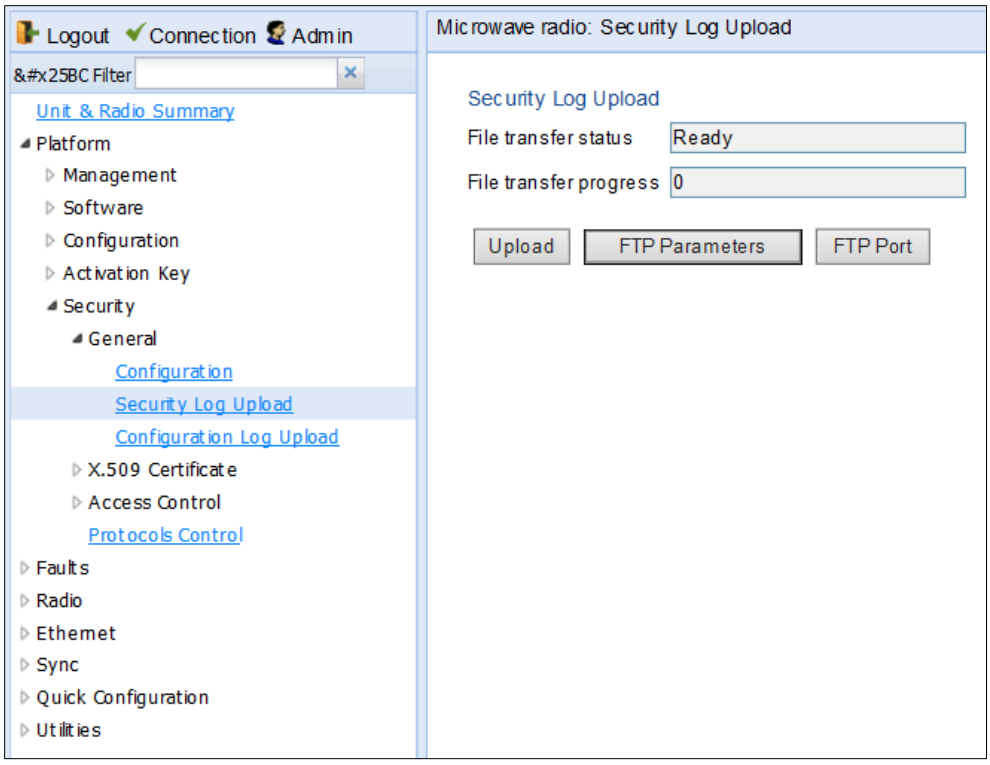
The security log is an internal system file which records all changes performed to any security feature, as well as all security related events.

When uploading the security log, the PTP 850 functions as an FTP or SFTP client. You must install FTP or SFTP server software on the PC or laptop you are using to perform the import or export. For details, see Installing and Configuring an FTP or SFTP Server.

To upload the security log:

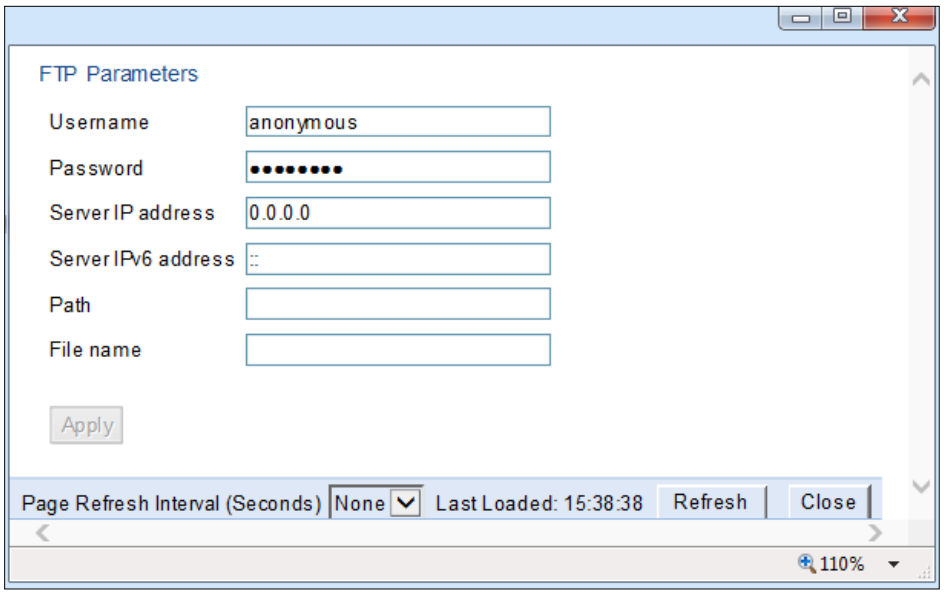
1. Install and configure an FTP server on the PC or laptop you are using to perform the upload. See Installing and Configuring an FTP or SFTP Server.
2. Select **Platform > Security > General > Security Log Upload**. The Security Log Upload page opens.

Figure 502 Security Log Upload Page



3. Click **FTP Parameters** to display the FTP Parameters page.

Figure 503 FTP Parameters Page (Security Log Upload)



4. In the **File transfer protocol** field, select the file transfer protocol you want to use (**FTP** or **SFTP**).
5. In the **Username** field, enter the user name you configured in the FTP server.
6. In the **Password** field, enter the password you configured in the FTP server. If you did not configure a password for your FTP user, simply leave this field blank.
7. If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the FTP server in the **Server IPV4 address** field. See Defining the IP Protocol Version for Initiating Communications.
8. If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the FTP server in the **Server IPv6 address** field. See Defining the IP Protocol Version for Initiating Communications.
9. In the **Path** field, enter the directory path to which you are uploading the files. Enter the path relative to the FTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
10. In the **File name** field, enter the name you want to give to the exported security log.
11. Click **Apply**, then **Close** to save the FTP parameters and return to the Security Log Upload page.
12. Click **Upload**. The upload begins.

The **File transfer operation status** field displays the status of any pending security log upload. Possible values are:

- **Ready** – The default value, which appears when no file transfer is in progress.
- **File-in-transfer** – The upload operation is in progress.

- **Success** – The file has been successfully uploaded.
- **Failure** – The file was not successfully uploaded.
- The **File transfer progress** field displays the progress of any current security log upload operation.

14.15 Uploading the Configuration Log

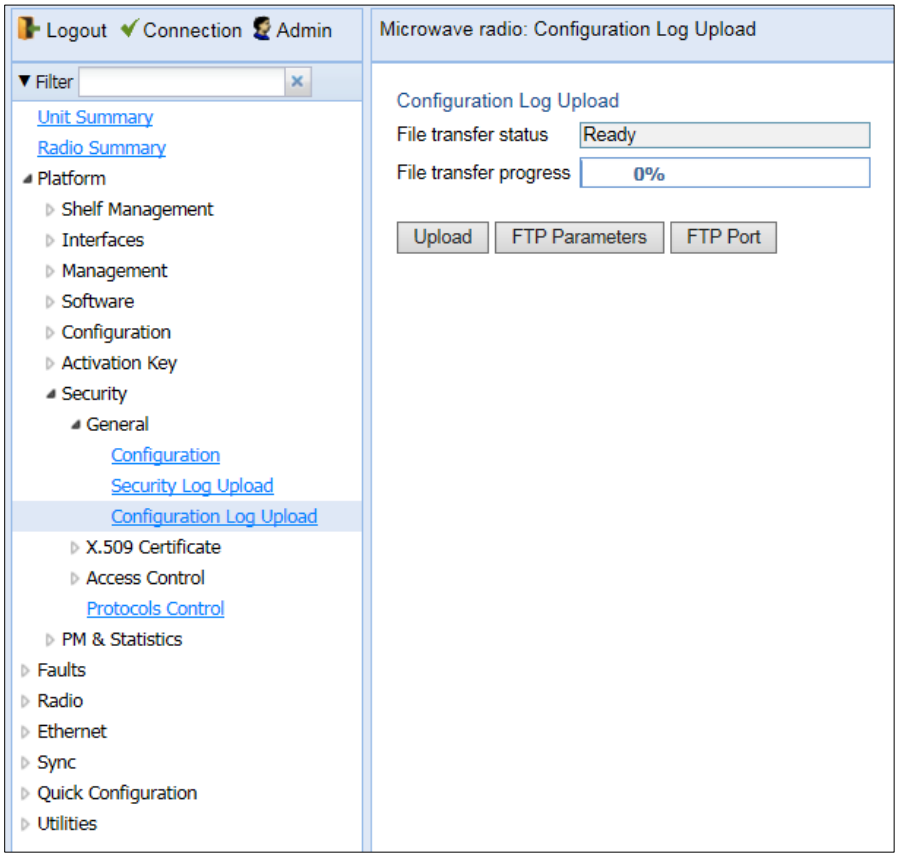
The configuration log lists actions performed by users to configure the system. This file is mostly used for security, to identify suspicious user actions. It can also be used for troubleshooting.

When uploading the configuration log, the PTP 850 functions as an FTP or SFTP client. You must install FTP or SFTP server software on the PC or laptop you are using to perform the upload. For details, see Installing and Configuring an FTP or SFTP Server.

To upload the configuration log:

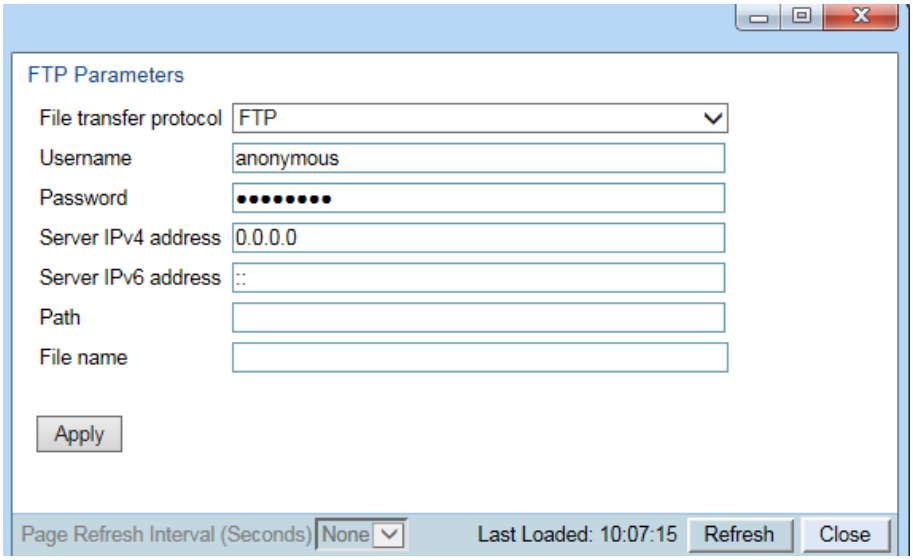
1. Install and configure an FTP server on the PC or laptop you are using to perform the upload. See Installing and Configuring an FTP or SFTP Server.
2. Select **Platform** > **Security** > **General** > **Configuration Log Upload**. The Configuration Log Upload page opens.

Figure 504 Configuration Log Upload Page



3. Click **FTP Parameters** to display the FTP Parameters page.

Figure 505 Configuration Log Upload Page



4. In the **File transfer protocol** field, select the file transfer protocol you want to use (**FTP** or **SFTP**).
5. In the **Username** field, enter the user name you configured in the FTP server.
6. In the **Password** field, enter the password you configured in the FTP server. If you did not configure a password for your FTP user, simply leave this field blank.
7. If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the FTP server in the **Server IPV4 address** field. See Defining the IP Protocol Version for Initiating Communications.
8. If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the FTP server in the **Server IPv6 address** field. See Defining the IP Protocol Version for Initiating Communications.
9. In the **Path** field, enter the directory path to which you are uploading the files. Enter the path relative to the FTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
10. In the **File Name** field, enter the name you want to give to the exported configuration log.



Note

The directory path and fie name, together, cannot be more than:

If the IP address family is configured to be IPv4: 236 characters
If the IP address family is configured to be IPv6: 220 characters

11. Click **Apply**, and **Close** to save the FTP parameters and return to the Configuration Log Upload page.
12. Click **Upload**. The upload begins.

The **File transfer operation status** field displays the status of any pending configuration log upload. Possible values are:

Ready – The default value, which appears when no file transfer is in progress.

File-in-transfer – The upload operation is in progress.

Success – The file has been successfully uploaded.

Failure – The file was not successfully uploaded.

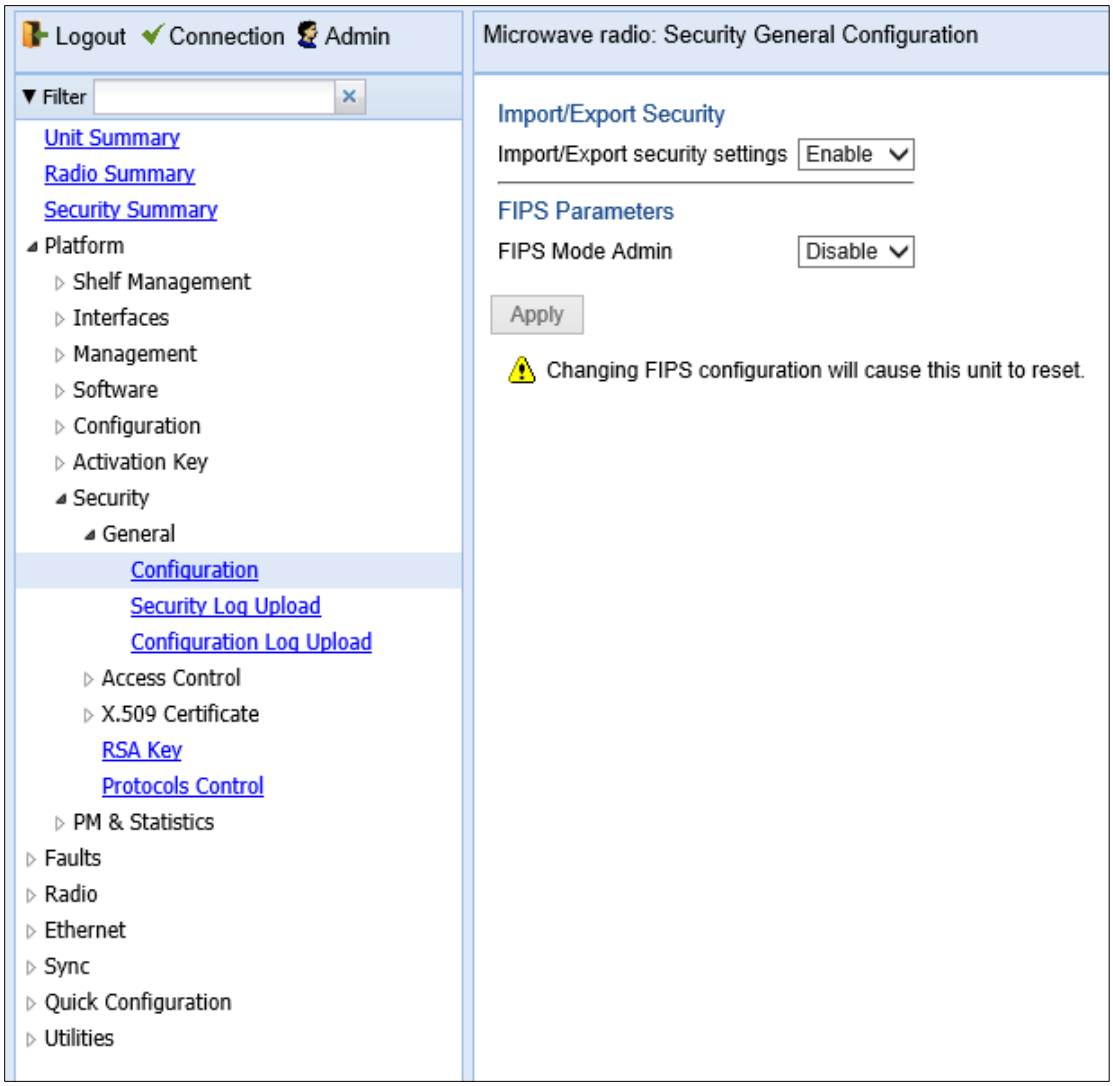
The **File transfer progress** field displays the progress of any current configuration log upload operation.

14.16 Configuring the Import/Export Security Settings

You can configure the unit to exclude security configurations from configuration backup files:

1 Select **Platform** > **Security** > **General** > **Configuration**. The Security General Configuration page opens.

Figure 506 Security General Configuration Page



2 The **Import/Export security settings** field determines whether security configurations are included in configuration backup files. To enhance unit security, it is recommended to select **Enable** in this field, so that security configurations will *not* be included in backup files.
3 Click **Apply**.

14.17 Configuring SSO Web Login with Microsoft Entra ID

System Release devices support remote user login via Microsoft Entra ID. Microsoft Entra ID is a cloud-based identity and access management service. It helps organizations securely manage users, applications, and devices by providing authentication, authorization, and identity protection. Through Entra ID, users can securely access external resources.

The following options are available for System Release devices:

- Single Sign-On (SSO) – Enables users to log in once and access multiple applications without needing to re-enter credentials.
- Multi-Factor Authentication (MFA) – Adds an extra layer of security beyond just a password. MFA is optional, and must be arranged by the customer as part of the customer's Microsoft Entra ID implementation.

Microsoft Entra ID includes the following elements:

- Microsoft Entra ID access management server – Receives the initial user authentication request and manages the authentication process through secure communication with the SSO server.
- SSO server (Redirect URI) – Receives redirects of authentication requests from the Microsoft Entra ID access management server and continues the authentication process based on a CA private key installed on the SSO server and the CA certificate installed on the device.

Acquisition and configuration of these elements is the responsibility of the customer and is not covered in this User Guide. This User Guides explains the prerequisites and configuration of Miscorsoft Entra ID on System Release devices. For further information and support, check with your Cambium representative.

SSO is only active for the browser type on which the user logs in with Microsoft. For example, if the user logs in with a Microsoft Edge browser, the user will be logged in via SSO while using a Microsoft Edge browser but will not be logged in via SSO from a Google Chrome browser, and vice versa.

When a user logs into a device with SSO enabled, the user is given the option to log in normally with the user's credentials or to log in via Microsoft.

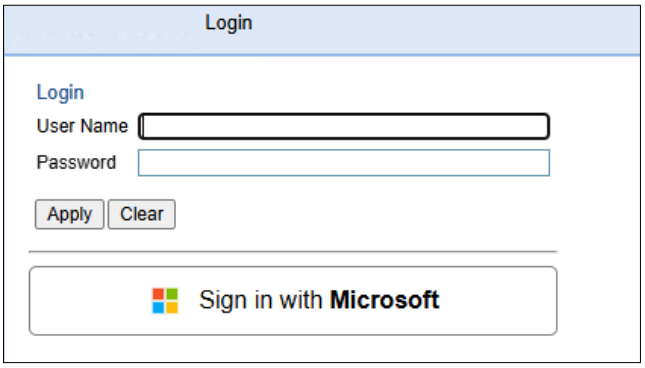


Figure 507: SSO Login Page

When a user logs out of a device to which the user is logged in with SSO, the user is given the option to log out of the local session only or to log out of Microsoft.

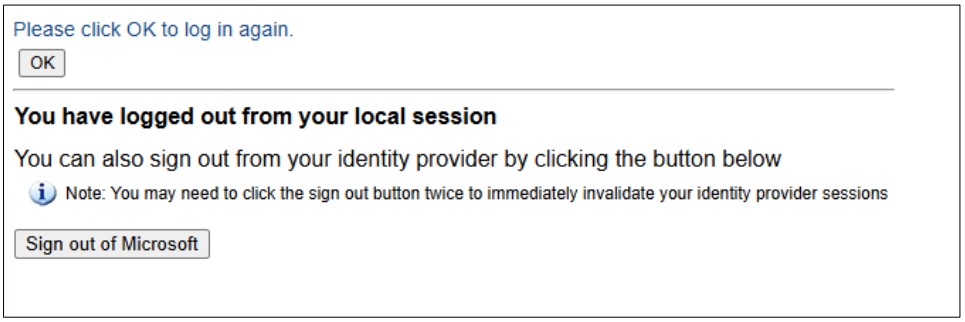
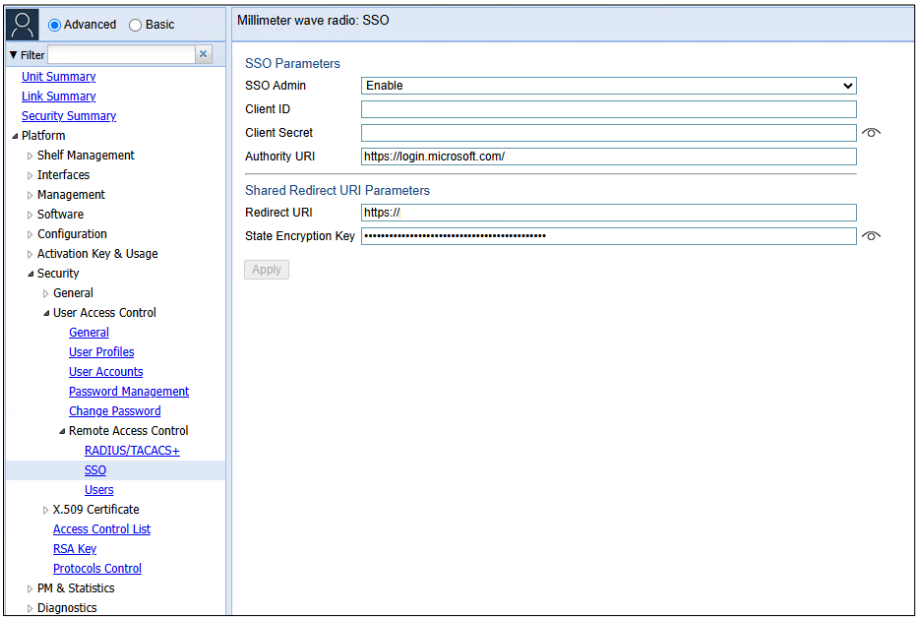


Figure 508: SSO Logout Page

To enable SSO on a CeraOS device:

1 Configure the Microsoft Entra ID access management server.
2 Configure the SSO server.
3 Verify that a Single Sign-On activation key (SL-SSO) has been applied to the device or that the device is using Smart Activation Key.
SSO cannot be used in Activation Key Demo mode.
4 Enable HTTPS. SSO will not function if HTTPS is not enabled on the device. See Enabling HTTPS.
5 Select **Platform > Security > User Access Control > Remote Access Control > SSO**. The SSO page opens.
Figure 509: SSO Page



6 In the **SSO Admin** field, select **Enable**.
7 In the **Client ID** field, enter the Client ID defined for the customer by Microsoft.
8 Optionally, in the **Client Secret** field, enter the Client Secret defined for the customer on the Microsoft Entra ID access management server. The Client Secret must be configured on the SSO server. If it is also configured on the device, the value configured on the device has precedence over the value configured on the SSO server.

The maximum valid period of a Client Secret is 24 months, after which it expires. It is the customer's responsibility to configure a new Client Secret on the SSO server and copy it to all managed devices before expiration.

9 In the **Authority URI** field, enter a link to the Microsoft Entra ID access management server.
10 In the **Redirect URI** field, enter a link to the SSO server.
11 In the **State Encryption Key** field, enter the key used to encrypt the state parameter during the authentication process. This must be the same as the `state_key` parameter configured on the SSO server.
12 Click **Apply**.

15. Alarm Management and Troubleshooting

This section includes:

- Viewing Current Alarms
- Viewing Alarm Statistics
- Viewing and Saving the Event Log
- Editing Alarm Text and Severity and Disabling Alarms and Events
- Configuring Voltage Alarm Thresholds and Displaying Voltage PMs
- Uploading Unit Info
- Configuring Syslog
- Performing Diagnostics



Note

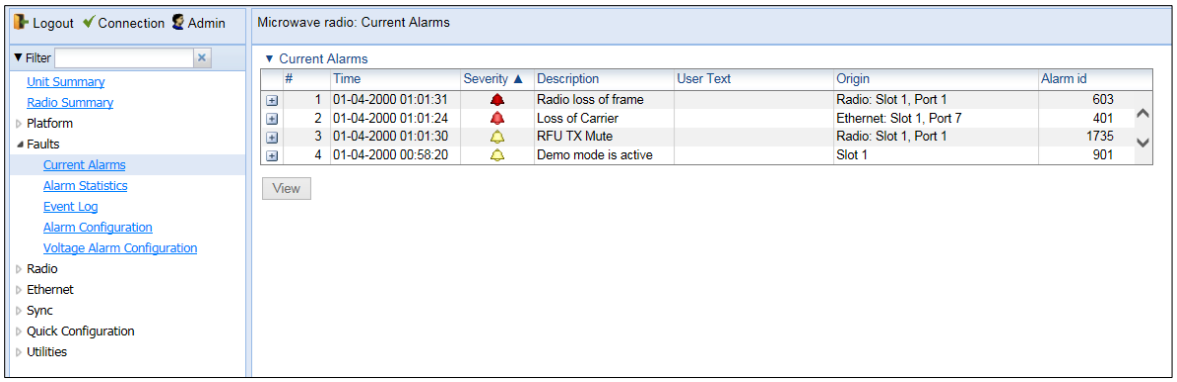
CW mode, used to transmit a single or dual frequency tones for debugging purposes, can be configured using the CLI.
You can configure a wait time of up to 120 seconds after an alarm is cleared in the system before the alarm is actually reported as being cleared. This prevents traps flooding the NMS in the event that some external condition causes the alarm to be raised and cleared continuously. By default, the timeout for trap generation is disabled. It can be enabled and disabled via CLI.

15.1 Viewing Current Alarms

To display a list of current alarms in the unit:

1. Select **Faults > Current Alarms**. The Current Alarms page opens. The Current Alarms page displays current alarms in the unit. Each row in the Current Alarms table describes an alarm and provides basic information about the alarm. For a description of the information provided in the Current Alarms page, see Table 88.

Figure 510 Current Alarms Page



2. To view more detailed information about an alarm, click + at the beginning of the row or select the alarm and click **View**.

Figure 511 Current Alarms - View Page

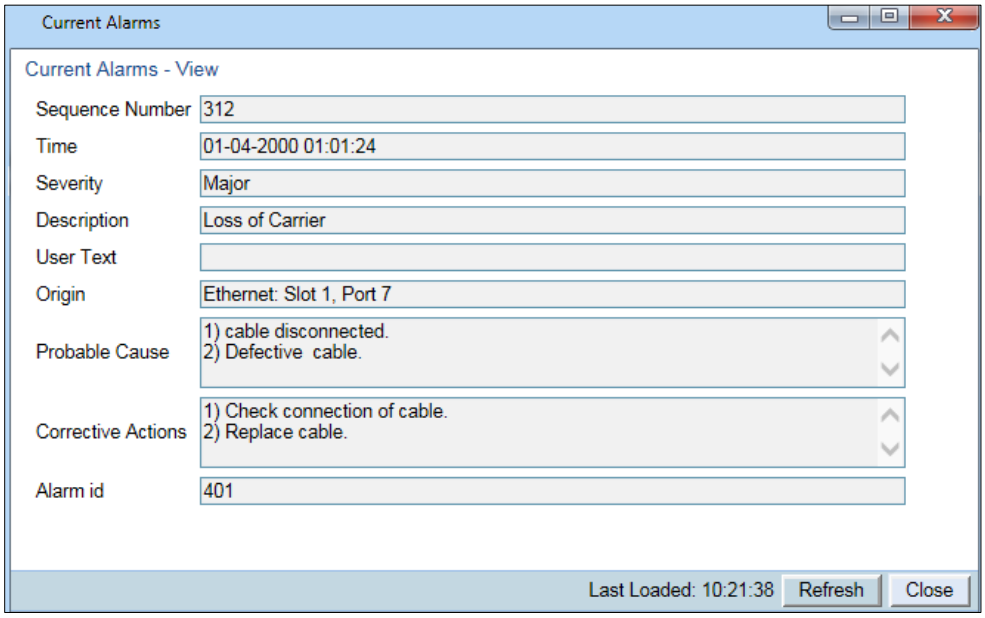


Table 88 Alarm Information

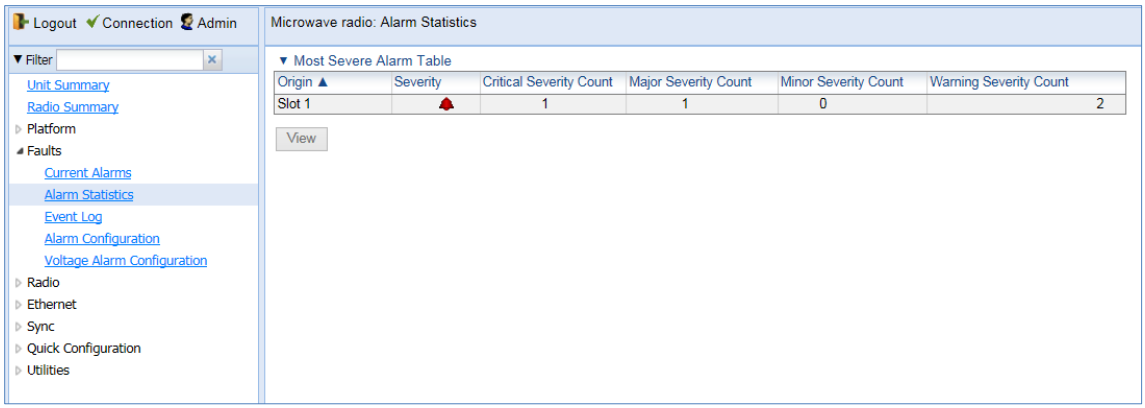
Parameter	Definition
Sequence Number (#)	A unique sequence number assigned to the alarm by the system.
Time	The date and time the alarm was triggered.
Severity	The severity of the alarm. In the Current Alarms table, the severity is indicated by a symbol. You can display a textual description of the severity by holding the cursor over the symbol. **Note:** You can edit the severity of alarm types in the Alarm Configuration page.
Description	A system-defined description of the alarm.
User Text	Additional text that has been added to the system-defined description of the alarm by users. **Note:** You can add user text to alarms in the Alarm Configuration page.
Origin	The module that generated the alarm.
Probable Cause	This field only appears in the Current Alarms - View page. One or more possible causes of the alarm, to be used for troubleshooting.
Corrective Actions	This field only appears in the Current Alarms - View page. One or more possible corrective actions to be taken in troubleshooting the alarm.
Alarm ID	A unique ID that identifies the alarm type.

15.2 Viewing Alarm Statistics

To display a summary of alarms per module and per interface:

1. Select **Faults > Alarm Statistics**. The Alarm Statistics page opens.

Figure 512 Alarm Statistics Page



The Alarm Statistics page displays the number of current alarms per severity level for each module, interface, and virtual interface (such as Multi-Carrier ABC groups) in the unit. Only modules and interfaces for which one or more alarms are currently raised are listed in the Alarm Statistics page.

15.3 Viewing and Saving the Event Log

The Event Log displays a list of current and historical events and information about each event.

To display the Event Log:

1. Select **Faults > Event Log**. The Event Log opens. For a description of the information provided in the Event Log, see Table 89 Event Log Information.
2. To export the Event Log to a CSV file, click **Export to CSV** in the lower right corner of the Event Log page.

Figure 513 Event Log

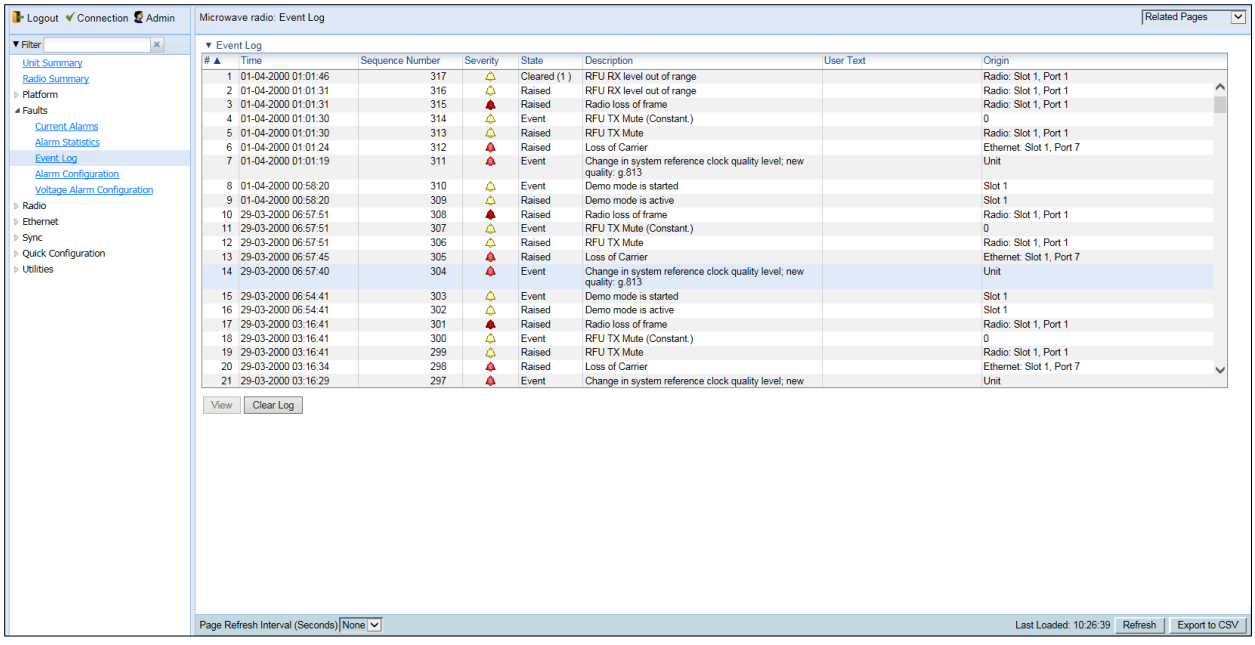


Table 89 Event Log Information

Parameter	Definition
Time	The date and time the event was triggered.
Sequence Number (#)	A unique sequence number assigned to the event by the system.
Severity	The severity of the event. In the Event Log table, the severity is indicated by a symbol. You can display a textual description of the severity by holding the cursor over the symbol. **Note:** You can edit the severity of event types in the Alarm Configuration page.
State	Indicates whether the event is currently raised or has been cleared.
Description	A system-defined description of the event.
User Text	Additional text that has been added to the system-defined description of the event by users. **Note:** You can add user text to events in the Alarm Configuration page.
Origin	The module that generated the event.

15.4 Editing Alarm Text and Severity | Disabling Alarms and Event

You can view a list of alarm types, edit the severity level assigned to individual alarm types, and add additional descriptive text to individual alarm types.

This section includes:

- Displaying Alarm Information
- Viewing the Probable Cause and Corrective Actions for an Alarm Type
- Editing an Alarm Type and Disabling Alarms and Events
- Setting Alarms to their Default Values

15.4.1 Displaying Alarm Information

To view the list of alarms defined in the system:

1. Select **Faults > Alarm Configuration**. The Alarm Configuration page opens. For a description of the information provided in the Alarm Configuration page.

Figure 514 Alarm Configuration Page

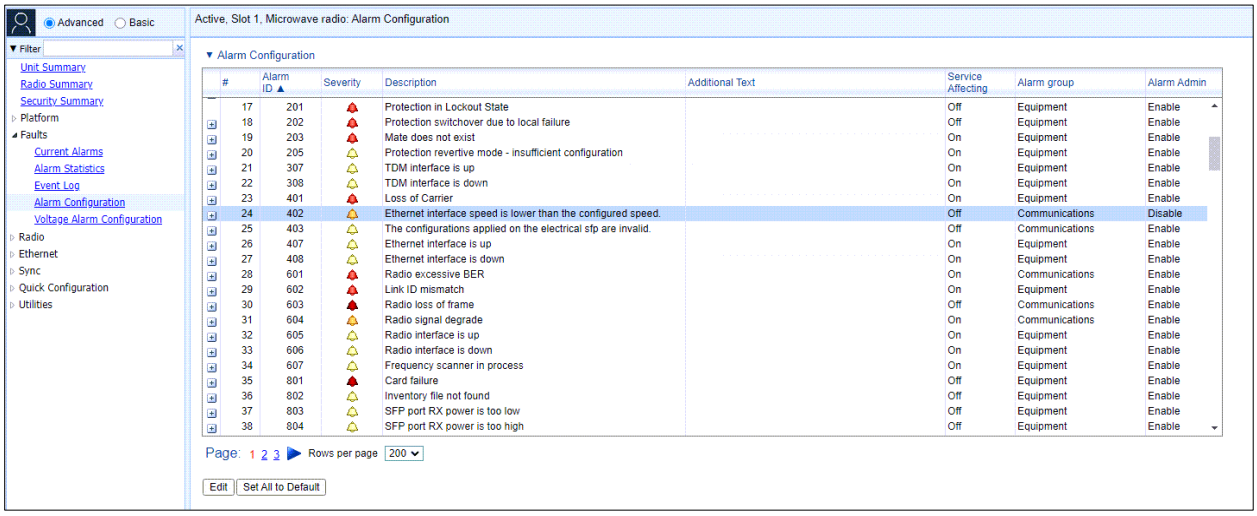


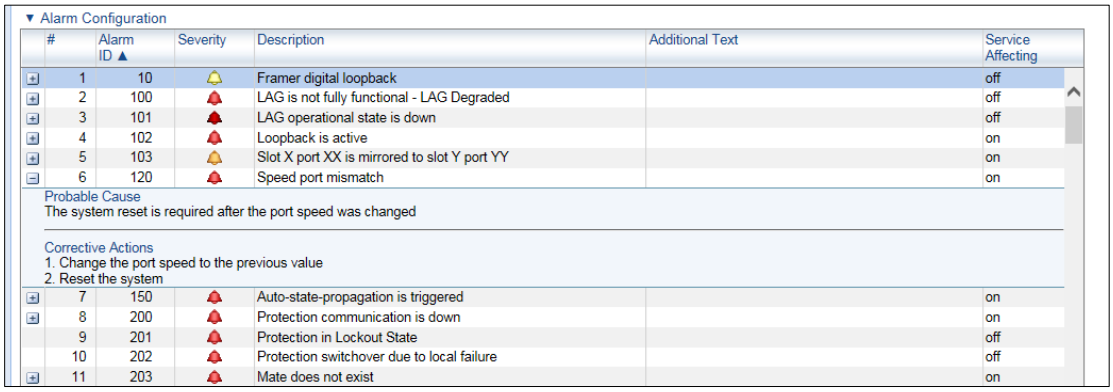
Table 90 Alarm Configuration Page Parameters

Parameter	Definition
Sequence Number (#)	A unique sequence number assigned to the row by the system.
Alarm ID	A unique ID that identifies the alarm type.
Severity	The severity assigned to the alarm type. You can edit the severity in the Alarm Configuration – Edit page.
Description	A system-defined description of the alarm.
Additional Text	Additional text that has been added to the system-defined description of the alarm by users. You can edit the text in the Alarm Configuration – Edit page.
Service Affecting	Indicates whether the alarm is considered by the system to be service-affecting (**on**) or not (**off**).
Alarm Group	The Alarm group to which the alarm belongs. The Alarm group is used to determine which alarms trigger an external alarm output.
Alarm Admin	Indicates whether the alarm is enabled or disabled. By default, all alarms except the Auto Negotiation Speed Alarm (Alarm ID 402) are enabled.

15.4.2 Viewing the Probable Cause and Corrective Actions for an Alarm Type

Most alarm types include a system-defined probable cause and suggested corrective actions. To view an alarm type's probable cause and corrective actions, click + on the left side of the alarm type's row in the Alarm Configuration page. The Probable Cause and Corrective Actions appear underneath the alarm type's row, as shown below. If there is no +, that means no Probable Cause and Corrective Actions are defined for the alarm type.

Figure 515 Alarm Configuration Page – Expanded



15.4.3 Editing an Alarm Type and Disabling Alarms and Events

You can change the severity of an alarm type, and add additional text to the alarm type's description.

You can also choose to disable selected alarms and events. Any alarm or event can be disabled, so that no indication of the alarm is displayed, and no traps are sent for the alarm.

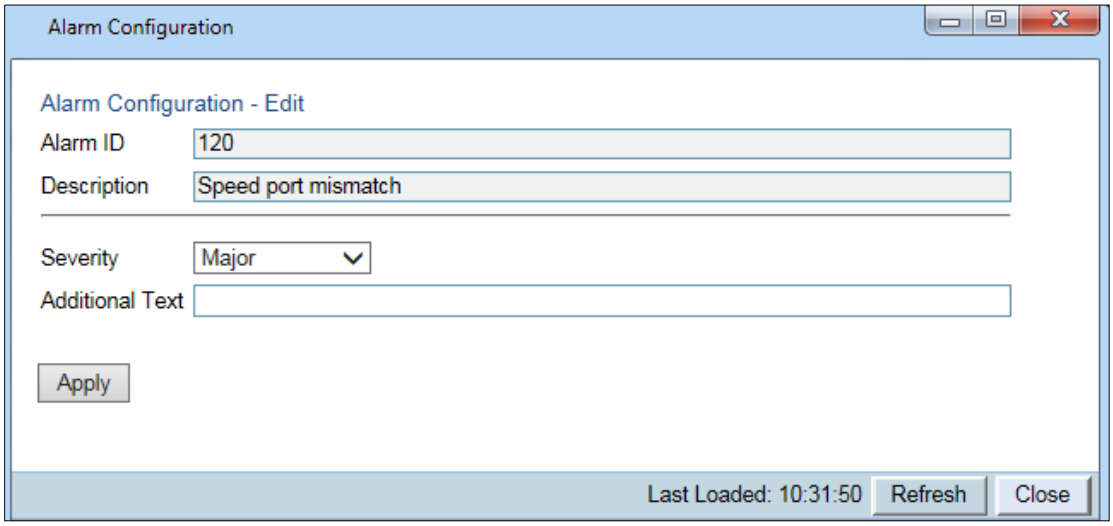
If you disable an alarm that is currently raised, the alarm is treated as if it has been cleared. If an alarm that has been disabled is enabled while it is in a raised state, the alarm is treated as if it has just been raised when it is enabled.

If a timeout for trap generation is configured, and a disabled alarm is enabled while the alarm is raised, the timeout count begins to run when the alarm is enabled. If an alarm is disabled while raised, the timeout count begins to run upon disabling the alarm, and an alarm cleared trap is sent when the timeout expires.

To change the severity of an alarm type and add additional text to the alarm type's description:

1. Select the alarm type in the Alarm Configuration page.
2. Click **Edit**. The Alarm Configuration - Edit page opens.

Figure 516 Alarm Configuration - Edit Page



3. Modify the **Severity** and/or **Additional Text** fields.
4. Click **Apply**, then **Close**.

15.4.4 Enabling the Auto Negotiation Speed Alarm

Alarm ID 402 is the Auto Negotiation Speed Alarm. When Auto Negotiation is enabled on an Ethernet interface, this alarm monitors the interface speed. The alarm is raised if the actual speed is lower than the configured speed. The alarm is cleared when any of the following occurs:

- Auto Negotiation is disabled on the interface.
- The actual speed becomes the same as the configured interface speed.
- The interface's operational status changes to Down.

Unlike other alarms and events, the Auto Negotiation Speed alarm is disabled by default. To enable the alarm:

1 Select the alarm in the Alarm Configuration page (Figure 514).
2 Click **Edit**. The Alarm Configuration – Edit page opens.

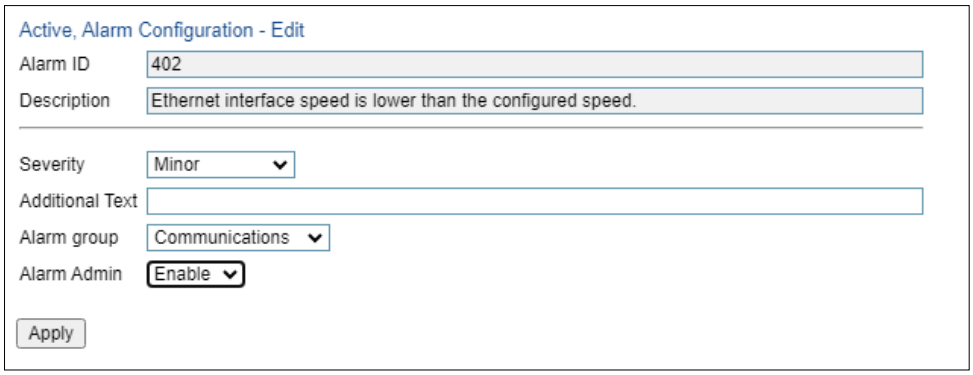


Figure 517: Alarm Configuration – Edit Page

3 In the **Alarm Admin** field, select **Enable**.
4 Click **Apply**.

15.4.5 Setting Alarms to their Default Values

To set all alarms to their default severity levels and text descriptions, click **Set All to Default** in the Alarm Configuration page.

Note: By default, all alarms except the Auto Negotiation Speed Alarm (Alarm ID 402) are enabled. Therefore, if you set all alarms to their default values, they will all be enabled except Alarm ID 402, which will be disabled.

15.5 Configuring Voltage Alarm Thresholds and Displaying Voltage PMs

You can configure undervoltage and overvoltage alarm thresholds and display voltage PMs.

The default thresholds for PTP 850E are:

- Undervoltage Raise Threshold: 36V

- Undervoltage Clear Threshold: 38V
- Overvoltage Raise Threshold: 60V
- Overvoltage Clear Threshold: 58V

These thresholds determine when the following alarms are raised and cleared:

- Alarm #32000: Under voltage
- Alarm #32001: Over voltage

To configure voltage alarm thresholds:

1 Select **Faults > Voltage Alarm Configuration**. The Voltage Alarm Configuration page opens.



Note

You can also open the Voltage Alarm Configuration page by selecting **Platform > PM & Statistics > Voltage** and clicking **Thresholds**.

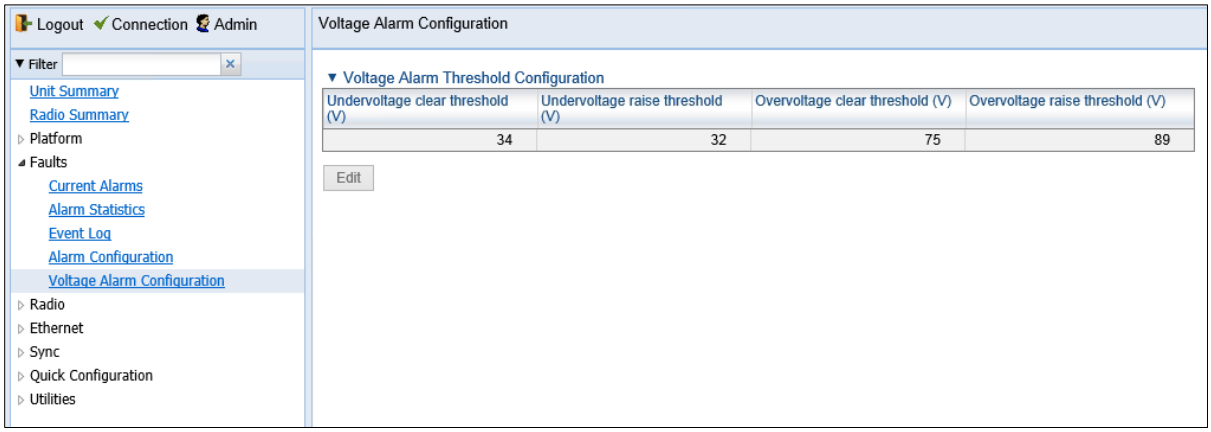


Figure 518 Voltage Alarm Configuration Page

2 Click **Edit**. The Voltage Alarm Configuration – Edit page opens.

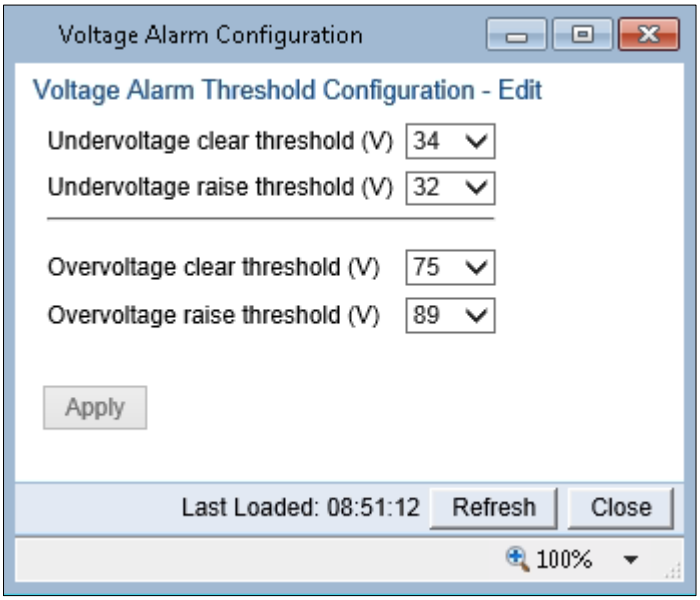


Figure 519 Voltage Alarm Configuration – Edit Page

3 Select the thresholds you want in the **Undervoltage clear threshold (V)**, **Undervoltage raise threshold (V)**, **Overvoltage clear threshold (V)**, and **Overvoltage raise threshold (V)** fields. The configurable values for these thresholds are 0-100V.

4 Click **Apply**.

To display voltage PMs:

1. Select **Platform > PM & Statistics > Voltage**. The Voltage PM Report page opens.

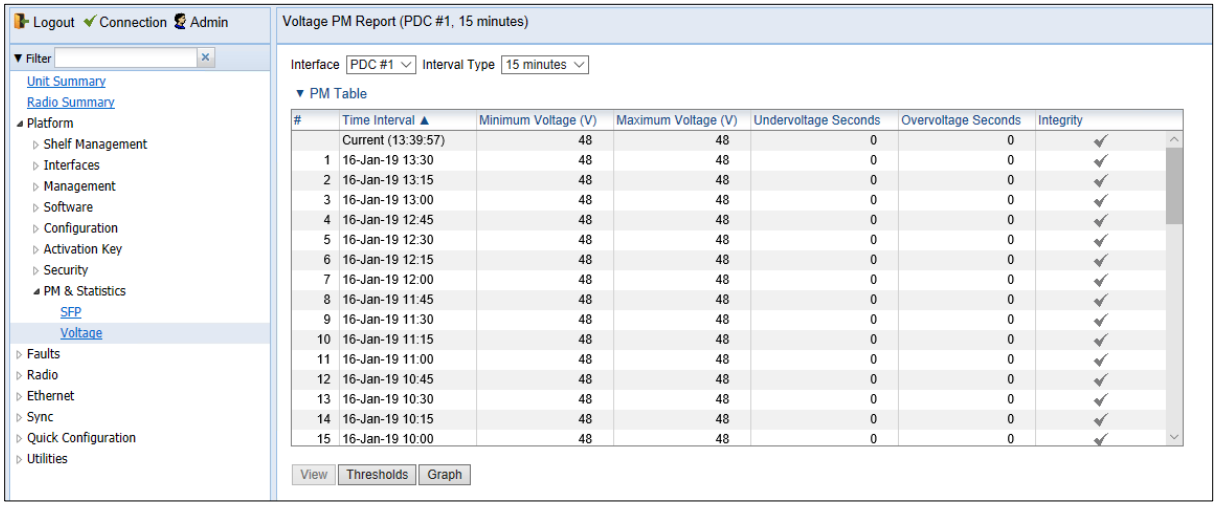


Figure 520 Voltage PM Report Page

2. In the **Interface** field, select the power input for which to display PMs.
3. In the **Interval Type** field:

- To display reports for the past 24 hours, in 15 minute intervals, select **15 minutes**.
- To display reports for the past month, in daily intervals, select **24 hours**.

Table 91 Voltage PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Minimum Voltage (V)	The lowest voltage during the measured period.
Maximum Voltage (V)	The highest voltage during the measured period.
Undervoltage Seconds	The number of seconds the unit was in an undervoltage state during the measured period.
Overvoltage Seconds	The number of seconds the unit was in an overvoltage state during the measured period.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred during the interval.

15.6 Uploading Unit Info

You can generate a Unit Information file, which includes technical data about the unit. This file can be uploaded and forwarded to customer support, at their request, to help in analyzing issues that may occur.

You can upload the Unit Information file using HTTP, HTTPS, FTP, or SFTP.

Note: For troubleshooting, it is important that an updated configuration file be included in User Info files that are sent to customer support. To ensure that an up-to-date configuration file is included, it is recommended to back up the unit's configuration before generating the Unit Info file.

15.6.1 Uploading a Unit Info File Via HTTP or HTTPS

To uploading a User Information file using HTTP or HTTPS:

1 **Platform > Management > Unit Info**. The Unit Info page opens.
2 Select **HTTP**.

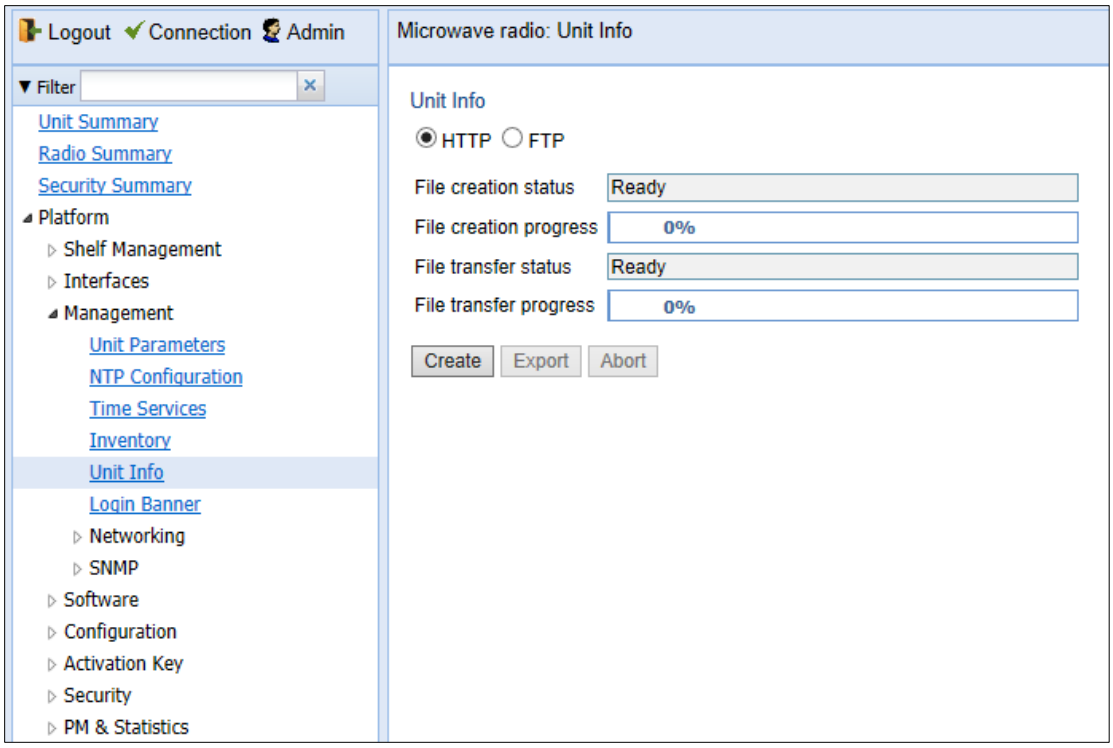


Figure 521: Unit Info Page – HTTP/HTTPS Upload

3 Select **HTTP**.

4 Click **Create** to create the Unit Information file. The following fields display the status of the file creation process:

- **File Creation Status** – Displays the file creation status. You must wait until the status is Success to upload the file. Possible values are:
  - **Ready** – The default value, which appears when no file is being created.
  - **Generating File** – The file is being generated.
  - **Success** – The file has been successfully created. You may now upload the file.
  - **Failure** – The file was not successfully created.
- **File Creation Progress** – Displays the progress of the current Unit Information file creation operation.

5 Click **Export**. The upload begins. The following fields display the status of the upload process:

- **File Transfer Status** – Displays the status of any pending Unit Information file upload. Possible values are:
  - **Ready** – The default value, which appears when no file transfer is in progress.
  - **File-in-transfer** – The upload operation is in progress.
  - **Success** – The file has been successfully uploaded.
  - **Failure** – The file was not successfully uploaded.

If you try to export the file before it has been created, the following error message appears: **Error #3-Invalid set value**.
If this occurs, wait about two minutes then click **Export** again.

- **File Creation Progress** – Displays the progress of the current Unit Information file upload operation.

15.6.2 Uploading a Unit Info File Via FTP or SFTP

When uploading a Unit Information file via FTP or SFTP, the PTP 850 functions as an FTP or SFTP client. You must install FTP or SFTP server software on the PC or laptop you are using to perform the upload. For details.

To generate and upload a Unit Information file via FTP or SFTP:

1 Install and configure an FTP server on the PC or laptop you are using to perform the upload.
2 Select **Platform** > **Management** > **Unit Info**. The Unit Info page opens.

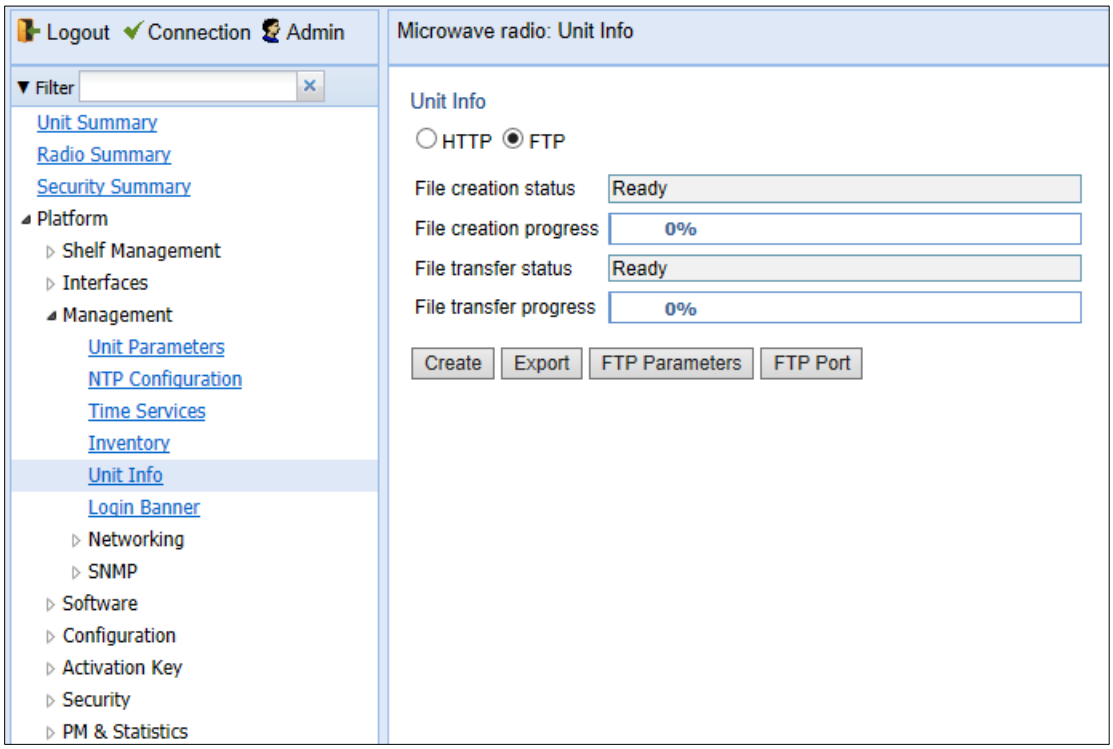


Figure 522: Unit Info Page – FTP/SFTP Upload

3 Select **FTP**.
4 Set the FTP parameters:

i Click **FTP Parameters**. The FTP Parameters page opens.

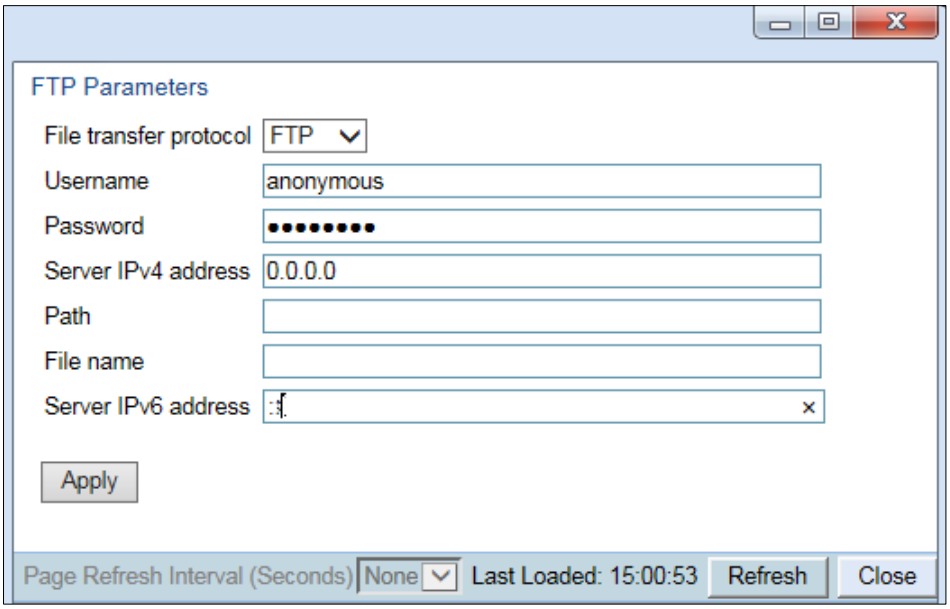


Figure 523: FTP Parameters Page

ii In the **File transfer protocol** field, select the file transfer protocol you want to use (**FTP** or **SFTP**).

iii In the **Username** field, enter the user name you configured in the FTP server.

iv In the **Password** field, enter the password you configured in the FTP server. If you did not configure a password for your FTP user, simply leave this field blank.

v If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the FTP server in the **Server IPv4 address** field. See Defining the IP Protocol Version for Initiating Communications.

vi In the **Path** field, enter the directory path to which you are uploading the files. Enter the path relative to the FTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".

vii In the **File name** field, enter the name you want to give to the exported security log.

viii If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the FTP server in the **Server IPv6 address** field. See Defining the IP Protocol Version for Initiating Communications.

ix Click **Apply**, then **Close**, to save the FTP parameters and return to the Unit Info page.

5 Click **Create** to create the Unit Information file. The following fields display the status of the file creation process:

- **File creation status** – Displays the file creation status. You must wait until the status is Success to upload the file. Possible values are:
  - **Ready** – The default value, which appears when no file is being created.
  - **Generating File** – The file is being generated.
  - **Success** – The file has been successfully created. You may now upload the file.
  - **Failure** – The file was not successfully created.
- **File creation progress** – Displays the progress of the current Unit Information file creation operation.

6 Click **Export**. The upload begins. The following fields display the status of the upload process:

- **File transfer status** – Displays the status of any pending Unit Information file upload. Possible values are:
  - **Ready** – The default value, which appears when no file transfer is in progress.
  - **File-in-transfer** – The upload operation is in progress.
  - **Success** – The file has been successfully uploaded.
  - **Failure** – The file was not successfully uploaded.
  - If you try to export the file before it has been created, the following error message appears: **Error #3-Invalid set value**. If this occurs, wait about two minutes then click **Export** again.
- **File transfer progress** – Displays the progress of the current Unit Information file upload operation.

15.7 Configuring Syslog

Syslog can be used to send Security Log, Event Log, and Configuration Log messages to up to two external Syslog servers. This can simplify network monitoring and maintenance for operators by enabling them to centralize troubleshooting and monitoring information for multiple network elements in a single location.

15.7.1 Syslog Overview

PTP 850's implementation of Syslog uses UDP protocol on port 514. The protocol and port are not configurable.

Syslog messages include the IP address of the device. This IP address is sent in the IP address format (IPv4 or IPv6) configured for the unit.

Optionally, for extra security you can enable TLS-based Secure Syslog. This enables server authentication, which means the client authenticates the Syslog server. This provides an extra layer of protection against various types of security threats, including masquerade, modification, and disclosure threats.

When Secure Syslog is enabled, the device uses the TCP port (6514) for Syslog messages.

Note: Secure Syslog requires that the server support TLS 1.2 or higher.

For units with unit redundancy, only the active unit sends Syslog messages. However, Syslog configurations are included in copy-to-mate actions.

Each Syslog message indicates the relevant log as follows:

- Security Log: Local0
- Event Log: Local1
- Configuration Log: Local2

Each Syslog message includes a numerical Priority value that categories messages according to their importance or severity, with lower Priority values indicating greater severity.

The Priority value is calculated according to the following formula:

(Facility Value*8) + Severity Value = Priority Value

The Facility Value is based on the log type, as follows:

- Security Log: 16
- Event Log: 17
- Configuration Log: 18

The Severity value is taken from Table 92: Syslog Severity Values. The mapping depends on the type of log and the severity of the item, as shown in Table 92.

Table 92: Syslog Severity Values

Device Entry Type	Syslog Severity	Syslog Description
	Emergency – 0	System is unusable
	Alert – 1	Action must be taken immediately
Event Log Entry with Severity = Critical	Critical – 2	Critical conditions
Event Log Entry with Severity = Major	Error – 3	Error conditions
Event Log Entry with Severity = Minor, Warning, or	Warning – 4	Warning conditions

Indeterminate		
	Notice – 5	Normal but significant condition
Security Log or Configuration Log Entry	Informational – 6	Informational messages
	Debug – 7	Debug-level messages

For example, a Major Alarm receives Syslog Priority 139. This is calculated as the Facility Value of 17, multiplied by 8, plus 3 based on the mapping in Table 92.

15.7.2 Syslog Configuration

You can configure up to two Syslog servers, using either IPv4 or IPv6 format. To configure Syslog:

1 Select **Platform > Management > Remote SysLog**. The Remote SysLog Server Configuration page opens.

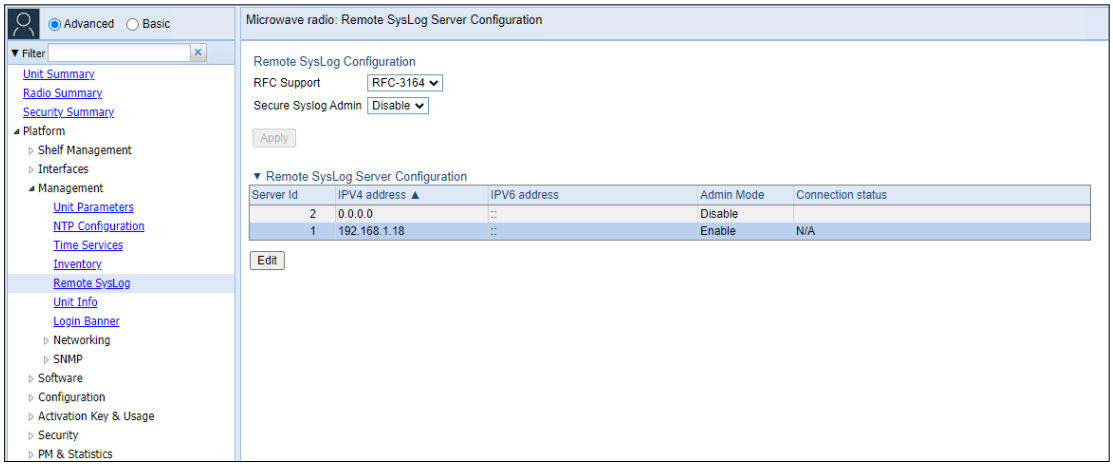


Figure 524: Remote SysLog Server Configuration Page

2 In the **RFC Support** field, select the message format. Options are:

- **RFC-3164** (default, also known as BSD format)
- **RFC-5424**

3 In the **Secure Syslog Admin** field, select **Enable** or **Disable** (default). Enabling Secure Syslog enables TLS-based Secure Syslog.

4 In the **Server ID** column, select 1 or 2 and click **Edit**.

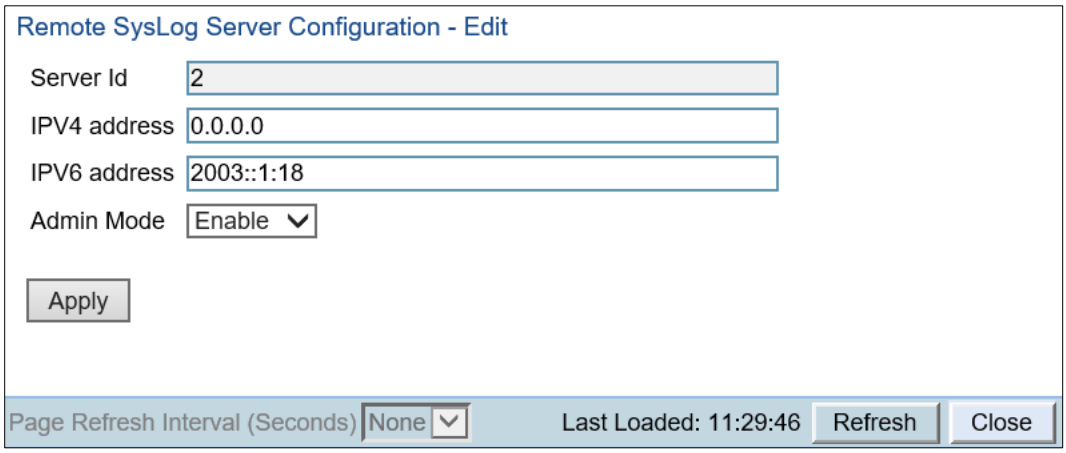


Figure 525: Remote SysLog Server Configuration Page – Edit

5 Enter an IP address in *either* the **IPV4 address** field or the **IPV6 address** field. You cannot enter an IP address in both formats for the same server.
6 In the **Admin Mode** field, select **Enable** to enable the server. Alternatively, you can select **Disable** and enable the server at a later time. The default setting is **Disable**.
7 Click **Apply**.

Note that events that exist as of when the Syslog server is enabled are *not* sent. Only events generated after the server is enabled are sent.

In the Remote SysLog Server Configuration page, the **Connection Status** column displays the status of the connection to each configured Syslog server. This is only applicable if **Secure Syslog Admin** is set to or **Enable**.

Possible values are:

- Status is empty – The **Admin Mode** for the server is set to **Disable**.
- **N/A** –**Secure Syslog Admin** is set to or **Disable**. Enabling Secure Syslog enables TLS-based Secure Syslog.
- **Unreachable** – The IP of the Syslog server is currently unreachable.
- **TLS Failure** – TLS handshake failed because of either TLS version mismatch or cipher suite mismatch during the TLS handshake.
- **Authentication Failure** – The server could not be authenticated.
- **Success** – TLS authentication was performed successfully and the device successfully connected to the Syslog server.

15.8 Performing Diagnostics

This section includes:

- Performing Radio Loopback
- Performing Ethernet Loopback
- Configuring Service OAM (SOAM) Fault Management (FM)

15.8.1 Performing Radio Loopback

Note

To perform radio loopback, the radio must be set to its maximum TX power. For reliable loopback results, the loopback should performed with the modulation at 1024 QAM or lower.

When performing RF loopback, the antenna port of the radio must be terminated. Due to a large variance in RF loopback measurements with PTP 850E, these measurements do not provide conclusive results about the radio status. Therefore we recommend not to use RF Loopback with PTP 850E.

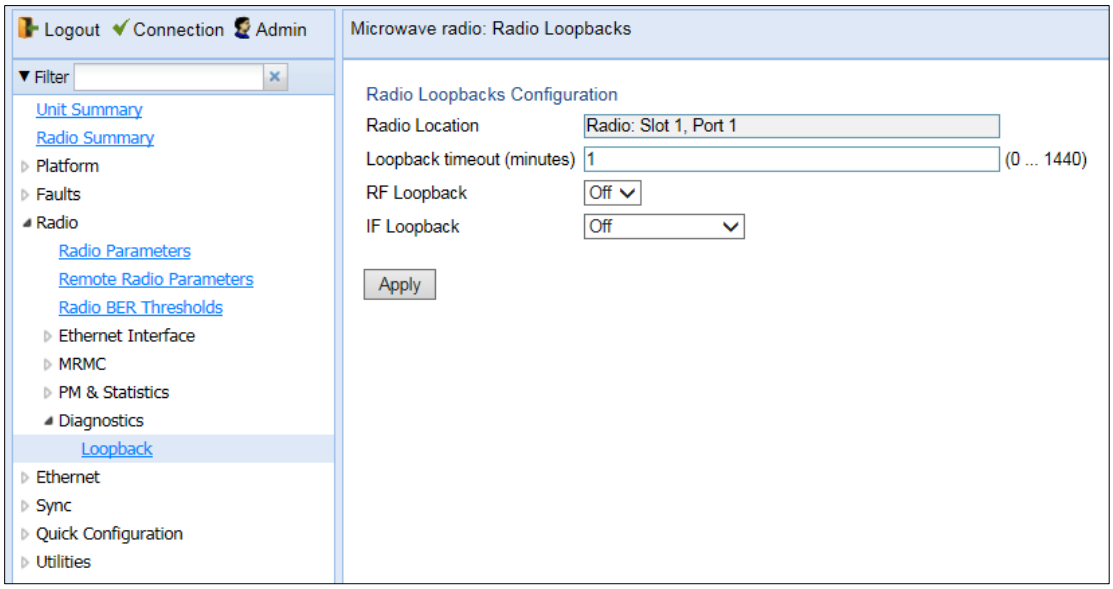
Setting radio loopback, either RF or IF, will cause full loss of the end-to-end traffic and in-band management to remote units. This is the case whether the loopback is on a single 1+0 radio link or on a member of a Multi-Carrier ABC group. To avoid permanent loss of traffic and in-band management, it is recommended to set a loopback timeout.

Do not change the TX or RX frequencies while radio loopback is active. Doing so will prevent the radio link from being re-established after the loopback has finished.

To perform loopback on a radio:

1. Select **Radio > Diagnostics > Loopback**. The Radio Loopbacks page opens.

Figure 526 Radio Loopbacks Page



2. In the **Loopback timeout (minutes)** field, enter the timeout, in minutes, for automatic termination of the loopback (0-1440). A value of 0 indicates that there is no timeout.
3. In the **RF loopback** field, select **On**.

Note

IF Loopback is planned for future release.

4. Click **Apply**.

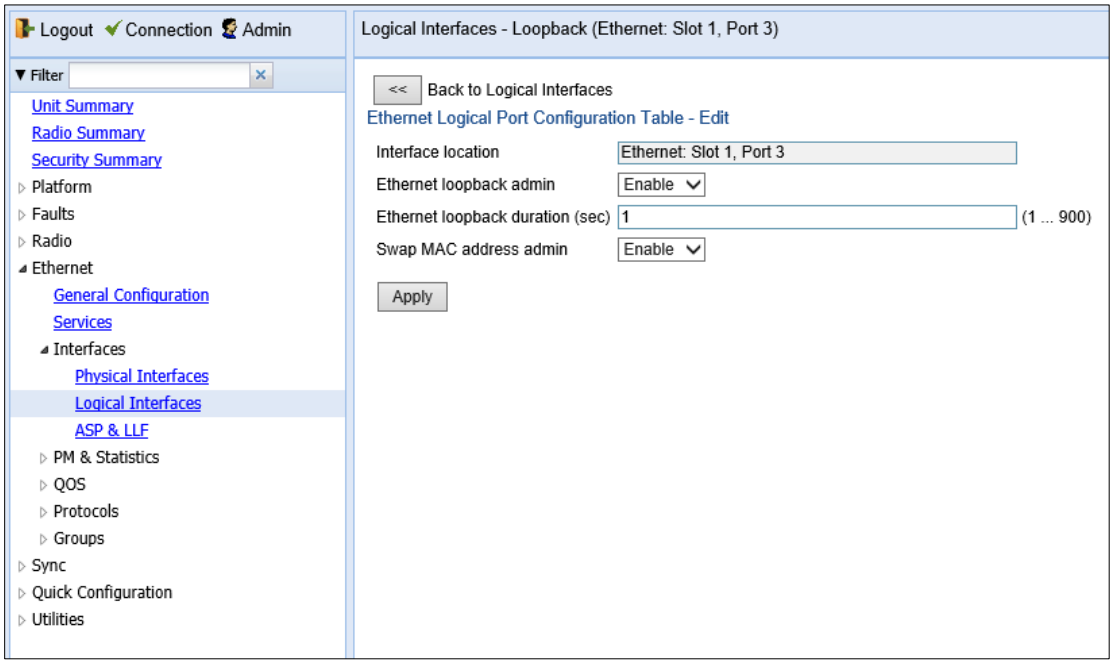
15.8.2 Performing Ethernet Loopback

Ethernet loopbacks can be performed on any logical Ethernet interface except a LAG. When Ethernet loopback is enabled on an interface, the system loops back all packets ingressing the interface. This enables loopbacks to be performed over the link from other points in the network.

To perform Ethernet loopback:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens.
2. Select an interface in the Ethernet Logical Port Configuration table and click **Loopback**. The Logical Interfaces – Loopback page opens.

Figure 527 Logical Interfaces – Loopback Page



3. In the **Ethernet loopback admin** field, select **Enable** to enable Ethernet loopback on the logical interface, or **Disable** to disable Ethernet loopback on the logical interface.
4. In the **Ethernet loopback duration (sec)** field, enter the loopback duration time (in seconds).
5. In the **Swap MAC address admin** field, select whether to swap DA and SA MAC addresses during the loopback. Swapping addresses prevents Ethernet loops from occurring. It is recommended to enable MAC address swapping if LLDP is enabled.
6. Click **Apply** to initiate the loopback.

15.8.3 Configuring Service OAM (SOAM) Fault Management (FM)

This section includes:

- SOAM Overview
- Configuring MDs
- Configuring MA/MEGs
- Configuring MEPs
- Displaying Remote MEPs
- Displaying Last Invalid CCMS
- Configuring MIPs with MHF Default
- Performing Loopback

SOAM Overview

The Y.1731 standards and the MEF-30 specifications define Service OAM (SOAM). SOAM is concerned with detecting, isolating, and reporting connectivity faults spanning networks comprising multiple LANs, including LANs other than IEEE 802.3 media.

Y.1731 Ethernet FM (Fault Management) consists of three protocols that operate together to aid in fault management:

- Continuity check
- Link trace
- Loopback



Note

Link trace is planned for future release.

PTP 850 utilizes these protocols to maintain smooth system operation and non-stop data flow.

The following are the basic building blocks of FM:

MD (Maintenance Domain) – An MD defines the management space on a network, typically owned and operated by a single entity, for which connectivity faults are managed via SOAM.

MA/MEG (Maintenance Association/Maintenance Entity Group) – An MA/MEG contains a set of MEPs or MIPs.

MEP (MEG End Points) – Each MEP is located on a service point of an Ethernet service at the boundary of the MEG. By exchanging CCMs (ContinuityCheck Messages), local and remote MEPs have the ability to detect the network status, discover the MAC address of the remote unit/port where the peer MEP is defined, and identify network failures.

MIP (MEG Intermediate Points) – Similar to MEPs, but located inside the MEG and can only respond to, not initiate, CCM messages.

CCM (Continuity Check Message) – MEPs in the network exchange CCMs with their peers at defined intervals. This enables each MEP to detect loss of connectivity or failure in the remote MEP.

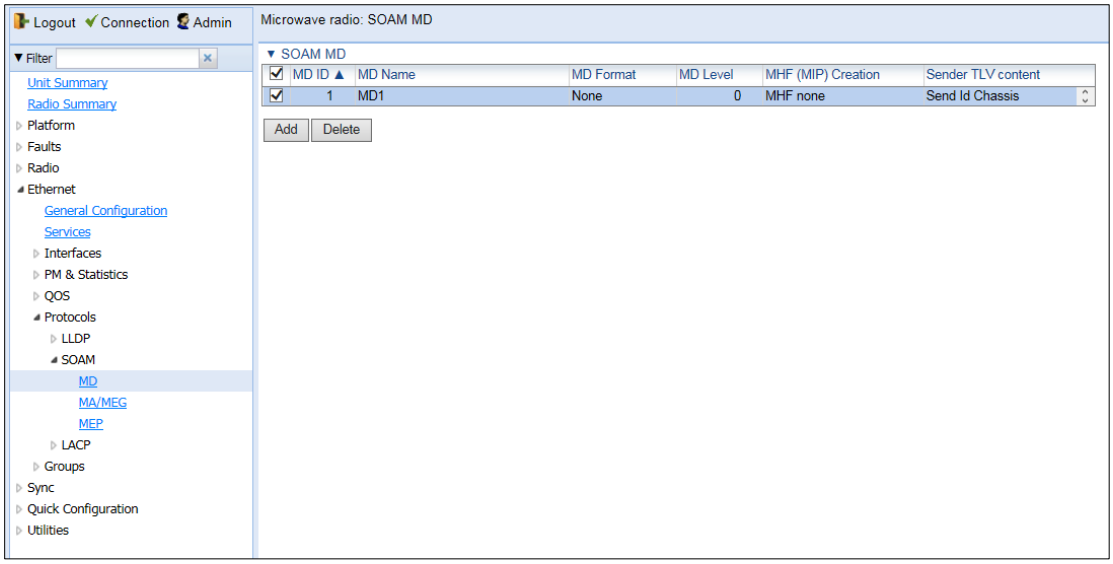
Configuring MDs

In the current release, you can define one MD, with an **MD Format** of **None**.

To add an MD:

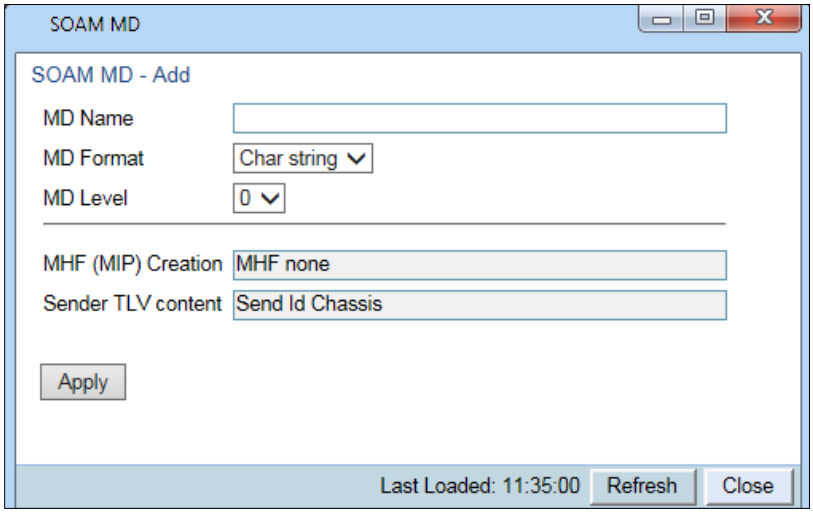
1. Select **Ethernet** > **Protocols** > **SOAM** > **MD**. The SOAM MD page opens.

Figure 528 SOAM MD Page



2. Click **Add**. The SOAM MD – Add page opens.

Figure 529 SOAM MD Page



3. In the **MD Name** field, enter an identifier for the MD (up to 43 alphanumeric characters). The MD Name should be unique over the domain.
4. In the **MD Format** field, select **None**.



Note

Support for MDs with the MD format Character String is planned for future release. In this release, the software enables you to configure such MDs, but they have no function.

5. In the **MD Level** field, select the maintenance level of the MD (1-7). The maintenance level ensures that the CFM frames for each domain do not interfere with each other. Where domains are nested, the encompassing domain must have a higher level than the domain it encloses. The maintenance level is carried in all CFM frames that relate to that domain. The **MD Level** must be the same on both sides of the link.



Note

In the current release, the MD level is not relevant to the SOAM functionality.

6. Click **Apply**, then **Close**.

The **MHF (MIP) Creation** field displays the contents of MHF format included in the CCMs sent in this MD (in the current release, this is **MHF none** and **MHF default**).

The **Sender TLV Content** field displays the contents of TLVs included in the CCMs sent in this MD (in the current release, this is only **Send ID Chassis**).

Configuring MA/MEGs

You can configure up to 64 MEP pairs per network element:

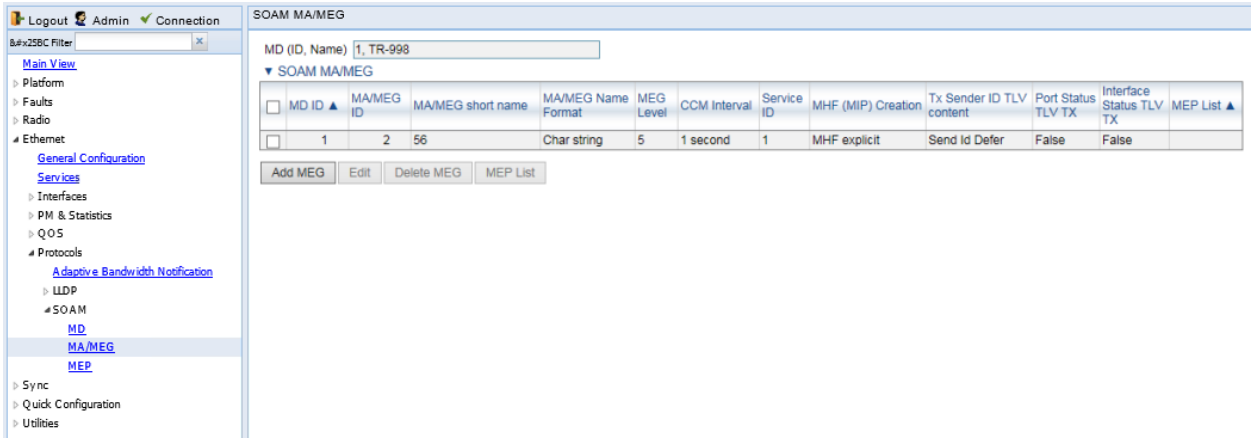
- Fast MEGs have a CCM interval of 1 second.
- Slow MEGs have a CCM interval of 10 seconds, 1 minute, or 10 minutes.

You can configure up to 32 MEP pairs per network element.

To add a MEG:

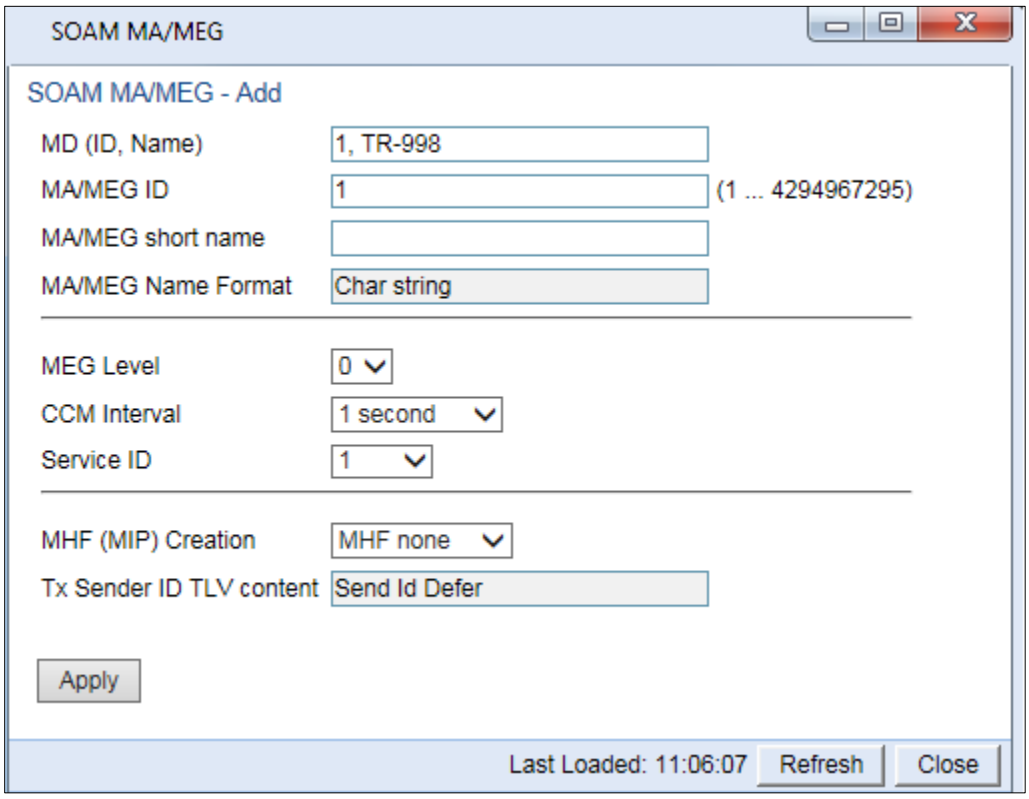
1. Select **Ethernet > Protocols > SOAM > MA/MEG**. The SOAM MA/MEG page opens.

Figure 530 SOAM MA/MEG Page



2. Click **Add MEG**. The SOAM MA/MEG – Add page opens.

Figure 531 SOAM MA/MEG – Add Page



3. Configure the fields described in Table 93.
4. Click **Apply**, then **Close**.

Table 94 describes the status (read-only) fields in the SOAM MA/MEG Component table.

Table 93 SOAM MA/MEG Configuration Parameters

Parameter	Definition
MD (ID, Name)	Select the MD to which you are assigning the MEP.
MA/MEG ID	Automatically generated by the system. You can change this value.
MA/MEG short name	Enter a name for the MEG (up to 44 alphanumeric characters).

Parameter	Definition
MEG Level	Select a MEG level (0-7). The MEG level must be the same for MEGs on both sides of the link. Higher levels take priority over lower levels. If MEGs are nested, the OAM flow of each MEG must be clearly identifiable and separable from the OAM flows of the other MEGs. In cases where the OAM flows are not distinguishable by the Ethernet layer encapsulation itself, the MEG level in the OAM frame distinguishes between the OAM flows of nested MEGs. Eight MEG levels are available to accommodate different network deployment scenarios. When customer, provider, and operator data path flows are not distinguishable based on means of the Ethernet layer encapsulations, the eight MEG levels can be shared among them to distinguish between OAM frames belonging to nested MEGs of customers, providers and operators. The default MEG level assignment among customer, provider, and operator roles is: • The customer role is assigned MEG levels 6 and 7. • The provider role is assigned MEG levels 3 through 5. • The operator role is assigned MEG levels: 0 through 2. The default MEG level assignment can be changed via a mutual agreement among customer, provider, and/or operator roles. The number of MEG levels used depends on the number of nested MEs for which the OAM flows are not distinguishable based on the Ethernet layer encapsulation.
CCM Interval	The interval at which CCM messages are sent within the MEG. Options are: • 1 second (default) • 10 seconds • 1 minute • 10 minutes It takes a MEP 3.5 times the CCM interval to determine a change in the status of its peer MEP. For example, if the CCM interval is 1 second, a MEP will detect failure of the peer 3.5 seconds after it receives the first CCM failure message. If the CCM interval is 10 minutes, the MEP will detect failure of the peer 35 minutes after it receives the first CCM failure message.

Parameter	Definition
Service ID	Select an Ethernet service to which the MEG belongs. You must define the service and add service points before you configure the MEG.
MHF (MIP) Creation	Determines whether MIPs are created on the MEG. Options are: • MHF none – No MIPs are created. • MHF default – MIPs are created automatically on any service point in the MEG's Ethernet service. • MHF explicit – MIPs are created on the service points of the MEG when a lower-level MEP exists on the service point. This option is usually used when the operator's domain is encompassed by another domain. MHF defer – No MIPs are created. Not used in the current release.

Table 94 SOAM MA/MEG Status Parameters

Parameter	Definition
MA/MEG Name Format	Reserved for future use. In the current release, this is Char String only.
Tx Sender ID TLV content	Reserved for future use. Sender ID TLV is not transmitted.
Port Status TLV TX	Reserved for future use. No Port Status TLV is transmitted in the CCM frame.
Interface Status TLV TX	Reserved for future use. No Interface Status TLV is transmitted in the CCM frame.
MEP List	Lists all local and remote MEPs that have been defined for the MEG.

Configuring MEPs

Each MEP is attached to a service point in an Ethernet service. The service and service point must be configured before you configure the MEP. See Configuring Ethernet Service(s).

Each MEP inherits the same VLAN, C-VLAN, or S-VLAN configuration as the service point on which it resides. See Configuring Service Points (CLI).Configuring Service Points

In order to set the VLAN used by CCM/LBM/LTM if the service point is defined ambiguously (for example PIPE, Bundle-C, Bundle-S, or All-to-One), the service point's C-VLAN/S-VLAN parameter should not be set to N.A.

To configure a MEP, you must:

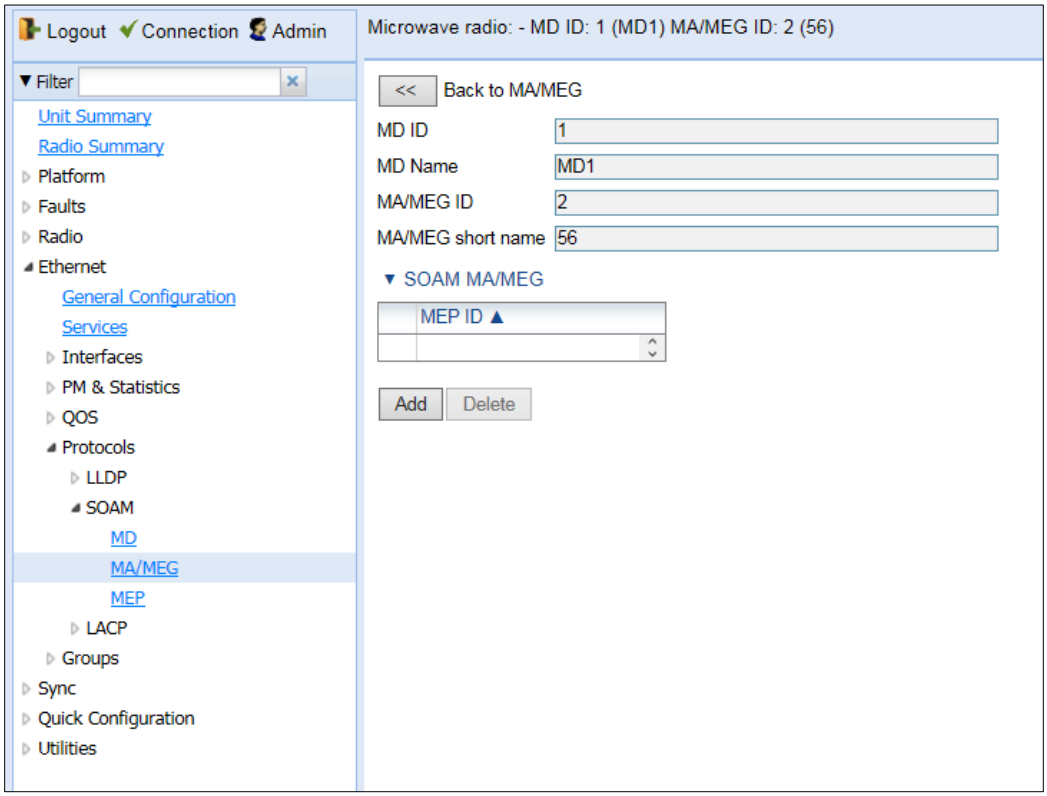
1. Add MEPs to the relevant MA/MEG. In this stage, you add both local and remote MEPs. The only thing you define at this point is the MEP ID. See Adding Local and Remote MEPs.
2. Configure the local MEPs. At this point, you determine which MEPs are local MEPs. The system automatically defines the other MEPs you configured in the previous step as remote MEPs. See Configuring the Local MEPs.
3. Enable the Local MEPs. See Enabling Local MEPs.

Adding Local and Remote MEPs

To add a MEP to the MA/MEG:

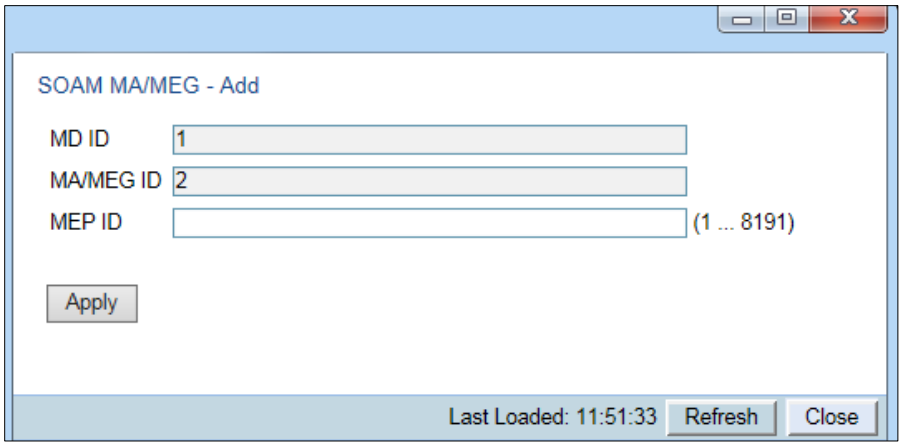
1. In the SOAM MA/MEG page, select a MA/MEG and click **MEP List**. The MEP List page opens.

Figure 532 MEP List Page



2. Click **Add**. The Add MEP page opens.

Figure 533 Add MEP Page



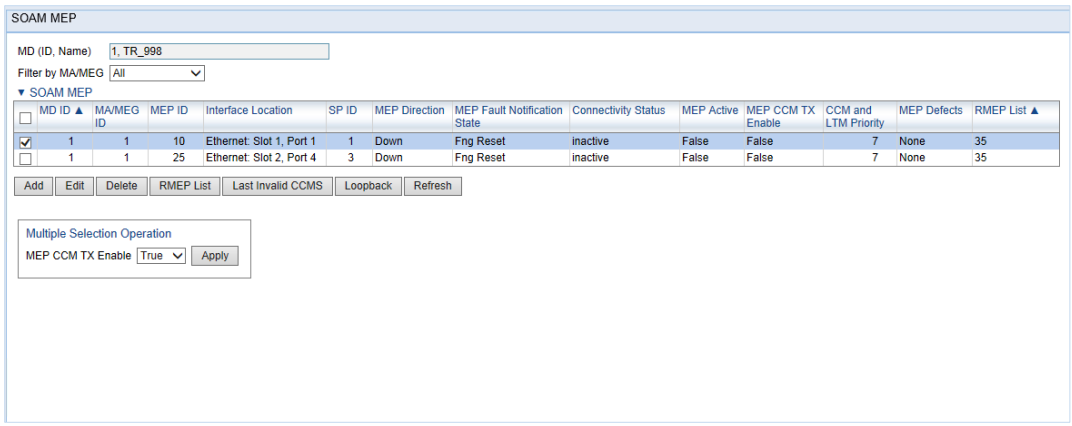
3. In the **MEP ID** field, enter a MEP ID (1-8191).
4. Click **Apply**, then **Close**.

Configuring the Local MEPs

Once you have added local and remote MEPs, you must define the MEPs and determine which are the local MEPs:

1. Select **Ethernet > Protocols > SOAM > MEP**. The SOAM MEP page opens. Table 95 lists and describes the parameters displayed in the SOAM MEP page.

Figure 534 SOAM MEP Page



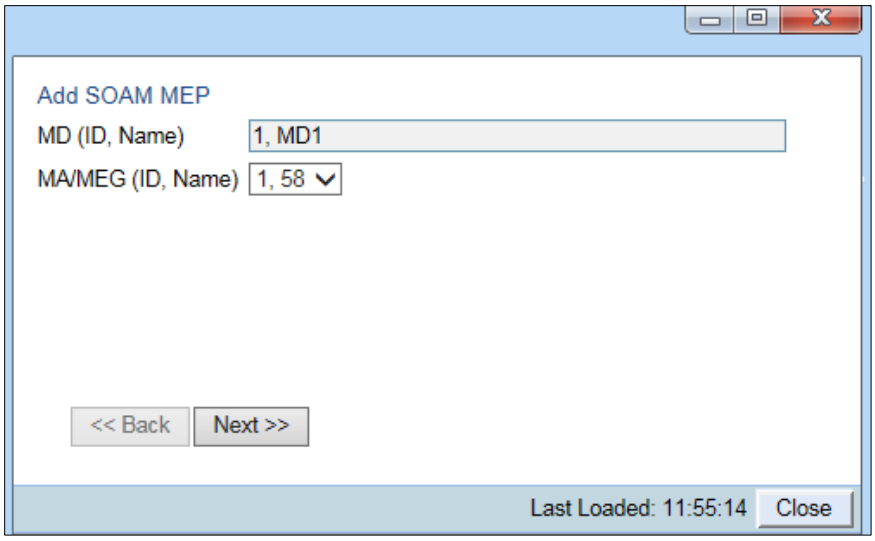


Note

To display MEPs belonging to a specific MEG, select the MEG in the **Filter by MA/MEG** field near the top of the SOAM MEP page. To display all MEPs configured for the unit, select **All**.

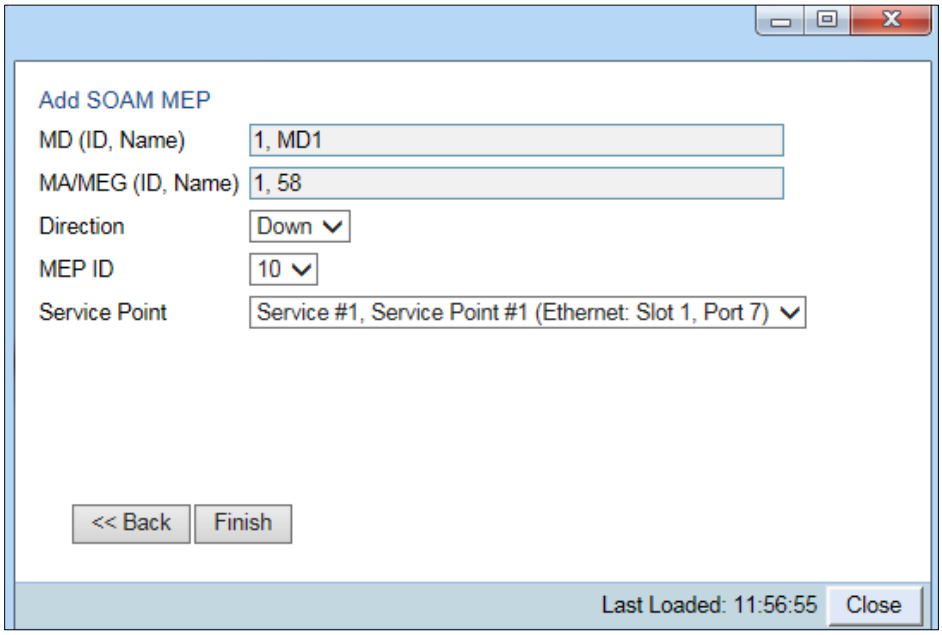
2. Click **Add**. Page 1 of the Add SOAM MEP wizard opens.

Figure 535 Add SOAM MEP Wizard – Page 1



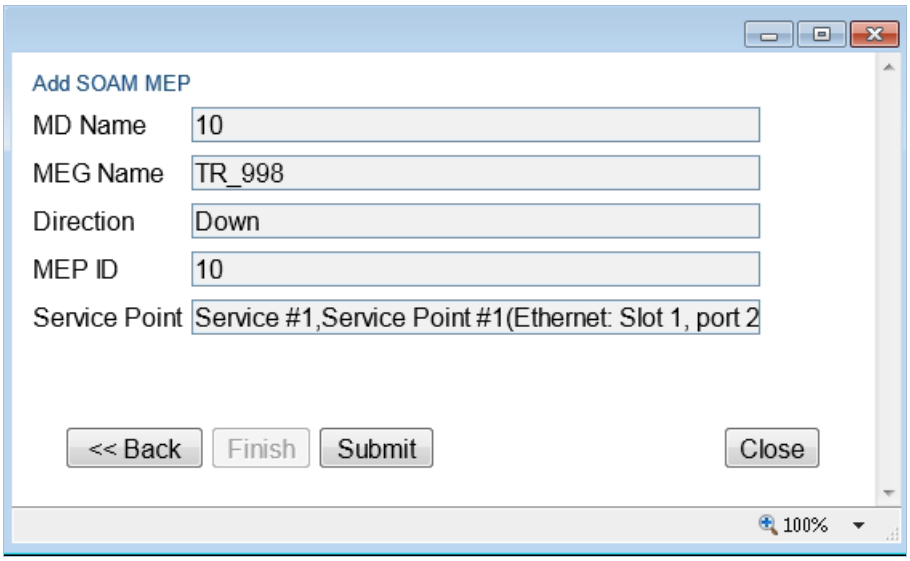
3. In the **MEG Name** field, select an MA/MEG.
4. Click **Next**. Page 2 of the Add SOAM MEP wizard opens.

Figure 536 Add SOAM MEP Wizard – Page 2



5. In the **Direction** field, select **Up** or **Down**.
6. In the **MEP ID** field, select a MEP ID from the list of MEPs you have added to the selected MEG.
7. In the **Service Point** field, select the service point on which you want to place the MEP.
8. Click **Finish**. The Add SOAM MEP wizard displays the parameters you have selected.

Figure 537 Add SOAM MEP Wizard –Summary Page



9. Verify that you want to submit the displayed parameters and click **Submit**.

Table 95 SOAM MEP Parameters

Parameter	Definition
MD (ID, Name)	The MD ID and name are automatically generated by the system.
MA/MEG (ID, Name)	The MA/MEG ID and name are automatically generated by the system.
MEP ID	The MEP ID.
Interface Location	The interface on which the service point associated with the MEP is located.
SP ID	The service point ID.
MEP Direction	**Up** or **Down**.
MEP Fault Notification State	The initial Indicates the status of the defect SOAM state machine. Possible values are: **Fng Reset** – Initial state. **Fng Defect** – Transient state when a defect is detected. **Fng Defect Reported** – The defect state is steady (stable). **Fng Defect Clearing** – Transient state when a defect is in the process of being cleared. **Fng Defect Cleared** – The defect has been cleared (Transient state).

Parameter	Definition
Connectivity Status	Indicates whether a MEP can exchange PDU (CCM, Loopback, LTR) with its remote MEP. A MEP with some defect or an inactive MEP cannot exchange PDUs. Possible values are: **inactive** – At least one of the MEPremote MEPs is enabled (**True**).in rMEPFailed status (not discovered). **active** – All remote MEPs are discovered correctly and have an rMEPOk status.
MEP Active	Indicates whether the MEP is enabled (**True**) or disabled (**False**).
MEP CCM TX Enable	Indicates whether the MEP is sending CCMs (**True/False**).
CCM and LTM Priority	The p-bit included in CCMs and/or LTM frames sent by this MEP (0 to 7).
MEP Defects	Indicates if a defect has been detected by the MEP level.
RMEP List	Once you have configured at least one local MEP, all other MEPs that you have added but not configured as local MEPs are displayed here, and are considered to be remote MEPs.

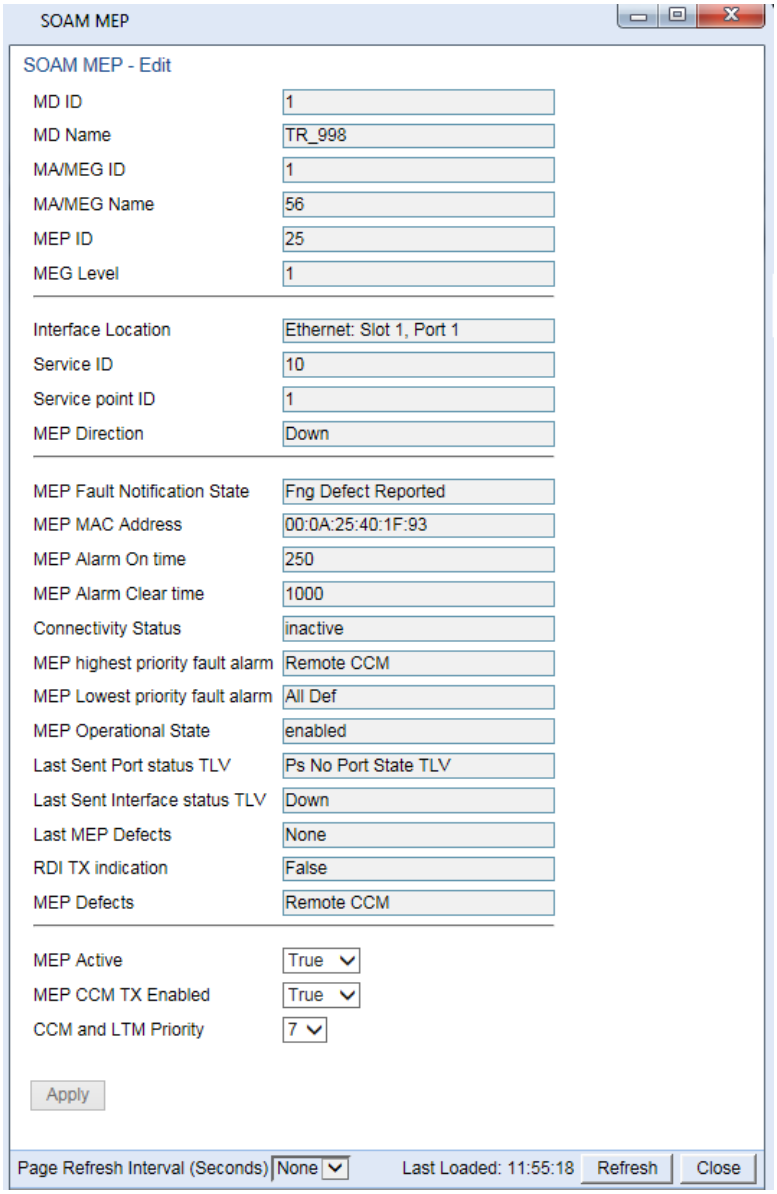
Enabling Local MEPs

Once you have added a MEP and defined it as a local MEP, you must enable the MEP.

To enable a MEP:

1. In the SOAM MEP page, select the MEP you want to enable.
2. Click **Edit**. The SOAM MEP - Edit page opens.

Figure 538 SOAM MEP - Edit Page



3. In the **MEP Active** field, select **True**.
4. In the **MEP CCM TX Enable** field, select **True**.
5. In the **CCM and LTM Priority** field, select the p-bit that will be included in CCMs sent by this MEP (0 to 7). It is recommended to select 7.
6. Click **Apply**, then **Close**.

15.8.3.2 Displaying Remote MEPs

To display a list of remote MEPs (RMEPs) and their parameters:

1. Select **Ethernet** > **Protocols** > **SOAM** > **MEP**. The SOAM MEP page opens.
2. Select a MEP and click **RMEP List**. The SOAM MEP DB table is displayed.

Figure 539 SOAM MEP DB Table

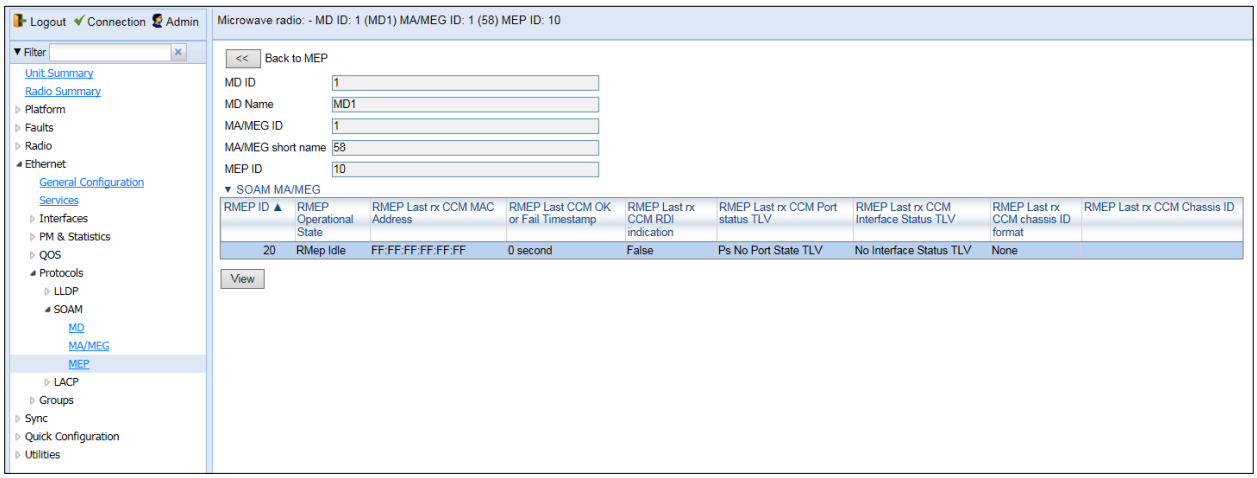


Table 96 lists and describes the parameters displayed in the SOAM MEP DB table. To return to the SOAM MEP page, click **Back to MEP**.

Note

To display these parameters in a separate window for a specific remote MEP, select the RMEP ID and click View.

Table 96 SOAM MEP DB Table Parameters

Parameter	Definition
RMEP ID	The remote MEP ID.
RMEP Operational State	The operational state of the remote MEP.
RMEP Last rx CCM MAC Address	The MAC Address of the interface on which the remote MEP is located.
RMEP Last CCM OK or Fail Timestamp	The timestamp marked by the remote MEP indicated the most recent CCM OK or failure it recorded. If none, this field indicates the amount of time since SOAM was activated.
RMEP Last rx CCM RDI Indication	Displays the state of the RDI (Remote Defect Indicator) bit in the most recent CCM received by the remote MEP: • True – RDI was received in the last CCM. • False – No RDI was received in the last CCM.
RMEP Last rx CCM Port Status TLV	The Port Status TLV in the most recent CCM received from the remote MEP. Reserved for future use.

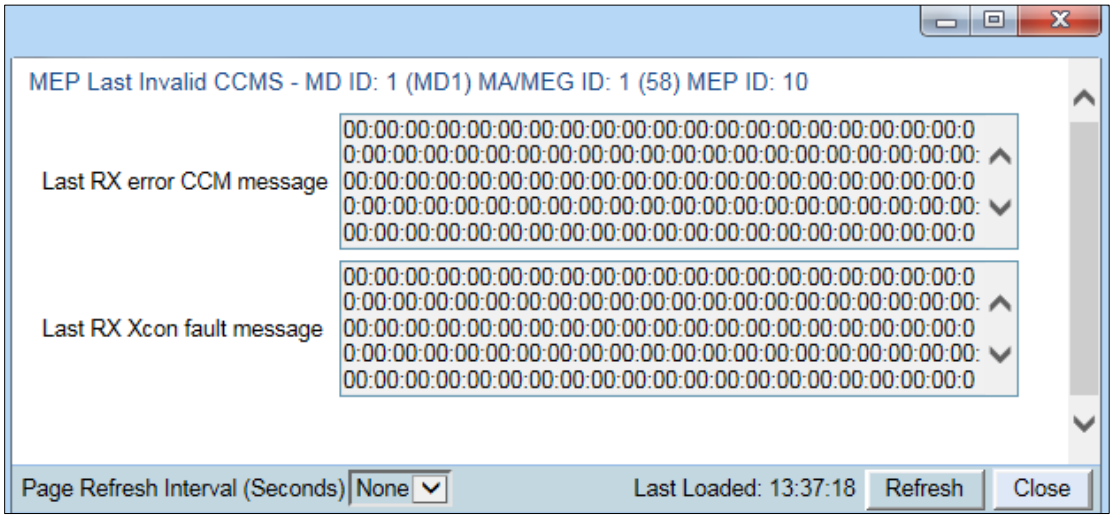
Parameter	Definition
RMEP Last rx CCM Interface Status TLV	Displays the operational status of the interface on which the remote MEP has been defined.
RMEP Last rx CCM Chassis ID Format	Displays the format of the remote chassis (always the MAC address).
RMEP Last rx CCM Chassis ID	Displays the MAC address of the remote chassis.

15.8.3.3 Displaying Last Invalid CCMS

To display the entire frame of the last CCM error message and the last CCM cross-connect error message received by a specific local MEP:

1. Select **Ethernet > Protocols > SOAM > MEP**. The SOAM MEP page opens (Figure 534).
2. Select a MEP and click **Last Invalid CCMS**. The MEP Last Invalid CCMS page opens.

Figure 540 MEP Last Invalid CCMS Page



The **Last RX error CCM message** field displays the frame of the last CCM that contains an error message received by the MEP.

The **Last RX Xcon fault message** field displays the frame of the last CCM that contains a cross-connect error message received by the MEP.

Note

A cross-connect error occurs when a CCM is received from a remote MEP that has not been defined locally.

Configuring MIPs with MHF Default

If you configure a MEG with the MHF default option, MIPS are created automatically on all service points of the service to which the MEG is attached. These MIPs cannot be displayed in the Web EMS, but can be displayed via CLI.

Creating MIPs is subject to the following limitations:

Once you have created a MEG that contains MIPS, i.e., a MEG with the MHF default attribute, you cannot create a MEG with the MHF none attribute on the same or higher level on the same Ethernet Service. However, you can create MEGs with the MHF none attribute on the same service on lower levels then the MEG with the MHF default attribute.

MEPs cannot be attached to a MEG with the MHF default attribute.

The Ethernet service and service points must already be defined before creating the MEG with the MHF default attribute in order for MIPs to be created on the service points.

To configure MEGs with MIPs:

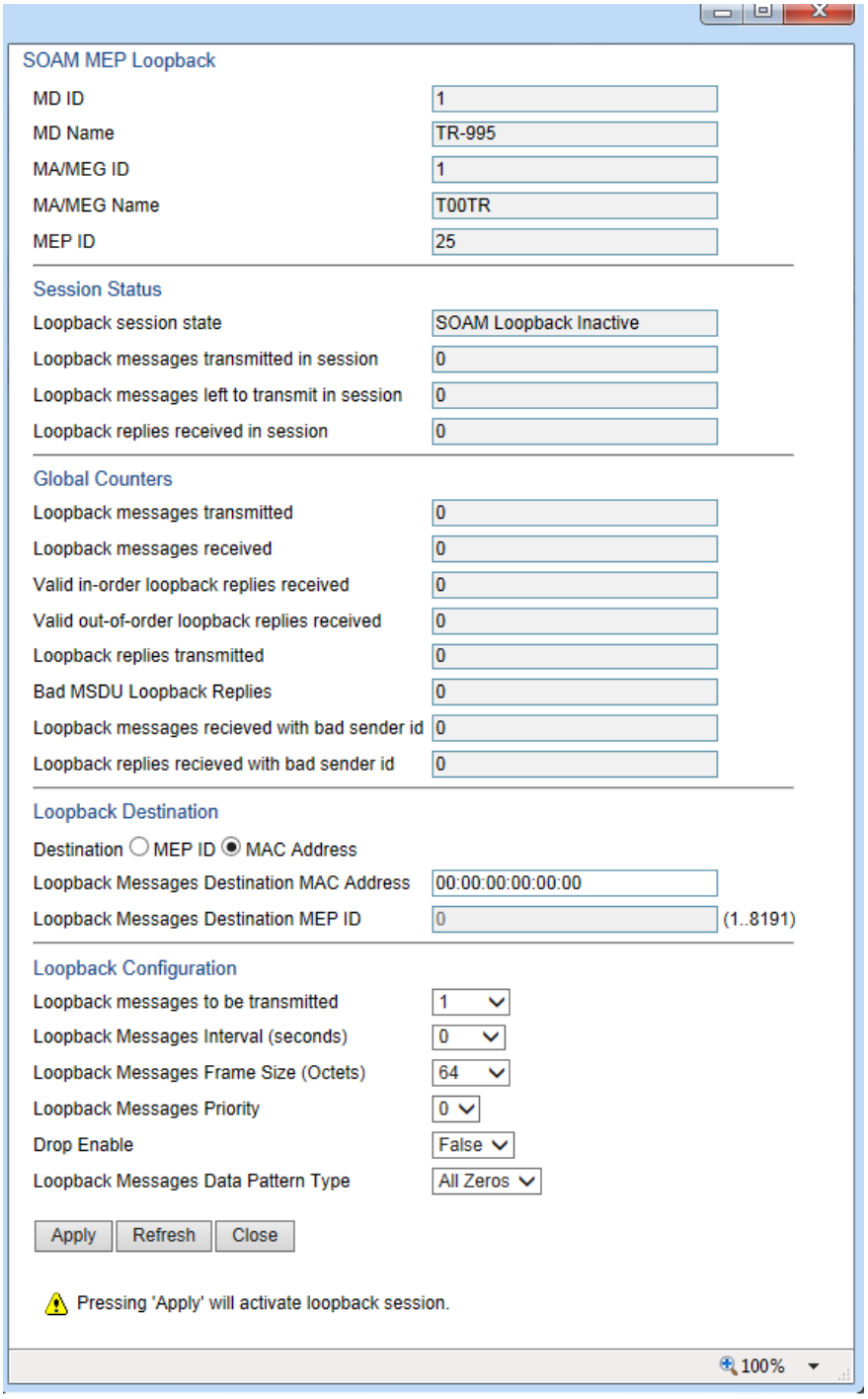
1. Create a MEG with the MHF none attribute on the intended Ethernet service. See Configuring MA/MEGs.
2. Select the MEG and click **Edit**. The SOAM MA/MEG – Edit page opens.
3. In the **MIP Creation** field, select **MHF Default**.
4. Click **Apply**, then **Close**.

Performing Loopback

To perform loopback on a MEP:

1. In the SOAM MEP page (Figure 534), select the MEP on which you want to perform the loopback.
2. Click **Loopback**. The SOAM MEP – Loopback page opens.

Figure 541 SOAM MEP Loopback Page



3. In the Loopback Destination area, select from the following options:

   MEP ID – If you select **MEP ID**, you must enter the MEP ID of the MEP on the interface to which you want to perform the loopback in the **Loopback Messages Destination MEP ID** field. If you select **MEP ID**, the loopback will only be activated if CCMs have already been received from the MEP. For this reason, it is recommended to initiate loopback via MAC address.

MAC Address (default) – If you select **MAC Address**, you must enter the MAC address of the interface to which you want to send the loopback in the **Loopback Messages Destination MAC Address**. If you are not sure what the interface's MAC address is, you can get it from the Interface Manager by selecting **Platform > Management > Interface Manager.**

4. In the **Loopback messages to be transmitted** field, select the number of loopback messages to transmit (0 – 1024). If you select 0, loopback will not be performed.
5. In the **Loopback Messages Interval** field, select the interval (in seconds) between each loopback message (0.1 – 60). You can select in increments of 1/10 second. However, the lowest possible interval is 1 second. If you select a smaller interval, the actual interval will still be 1 second.
6. In the **Loopback Messages Frame Size** field, select the frame size for the loopback messages (64 – 1516). Note that for tagged frames, the frame size will be slightly larger than the selected frame size.
7. In the **Loopback Messages Priority** field, select a value (0 – 7) for the priority bit for tagged frames.
8. In the **Drop Enable** field, choose the value of the DEI field for tagged loopback frames (**True** or **False**). The default value is **False**.
9. In the **Loopback Messages Data Pattern Type** field, select the type of data pattern to be sent in an OAM PDU Data TLV. Options are **All Zeros** and **All Ones**. The default value is **All Zeros**.
10. Click **Apply** to begin the loopback. The **Loopback session state** field displays the status of the loopback:
    - **SOAM Loopback Complete** – The loopback has been successfully completed.
    - **SOAM Loopback Stopped** – The loopback has been manually stopped.
    - **SOAM Loopback Failed** – The loopback failed.
    - **SOAM Loopback Active** – The loopback is currently active.
    - **SOAM Loopback Inactive** – No loopback has been initiated.

The remote interface will answer and the loopback session will be completed if either of the following is true:

A remote MEP has been defined on the destination interface.

A MIP has been defined on the destination interface. See Configuring MIPs with MHF Default.



Note

To manually stop a loopback, you must use the CLI. Enter the following command in root view:
root> ethernet soam loopback stop meg-id <meg-id> mep-id <mep-id>

16. Web EMS Utilities

This section includes:

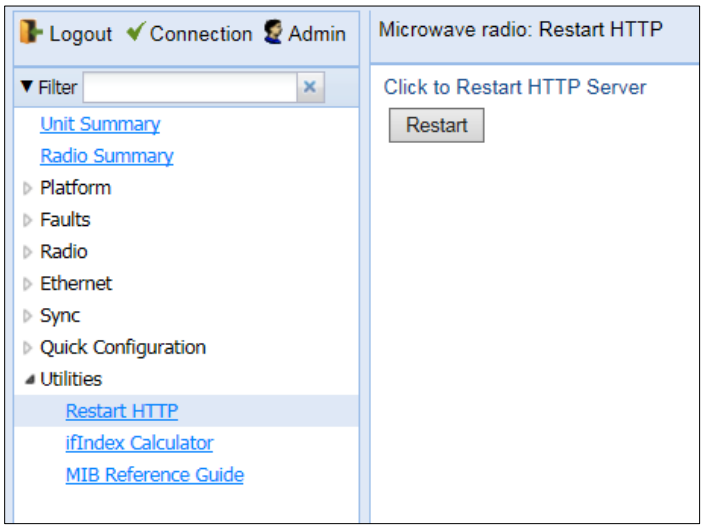
- Restarting the HTTP Server
- Calculating an ifIndex
- Displaying, Searching, and Saving a list of MIB Entities

16.1 Restarting the HTTP Server

To restart the unit's HTTP server:

1 Select **Utilities > Restart HTTP**. The Restart HTTP page opens.

Figure 542 Restart HTTP Page



2 Click **Restart**. The system prompts you for confirmation.

3 Click **OK**. The HTTP server is restarted, and all HTTP sessions are ended. After a few seconds, the Web EMS prompts you to log in again.

16.2 Calculating an ifIndex

The ifIndex calculator enables you to:

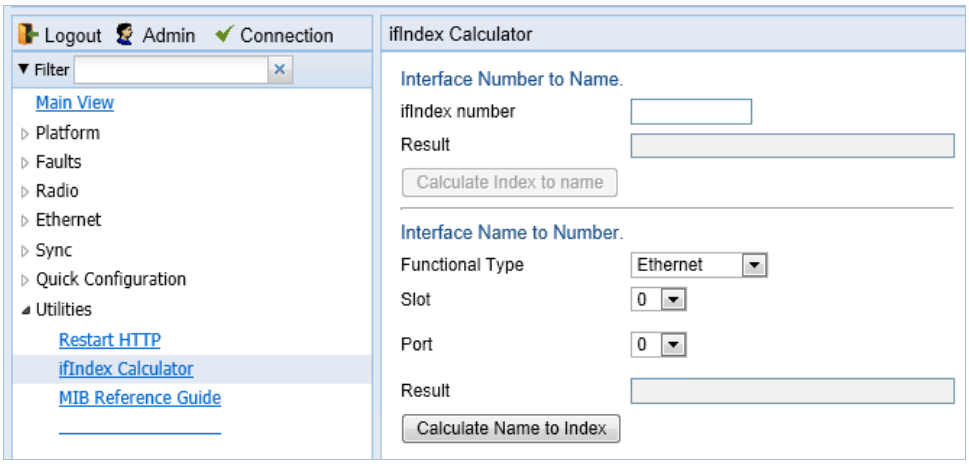
Calculate the ifIndex for any object in the system.

Determine the object represented by any valid ifIndex.

To use the ifIndex calculator:

1 Select **Utilities > ifCalculator**. The ifIndex Calculator page opens.

Figure 543 ifIndex Calculator Page



If you have an ifIndex and you want to determine which hardware item in the unit it represents, enter the number in the **ifIndex number** field and click **Calculate Index to name**. A description of the object appears in the **Result** field.

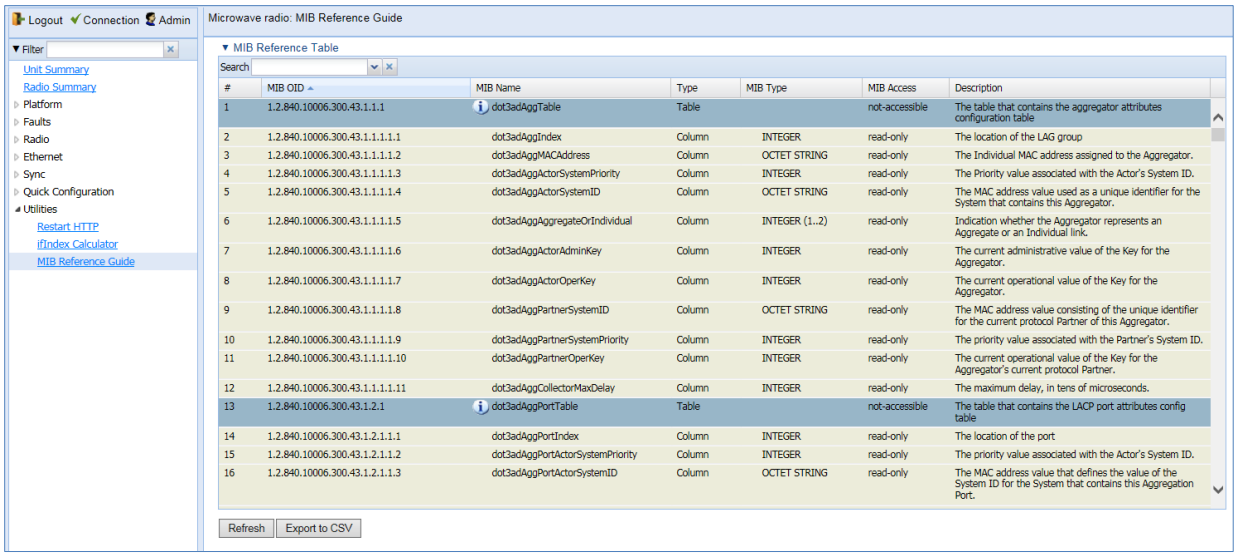
To determine the ifIndex of a hardware item in the unit, such as an interface, card, or slot, select the object type in the **Functional Type** field, select the **Slot** and **Port** (if relevant), and click **Calculate Name to Index**. The object's ifIndex appears in the **Result** field.

16.3 Displaying, Searching, and Saving a list of MIB Entities

To display a list of entities in the PTP 850 private MIB:

1 Select **Utilities > ifCalculator**. The ifIndex Calculator page opens.

Figure 544 MIB Reference Table Page



Note

Some of the entities listed in the Table may not be relevant to the particular unit you are using. This may occur because of activation key restrictions, minor differences between hardware types, or simply because a certain feature is not used in a particular configuration.

To search for a text string, enter the string in the Search field and press <Enter>. Items that contain the string are displayed in yellow. Searches are not case-sensitive.

To save the MIB Reference Table as a .csv file, click **Save to File**.

17. Getting Started (CLI)

This section includes:

- General (CLI)
- Establishing a Connection (CLI)
- Logging On (CLI)
- General CLI Commands
- Changing Your Password (CLI)
- Configuring In-Band Management (CLI)
- Changing the Management IP Address (CLI)
- Enabling Dynamic IPv6 Addresses Via DHCPv6 (CLI)
- Configuring DSCP/TC for Management (CLI)
- Configuring the Activation Key (CLI)
- Setting the Time and Date (Optional) (CLI)
- Enabling the Interfaces (CLI)
- Configuring the Radio (MRMC) Script(s) (CLI)
- Configuring the RSL Threshold Alarm (CLI)
- Creating Service(s) for Traffic (CLI)
- Configuring CPRI (CLI)
- Operating in FIPS Mode (CLI)
- Encrypting the External Protection Link (CLI)

17.1 General (CLI)

Before connection over the radio hop is established, it is of high importance that you assign to the PTP 850 unit a dedicated IP address, according to an IP plan for the total network.

By default, a new PTP 850 unit has the following IP settings:

- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0



Caution

If the connection over the link is established with identical IP addresses, an IP address conflict will occur and remote connection to the element on the other side of the link may be lost.

17.2 Establishing a Connection (CLI)

Connect the PTP 850 unit to a PC by means of a Twisted Pair cable. The cable is connected to the MGT port on the PTP 850 and to the LAN port on the PC. Refer to the Installation Guide for the type of unit you are connecting for cable connection instructions.



Note

The PTP 850 IP address, as well as the password, should be changed before the system is set in operation.

17.2.1 PC Setup (CLI)

To obtain contact between the PC and the PTP 850 unit, it is necessary to have an IP address on the PC within the same subnet as the PTP 850 unit. The default PTP 850 IP address is 192.168.1.1. Set the PC address to e.g. 192.168.1.10 and subnet mask to 255.255.255.0. Note the initial settings before changing.



Note

The PTP 850 IP address, as well as the password, should be changed before operating the system is set in operation.

17.3 Logging On (CLI)

Use a telnet connection to manage the PTP 850 via CLI. You can use any standard telnet client, such as PuTTy or ZOC Terminal. Alternatively, you can simply use the `telnet <ip address>` command from the CMD window of your PC or laptop.

The default IP address of the unit is 192.168.1.1. Establish a telnet connection to the unit using the default IP address.

When you have connected to the unit, a login prompt appears. For example:

```
login:
```

At the prompt, enter the default login user name: `admin`

A password prompt appears. Enter the default password: `admin`

The root prompt appears. For example:

```
login as: admin
```

```
admin@192.168.1.1's password:

Last login: Sat Apr 1 01:46:26 from 192.168.1.10

root>
```

17.4 General CLI Commands

To display all command levels available from your current level, press <TAB> twice. For example, if you press <TAB> twice at the root level, the following is displayed:

```
root>
auto-state-propagation    ethernet  exit   multi-carrier-abc
platform        quit        radio      radio-groups
switch-back    switch-to     wait
```

Some of these are complete commands, such as `quit` and `exit`. Others constitute the first word or phrase for a series of commands, such as `ethernet` and `radio`.

Similarly, if you enter the word “platform” and press <TAB> twice, the first word or phrase of every command that follows platform is displayed:

```
root> platform
activation-key     configuration   if-manager      management
security      software                status
sync       unit-info      unit-info-file
root> platform
```

To auto-complete a command, press <TAB> once.

Use the up and down arrow keys to navigate through recent commands.

Use the ? key to display a list of useful commands and their definitions.

> At the prompt, or at any point in entering a command, enter the word `help` to `display` a list of available commands. If you enter `help` at the prompt, a list of all commands is displayed. If you enter `help after entering part of a command, a list of commands that start with the portion of the command you have already entered is displayed.`

To scroll up and down a list, use the up and down arrow keys.

To end the list and return to the most recent prompt, press the letter `q`.

To ping another network device, enter one of the following commands:

```
root> ping ipv4-address <x.x.x.x> count <number of echo packets>
packet-size <packet-size>

root> ping ipv6-address <ipv6> count <number of echo packets>
packet-size <packet-size>
```

The optional `count` parameter determines how many packets are sent. This parameter can be an integer from 1 to 1000. The default value is 4.

The optional `packet-size` parameter determines the size of each packet, in bytes. This parameter can be an integer from 64 to 1480. The default value is 64.

The `ping` command is available from all views (e.g., root, interface views, group views).

17.4.1 Changing Your Password (CLI)

It is recommended to change your default Admin password as soon as you have logged into the system. If you do not change your default Admin password within ten days after the first unit boot up, or the first unit boot up after upgrading to System release 12.7 or higher from an earlier System release version, an alarm is raised:

- Alarm Name: admin-password-change-required-alarm
- Alarm Description: 'admin' user password needs to be changed

Note: If the system reboots within ten days, the 10 day count starts over.

In addition to the Admin password, there is an additional password protected user account, “root user”, which is configured in the system. The root user password and instructions for changing this password are available from Cambium Customer Support. It is strongly recommended to change this password.

To change your password, enter the following command in root view:

```
root> platform security access-control password edit own-password
```

The system will prompt you to enter your existing password. The system will then prompt you to enter the new password.

If Enforce Password Strength is activated, the password must meet the following criteria:

- Password length must be at least eight characters.
- Password must include characters of at least three of the following character types: lower case letters, upper case letters, digits, and special characters.
- No character can be repeated three times, e.g., aaa, ###, 333.
- No more than two consecutive characters can be used, e.g., ABC, DEF, 123.
- The user name string cannot appear in the password, either in order or in reverse order. For example, if the user name is “admin”, neither of the following passwords are allowed: %Asreadmin!df23 and %Asrenimda!df23.

17.5 Configuring In-Band Management (CLI)

You can configure in-band management in order to manage the unit remotely via its radio and/or Ethernet interfaces.



Note

Before configuring in-band management, it is recommended to review the configuration recommendations for in-band management listed in Configuration Tips.

Each PTP 850E unit includes a pre-defined management service with Service ID 1025. The management service is a multipoint service that connects the two local management ports and the network element host CPU in a single service. In order to enable in-band management, you must add at least one service point to the management service, in the direction of the remote site or sites from which you want to access the unit for management. For instructions on adding service points, see Configuring Service Points (CLI).

After adding service points, you must enable in-band management using the following command in root view:

```
root> platform management in-band state set admin enable
```

To display the current in-band management admin status, enter the following command in root view:



Note

In order to use in-band management, it must be supported on the external switch.

```
root> platform management in-band state show
```

17.6 Changing the Management IP Address (CLI)

Related Topics:

- Defining the IP Protocol Version for Initiating Communications (CLI)
- Configuring the Remote Unit's IP Address (CLI)

You can enter the unit's address in IPv4 format and/or in IPv6 format. The unit will receive communications whether they were sent to its IPv4 address or its IPv6 address.

To set the unit's IP address in IPv4 format, enter the following command in root view to configure the IP address, subnet mask, and default gateway:

```
root> platform management ip set ipv4-address <ipv4-address> subnet <subnet>
gateway <gateway> name <name> description <name>
```

Table 97 IP Address (IPv4) CLI Parameters

Parameter	Input Type	Permitted Values	Description
ipv4-address	Dotted decimal format.	Any valid IPv4 address.	The IP address for the unit.
subnet	Dotted decimal format.	Any valid subnet mask.	The subnet mask for the unit.
gateway	Dotted decimal format.	Any valid IPv4 address.	The default gateway for the unit (optional).

Parameter	Input Type	Permitted Values	Description
name	Text String.		Enter a name (optional).
description	Text String.		Enter a description (optional).

To set the unit's IP address in IPv6 format, enter the following command in root view to configure the IP address, subnet mask, and default gateway:

```
root> platform management ip set ipv6-address <ipv6-address>
prefix-length <prefix-length> gateway <gateway>
```



Note

It is recommended not to configure addresses of type FE:80::/64 (Link Local addresses) because traps are not sent for these addresses.

Table 98 IP Address (IPv6) CLI Parameters

Parameter	Input Type	Permitted Values	Description
ipv6-address	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The IP address for the unit.
prefix-length	Number.	1-128	The prefix-length for the unit.
gateway	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The default gateway for the unit (optional).

Examples

The command below sets the following parameters:

IPv4 Address - 192.168.1.160

Subnet Mask – 255.255.0.0

Default Gateway – 192.168.1.100

```
root> platform management ip set ipv4-address 192.168.1.160
subnet 255.255.0.0 gateway 192.168.1.100
```

The command below sets the following parameters:

IPv6 Address - FE80:0000:0000:0000:0202:B3FF:FE1E:8329

Prefix length – 64

Default Gateway - FE80:0000:0000:0000:0202:B3FF:FE1E:8329

```
root> platform management ip set ipv6-address
FE80:0000:0000:0000:0202:B3FF:FE1E:8329 prefix-length 64 gateway
FE80:0000:0000:0000:0202:B3FF:FE1E:8329
```

17.7 Configuring the Activation Key (CLI)

This section includes:

- Activation Key Overview (CLI)
- Viewing the Activation Key Status Parameters (CLI)
- Entering the Activation Key (CLI)
- Activating a Demo Activation Key (CLI)
- Displaying a List of Activation-Key-Enabled Features (CLI)

17.7.1 Activation Key Overview (CLI)

PTP 850 offers a pay-as-you-grow concept in which future capacity growth and additional functionality can be enabled with activation keys. For purposes of the activation keys, each PTP 850 chassis is considered a distinct device, regardless of which cards are included in the chassis. Each device contains a single unified activation key cipher.

New PTP 850 units are delivered with a default activation key that enables you to manage and configure the unit. Additional feature and capacity support requires you to enter an activation key. Contact your vendor to obtain your activation key cipher.

Each required feature and capacity should be purchased with an appropriate activation key. It is not permitted to enable features that are not covered by a valid activation key. In the event that the activation-key-enabled capacity and feature set is exceeded, an Activation Key Violation alarm occurs and the Web EMS displays a yellow background and an activation key violation warning. After a 48-hour grace period, all other alarms are hidden until the capacity and features in use are brought within the activation key's capacity and feature set.

In order to clear the alarm, you must configure the system to comply with the activation key that has been loaded in the system. The system automatically checks the configuration to ensure that it complies with the activation-key-enabled features and capacities. If no violation is detected, the alarm is cleared.

When entering sanction state, the system configuration remains unchanged, even after power cycles. However, the alarms remain hidden until an appropriate activation key is entered or the features and capacities are re-configured to be within the parameters of the current activation key.

A demo activation key is available that enables all features for 60 days. When the demo activation key expires, the most recent valid activation key goes into effect. The 60-day period is only counted when the system is powered up. Ten days before the demo activation key expires, an alarm is raised indicating that the demo activation key is about to expire.

17.7.2 Viewing the Activation Key Status Parameters (CLI)

To display information about the currently installed activation key, enter the following command in root view:

```
root> platform activation-key show all
```

17.7.3 Entering the Activation Key (CLI)

To enter the activation key, enter the following command in root view.

```
root> platform activation-key set key string <key string>
```

If the activation key is not legal (e.g., a typing mistake or an invalid serial number), an Activation Key Loading Failure event is sent to the Event Log. When a legal activation key is entered, an Activation Key Loaded Successfully event is sent to the Event Log.

To set the default activation key, enter the following command in root view:

```
root> platform activation-key set key string "Default Activation Key"
```



Note: Make sure to enter the command using the exact syntax above, including the spaces

	and quotation marks, or an error will be returned.

17.7.4 Activating a Demo Activation Key (CLI)

To activate the demo activation key, enter the following command in root view:

```
root> platform activation-key set demo admin enable
```

To display the current status of the demo activation key, enter the following command in root view:

```
root> platform activation-key show demo status
```

17.7.5 Activation Key Reclaim (CLI)

If it is necessary to deactivate an PTP 850E device, whether to return it for repairs or for any other reason, the device's activation key can be reclaimed for a credit that can be applied to activation keys for other devices.

A composite type activation key provides free activation keys when certain activation keys are purchased. For example, if a customer purchases an activation key for one GB ethernet port, two FE ethernet port activation keys are also provided. If the customer reclaims the activation key, the customer only gets credit for the original activation key, not for the composite items.

Where the customer has purchased upgrade activation keys, credit is given for the full feature or capacity, not for each individual upgrade. For example, if the customer purchased two capacity activation keys for 300M and later purchased one upgrade activation key to 350M, credit is given as if the customer had purchased one activation key for 350M and one activation key for 300M.

For instructions on how to reclaim an activation key, refer to the User Guide for the Cambium Activation Key Management System, Rev A.15 or later, Chapter 7, Reclaiming an Activation Key. During the activation key reclaim procedure, you will need to obtain a Validation Number from the PTP 850E unit. To display the Validation Number, enter the following command in root view:

```
root> platform activation-key show all
```

17.7.6 Displaying a List of Activation-Key-Enabled Features (CLI)

To display a list of features that your current activation key supports, and usage information about these features, enter the following command in root view:

```
root> platform activation-key show usage all
```

To display a list of the radio capacities that your current activation key supports and their usage information, enter the following command in root view:

```
root> platform activation-key show usage radio
```

17.8 Setting the Time and Date (Optional) (CLI)

Related Topics:

Configuring NTP (CLI)

PTP 850E uses the Universal Time Coordinated (UTC) standard for time and date configuration. UTC is a more updated and accurate method of date coordination than the earlier date standard, Greenwich Mean Time (GMT).

Every PT 850E unit holds the UTC offset and daylight savings time information for the location of the unit. Each management unit presenting the information uses its own UTC offset to present the information with the correct time.



Note

If the unit is powered down, the time and date are saved for 96 hours (four days). If the unit remains powered down for longer, the time and date may need to be reconfigured.

To set the UTC time, enter the following command in root view:

```
root> platform management time-services utc set date-and-time
<date-and-time>
```

To set the local time offset relative to UTC, enter the following command in root view:

```
root> platform management time-services utc set offset hours-
offset <hours-offset> minutes-offset <minutes-offset>
```

To display the local time configurations, enter the following command in root view:

```
root> platform management time-services show status
```

Table 99 Local Time Configuration CLI Parameters

Parameter	Input Type	Permitted Values	Description
date-and-time	Number	dd-mm-yyyy,hh:mm:ss where: dd = date mm = month yyyy= year hh = hour mm = minutes ss = seconds	Sets the UTC time.
hours-offset	Number	-12 – 13	The required hours offset (positive or negative) relative to GMT. This is used to offset the clock relative to GMT, according to the global meridian location.
minutes-offset	Number	0 – 59	The required minutes relative to GMT. This is used to offset the clock relative to GMT, according to the global meridian location.

The following command sets the GMT date and time to January 30, 2014, 3:07 pm and 58 seconds:

```
root>  platform management time-services utc set date-and-time
30-01-2014,15:07:58
```

The following command sets the GMT offset to 13 hours and 32 minutes:

```
root> platform management time-services utc set offset hours-
offset 13 minutes-offset 32
```

17.8.1 Setting the Daylight Savings Time (CLI)

To set the Daylight Savings Time (DST) parameters, several commands are available. You can set DST to start and end on fixed dates or according to the following rules:

- **On or after**: DST starts or ends on the first occurrence of a specified day of the week immediately after a specified date. For example, if the day of the week is set to Friday, DST starts or ends the first Friday after the specified month and day. If the month and day fall on a Friday, DST starts or ends on that date, at the specified time.
- **On or before**: DST starts or ends on the first occurrence of a specified day of the week immediately before a specified date. For example, if the day of the week is set to Friday, DST starts or ends the last Friday before the specified month and day. If the month and day fall on a Friday, DST starts or ends on that date, at the specified time.
- **Last**: DST starts or ends on the last occurrence of a specified day of the week in a specified month specified, at the specified time.

To set the DST start date to a fixed time and date, enter the following command in root view:

```
root> platform management time-services daylight-savings-time
start set  policy on-date month <month> day <day> time <time>
offset <offset>
```

To set the DST end date to a fixed time and date, enter the following command in root view:

```
root> platform management time-services daylight-savings-time end
set policy on-date month <month> day <day> time <time>
```

Alternatively, you can set the DST start and end dates in a single command, but without the ability to specify the time:

```
root> platform management time-services daylight-savings-time set
start-date-month <start-date-month> start-date-day <start-date-
day> end-date-month <end-date-month> end-date-day <end-date-day>
offset <offset>
```

To set DST to start on the first occurrence of a specific day of the week after a specific date, enter the following command in root view:

```
root> platform management time-services daylight-savings-time
start set policy after month <month> day <day> day-of-week <day-
of-week> time <time> offset <offset>
```

To set DST to end on the first occurrence of a specific day of the week after a specific date, enter the following command in root view:

```
root> platform management time-services daylight-savings-time end
set policy after month <month> day <day> day-of-week <day-of-
week> time <time>
```

To set DST to start on the first occurrence of a specific day of the week before a specific date, enter the following command in root view:

```
root> platform management time-services daylight-savings-time
start set policy before month <month> day <day> day-of-week <day-
of-week> time <time> offset <offset>
```

To set DST to end on the first occurrence of a specific day of the week before a specific date, enter the following command in root view:

```
root> platform management time-services daylight-savings-time end
set policy before month <month> day <day> day-of-week <day-of-
week> time <time>
```

To set DST to start on the last occurrence of a specific day of the week in a specific month, enter the following command in root view:

```
root> platform management time-services daylight-savings-time
start set policy last month <month> day-of-week <day-of-week>
time <time> offset <offset>
```

To set DST to end on the last occurrence of a specific day of the week in a specific month, enter the following command in root view:

```
root> platform management time-services daylight-savings-time end
set policy last month <month> day-of-week <day-of-week> time
<time>
```

Table 100: Daylight Savings Time CLI Parameters

Parameter	Input Type	Permitted Values	Description
month	Number	1-12	This parameter operates

Parameter	InputType	PermittedValues	Description
			according to the selected Policy, as described above. Th

Parameter	InputType	PermittedValues	Description
			edefaultvalueis***1***(January).

day	Number	1–31	This parameter operates according to the selected Policy, as described above. Th

Parameter	InputType	PermittedValues	Description
			edefaultvalueis1.

time			**The Time at which DST begins, in the format 00:00. The default value is 02:00 (2:00 A**

Parameter	InputType	PermittedValues	Description
			M).

day-of-week	Variable	sun mon tue wed thu fri sat	This parameter operates according to the selected Policy, as described above. Th

Parameter	InputType	PermittedValues	Description
			edefaultvalueissun.

offset	Number	0–23	The required offset, in hours, for Daylight Savings Time. Only positive offset is supp or

Parameter	InputType	PermittedValues	Description
			ted.
start-date-month	Number	1–12	The month when Daylight Savings Time begins.
sta	Num	1–	The

Parameter	InputType	PermittedValues	Description
rt-date-day	ber	31	date in the month when nDaylightSavingsTimebegins.
end	Num	1–	The

Parameter	InputType	PermittedValues	Description
-date-month	ber	12	month when Daylight Savings Time ends.
end-dated-	Number	1–31	The date in the em

Parameter	InputType	PermittedValues	Description
ay			onthwhenDaylightSavingsTimeends.

The following command configures DST to start on May 30 at 2:00 AM, with an offset of 2 hours.

```
root> platform management time-services daylight-savings-time
start set  policy on-date month 5 day 30 time 02:00 offset 2
```

The following command configures DST to end on October 1 at 2:00 AM.

```
root> platform management time-services daylight-savings-time end
set  policy on-date month 10 day 1 time 02:00
```

The following command configures DST to start on May 30 and end on October 1, with an offset of 20 hours.

```
root> platform management time-services daylight-savings-time set
start-date-month 5 start-date-day 30 end-date-month 10 end-date-
day 1 offset 20
```

The following command configures DST to start on the first Monday after April 27, at 3:00 AM, with an offset of 2 hours:

```
root> platform management time-services daylight-savings-time
start set policy after month 4 day 27 day-of-week mon time 03:00
offset 2
```

The following command configures DST to end on the first Monday before October 10, at 3:00 AM:

```
root> platform management time-services daylight-savings-time end
set policy before month 10 day 10 day-of-week mon time 03:00
```

The following command configures DST to end on the last Tuesday of October, at 2:00 AM:

```
root> platform management time-services daylight-savings-time end
set policy last month 10 day-of-week tue time 02:00
```

The following is a sample output of the platform management time-services show status command:

```
root>platform management time-services show status
Local Time              04-02-2024,12:27:01
UTC date & time         04-02-2024,10:27:01
UTC offset hours                2
UTC offset minutes              0


Daylight Saving Time (DST) settings:
DST-start-policy                On-or-After
DST-start-day-of-week   Mon
Start-Date <month/day/hour>     4/27 03:00


DST-end-policy                  On-or-Before
DST-end-day-of-week     Mon
End-Date   <month/day/hour>     10/27 03:00
Offset in hours         2
```

17.9 Enabling the Interfaces (Interface Manager)

By default:

- Ethernet traffic interfaces are disabled and must be manually enabled.
- The Ethernet management interface is enabled.
- Radio interfaces are enabled.



Note

In System release 12.9:
For PTP 850C, Ethernet Slot 1, Ports 1, 2, 3, and 4 are supported.

For PTP 850E, Ethernet Slot 1, Ports 2 through 7 are supported. Port 2 can only be used in Multiband configurations to connect the PTP 850E with the paired unit. The Management port (Management: Slot 1 Port 1) can also be used for traffic. For details on using the Management port for traffic, see PTP 850E Management Interface (CLI).

For PTP 850E, the QSFP port (Port 4), is displayed as follows.

- In a 4x1/10G configuration the QSFP port can provide four Ethernet interfaces: Eth 3, Eth 4, Eth 5, and Eth 6. In this configuration, a QSFP transceiver is attached to the QSFP port, and an MPO-MPO cable is connected between the transceiver and a splitter. The splitter splits the traffic between four Ethernet cables connecting the splitter to the customer equipment.
- The QSFP port can also be used with a QSFP-to-SFP adaptor to provide a 1x1/10G configuration. In this configuration, only Eth 3 is relevant.
- In 1x40G configurations, only Eth 3 is relevant.

Note: Setting an Enhanced Multi-Carrier ABC group to Admin = Down does not affect the radio interfaces on the remote unit, which will continue to transmit traffic. Therefore, to disable the link, it is recommended to mute the radio interfaces rather than setting the group to Admin = Down.

The QSFP port requires special configuration.

To enable or disable an interface, enter the following command in root view:

```
root> platform if-manager set interface-type <interface-type>
slot <slot> port <port> admin <admin>
```

To enable or disable a Multi-Carrier ABC group, enter the following command in root view:

```
root> platform if-manager set group-on-slot-type enhanced-abc
slot 1 group-number <group-number> admin <up|down>
```

To display the status of all the interfaces in the unit, enter the following command in root view:

```
root> platform if-manager show interfaces
```

Table 101 Interface Configuration CLI Parameters

Parameter	Input Type	Permitted Values	Description
interface-type	Variable	ethernet radio	ethernet – an Ethernet traffic interface. radio – a radio interface.
slot	Number	net: 1 Radio: 850C and PTP 850E: 1 PTP 850S: 2	The slot on which the interface is located.

Parameter	Input Type	Permitted Values	Description
port	Number	Ethernet: PTP 850C: 1, 3-4 PTP 850E: 1-7 Radio: PTP 850C: 1-2 PTP 850E: 1 Management: 1	The specific interface you want to enable or disable.
admin	Variable	up down	Enter **up** to enable the interface or **down** to disable the interface.

The following command enables Ethernet port 7:

```
root> platform if-manager set interface-type ethernet slot 1 port
7 admin up
```

The following command enables radio interface:

```
root> platform if-manager set interface-type radio slot 1 port 1
admin up
```

The following command disables the radio interface:

```
root> platform if-manager set interface-type radio slot 1 port 1
admin down
```

The following command disables the management interface:

```
root> platform if-manager set interface-type management slot 1
port 1 admin down
```

17.9.1 PTP 850E Management Interface (CLI)

The management interface on PTP 850E (Port 2) can be used for traffic as well as management and PoE. For important information and limitations regarding this port,

To use the PTP 850E management port for traffic, you should perform the following configurations as described in more detail in the following sections:

- Remove the L3 Shaper.
- Modify the management service point.
- Enable the LOC alarm (Alarm ID 401) for the management port. By default, this alarm is disabled on the management port and must be manually enabled when using the port for traffic.

  To enable the LOC alarm:

  1 Use the following command to enter management port view:

  ```
  root> ethernet interfaces mng slot 1 port 1
  ```

  2 In port view, use the following command:

```
eth type mng [1/1]> loc-alarm-supported set yes
```

If at some point you stop using the management port for traffic and use it instead exclusively for management, enter the following command in port view to disable the LOC alarm:

```
eth type mng [1/1]> loc-alarm-supported set no
```

To display the current LOC alarm status for the management port, enter the following command in port view:

```
eth type mng [1/1]> loc-alarm-supported show
```

17.10 Configuring the Radio (MRMC) Script(s) (CLI)

Multi-Rate Multi-Constellation (MRMC) radio scripts define how the radio utilizes its available capacity. Each script is a pre-defined collection of configuration settings that specify the radio's transmit and receive levels, link modulation, channel spacing, and bit rate. Scripts apply uniform transmit and receive rates that remain constant regardless of environmental impact on radio operation.



Note

The list of available scripts reflects activation-key-enabled features. Only scripts within your activation-key-enabled capacity will be displayed.

17.10.1 Displaying Available MRMC Scripts (CLI)

To display all scripts that are available for a specific radio carrier in your unit:

Use the following command to enter radio view:

```
root> radio slot 1 port 1
```

Enter the following command in radio view:

```
radio[1/1]>mrmc script show script-type <script-type> acm-support
<acm-support>
```



Note

The list of available scripts reflects activation-key-enabled features. Only scripts within your activation-key-enabled capacity will be displayed.

Table 102 MRMC Script CLI Parameters

Parameter	Input Type	Permitted Values	Description
script-type	Variable	Normal asymmetrical	Determines the type of scripts to be displayed: • **normal** – Scripts for symmetrical bandwidth. • **asymmetrical** – Scripts for asymmetrical bandwidth. **Note:** Asymmetrical scripts are not supported in this release.
acm-support	Boolean	Yes no	Determines whether to display scripts that support Adaptive Coding Modulation (ACM). In ACM mode, a range of profiles determines Tx and Rx rates. This allows the radio to modify its transmit and receive levels in response to environmental conditions.

The following command displays available symmetrical (normal) scripts for an PTP 850C:

```
root>radio slot 1 port 1
radio [1/1]>mrmc script show script-type normal acm-support yes
Script    |Script-Name
ID#       |

-----------------------------------------------------
<4501>      |mdN_A080080X_106_4501
<4502>      |mdN_A056056X_113_4502
<4504>      |mdN_A028028X_130_4504
<4505>      |mdN_A028028X_109_4505
<4506>      |mdN_A056056X_109_4506
<4507>      |mdN_A040040X_109_4507
<4509>      |mdN_A014014X_109_4509
<4510>      |mdN_A050050X_109_4510
<4511>      |mdN_A112112X_129_4511
<4513>      |mdN_A070070X_102_4513
<4514>      |mdN_A028028X_101_4514
<4517>      |mdN_A040040X_101_4517
<4521>      |mdN_A020020X_103_4521
<4525>      |mdN_A025025X_107_4525
-----------------------------------------------------
radio [1/1]>
```

The following command displays available symmetrical (normal) scripts for an PTP 850E:

```
radio [1/1]>mrmc script show script-type normal acm-support yes
Script    |Script-Name
ID#       |
-----------------------------------------------------
<5703>      |mdN_A250250N_5_5703
<5704>      |mdN_A500500N_5_5704
<5706>      |mdN_A10001000N_5_5706
<5710>      |mdN_A20002000N_5_5710
-----------------------------------------------------
radio [1/1]>
```

17.10.2 Assigning an MRMC Script to a Radio Carrier (CLI)

Once you have a list of valid scripts, you can assign a script to the radio carrier. The command syntax differs depending on whether you are assigning a script with ACM support or a script without ACM support.



Note

When you enter a command to change the script, a prompt appears

informing you that changing the script will reset the unit and affect traffic. To continue, enter yes. Changing the maximum or minimum profile does not reset the radio interface.

When using an 80 or 112 MHz script with PTP 850C, the same script must be assigned to both carriers. The system cannot be configured to operate with the 80 or 112 MHz script on one of the carriers and a different script on the other carrier.

To assign a script with ACM enabled, enter the following command in radio view:

```
radio[1/1]> mrmc set acm-support script-id <script-id> modulation
adaptive max-profile <max-profile> min-profile <min-profile>
```

To assign a script without ACM enabled, enter the following command in radio view:

```
radio[1/1]> mrmc set acm-support script-id <script-id> modulation
fixed profile <profile>
```

To display the current MRMC script configuration, enter the following command in radio view:

```
radio[1/1]> mrmc show script-configuration
```

Table 103: MRMC Script Assignation to Radio Carrier CLI Parameters

Parameter	InputType	PermittedValues	Description
script-id	Number		The ID of the script you want to assign to the radio carrier.

Parameter	InputType	PermittedValues	Description
modulation	Variable	adaptivefixed	Determines whether ACM is enabled (adaptive) or disabled (fixed).

max-profile	Number		Adaptive ACM mode only: The maximum profile for the script. For example, if you select a maximum profile of 5,

			the system will not climb above profile 5, even if channel fading conditions allow it.
min-profile	Number		Adaptive ACM mode only:

			The minimum profile for the script. For example, if you select a minimum profile of 3, the system will not go below

			w pr ofi le 3 re ga rdl es s of th e ch an ne l fa di ng co nd iti on s. Th e mi ni m u m pr ofi le ca nn ot be gr ea ter th an th e m axi m u m pr

			ofile, but it can be equal to it. If you do not include this parameter in the command, the minimum profile is set at th

Parameter	InputType	PermittedValues	Description
			e de fa ult val ue of 2.

Parameter	InputType	PermittedValues	Description
profile	Number		FixedACMmode only: The profile in which the system will operate



Note

It is recommended that the MRMC script configurations be symmetric on both sides of the link, including the

	same script and minimum and maximum ACM profiles. For a list and description of available profiles. Note that for PTP 850E, channels of 250 MHz and higher, Profiles 0 and 1 require a special activation key (SL-ACMB). These profiles are used with ACMB, which is an enhancement of ACM that provides further flexibility to mitigate fading at BPSK by reducing the channel spacing to one half or one quarter of the original channel bandwidth when fading conditions make this appropriate.

The following command assigns MRMC script ID 5703, with ACM enabled, a minimum profile of 3, and a maximum profile of 9, to the radio carrier in an PTP 850E:

```
radio[1/1]>mrmc set acm-support script-id 5703 modulation
adaptive max-profile 9 min-profile 3
```

The following command assigns MRMC script ID 5704, with ACM disabled and a profile of 5, to the radio carrier in an PTP 850E:

```
radio[1/1]>mrmc set acm-support script-id 5704 modulation fixed
profile 5
```

The following command assigns MRMC script ID 5710, with ACM enabled, minimum profile of 2, and a maximum profile of 8, to the radio carrier in an PTP 850E:

```
radio[1/1]>mrmc set acm-support script-id 5710 modulation max-
profile 8 min-profile 2
```

The following command assigns MRMC script ID 4507, with ACM enabled, a minimum profile of 5, and a maximum profile of 12, to radio carrier 1 in an PTP 850C:

```
radio[1/1]>mrmc set acm-support script-id 4507 modulation
adaptive max-profile 5 min-profile 12
```

17.11 Configuring the Radio Parameters (CLI)

In order to establish a radio link, you must:

- Enter radio view.
- For PTP 850C 1+0 configurations, verify that the default carrier matches the physical configuration of the device (Horizontal or Vertical) and change it if necessary.
- Verify that the radio is muted (the **Mute Status** should be **On**).
- Configure the radio frequencies.



Note

Even if you are using the default frequencies, it is mandatory to actually configure the frequencies.

- Configure the TX level.
- Set **Mute Admin** to **Off**.
- Verify that the radio is unmuted (the **Mute Status** should be **Off**).

17.11.1 Entering Radio View (CLI)

To view and configure radio parameters, you must first enter the radio's view level in the CLI.

To enter a radio's view level, enter the following command in root view:

```
root> radio slot <slot> port <port>
```

The following prompt appears:

```
radio[1/1]>
```

17.11.2 Changing the Default Carrier (PTP 850C only)

For PTP 850C, the Default Carrier parameter enables you to use the Horizontal carrier (Port 1) or the Vertical carrier (Port 2) for 1+0 configurations. By default, Horizontal is selected. If you are configuring a Vertical 1+0 configuration, you must change the Default Carrier to Vertical (Port 2).

Note: You cannot change the default carrier if there are services configured on either of the carriers or if either or both carriers belong to a Multi-Carrier ABC group.

Use the following command to make Port 1 (Horizontal) the Default Carrier:

```
root> radio default-carrier set carrier first-carrier
```

Use the following command to make Port 2 (Vertical) the Default Carrier:

```
root> radio default-carrier set carrier second-carrier
```

Use the following command to display the currently configured Default Carrier:

```
root> radio default-carrier show
```

17.11.3 Muting and Unmuting a Radio (CLI)

To mute or unmute the radio, enter the following command:

```
radio[x/x]>rf mute set admin <admin>
```

To configure a timed mute, enter the following command in radio view:

```
radio[1/1]> rf mute set admin on-with-timer timeout-value <1-1440>
```

When the timer expires, the radio is automatically unmuted. A timed mute provides a fail-safe mechanism for maintenance operations that eliminates the possibility of accidently leaving the radio muted after the maintenance has been completed. By default, the timer is 10 minutes.



Note

In contrast to an ordinary mute, a timed mute is not persistent. This means that if the unit is reset, the radio is not muted when the unit comes back online, even if the timer had not expired.

To display the mute status of a radio, enter the following command in radio view:

```
radio[1/1]>rf mute show status
```

The following command mutes the radio:

```
radio[1/1]>rf mute set admin on
```

The following command unmutes the radio:

```
radio[1/1]>rf mute set admin off
```

The following command configures a timed mute. This mute will automatically expire in 30 minutes.

```
radio[1/1]> rf mute set admin on-with-timer timeout-value 30
```

17.11.4 Configuring the Transmit (TX) Frequency (CLI)

To set the transmit (TX) frequency of a radio, enter the following command in radio view. This command includes an option to set the remote RX frequency in parallel:

```
radio[1/1]>rf set tx-frequency <0-4294967295> local-remote
<enable|disable>
```

Note: System release 10.6 does not support the ability to set the remote RX frequency.

The following command sets the TX frequency of the radio in an PTP 850E unit to 71000000 KHz, and sets the RX frequency of the remote unit to the same value.

```
radio[1/1]> rf set tx-frequency 71000000 local-remote enable
```

The following command sets the TX frequency of the radio in an PTP 850E unit to 71000000 KHz, but does not set the RX frequency of the remote unit.

```
radio[1/1]> rf set rx-frequency 71000000 local-remote disable
```

17.11.5 Configuring the Transmit (TX) Level (CLI)

To set the transmit (TX) level of a radio, enter the following command in radio view:

```
radio[1/1]>rf set tx-level <-50-50>
```

To display the maximum transmit (TX) level of a radio, enter the following command in radio view:

```
radio[1/1]>rf show max-tx-level
```

The following command sets the TX level of the radio to 10 dBm:

```
radio[1/1]>rf set tx-level 10
```

When Adaptive TX power is enabled, this command determines the maximum TX level.

17.11.6 Enabling ACM with Adaptive Transmit Power (CLI)

When Adaptive TX Power is enabled, the radio adjusts its TX power dynamically based on the current modulation. When the modulation is at a high level, the TX power is adjusted to the level required with the high modulation. If the modulation goes down to a lower level, the TX power increases to compensate for the lower modulation. The TX level configured by the `rf set tx-level` command determines the maximum TX level, but the actual TX level as shown in the Operational TX Level (dBm) field can be expected to be lower when the radio is operating at high modulations requiring less TX power.

To enable Adaptive TX Power, enter the following command in radio view:

```
radio[1/1]>rf adaptive-power admin enable
```

To disable Adaptive TX Power for a radio, enter the following command in radio view:

```
radio[1/1]>rf adaptive-power admin disable
```

To display whether Adaptive TX Power is enabled, enter the following command in radio view:

```
radio[1/1]>rf adaptive-power show status
```

The output of this command is:

```
radio [x/x]>rf adaptive-power show status

RF adaptive power admin status: [enable/disable]
RF adaptive power operational status: [up/down]
```

`RF adaptive power operational status: Up` means the feature is enabled and fully functional for that radio link.



Note

Adaptive TX Power only operates when the MRMC script is configured to Adaptive mode. If the script is configured to Fixed mode (or Adaptive mode with the Minimum and Maximum Profile set to the same value), you can set `adaptive-power` to `enable`, but the `adaptive power operational status` will be `down`.

17.11.7 Enabling Adjacent Channel Mode (CLI)

In certain adjacent channel configurations with PTP 850C, interference from the adjacent channel may prevent the link from reaching the maximum ACM profile that might otherwise be available.

In addition, if the TX is muted, and Adaptive TX Power is enabled on the remote side, the remote side will reach LOF and its increased TX power may lead to poor MSE on the local adjacent receiver.

These problems can be eliminated by enabling Adjacent Channel Mode. To enable or disable Adjacent Channel mode, enter the following command in radio view. By default, Adjacent Channel mode is disabled.

```
radio[1/1]>rf set adjacent-channel <enable|disable>
```

It is not recommended to enable this parameter for other products or configurations. It should only be used for adjacent channel configurations with PTP 850C.

Note: Enabling or disabling Adjacent Channel mode may cause a brief loss of traffic.

17.12 Configuring the RSL Threshold Alarm (CLI)

You can enable an alarm to be triggered in the event that the RSL falls beneath a defined threshold. This alarm is alarm ID 1610, *Radio Receive Signal Level is below the configured threshold*. By default, the alarm is disabled.

To enable the RSL threshold alarm, enter the following command in radio view:

```
radio[1/1]> rf rsl-degradation set admin enable
```

To disable the RSL threshold alarm, enter the following command in radio view:

```
radio[1/1]> rf rsl-degradation set admin disable
```

To set the threshold of the RSL threshold alarm, enter the following command in radio view:

```
radio[1/1]> rf rsl-degradation set threshold <-99-0>
```

The default threshold is -68 dBm.

To display the current alarm configuration, enter the following command in radio view:

```
radio[1/1]> rf rsl-degradation show status
```

The following commands enable the RSL threshold alarm and set the threshold to -55 dBm in an PTP 850E.

```
root> radio slot 1 port 1
radio [1/1]>rf rsl-degradation set admin enable
radio [1/1]>rf rsl-degradation set threshold -55
radio [1/1]>rf rsl-degradation show status

RSL degradation alarm admin: enable
RSL degradation threshold: -55

radio [1/1]>
```

The alarm is cleared when the RSL goes above the configured threshold. The alarm is masked if the radio interface is disabled, the radio does not exist, or a communication-failure alarm (Alarm ID #1703) is raised.

17.13 Creating Service (s) for Traffic (CLI)

In order to pass traffic through the PTP 850, you must configure Ethernet traffic services. For configuration instructions, see Configuring Ethernet Services (CLI).

17.14 Configuring CPRI (CLI)

Optionally, PTP 850E can be used with a CPRI module. The CPRI module is inserted in the PTP 850E's QSFP port (P4), and provides up to 10 Gbps capacity for CPRI traffic. The CPRI module converts CPRI signals to Ethernet and Ethernet to CPRI in accordance with Radio over Ethernet (RoE) standard IEEE 1914.3 and CPRI specification v7.0. For more details, see the Technical Description for PTP 850E.

Note: Support for CPRI is released for Controlled Availability.

CPRI Configuration Overview (CLI)

Before configuring the QSFP port (P4) for CPRI, make sure the following preconditions are met for the logical ports that correspond to P4 (Ethernet Slot 1, Port 3, Ethernet Slot 1, Port 4, Ethernet Slot 1, Port 5, and Ethernet Slot 1, Port 6):

- In the Interface Manager, the ports must all be set to **Admin Status** = **Down**.
- None of the ports belong to a group (e.g., LAG).
- None of the ports are used as a synchronization source.
- No service point is attached to any of the ports.
- 1588 Boundary Clock is not configured on any of the ports.

Once these conditions are met, the following configurations must be made for P4:

- Set the QSFP mode to CPRI.
- Configure the CPRI parameters.

- Enable the CPRI port.
- Configure Synchronization for CPRI traffic.
- Create an Ethernet service for CPRI traffic.

Setting the QSFP Mode to CPRI (CLI)

To set the QSFP mode of the QSFP port to CPRI, enter the following command in root view:

```
root> platform qsfp expected set slot 1 id 1 type CPRI
```

Configuring the CPRI Parameters (CLI)

To configure the CPRI parameters:

1 Go to CPRI module view by entering the following command in root view:

```
root>cpri slot 1 port 1

CPRI slot[1] port[1]>
```

2 Enter the following command to configure the bit rate option for the CPRI module. This parameter must be set to the same value on both sides of the CPRI link.

```
CPRI slot[1] port[1]> cpri option set value <3|5|7>
```

The following options are available:

- **3** – 2457.6Mbps, 8B/10B line coding
- **5** – 4915.2Mbps, 8B/10B line coding
- **7** – 9830.4Mbps, 8B/10B line coding (default)

Note: If you choose **Option 7**, make sure you are using an MRMC script that supports at least 10 Gbps.

3 Enter the following command to configure the system mode. This parameter must be set to the same value on both sides of the CPRI link.

```
CPRI slot[1] port[1]> mode set value <line-code-aware|tunneling>
```

The following options are available:

- **line-code-aware** – (default)
- **tunneling** – Only works with **normal-operation** as the sub mode. Does not work with bit rate option **7**.

4 Enter the following command to configure the sub-mode. This parameter must be set to the same value on both sides of the CPRI link.

```
CPRI slot[1] port[1]>lca submode set value <normal-operation|special-characters>
```

The following options are available:

- **normal-operation** – (default)
- **special-characters** – Only works with **line-code-aware** as the system mode.

5 Enter the following command to configure the number of bytes that must be in the buffer before a CPRI signal is transmitted. This parameter must be set to the same value on both sides of the CPRI link.

```
CPRI slot[1] port[1]>buffer size set <1500-20000>
```

Enter a multiple of 16, within the range of 1500 and 20000. The default value is 3008.

It is recommended to increase the buffer size of the traffic from either side is not continuous, but rather, comes in bursts.

6 Enter the following command to configure the RoE payload length, in bytes. This includes only CPRI data, not the RoE header. The default value is 512. This parameter must be set to the same value on both sides of the CPRI link.

```
CPRI slot[1] port[1]>roe payload set size <64-1488>
```

The available options depend on the mode and sub-mode configuration, as follows:

- When the mode is **line-code-aware** and the sub-mode is **normal-operation**, supported values are 256, 512, and 1024.
- When the mode is **line-code-aware** and the sub-mode is **special characters**, supported values are 512 and 1024.
- When the mode is **tunneling** and the sub-mode is **normal-operation**, supported values are multiples of 16 within a range of 64 to 1488.

7 Enter the following command to configure the destination MAC address:

```
CPRI slot[1] port[1]> mac set destination address <MAC-address>
```

- If the CPRI module is connected to a BBU, enter the MAC address of the CPRI module connected to the RRH.
- If the CPRI module is connected to a RRH, enter the MAC address of the CPRI module connected to the BBU.

8 Enter the following command to configure an ID to be used in the RoE conversion:

```
CPRI slot[1] port[1]> flow ID set value <0-10>
```

The default is 1. This parameter must be set to the same value on both sides of the CPRI link.

9 Enter the following command to configure whether the TX is turned off if a fault is discovered.

```
CPRI slot[1] port[1]>turn off TX at fault set to <yes|no>
```

If this parameter is set to **yes**, the TX is turned off if a fault is discovered. The default value is **no**.

Enabling the CPRI Port (CLI)

You must enable the CPRI port (CPRI Slot 1 Port 1). To enable the CPRI port, enter the following command in root view:

```
root> platform if-manager set interface-type cpri slot 1 port 1
admin up
```

Configuring Synchronization for CPRI Traffic (CLI)

Synchronization for the CPRI module should be configured as follows:

- If the CPRI module is connected to a Baseband Unit (BBU), CPRI Slot 1 Port 1 should be configured as the lowest priority synchronization source. Use the following command to configure the CPRI module as a synchronization source:

```
platform sync source add cpri-interface slot 1 port 1 priority 1
quality g.813/8262
```

- If the CPRI module is connected to the Remote Radio Head (RRH, also known as the Remote Radio Unit, RRU), Radio Slot 1 Port 1 should be configured as the lowest priority synchronization source. Use the following command to configure the radio as a synchronization source:

```
platform sync source add radio-interface slot 1 port 1 radio-
channel 0 priority 1 quality g.813/8262>
```

For general instructions on configuring the Synchronization source.

Creating an Ethernet Service for CPRI Traffic (CLI)

You must configure a point-to-point Ethernet service with the following service points to carry CPRI traffic:

- Create a service point on the radio interface.
- Create a service point on the CPRI interface (CPRI Slot 1 Port 1)

Use the following command syntax to create a service to carry traffic between the radio and the CPRI interface:

```
root> ethernet service add type p2p sid <1-4095> admin
operational evc-id <up to 20 characters> description <up to 64
characters>
```

Use the following commands to create service points on the CPRI interface and the radio:

```
root> ethernet service sid <sid>

service[x]> sp add sp-type pipe int-type dot1q spid 1 interface
cpri slot 1 port 1 sp-name <string>

service[x]> sp add sp-type pipe int-type dot1q spid 2 interface
radio slot 1 port 1 sp-name <string>
```

For general information about configuration Ethernet services, see Configuring Ethernet Services (CLI).

Operating in FIPS Mode (CLI)

Notes: FIPS 140-3 compliance is only available with System release 12.7.

PTP 850C and PTP 850E can be configured to be FIPS 140-3-compliant in specific hardware and software configurations, as described in this section.

17.14.1 Requirements for FIPS Compliance (CLI)

For a full list of FIPS requirements, refer to the *FIPS 140-3 Non-Proprietary Security Policy*, available upon request. It is the responsibility of the customer to ensure that these requirements are met.

For details on hardware requirements for operating in FIPS mode, see Requirements for FIPS Compliance.

Unit redundancy configurations can be configured to be FIPS 140-3-compliant. This requires encryption of the protection link between the two units. See Encrypting the External Protection Link (CLI).

Enabling FIPS Mode (CLI)

To set the unit to operate in FIPS mode, enter the following command in root view:

```
root> platform security fips-mode set admin enable
```

To disable FIPS mode, enter the following command in root view:

```
root> platform security fips-mode set admin disable
```

Note: Changing the FIPS configuration causes a unit reset.

To display the unit's current FIPS setting, enter the following command in root view:

```
root> platform security fips-mode show
```

Status values are:

- `enable` – FIPS mode is enabled.
- `disable` – FIPS mode is disabled.

Changing the FIPS configuration causes a unit reset. After this or any other system reset in FIPS mode, the length of time before users can log back into the system is longer than usual due to FIPS-related self-testing.

Note: Note that when FIPS is enabled in a link with unit redundancy or, for PTP 850E, 2+0 XPIC, this state is propagated to the mate unit, causing reset of both units. Note also that when FIPS is enabled in a link with unit redundancy, IPsec encryption is automatically enabled on the external protection link. For details, see Encrypting the External Protection Link (CLI).

After enabling FIPS:

- The MD5 option for SNMPv3 is blocked.

For a full list of FIPS requirements, including software configuration requirements, refer to the FIPS 140-3 Non-Proprietary Security Policy, available upon request.

Note that whenever one of the following occurs with FIPS mode enabled (Admin = Enable), a Key Derivation Function self-test (Known Answer Test - KAT) is initiated:

- SNMP is enabled or disabled.
- An SNMPv3 user is added or removed
- IPsec mode is enabled (Admin = Enable)
- The IPsec pre-shared key is changed

If the Key Derivation Function self-test fails, the unit is automatically rebooted. If the self-test fails again after reboot has been completed, another reboot is initiated and a soft-zeroization takes place, as part of which all sensitive security parameters are erased from the device's persistent storage and FIPS mode is disabled.

Encrypting the External Protection Link (CLI)

Optionally, you can encrypt the protection link using IPSec. This encrypts all IP packets that pass between the Protection ports of the two PTP 850 units.

IPSec uses a 32-character pre-shared key. The pre-shared key is a 32-byte symmetric encryption key. The same pre-shared key must be configured on both ends of the encrypted link. The default value of the pre-shared key is:

```
protectionpresharedkey0123456789
```

You should make sure to change the default value when enabling IPSec encryption. If the default value is not changed, the following alarm is triggered:

- 5113 – IPSec Pre-Shared Key has the default value

If you are encrypting the protection link when initially configuring Unit Redundancy, it is recommended to configure encryption *before* enabling Unit Redundancy. In this case, configure IPSec encryption separately on both PTP 850 units on both sides of the link, making sure to use the same pre-shared key.

If you are encrypting the protection link in a configuration in which Unit Redundancy has already been configured, configure IPSec on the Active unit on both sides of the link. The IPSec configuration will be copied automatically to the Standby units.

To configure IPSec encryption of the protection link:

1 Verify that the web interface protocol for accessing the unit is configured to HTTPS. See Enabling HTTPS (CLI).
2 Enter the following command to configure the pre-shared key. The key must be *exactly* 32 characters.

```
root> platform security ipsec set pre-shared-key <key>
```

Note: If you are configuring IPSec after Unit Redundancy has already been enabled, communication with the Standby unit may be lost for up to a minute while the key is being copied.

3 Enter the following command to enable IPSec:

```
root> platform security ipsec set admin enable
```

To disable IPSec, enter the following command:

```
root> platform security ipsec set admin disable
```

To display the pre-shared key, enter the following command:

```
root> platform security ipsec show pre-shared-key
```

To clear the pre-shared key, enter the following command:

```
root> platform security ipsec clear pre-shared-key
```

To display the unit's current IPSec Admin status, enter the following command:

```
root> platform security ipsec show admin
```

Initial Configuration of FIPS-Compliant Unit Redundancy Configuration (CLI)

For unit redundancy configurations, the external protection link must be encrypted using IPsec. This encrypts all IP packets that pass between the management ports of the two PTP 850 units.

To set up a unit redundancy configuration that is FIPS 140-3-compliant, you must follow these steps:

1 Configure and enable unit redundancy on both units.
2 Enable FIPS on both PTP 850 units. See Enabling FIPS Mode (CLI).
When you enable FIPS mode, IPsec encryption will automatically be enabled on the protection link, using the default protection pre-shared key. Alarm 5113 will be raised.
3 Configure a new pre-shared key on the active unit. To configure a protection key:

i Verify that the web interface protocol for accessing the unit is configured to HTTPS. See Configuring X.509 CSR Certificates (CLI).
ii Enter the following command in root view:

```
root>platform management protection set pre-shared-key <key>
```

The key must be *exactly* 32 characters.

Note: Communication with the standby unit may be lost for a few seconds while the key is being copied.

To clear the user-defined protection pre-shared key and restore it to its default value, enter the following command in root view:

```
root> platform management protection clear pre-shared-key
```

To display the protection pre-shared key, enter the following command in root view:

```
root> platform management protection show pre-shared-key
```

Replacing a Unit in a FIPS-Compliant Unit Redundancy Configuration (CLI)

If it becomes necessary to replace a unit in a FIPS 140-3-compliant unit redundancy configuration, you must pre-configure the replacement unit as follows:

1. Enable FIPS on the replacement unit. See Enabling FIPS Mode (CLI).
2. Configure the protection pre-shared key on the replacement unit. See Initial Configuration of FIPS-Compliant Unit Redundancy Configuration (CLI), Step 3.
3. Configure and enable unit redundancy on the replacement unit.

18. Configuration Guide (CLI)

18.1 System Configurations (CLI)

This section lists the basic PTP 850C, PTP 850E, and PTP 850S system configurations, with links to configuration instructions.

Table 104 System Configurations (CLI)

Configuration	Supported Products	Link to Configuration Instructions
1+0	All	Configuring a 1+0 Link Using the Quick Configuration Wizard
2+0 Enhanced Multi-Carrier ABC	PTP 850C	Configuring a 2+0 Multi-Carrier ABC Link Using the Quick Configuration Wizard OR Configuring Multi-Carrier ABC (CLI)
Multiband	PTP 850E	Configuring a Multiband (Enhanced Multi-Carrier ABC) Link Using the Quick Configuration Wizard OR Configuring Multiband (CLI)
2+0 XPIC	PTP 850C PTP 850E	Configuring XPIC (CLI)

1+1 HSB Unit Protection	PTP 850E	Configuring 1+1 HSB Unit Protection (CLI)
Link Aggregation (LAG) (PTP 850S only)		Configuring Link Aggregation (LAG) and LACP (Optional) (CLI)

18.2 Configuring Multi-Carrier ABC (CLI)

This option is only relevant for PTP 850C.

- Multi-Carrier ABC Overview (CLI)
- Configuring a Multi-Carrier ABC Group (CLI)
- Removing Members from a Multi-Carrier ABC Group (CLI)
- Deleting a Multi-Carrier ABC Group (CLI)

18.2.1 Multi-Carrier ABC Overview (CLI)

For an overview of Multi-Carrier ABC, see Multi-Carrier ABC Overview.

18.2.2 Configuring a Multi-Carrier ABC Group (CLI)

Note: Radio slot 2 port 1 should always be configured on channel 1 while Radio slot 2 port 2 should always be configured on channel 2.

To configure a Multi-Carrier ABC group:

1 Create the group by entering the following command in root view:

```
root> multi-carrier-abc create group group_id 1 slot 1 type
Enhanced

multi-carrier-abc enhanced-group-id [1] slot [1]>
```

2 Enter Multi-Carrier ABC Group view by entering the following command in root view:

```
root>multi-carrier-abc group-id 1 slot 1 type Enhanced
```

3 Add members to the group as follows:

- To add a radio interface to the group, enter the following command in Multi-Carrier ABC Group view. Repeat this command for each radio interface you want to add.

```
attach-member slot 1 port <1-2> channel-id <1-16>
```

- The Channel ID identifies the interface within the group.

4 Repeat for the second radio interface.

The following commands create a Multi-Carrier ABC group.

```
multi-carrier-abc create group group_id 1 slot 1 type Enhanced
multi-carrier-abc enhanced-group-id [1] slot [1]> attach-member
slot 1 port 1 channel-id 1
multi-carrier-abc enhanced-group-id [1] slot [1]> attach-member
slot 1 port 2 channel-id 2
```

Removing Members from a Multi-Carrier ABC Group (CLI)

To remove members from a Multi-Carrier ABC group:

1 To remove an individual radio interface from the Multi-Carrier ABC group, go to Multi-Carrier ABC group view and enter the following command:

```
multi-carrier-abc enhanced-group-id [1] slot [1]> detach-member
channel-id <channel-id>
```

Deleting a Multi-Carrier ABC Group (CLI)

To delete a Multi-Carrier ABC group:

1 Remove the members from the group.

2 Delete the group by entering the following command in root view:

```
root> multi-carrier-abc delete group group_id 1 slot 1 type
Enhanced
```

18.2.3 Configuring 4+0 Layer 1 Link Bonding (CLI)

Note: This section is only relevant for PTP 850C.

4+0 Layer 1 Link Bonding links can also be configured using the Quick Configuration wizard. It is recommended to use the wizard whenever possible. See Configuring a Layer 1 Link Bonding Link Using the Quick Configuration Wizard.

For PTP 850C 4+0 Layer 1 Link Bonding links, line redundancy is available. For details, refer to Layer 1 Link Bonding and Line Redundancy and Configuring Line Redundancy for Link Bonding Configurations (CLI).

4+0 Layer 1 Link Bonding links can also be configured using the Quick Configuration wizard. It is recommended to use the wizard whenever possible.

This section includes:

- Configuring Synchronization in a 4+0 Layer 1 Link Bonding Node (CLI)

- Editing a Link Bonding Group or its Members (CLI)
- Displaying Statistics for a Link Bonding Group (CLI)
- Deleting a Link Bonding Group (CLI)

For an overview of 4+0 Layer 1 Link Bonding, see 4+0 Layer 1 Link Bonding Overview.

18.2.4 Configuring 4+0 Layer 1 Link Bonding (CLI)

To configure a 4+0 Layer 1 Link Bonding node:

1 Connect the external switch to Eth 1 (P2, the PoE port) or Eth 3 (P4, the MIMO port) on the main PTP 850C unit.
2 On both the main unit and the paired unit, configure the port speed of the port to be used for carrying traffic between the two units (Eth 3 or Eth 4) to 10 Gbps.
3 On both the main unit and the paired unit, configure the port speed of Eth 2 to 2.5 Gbps.
4 Connect an optical cable between the ports used to transmit traffic between the two units (Eth 3/P4 or Eth 4/P5).
5 Set the port connected to the paired unit for passing traffic between the two units (Eth 3 or Eth 4) to **Admin** = **Down**.
6 Connect an optical cable between Eth 2 (P3) of each PTP 850C unit. This cable carries L2 protocol data between the two units.

Note: Special SFP+ modules must be used for both the inter-unit traffic ports (Eth 3/P4 or Eth 4/P5) and the Protocols ports (Eth 2, P3). For details and the marketing models of the required SFP+ modules, as well as the optical cables, see the Installation Guide for PTP 850C.

7 Configure the script and radio settings for both the main unit and the paired unit, including XPIC.
8 On both the main unit and the paired unit, configure a Multi-Carrier ABC group that includes both of the unit's radio carriers.
9 On the main unit only, configure a Link Bonding group that includes the Multi-Carrier ABC group and the Ethernet interface carrying traffic between the two units (Eth 3 or Eth 4) connected to the paired unit:

Note: Before adding a group member, make sure that no shapers or service points are configured on the interface or group.

i Create the group by entering the following command in root view:

```
root> ethernet link-bonding create group group_id <1-6> group-
name <string>
```

Note: The `name` parameter is optional.

ii Enter the group view by entering the following command in root view:

```
root>ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

iii Add the Ethernet interface carrying traffic between the two units (Eth 3 or Eth 4) to the Link Bonding Group by entering the following command in group view.

```
eth group [lbx]> lb-member add interface eth slot 1 port <3|4>
shaper-bit-rate <0-30000> vlan untag l1-header-compensation-
enabled no l1-header-compensation-value <(-63)-63> l2-header-
compensation-value <(-63)-63>
```

iv Add the Multi-Carrier ABC group to the Link Bonding Group by entering the following command in group view:

```
eth group [lbx]> lb-member add group-on-slot enhanced-abc slot 1
group-id <1-4> shaper-bit-rate <0-30000> vlan untag l1-header-
compensation-enabled no l1-header-compensation-value <(-63)-63>
l2-header-compensation-value <(-63)-63>
```

- The `shaper-bit-rate` parameter enables you to adjust the shaper for either or both interfaces in the group. This shaper controls the distribution of traffic between the main Unit (the Multi-Carrier ABC group) and the paired unit (the Ethernet interface). Generally, there is no need to change this parameter from its default value of 30000 Mbps.

Note: In order to change the `shaper-bit-rate` parameter, you must first verify that Inband Management is enabled. Otherwise, the change will have no effect. See Configuring In-Band Management (CLI).

- The `l1-header-compensation-enabled` parameter should be set to `no` for both interfaces.
- The `l2-header-compensation-enabled` parameter should be set to `yes` for both interfaces.
- The `l2-header-compensation-value` parameter should be set to their default values of 26.

10 In the Interface Manager, set the port connected to the paired unit for passing traffic between the two units to **Admin** = **Up**.

11 To ensure proper fault handling, configure Automatic State Propagation (ASP as follows:

i On the local and remote main units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The Link Bonding group
- Controlled Port: The port connected to the external switch (Eth 1 or Eth 3).

ii On the local and remote paired units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The Multi-Carrier ABC group
- Controlled Port: The port carrying traffic between the two units (Eth 3 or Eth 4)

12 Inband management can be carried between the main unit and the paired unit via the Protocols cable that connects Eth 2 (P3) of each unit. To configure inband management, you must enable inband management on both units and define a management service that connects Eth 2 of both units, the Link Bonding groups, and the ingress port of the main unit:

i On the local main unit, configure a service point on the port connected to the external switch (Eth 1 or Eth 3).
ii On the local main unit, configure a service point on Eth 2.
iii On the local main unit, configure a service point on the Link Bonding group.
iv On the local paired unit, configure a service point on Eth 2.
v On the remote paired unit, configure a service point on Eth 2.
vi On the remote main unit, configure a service point on Eth 2.

vii On the remote main unit, configure a service point on the Link Bonding group.

13 Radio Bandwidth Notification on the paired unit must be configured via the Web EMS.

14 On the paired unit on both sides of the link, configure a point-to-point service for Radio Bandwidth Notification, with service points on the Multi-Carrier ABC group and Eth 2. The service points should be configured as follows:

- Create a service point on the paired unit's Multi-Carrier ABC group with the following parameters:
  - Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation: 4090
  - Allow Flooding: Allow
  - Learning Admin: Disable
- Create a service point on Eth 2 of the paired unit with the following parameters:
  - Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation: 4090
  - Allow Flooding: Allow
  - Learning Admin: Disable

See Configuring Service Points (CLI).

18.2.5 Configuring Synchronization in a 4+0 Layer 1 Link Bonding Node (CLI)

SyncE and 1588 PTP can be used with 4+0 Layer 1 Link Bonding. SyncE and 1588 PTP can be configured for both the main unit and the paired unit. Synchronization messages are passed between the units via the Protocols cable.

18.2.5.1 Configuring SyncE in a 4+0 Layer 1 Link Bonding Node

To configure SyncE on a 4+0 Layer 1 Link Bonding node:

- On the local main unit, configure the following:
  - Configure the port connected to the external switch (Eth 1 or Eth 3) as a sync source with priority 1.
  - Configure radio interface 1 as a sync source with priority 2.
  - Configure radio interface 2 as a sync source with priority 3.
  - Configure Eth 2 as a sync source with priority 4.
- On the local paired unit, configure the following:
  - Configure Eth 2 as a sync source with priority 1.
  - Configure radio interface 1 as a sync source with priority 2.
  - Configure radio interface 2 as a sync source with priority 3.
- On the remote paired unit, configure the following:

- Configure radio interface 1 as a sync source with priority 1.
- Configure radio interface 2 as a sync source with priority 2.
- Configure Eth 2 as a sync source with priority 3.

- On the remote main unit, configure the following:
  - Configure Eth 2 as a sync source with priority 1.
  - Configure radio interface 1 as a sync source with priority 2.
  - Configure radio interface 2 as a sync source with priority 3.
  - Configure the port connected to the external switch (Eth 1 or Eth 3) as a sync source with priority 4.

All sync sources should be configured with Sync Interface Quality G.813/8262. For instructions on configuring SyncE.

18.2.5.2 Configuring 1588 PTP in a Layer 1 Link Bonding Node

To use 1588 PTP on a Layer 1 Link Bonding node, you must configure Boundary Clock on the main unit and Transparent Clock on all of the units, as described below. 1588 messages are generated by the Boundary Clock mechanism on the main unit and sent untagged to the paired unit via the Protocols cable. They receive VLAN tagging on the paired unit in order to separate them from user traffic.

Note: If the paired unit goes down, 1588 packets will not be transmitted to the other side of the link.

To configure 1588 PTP for the 4+0 Layer 1 Link Bonding node:

1 Configure SyncE following the instructions.
2 Enable 1588 PTP on each unit, including the main unit and the paired unit on both sides of the link, using the following command in each unit:

```
root> platform sync ptp set admin enable
```

3 On the main unit on both sides of the link, enable Boundary clock on:

- The port connected to the external switch (Eth 1 or Eth 3).
- Eth 2.

4 On the paired unit on both sides of the link, enable Transparent Clock on the Multi-Carrier ABC group.
5 On the paired unit on both sides of the link, configure a point-to-point service with service points on the Multi-Carrier ABC group and Eth 2. The service points should be configured as follows:

- Service point on the Multi-Carrier ABC group:
  - Service Point Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation: Per customer's choice
  - Allowing Flooding: Allow
  - Learning Admin: Disable
- Service point on Eth 2:
  - Service Point Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation: Untagged
  - Allowing Flooding: Allow
  - Learning Admin: Disable

18.2.5.3 Enabling Link Bonding Throughput Enhancement for 4+0 Layer 1 Link Bonding (CLI)

After configuring a Link Bonding node, it is recommended to enable Link Bonding Throughput Enhancement. Link Bonding Throughput Enhancement is available for the main unit only, not for the paired unit.

Link Bonding Throughput Enhancement is enabled on the main unit's Multi-Carrier ABC group. When it is enabled, the L2 Header Compensation for the group must be reduced by 12.

The Link Bonding Throughput Enhancement and L2 Header Compensation settings must be the same for the main units on both sides of the link. Therefore, the changes should be applied in the following order to ensure that management is not lost:

1 Enable Link Bonding Throughput Enhancement on the remote unit by entering the following commands:

```
root> multi-carrier-abc group-id 1 slot 1 type Enhanced
multi-carrier-abc enhanced-group-id [1] slot [1]> lb-throughput-
enhancement set admin enable
```

2 Enable Link Bonding Throughput Enhancement on the local unit by entering the following commands:

```
root> multi-carrier-abc group-id 1 slot 1 type Enhanced
multi-carrier-abc enhanced-group-id [1] slot [1]> lb-throughput-
enhancement set admin enable
```

3 Modify the L2 Header Compensation (decrease by 12) on the remote unit by entering the following commands:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]>ethernet link-bonding-member group-on-slot
enhanced-abc slot 1 group-id 1
lbg-member[enhanced-abc1/1]>admin set disable
lbg-member[enhanced-abc1/1]> l2-header-compensation edit l1-
header-compensation-enabled <yes|no> l2-header-compensation-value
<(-63)-63>
lbg-member[enhanced-abc1/1]>admin set enable
```

The l2-header-compensation-value parameter should be reduced by 12. For example, if the parameter was set to the default value of 26, change it to 14. To display the current parameter, enter the following command:

```
lbg-member[enhanced-abc1/1]> l2-header-compensation show
```

4 Modify the L2 Header Compensation (decrease by 12) on the local unit by entering the following commands:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]>ethernet link-bonding-member group-on-slot
enhanced-abc slot 1 group-id 1
lbg-member[enhanced-abc1/1]>admin set disable
lbg-member[enhanced-abc1/1]> l2-header-compensation edit l1-
header-compensation-enabled <yes|no> l2-header-compensation-value
<(-63)-63>
lbg-member[enhanced-abc1/1]>admin set enable
```

The l2-header-compensation-value parameter should be reduced by 12. For example, if the parameter was set to the default value of 26, change it to 14. To display the current parameter, enter the following command:

```
lbg-member[enhanced-abc1/1]> l2-header-compensation show
```

18.2.5.4 Enabling Link Bonding Throughput Enhancement for 4+0 Layer 1 Link Bonding

After configuring a Link Bonding node, it is recommended to enable Link Bonding Throughput Enhancement. Link Bonding Throughput Enhancement is available for the main unit only, not for the paired unit.

Link Bonding Throughput Enhancement is enabled on the main unit's Multi-Carrier ABC group. When it is enabled, the L2 Header Compensation for the group must be reduced by 12.

The Link Bonding Throughput Enhancement and L2 Header Compensation settings must be the same for the main units on both sides of the link. Therefore, the changes should be applied in the following order to ensure that management is not lost:

1 Enable Link Bonding Throughput Enhancement on the remote unit:

i Select **Radio** > **Ethernet Interface** > **Configuration**. The Radio Ethernet Interface Configuration page opens.

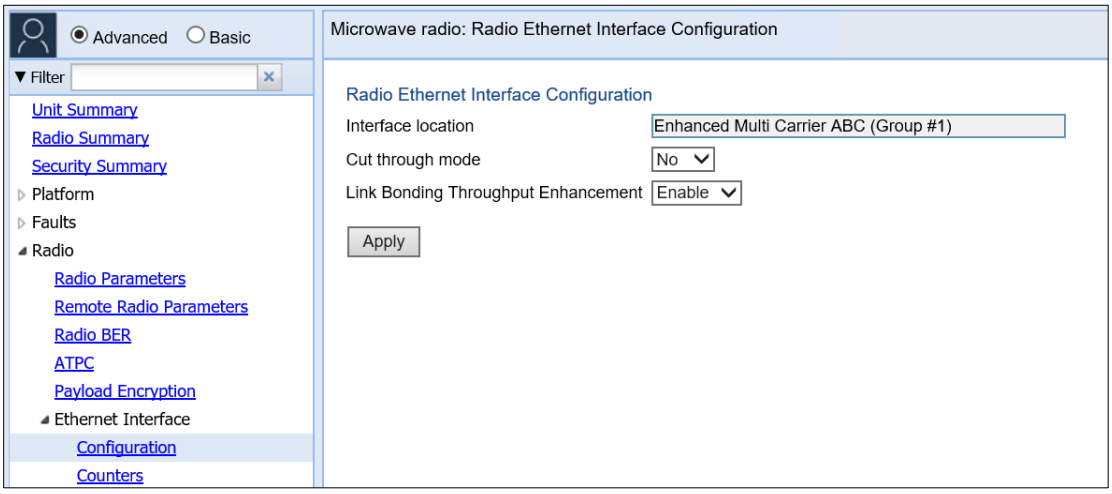


Figure 545: Radio Ethernet Interface Configuration Page (PTP 850C)

ii In the **Link Bonding Throughput Enhancement** field, select **Enable**.
iii Click **Apply**.

2 Enable Link Bonding Throughput Enhancement on the local unit:

i Select **Radio** > **Ethernet Interface** > **Configuration**. The Radio Ethernet Interface Configuration page opens (Figure 545).
ii In the **Link Bonding Throughput Enhancement** field, select **Enable**.
iii Click **Apply**.

3 Modify the L2 Header Compensation (decrease by 12) on the remote unit:

i Select **Ethernet** > **Groups** > **Link Bonding**. The Link Bonding page opens.
ii In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page opens (**Figure 181**).
iii In the **L2 header compensation** column, reduce the value for the Enhanced Multi Carrier ABC group by 12. For example, if the group was set to the default value of 26, change it to 14.
iv Click **Apply**.

4 Modify the L2 Header Compensation (decrease by 12) on the local unit:

i Select **Ethernet** > **Groups** > **Link Bonding**. The Link Bonding page opens.
ii In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page opens.
iii In the **L2 header compensation** column, reduce the value for the Enhanced Multi Carrier ABC group by 12. For example, if the group was set to the default value of 26, change it to 14.

18.2.6 Editing a Link Bonding Group or its Members (CLI)

To modify or display the parameters of the Link Bonding group, enter the following command to enter group view:

```
root>ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

To change the name of the Link Bonding group, enter the following command in group view:

```
eth group [lbx]> edit group-name <string>
```

To modify the attributes of a Link Bonding group member, you must first enter one of the following commands to enter the group member's view.

To enter the radio member's view, enter the following command in group view:

```
eth group [lb1]>ethernet link-bonding-member group-on-slot
enhanced-abc slot 1 group-id <1-4>
```

To enter the Ethernet member's view, enter the following command in group view:

```
eth group [lbx]>ethernet link-bonding-member interface eth slot 1
port 4
```

To change the Admin Status of a group member, enter the following command in group member view:

```
lbg-member[radio/ethx/x]>admin set admin set <enable|disable>
```

For example, to disable the radio interface in Link Bonding group 1, enter the following command in group view:

```
lbg-member[enhanced-abc1/1]>admin set admin set disable
```

To display the Admin Status of a group member, enter the following command in group member view:

```
lbg-member[radio/ethx/x]>admin state show
```

You can adjust the maximum shaper for either or both interfaces in the group. Generally, there is no need to change this parameter from its default value of 30000 Mbps. However, if you want to configure a different value in order to limit traffic distribution to either the main unit (the Multi-Carrier ABC group) and the paired unit (the Ethernet interface, through which traffic is sent to the paired unit), enter the following command in group member view:

```
lbg-member[ethx/y]>edit shaper-bit-rate <0-30000>
```

Note: In order to change the maximum shaper, you must first verify that Inband Management is enabled. Otherwise, the change will have no effect. See Configuring In-Band Management (CLI).

To display configuration of the group member, including its Admin Status and maximum shaper bit rate, enter the following command in group member view:

```
lbg-member[radio/ethx/x]> configuration show
```

The `l1-header-compensation-enabled` parameter should be set to `no` for both interfaces. If you did not set this parameter properly when configuring the Link Bonding group, or if you need to set them to a different value for any reason, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l1-header-compensation edit l1-header-
compensation-enabled <yes|no> l1-header-compensation-value <(-
63)-63>
```

The `l2-header-compensation-enabled` parameter should be set to `yes` for both members of the group. The l2-header-compensation parameter should be set to its default value. If you did not set these parameters properly when configuring the group, or if you need to set them to a different value for any reason, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l2-header-compensation edit l1-header-
compensation-enabled <yes|no> l2-header-compensation-value <(-
63)-63>
```

Note: Before changing the `l2-header-compensation-enabled` parameter, the Admin status of the group member in the group must be set to `disable`. Otherwise, the change will have no effect. After changing the `l2-header-compensation-enabled` parameter, make sure to set the Admin status of the group member in the group back to `enable`.

To display the L1 Header Compression settings for the group member, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l1-header-compensation show
```

To display the L2 Header Compression settings for the group member, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l2-header-compensation show
```

18.2.7 Displaying Statistics for a Link Bonding Group (CLI)

Enter the group view by entering the following command in root view:

```
root>ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

To display the actual current traffic distribution between the main unit (the Multi-Carrier ABC group) and the paired unit (the Ethernet interface, enter the following command in group member view:

```
eth group [lb1]> lb-member status show all
```

For example:

```
eth group [lb1]>lb-member status show all
Link Bonding members status Table:

--------------------------------------------------------------------------------
--------
Member Location           VLAN ID    Group Location           Shaper actual
bit rate
--------------------------------------------------------------------------------
--------
Ethernet: Slot 1,                Port 4  untagged   Link Bonding: Group
#1   1898804
Multi Carrier ABC (Slot 1, Group 1)      untagged   Link Bonding: Group
#1   9905046
```

To display the total number of segments and bytes (TX and RX) that have passed through each member of the Link Bonding group, enter the following command in group member view:

```
eth group [lb1]> statistics show
```

For example:

```
eth group [lb1]>statistics show
         txPkts                          17304248327
         txOctets                        22885762312
         rxPkts                          0
         rxOctets                        0
         txUnicastPkts                   17304246993
         txMulticastPkts                 0
         txBroadcastPkts                 0
         txPkts64Octets                  0
         txPkts65to127Octets             0
         txPkts128to255Octets            17304248327
         txPkts256to511Octets            0
         txPkts512to1023Octets           0
         txPkts1024to1518Octets          0
         txPkts1519Octets                0
eth group [lb1]>
```

Note: The ability to clear these statistics is planned for future release.

18.2.8 Deleting a Link Bonding Group (CLI)

To delete a Link Bonding group, you must first remove the members from the group:

1 Enter the group view by entering the following command in root view:

```
root>ethernet interfaces group lb<1-6>
```

2 Enter the following commands to remove the group members:

```
eth group [lb1]>lb-member delete group-on-slot enhanced-abc slot
1 group-id <1-4>
eth group [lb1]>lb-member delete interface eth slot 1 port 4
```

3 Exit group view.
4 Remove any service points on the Link Bonding group.
5 In root view, enter the following command to delete the group:

```
root>ethernet link-bonding delete group group_id <1-6>
```

18.2.9 Configuring Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP (CLI)

Note: This section is only relevant for PTP 850C.

Layer 1 Link Bonding links can also be configured using the Quick Configuration wizard. It is recommended to use the wizard whenever possible.

This section includes:

- Configuring a Layer 1 Link Bonding Node with PTP 850C and PTP 820C or PTP 820C-HP (CLI)
- Configuring Synchronization in a Layer 1 Link Bonding Node with PTP 850C and PTP 820C or PTP 820C-HP (CLI)
- Editing a Link Bonding Group or its Members (CLI)
- Displaying Statistics for a Link Bonding Group (CLI)

- Deleting a Link Bonding Group (CLI)

18.2.10 Configuring a Layer 1 Link Bonding Node with PTP 850C and PTP 820C or PTP 820C-HP (CLI)

To configure a Layer 1 Link Bonding node with PTP 850C and PTP 820C or PTP 820C-HP:

1 Connect the external switch to Eth 1 (P2, the PoE port), Eth 3 (P4, the MIMO port), or Eth 4 (P5, SFP+) on the main PTP 850C unit.
2 On both the main unit and the paired unit, configure the port speed of Eth 2 to 1 Gbps.
3 On the main unit, select either Eth 3 (P4) or Eth 4 (P5) to carry L2 protocol data between the main unit and the paired unit. Configure the port speed of the port you select to 1 Gbps.
4 On the PTP 820C or PTP 820C-HP, use Eth 3 to carry L2 protocol data between the main unit and the paired unit.
5 Connect an optical cable between Eth 2 of each unit. This cable carries traffic between the two units.
6 Set the port connected to the paired unit for passing traffic between the two units (Eth 2) to **Admin** = **Down**.
7 Connect an optical cable between the ports on each unit carrying L2 protocol data between the two units.
8 Configure the script and radio settings for both the main unit and the paired unit, including XPIC.
9 On both the main unit and the paired unit, configure a Multi-Carrier ABC group that includes both of the unit's radio carriers.
10 On the main unit only, configure a Link Bonding group that includes the port connected to the external switch and the Multi-Carrier ABC group:

Note: Before adding a group member, make sure that no shapers or service points are configured on the interface or group.

iv Create the group by entering the following command in root view:

```
root> ethernet link-bonding create group group_id <1-6> group-
name <string>
```

Note: The `name` parameter is optional.

v Enter the group view by entering the following command in root view:

```
root>ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

vi Add Eth 2 to the Link Bonding Group by entering the following command in group view. Eth 2 is the port connected to the paired unit.

```
eth group [lbx]> lb-member add interface eth slot 1 port 2
shaper-bit-rate <0-30000> vlan untag l1-header-compensation-
enabled no l1-header-compensation-value <(-63)-63> l2-header-
compensation-enabled <yes|no> l2-header-compensation-value <(-
63)-63>
```

vii Add the Multi-Carrier ABC group to the Link Bonding Group by entering the following command in group view:

```
eth group [lbx]> lb-member add group-on-slot enhanced-abc slot 1 group-id <1-
4> shaper-bit-rate <0-30000> vlan untag l1-header-compensation-enabled no l1-
header-compensation-value <(-63)-63> l2-header-compensation-enabled <yes|no>
l2-header-compensation-value <(-63)-63>
```

- The shaper-bit-rate parameter enables you to adjust the shaper for either or both interfaces in the group. This shaper controls the distribution of traffic between the main Unit (the Multi-Carrier ABC group) and the paired unit (the Ethernet interface). Generally, there is no need to change this parameter from its default value of 30000 Mbps.

Note: In order to change the shaper-bit-rate parameter, you must first verify that Inband Management is enabled. Otherwise, the change will have no effect.

- The l1-header-compensation-enabled parameter should be set to no for the radio member. For instructions on setting this parameter for the Ethernet member,
- The l2-header-compensation-enabled parameter should be set to yes for both interfaces.
- The l2-header-compensation-value parameter should be set to 26 for the Multi-Carrier ABC group and 30 for the Ethernet interface. If Header De-Duplication is enabled on the PTP 820C or PTP 820C-HP, this parameter should be set to 14 for the Ethernet interface.

11 In the Interface Manager, set the port connected to the paired unit for passing traffic between the two units (Eth 2) to **Admin** = **Up**.

12 To ensure proper fault handling, configure Automatic State Propagation (ASP) as follows:

i On the local and remote main units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The Link Bonding group
- Controlled Port: The port connected to the external switch (Eth 1, Eth 3, or Eth 4)

ii On the local and remote paired units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The Multi-Carrier ABC group or radio interface
- Controlled Port: The port used to carry traffic between the two units (Eth 2)

13 Inband management can be carried between the main unit and the paired unit via the Protocols cable between the two units. To configure inband management, you must define a management service that connects the L2 protocol data ports on each unit, the Link Bonding groups, and the ingress port of the main unit:

i On the local main unit, configure a service point on the port connected to the external switch (Eth 1, Eth 3, or Eth 4).
ii On the local main unit, configure a service point on the L2 protocol data port (Eth 3 or Eth 4).
iii On the local main unit, configure a service point on the Link Bonding group.
iv On the local paired unit, configure a service point on the L2 protocol data port (Eth 3).
v On the remote paired unit, configure a service point on the L2 protocol data port (Eth 3).
vi On the remote main unit, configure a service point on the L2 protocol data port (Eth 3 or Eth 4).
vii On the remote main unit, configure a service point on the Link Bonding group.

14 If the paired unit is an PTP 820C or PTP 820C-HP, you must configure Radio Bandwidth Notification on the PTP 820C or PTP 820C-HP via the Web EMS.

15 On the paired unit on both sides of the link, configure a point-to-point service for Radio Bandwidth Notification, with service points on the Multi-Carrier ABC group and Eth 3. The service points should be configured as follows:

- Create a service point on the Multi-Carrier ABC group with the following parameters:
  - Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation: 4090
  - Allow Flooding: Allow
  - Learning Admin: Disable
- Create a service point on Eth 3 with the following parameters:
  - Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation: 4090
  - Allow Flooding: Allow
  - Learning Admin: Disable

16 On the paired unit on both sides of the link, configure a point-to-point service for Link Bonding traffic, with service points on the Multi-Carrier ABC group and Eth 2. The service points should be configured as follows:

i Create a service point on the Multi-Carrier ABC group with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Any VLAN
- Allow Flooding: Allow
- Learning Admin: Disable

ii Create a service point on Eth 2 with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Untagged
- Allow Flooding: Allow
- Learning Admin: Disable

18.2.11 Configuring Synchronization in a Layer 1 Link Bonding Node with PTP 850C and PTP 820C or PTP 820C-HP (CLI)

SyncE and 1588 PTP can be used with Layer 1 Link Bonding. SyncE and 1588 PTP can be configured for both the main unit and the paired unit. Synchronization messages are passed between the units via the Protocols cable.

18.2.11.1 Configuring SyncE in a Layer 1 Link Bonding Node with PTP 850C and PTP 820C or PTP 820C-HP (CLI)

To configure SyncE on a Layer 1 Link Bonding Node with PTP 850C and PTP 820C or PTP 820C-HP:

- On the local main unit, configure the following:
  - Configure the port connected to the external switch as a sync source with priority 1.
  - Configure radio interface 1 as a sync source with priority 2.
  - Configure radio interface 2 as a sync source with priority 3.
  - Configure Eth 3 as a sync source with priority 4.
- On the local paired unit, configure the following:
  - Configure the L2 Protocols port as a sync source with priority 1.
  - Configure radio interface 1 as a sync source with priority 2.
  - Configure radio interface 2 as a sync source with priority 3.
- On the remote paired unit, configure the following:
  - Configure radio interface 1 as a sync source with priority 1.
  - Configure radio interface 2 as a sync source with priority 2.
  - Configure the L2 Protocols port as a sync source with priority 2 or 3.
- On the remote main unit, configure the following:
  - Configure Eth 3 as a sync source with priority 1.
  - Configure radio interface 1 as a sync source with priority 2.
  - Configure radio interface 2 as a sync source with priority 3.
  - Configure the port connected to the external switch as a sync source with priority 4.

All sync sources should be configured with Sync Interface Quality G.813/8262. For instructions on configuring SyncE.

18.2.11.2 Configuring 1588 PTP in a Layer 1 Link Bonding Node with PTP 850C and PTP 820C or PTP 820C-HP (CLI)

To use 1588 PTP on a Layer 1 Link Bonding node, you must configure Boundary Clock on the main unit and Transparent Clock on all of the units, as described below. 1588 messages are generated by the Boundary Clock mechanism on the main unit and sent untagged to the paired unit via the Protocols cable. They receive VLAN tagging on the paired unit in order to separate them from user traffic.

Note: If the paired unit goes down, 1588 packets will not be transmitted to the other side of the link.

To configure 1588 PTP for the Layer 1 Link Bonding node:

1 Configure SyncE following the instructions.
2 Enable 1588 PTP on each unit, including the main unit and the paired unit on both sides of the link, using the following command in each unit:

```
root> platform sync ptp set admin enable
```

3 On the main unit on both sides of the link, enable Boundary clock on:
   - The port connected to the external switch.
   - Eth 3.

4 On the paired unit on both sides of the link, enable Transparent Clock on the Multi-Carrier ABC group.
5 On the paired unit on both sides of the link, configure a point-to-point service with service points on the Multi-Carrier ABC group and the Layer 2 Protocols port. The service points should be configured as follows:

- Service point on the Multi-Carrier ABC group or radio interface:
  - Service Point Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation: Per customer's choice
  - Allowing Flooding: Allow
  - Learning Admin: Disable
- Service point on the L2 Protocols port:
  - Service Point Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation: Untagged
  - Allowing Flooding: Allow
  - Learning Admin: Disable

See Configuring Service Points (CLI).

18.2.12 Enabling Link Bonding Throughput Enhancement for Layer 1 Link Bonding with PTP 850C and PTP 820C or PTP 820C-HP

After configuring a Link Bonding node, it is recommended to enable Link Bonding Throughput Enhancement. Link Bonding Throughput Enhancement is available for the main unit only, not for the paired unit.

Link Bonding Throughput Enhancement is enabled on the main unit's Multi-Carrier ABC group. When it is enabled, the L2 Header Compensation for the group must be reduced by 12.

The Link Bonding Throughput Enhancement and L2 Header Compensation settings must be the same for the main units on both sides of the link. Therefore, the changes should be applied in the following order to ensure that management is not lost:

1. Enable Link Bonding Throughput Enhancement on the remote unit:
   i. Select **Radio > Ethernet Interface > Configuration**. The Radio Ethernet Interface Configuration page opens.
   ii. In the **Link Bonding Throughput Enhancement** field, select **Enable**.
   iii. Click **Apply**.
2. Enable Link Bonding Throughput Enhancement on the local unit:
   i. Select **Radio > Ethernet Interface > Configuration**. The Radio Ethernet Interface Configuration page opens.
   ii. In the **Link Bonding Throughput Enhancement** field, select **Enable**.
   iii. Click **Apply**.
3. Modify the L2 Header Compensation (decrease by 12) on the remote unit:
   i. Select **Ethernet** > **Groups** > **Link Bonding**. The Link Bonding page opens.
   ii. In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page opens.
   iii. In the **L2 header compensation** column, reduce the value for the Enhanced Multi Carrier ABC group by 12. For example, if the group was set to the default value of 26, change it to 14.
   iv. Click **Apply**.
4. Modify the L2 Header Compensation (decrease by 12) on the local unit:

i Select **Ethernet** > **Groups** > **Link Bonding**. The Link Bonding page opens.
ii In the Link Bonding page, select the group and click **Edit Members**. The Edit Members page opens.
iii In the **L2 header compensation** column, reduce the value for the Enhanced Multi Carrier ABC group by 12. For example, if the group was set to the default value of 26, change it to 14.

iv Click **Apply**.

18.2.13 Editing a Link Bonding Group or its Members (CLI)

To modify or display the parameters of the Link Bonding group, enter the following command to enter group view:

```
root>ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

To change the name of the Link Bonding group, enter the following command in group view:

```
eth group [lbx]> edit group-name <string>
```

To modify the attributes of a Link Bonding group member, you must first enter one of the following commands to enter the group member's view.

To enter the radio member's view, enter the following command in group view:

```
eth group [lb1]>ethernet link-bonding-member group-on-slot
enhanced-abc slot 1 group-id <1-4>
```

To enter the Ethernet member's view, enter the following command in group view:

```
eth group [lbx]>ethernet link-bonding-member interface eth slot 1
port 4
```

To change the Admin Status of a group member, enter the following command in group member view:

```
lbg-member[radio/ethx/x]>admin set admin set <enable|disable>
```

For example, to disable the radio interface in Link Bonding group 1, enter the following command in group view:

```
lbg-member[enhanced-abc1/1]>admin set admin set disable
```

To display the Admin Status of a group member, enter the following command in group member view:

```
lbg-member[radio/ethx/x]>admin state show
```

You can adjust the maximum shaper for either or both interfaces in the group. Generally, there is no need to change this parameter from its default value of 30000 Mbps per second

To adjust the maximum shaper for a group member, enter the following command in group member view:

```
lbg-member[ethx/y]>edit shaper-bit-rate <0-30000>
```

Note: In order to change the maximum shaper, you must first verify that Inband Management is enabled. Otherwise, the change will have no effect. See Configuring In-Band Management (CLI).

To display configuration of the group member, including its Admin Status and maximum shaper bit rate, enter the following command in group member view:

```
lbg-member[radio/ethx/x]> configuration show
```

In most cases, the l1-header-compensation-enabled parameter should be set to no for both interfaces. However, if the nominal bandwidth of the Multi-Carrier ABC group or radio interface on the PTP 820C or PTP 820C-HP (the paired unit) is over 853 Mbps (with Header De-Duplication disabled) or 833 Mbps (with Header-De-Duplication enabled), then l1-header-compensation-enabled should be enabled for the Ethernet interface of the PTP 850C and set to the values in the right column.

If you did not set these parameters properly when configuring the Link Bonding group, or if you need to set them to a different value for any reason, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l1-header-compensation edit l1-header-compensation-enabled <yes|no> l1-header-compensation-value <(-63)-63>
```

The l2-header-compensation-enabled parameter should be set to yes for both members of the group.

The l2-header-compensation-value parameter should be set to 26 for the Multi-Carrier ABC group and 30 for the Ethernet interface. If Header De-Duplication is enabled on the PTP 820C or PTP 820C-HP, this parameter should be set to 14 for the Ethernet interface.

To set the l2 header compensation parameters, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l2-header-compensation edit l1-header-compensation-enabled <yes|no> l2-header-compensation-value <(-63)-63>
```

Note: Before changing the l2-header-compensation-enabled parameter, the Admin status of the group member in the group must be set to disable. Otherwise, the change will have no effect. After changing the l2-header-compensation-enabled parameter, make sure to set the Admin status of the group member in the group back to enable.

To display the L1 Header Compression settings for the group member, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l1-header-compensation show
```

To display the L2 Header Compression settings for the group member, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l2-header-compensation show
```

18.2.14 Displaying Statistics for a Link Bonding Group (CLI)

Enter the group view by entering the following command in root view:

```
root>ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

To display the total number of segments and bytes (TX and RX) that have passed through each member of the Link Bonding group, enter the following command in group member view:

```
eth group [lb1]> lb-member status show all
```

For example:

```
eth group [lb1]>lb-member status show all
Link Bonding members status Table:

-------------------------------------------------------------------------------
Member Location           VLAN ID    Group Location           Shaper actual bit rate
-------------------------------------------------------------------------------
Ethernet: Slot 1, Port 2                  untagged   Link Bonding: Group #1   1898804
Multi Carrier ABC (Slot 1, Group 1)       untagged   Link Bonding: Group #1   9905046
```

To display statistics for overall traffic passing through the group, enter the following command in group member view:

```
eth group [lb1]> statistics show
```

For example:

```
eth group [lb1]>statistics show
         txPkts                          17304248327
         txOctets                        22885762312
         rxPkts                          0
         rxOctets                        0
         txUnicastPkts                   17304246993
         txMulticastPkts                 0
         txBroadcastPkts                 0
         txPkts64Octets                  0
         txPkts65to127Octets             0
         txPkts128to255Octets            17304248327
         txPkts256to511Octets            0
         txPkts512to1023Octets           0
         txPkts1024to1518Octets          0
         txPkts1519Octets                0
eth group [lb1]>
```

Note: The ability to clear these statistics is planned for future release.

18.2.15 Deleting a Link Bonding Group (CLI)

To delete a Link Bonding group, you must first remove the members from the group:

1 Enter the group view by entering the following command in root view:

```
root>ethernet interfaces group lb<1-6>
```

2 Enter the following commands to remove the group members:

```
eth group [lb1]>lb-member delete group-on-slot enhanced-abc slot
1 group-id <1-4>
eth group [lb1]>lb-member delete interface eth slot 1 port 4
```

3 Exit group view.
4 Remove any service points on the Link Bonding group.
5 In root view, enter the following command to delete the group:

```
root>ethernet link-bonding delete group group_id <1-6>
```

18.3 Configuring Multiband (CLI)

Multiband Overview (CLI)

For general information about Multiband and how it operates, see *Multiband Overview*.

Multiband Configuration (CLI)

To configure a Multiband node:

1 Connect the external switch to any operational traffic port on the PTP 850E.

2 Connect the Traffic port on the PTP 850E (Port 3, Eth2) to the paired unit. When the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, use the Eth2 port on the PTP 820C, PTP 820C-HP, or PTP 820S. When the paired unit is an PTP 820N or PTP 820A, use any SFP port on the PTP 820N or PTP 820A.

3 Verify that the **Admin** status of Eth2 on the PTP 850E is **Down**. See *Enabling the Interfaces (CLI)*.

4 Verify that no service points are configured on the Eth2 port of the PTP 850E. If there are service points on Eth2, remove them. See *Deleting a Service Point (CLI)*.

5 On the PTP 850E, configure a Multiband group that includes Eth2 and the radio: i Create the group by entering the following command in root view:

```
root>multi-carrier-abc create group group_id 1 slot 1 type
Enhanced
```

ii Enter Multi-Carrier ABC Group view by entering the following command in root view:

```
root>multi-carrier-abc group-id 1 slot 1 type Enhanced
multi-carrier-abc enhanced-group-id [1] slot [1]>
```

iii In Multi-Carrier ABC Group view, add the radio interface by entering the following command:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>attach-member
slot 1 port 1 channel-id 1
```

iv In Multi-Carrier ABC Group view, add the Ethernet interface by entering the following command:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>attach-eth-
member slot 1 port 2 channel-id 2
```

v In Multi-Carrier ABC Group view, use the following command to set the maximum traffic that the PTP 850E will pass to the paired unit:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-set-eth-
max-bandwidth slot 1 port 2 max-bandwidth <1-1000>
```

◦ When using Fixed ACM mode, set this parameter to the actual rate you want the paired unit to broadcast.

- When using Adaptive ACM mode, set this parameter to the maximum of the

paired unit's capacity.

The default value is 1000 Mbps.

For example, the following command sets the maximum traffic to 900 Mbps:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-set-eth-
max-bandwidth slot 1 port 2 max-bandwidth 900

Maximum bandwith: 900 Mbps
```

Use the following command in Multi-Carrier ABC Group view to display the current maximum traffic setting:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-show-eth-
max-bandwidth slot 1 port 2
```

Note: The Maximum Bandwidth represents the L1 capacity of the radio link

connected to the Ethernet member. The actual bandwidth that will be available for traffic is less due to overhead.

When using a third-party radio as the paired unit, it is particularly

important to set this parameter properly in order to ensure optimal performance. Failure to properly set this parameter may lead to frequent pauses as the queue fills up during low capacity periods, such as when weather conditions cause the ACM profile to drop.

vi In Multi-Carrier ABC Group view, use the following command to set the bandwidth margin, in Mbps. This parameter deducts the specified throughput from the throughput the PTP 850E would otherwise pass to the paired unit. The purpose of this parameter is to provide a margin of safety that will avoid loss of traffic in the event that the ACM profile is reduced on the paired unit.

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-set-eth-
bandwidth-margin slot 1 port 2 bandwidth-margin 100 <5-100>
```

It is recommended to configure this parameter as follows:

- If the paired unit is an PTP 820 microwave radio, or a third-party device with a bandwidth notification mechanism that will inform the PTP 850E of an impending reduction of the ACM profile before the reduction takes place, it is recommended to leave this parameter at its default value of 5 Mbps.
- If the paired unit is a third-party device without a bandwidth notification mechanism that will inform the PTP 850E of an impending reduction of the ACM profile before the reduction takes place, it is recommended to set this parameter to an amount equal to or greater than the largest throughput

differential between any two adjacent profiles for the script configured on the paired unit.

The range of values is 5 to 100 Mbps.

For example, the following command sets the bandwidth margin to 100 Mbps:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-set-eth-
bandwidth-margin slot 1 port 2 bandwidth-margin 100
```

Use the following command in Multi-Carrier ABC Group view to display the current bandwidth margin:

```
abc-show-eth-bandwidth-margin slot 1 port 2
```

6 Enable the Eth2 interface. See *Enabling the Interfaces (CLI)*.

7 On the paired unit, configure a service between the port receiving traffic from the PTP 850E and the radio or Multi-Carrier ABC group.

Note: If the paired unit is an PTP 820C, PTP 820C-HP, PTP 820S, or third-party microwave radio, the service must be a Pipe service. If the paired unit is an PTP 820N or PTP 820A, any service type can be used. However, this service *must* be given higher priority than any other service attached to the interfaces used for Multiband.

8 On the paired unit, configure Automatic State Propagation with **ASP trigger by remote fault** enabled.

9 If the paired unit is an PTP 820 microwave radio, configure RBN. Bandwidth Notification must be configured via the Web EMS. See *Multiband Configuration*, Step 10.

Note: If the paired unit is a third-party radio, enable 802.3X Flow Control.

i Enter one of the following commands in root view to create a Radio Bandwidth Notification entity:

If the paired unit is using a Multi-Carrier ABC group:

```
root> ethernet abn abn-entity-create protocol-type-rbn abn-name <name>
monitored-group-on-slot enhanced-abc slot 1 group-id 1 vlan untag
```

If the paired unit is using a single radio interface:

```
root> ethernet abn abn-entity-create protocol-type-rbn abn-name <name>
monitored-interface radio monitored-slot 2 monitored-port 1 vlan untag
```

Note: Once you configure the RBN entity, you cannot edit the name later. The only way to change the name is to delete and reconfigure the RBN entity.

To display information about the Radio Bandwidth Notification entity, enter the following command in root view:

```
root> ethernet abn abn-entity-show abn-name <name>
```

ii Enter the following command in root view to set the VLAN type to C-VLAN:

```
root> ethernet abn abn-vlan-type-set abn-name <name> vlan-type c-vlan
```

iii Enter the following command in root view to set the VLAN ID to the same VLAN you configured for the main unit :

```
root> ethernet abn abn-vlan-set abn-name <name> vlan <1-4094>
```

iv Enter the following command in root view to set the Admin status of the Radio Bandwidth Notification entity to Up:

```
root> ethernet abn abn-admin-set abn-name <name> admin up
```

18.3.1 Multiband Overview (CLI)

For general information about Multiband and how it operates, see Multiband Overview.

18.3.2 Multiband Configuration (CLI)

To configure a Multiband node:

1. Connect the external switch to any operational traffic port on the PTP 850E.
2. Connect the Multiband port on the PTP 850E (Port 3, Eth2) to the paired unit. When the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, use the Eth2 port on the PTP 820C, PTP 820C-HP, or PTP 820S.
3. Verify that the **Admin** status of Eth2 on the PTP 850E is **Down**. See *Enabling the Interfaces (CLI)*.
4. Verify that no service points are configured on the Eth2 port of the PTP 850E. If there are service points on Eth2, remove them. See *Deleting a Service Point (CLI)*.
5. On the PTP 850E, configure a Multiband group that includes Eth2 and the radio:
   - Create the group by entering the following command in root view:

```
root>multi-carrier-abc create group group_id 1 slot 1 type
Enhanced
```

   - Enter Multi-Carrier ABC Group view by entering the following command in root view:

```
root>multi-carrier-abc group-id 1 slot 1 type Enhanced
multi-carrier-abc enhanced-group-id [1] slot [1]>
```

   - In Multi-Carrier ABC Group view, add the radio interface by entering the following command:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>attach-member
slot 1 port 1 channel-id 1
```

   - In Multi-Carrier ABC Group view, add the Ethernet interface by entering the following command:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>attach-eth-
member slot 1 port 2 channel-id 2
```



Note

The channel-id parameter must be set to 1 for the radio interface and 2 for the Ethernet interface.

- In Multi-Carrier ABC Group view, use the following command to set the maximum traffic that the PTP 850E will pass to the paired unit:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-set-eth-
max-bandwidth slot 1 port 2 max-bandwidth <1-1000>
```

  - When using Fixed ACM mode, set this parameter to the actual rate you want the paired unit to broadcast.
  - When using Adaptive ACM mode, set this parameter to the maximum

of the paired unit's capacity.

The default value is 1000 Mbps.

For example, the following command sets the maximum traffic to 900 Mbps:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-set-eth-
max-bandwidth slot 1 port 2 max-bandwidth 900


Maximum bandwith: 900 Mbps
```

Use the following command in Multi-Carrier ABC Group view to display the current maximum traffic setting:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-show-eth-
max-bandwidth slot 1 port 2
```



Note

The Maximum Bandwidth represents the L1 capacity of the radio link connected to the Ethernet member. The actual bandwidth that will be available for traffic is less due to overhead.

When using a third-party radio as the paired unit, it is particularly important to set this parameter properly in order to ensure optimal performance. Failure to properly set this parameter may lead to frequent pauses as the queue fills up during low capacity periods, such as when weather conditions cause the ACM profile to drop.

- In Multi-Carrier ABC Group view, use the following command to set the bandwidth margin, in Mbps. This parameter deducts the specified throughput from the throughput the PTP 850E would otherwise pass to the paired unit. The purpose of this parameter is to provide a margin of safety that will avoid loss of traffic in the event that the ACM profile is reduced on the paired unit.

```
multi-carrier-abc enhanced-group-id [1] slot
[1]>abc-set-eth- bandwidth-margin slot 1 port 2
bandwidth-margin 100 <5-100>
```

It is recommended to configure this parameter as follows:

- If the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, or a third-party device with a bandwidth notification mechanism that will inform the PTP 850E of an impending reduction of the ACM profile before the reduction takes place, it is recommended to leave this parameter at its default value of 5 Mbps.
- If the paired unit is a third-party device without a bandwidth notification mechanism that will inform the PTP 850E of an impending reduction of the ACM profile before the reduction takes place, it is recommended to set this parameter to an amount equal to or greater than the largest throughput differential between any two adjacent profiles for the script configured on the paired unit.

The range of values is 5 to 100 Mbps.

For example, the following command sets the bandwidth margin to 100 Mbps:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-set-eth-
bandwidth-margin slot 1 port 2 bandwidth-margin 100
```

Use the following command in Multi-Carrier ABC Group view to display the current bandwidth margin:

```
abc-show-eth-bandwidth-margin slot 1 port 2
```

1. Enable the Eth2 interface. See *Enabling the Interfaces (CLI)*.

2. If the paired unit is an PTP 820C or PTP 820C-HP, verify that XPIC is disabled on the PTP 820C or PTP 820C-HP.
3. On the paired unit, configure a Pipe service between the port receiving traffic from the PTP 850E and the radio or Multi-Carrier ABC group.
4. On the paired unit, configure Automatic State Propagation with **ASP trigger by remote fault** enabled.
5. If the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, configure Radio BNM. For instructions, refer to the *User Guide for PTP 820 All-Outdoor Products*. Make sure to define a Name for the Radio BNM group.

> **Note:** If the paired unit is a third-party radio, enable 802.3X Flow Control.

18.3.3 Multiband Management (CLI)

The PTP 850E unit in a Multiband configuration can be managed normally, as in any other configuration. For in-band management of the PTP 850E, configure the management service on the PTP 850E Multiband group. See *Configuring In-Band Management (CLI)*.

The following options are available for managing the paired unit in a Multiband configuration:

- Inband management via the PTP 850E
- Inband management directly from the external switch
- Out-of-Band management

For a detailed explanation of these options and their requirements, see Multiband Management.

18.3.3.1 Configuring Synchronization in a Multiband Node (CLI)

SyncE and 1588 Boundary Clock can be used in Multiband nodes. SyncE and 1588 Boundary Clock can be configured for both the PTP 850E and the unit paired with the PTP 850E. SyncE packets are carried between the units along with traffic; no special cables are required.



Note

When a third-party unit is paired with the PTP 850E, it is a prerequisite that the third-party radio unit support SyncE in order to provide synchronization for the Multiband node.

For details, see Configuring Synchronization in a Multiband Node.

For instructions on configuring SyncE, see Configuring the Sync Source (CLI).

18.3.3.2 Deleting a Multiband Group (CLI)

If you need to delete the Multiband group, you must first remove the group's members, then delete the group.

To remove members from a Multi-Carrier ABC group, go to Multi-Carrier ABC group view and enter the following command for each interface in the group:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>detach-member
channel-id <1-2>
```

After removing the members, enter the following command in root view:

```
root> multi-carrier-abc delete group group_id 1 slot 1 type Enhanced
```

18.3.3.3 Displaying Multiband Group Statistics (CLI)

To display general information about a Multiband group, including the group's TX and RX capacity, go to Multi-Carrier ABC group view and enter the following command:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>summary-show
```

To display port counters for a Multiband group, go to Multi-Carrier ABC group view and enter the following command:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>show-ethernet-
port-counters
```

18.4 Configuring Multiband with Layer 1 Link Bonding (CLI)

Note: This section is relevant for Multiband configurations using Layer 1 Link Bonding. These configurations utilize PTP 850E for E-band and PTP 850C, PTP 850CX, PTP 820C, PTP 820C-HP, or a third-party device for Microwave.

Multiband with Layer 1 Link Bonding links can also be configured using the Quick Configuration wizard unless the attached unit is a third-party device. It is recommended to use the wizard whenever possible. See Configuring a Multiband Link with Layer 1 Link Bonding Using the Quick Configuration Wizard.

For Multiband with Layer 1 Link Bonding links using PTP 850C, line redundancy is available. For details, refer to Layer 1 Link Bonding and Line Redundancy and Configuring Line Redundancy for Link Bonding Configurations (CLI).

Multiband with Layer 1 Link Bonding links can also be configured using the Quick Configuration wizard unless the paired unit is a third-party device. It is recommended to use the wizard whenever possible.

This section includes:

- Configuring Multiband with Layer 1 Link Bonding (CLI)
- Configuring Line Redundancy with Multiband and Link Bonding (CLI)
- Enabling Link Bonding Throughput Enhancement for Multiband with Layer 1 Link Bonding (CLI)
- The Link Bonding Throughput Enhancement and L2 Header Compensation settings must be the same for the main units on both sides of the link. Therefore, the changes should be applied in the following order to ensure that management is not lost:

Note: The settings on attached units do not affect management, and can be changed in any order.

1 Enable Link Bonding Throughput Enhancement on the remote unit (main and/or attached unit) by entering the following commands:

```
root> radio slot 1 port 1
radio [1/1]> lb-throughput-enhancement set admin enable
```

2 Enable Link Bonding Throughput Enhancement on the local unit (main and/or attached unit) by entering the following commands:

```
root> radio slot 1 port 1
radio [1/1]> lb-throughput-enhancement set admin enable
```

3 Modify the L2 Header Compensation on the remote unit (main and/or attached unit) by entering the following commands:

- For the main unit, enter the following commands to modify the L2 Header Compensation for the radio interface:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface radio
slot 1 port 1
lbg-member[radio1/1]> admin set disable
lbg-member[radio1/1]> l2-header-compensation edit l1-header-
compensation-enabled <yes|no> l2-header-compensation-value
<(-63)-63>
lbg-member[radio1/1]> admin set enable
```

To display the current parameter, enter the following command:

```
lbg-member[radio1/1]> l2-header-compensation show
```

- For the attached unit, enter the following commands to modify the L2 Header Compensation for the interface connected to the attached unit:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface eth
slot 1 port 4
lbg-member[eth4]>admin set disable
lbg-member[eth4]> l2-header-compensation edit l1-header-
compensation-enabled <yes|no> l2-header-compensation-value <(-
63)-63>
lbg-member[eth4]>admin set enable
```

To display the current parameter, enter the following command:

```
lbg-member[eth4]> l2-header-compensation show
```

Note: For recommended values, see L1 and L2 Header Compensation Values.

4 Modify the L2 Header Compensation on the local unit (main and/or attached unit) by entering the following commands:

- For the main unit, enter the following commands to modify the L2 Header Compensation for the radio interface:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface radio
slot 1 port 1
lbg-member[radio1/1]> admin set disable
lbg-member[radio1/1]> l2-header-compensation edit l1-header-
compensation-enabled <yes|no> l2-header-compensation-value
<(-63)-63>
lbg-member[radio1/1]> admin set enable
```

To display the current parameter, enter the following command:

```
lbg-member[radio1/1]> l2-header-compensation show
```

- For the attached unit, enter the following commands to modify the L2 Header Compensation for the interface connected to the attached unit:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface eth slot 1 port
4
lbg-member[eth4]>admin set disable
lbg-member[eth4]> l2-header-compensation edit l1-header-compensation-
enabled <yes|no> l2-header-compensation-value <(-63)-63>
lbg-member[eth4]>admin set enable
```

To display the current parameter, enter the following command:

```
lbg-member[eth4]> l2-header-compensation show
```

Note: For recommended values, see L1 and L2 Header Compensation Values.

- Editing a Multiband Link Bonding Group or its Members (CLI)
- Displaying Group Statistics for a Multiband Link Bonding Group (CLI)
- Deleting a Multiband Link Bonding Group (CLI)

For an overview of Multiband with Layer 1 Link Bonding, see Overview of Multiband with Layer 1 Link Bonding.

18.4.1 Configuring Multiband with Layer 1 Link Bonding (CLI)

Note: For configurations in which the PTP 850E is connected to a third-party device via the PTP 850E's Management port, make sure to reconfigure management according to the instructions. Failure to do so will lead to loss of management and may lead to RMA at the customer's expense.

To configure a Multiband node with Layer 1 Link Bonding:

1. Connect the external switch to the QSFP port (P4, Eth 3 – Eth 6) on the PTP 850E. This port can be configured to operate in QSFP mode (40 Gbps) or SFP+ mode (10 Gbps). If the configuration includes Line Redundancy, you must configure this port to 10 Gbps.
2. In the Interface Manager, make sure the port connected to the paired unit for passing traffic between the two units is set to **Admin** = **Down**.
3. Configure the speed as follows:
   - For configurations with PTP 850C, set the traffic ports to 10 Gbps.
   - For configurations with PTP 820C or PTP 820C-HP, set the traffic ports to 1 Gbps.
   - For configurations with a third-party device, set the traffic ports to whatever speed is appropriate for the third-party device, making sure the configuration is symmetrical for the main and paired units.

   Note: If you are using an SFP port on the PTP 850E with an electrical SFP module, you must configure the port speed *after* adding the port to the Link Bonding group. Adding the port to the Link Bonding group automatically configures the port to 10G, which is not supported SFP ports with electrical SFP modules. This is why you must set or reset the port speed to 1G *after* adding the port to the Link Bonding group.
4. If you are using a separate Protocols cable:

- For configurations with PTP 850C, configure the port speed of the protocols ports to 2.5 Gbps.
- For configurations with PTP 820C or PTP 820C-HP, configure the port speed of the protocols ports to 1 Gbps.
- For configurations with a third-party device, set the ports to 1 Gbps or 2 Gbps, making sure the configuration is symmetrical for the main and paired units.

5 Connect an optical cable between the traffic ports. This cable carries traffic and (optionally) L2 protocol data between the two units.

6 Optionally, connect an optical cable between the Protocols ports of each unit. This cable carries L2 protocol data between the two units.

Note: Alternatively, if the paired unit is a third-party device, you can connect a CAT-5 cable between the PTP 850E Management port and an electrical port on the third-party device for traffic and protocols.

7 Configure the scripts and radio settings for both units, including XPIC on the paired unit if so desired.

Note: If the paired unit is a third-party device, the radio must be configured to fixed mode, not ACM.

8 If the paired unit supports Multi-Carrier ABC, configure a Multi-Carrier ABC group that includes both of the unit's radio carriers. In this manual for PTP 850C or in the User Manual for PTP 820 All-Outdoor Products for PTP 820C and PTP 820C-HP.

9 On the PTP 850E only, configure a Link Bonding group that includes the radio interface and the Ethernet interface connected to the paired unit for traffic:

Note: Before adding a group member, make sure that no shapers or service points are configured on the interface.

i Create the group by entering the following command in root view:

```
root> ethernet link-bonding create group group_id <1-6> group-
name <string>
```

Note: The `name` parameter is optional.

ii Enter the group view by entering the following command in root view:

```
root>ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

iii In most configurations, add Eth 7 to the Link Bonding Group by entering the following command in group view. Eth 7 is the port connected to the paired unit for passing traffic between the two units.

```
eth group [lbx]> lb-member add interface eth slot 1 port 7
shaper-bit-rate <0-30000> vlan untag l1-header-compensation-
enabled no l1-header-compensation-value <> l2-header-
compensation-enabled yes|no> l2-header-compensation-value <>
```

In configurations with a third-party device in which the PTP 850E Management port is connected to an electrical port on the third-party device, add the Management port to the Link Bonding Group by entering the following command in group view:

```
eth group [lbx]> lb-member add interface mng slot 1 port 1
shaper-bit-rate <0-30000> vlan untag l1-header-compensation-
enabled no l1-header-compensation-value <> l2-header-
compensation-enabled yes|no> l2-header-compensation-value <>
```

iv Add the radio interface to the Link Bonding Group by entering the following command in group view:

```
eth group [lbx]> lb-member add interface radio slot 1 port 1
shaper-bit-rate <0-30000> vlan untag l1-header-compensation-
enabled yes l1-header-compensation-value <> l2-header-
compensation-enabled yes|no> l2-header-compensation-value <>
```

- The `shaper-bit-rate` parameter enables you to adjust the shaper for either or both interfaces in the group. This shaper controls the distribution of traffic between the paired unit (the radio interface) and the PTP 850E (the Ethernet interface). You should set this according to the maximum capacity of the radio interface, or the maximum radio capacity of the paired unit connected to the Ethernet member. The default value is 30000 Mbps.
- The l1-header-compensation-enabled parameter should be set to no for the Ethernet member.
- The l2-header-compensation-enabled parameter should be set to yes for both interfaces.

The l2-header-compensation-value parameter should be set according to the recommended values in L1 and L2 Header Compensation Values.

v In Link Bonding group view, enter the following command:

```
eth group [lbx]> edit lbg-mode <enhanced|standard>
```

You must configure the group to *enhanced* mode if the configuration uses a single cable for traffic and L2 protocol data. The default value is *standard*. See Requirements and Limitations for Enhanced Link Bonding Mode.
For example, use the following commands to set Link Bonding group 1 to *enhanced* mode:

```
root>ethernet interfaces group lb1
eth group [lb1]>edit lbg-mode enhanced
```

To display the currently configured Link Bonding Mode for a specific Link Bonding group, enter the following command in root view:

```
root>ethernet link-bonding show group group_id <1-6>
```

To display the currently configured Link Bonding Mode for all Link Bonding groups configured on the device, enter the following command in root view:

```
root>ethernet link-bonding show all
```

Note: Although most PTP 850C and PTP 850E devices support Enhanced Link Bonding mode, some do not. For details, see Requirements and Limitations for Enhanced Link Bonding Mode.

10 In the Interface Manager, set the port connected to the paired unit for passing traffic between the two units to **Admin** = **Up**.
11 Enable PDU encapsulation on the paired unit:

Note: This step is crucial since it ensures that protocols packets are properly tagged and separated from traffic. If the paired unit is a third-party device, this step is optional, but recommended if the third-party device supports PDU encapsulation. Any other protocols on the third-party device that might interfere with protocols transmission should be disabled.

i Enter interface view for the port carrying L2 protocols data between the two units. In a single-cable configuration, this is the port that carries traffic and L2 protocols data between the two units. In a two-cable configuration, this is the port to which the Protocols cable is connected.

To enter interface view, enter the following command in root view:

```
root>ethernet interfaces eth slot 1 port <port>
eth type eth [x/x]
```

If the Protocols port is the PTP 850E Management port, use the following command syntax:

```
root>ethernet interfaces mng slot 1 port 1
eth type mng [1/1]>
```

ii In interface view, enter the following command:

```
eth type eth|mng [x/x]>pdu-encapsulation set yes
```

For example, if the configuration uses a separate Protocols cable, use the following commands to enable PDU encapsulation on Eth 2:

```
root>ethernet interfaces eth slot 1 port 2
eth type eth [1/2]>pdu-encapsulation set yes
```

To display the current PDU encapsulation setting, enter the following command in interface view:

```
eth type eth|mng [x/x]>pdu-encapsulation show
```

Note: The following step is unnecessary if the paired unit is a third-party device. Instead, you must configure OAM CCM to ensure that any traffic flow issues on the paired unit are reported to the main unit. See Procedure for Configuring Third-Party Devices for Operation in Link Bonding Configurations.

12 To ensure proper fault handling, configure Automatic State Propagation (ASP). For single-cable configurations, you must enable ASP Management Safe mode (CSF mode) to ensure that in-band management is not disrupted in case of a fault on one of the ports connecting the main and paired units. This includes configuring the peer unit to receive CSF PDUs.

i On the local and remote PTP 850E units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The Link Bonding group
- Controlled Port: The port connected to the external switch (Eth 3, Eth 4, Eth 5, or Eth 6).

ii On the local and remote paired units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The Multi-Carrier ABC group
- Controlled Port: The port carrying traffic between the two units

13 In-band management can be carried between the PTP 850E and the paired unit via the cable carrying L2 protocols data between the units. This can be the traffic cable or a separate Protocols cable.

To configure in-band management, you must enable in-band management on both units and define a management service that connects the port used for L2 protocols data (the Protocols port) on both units, the Link Bonding groups, and the ingress port of the PTP 850E:

i On the local PTP 850E, configure a service point on the port connected to the external switch (Eth 3, Eth 4, Eth 5, or Eth 6).

ii On the local PTP 850E, configure a service point on the Protocols port.
iii On the local PTP 850E, configure a service point on the Link Bonding group.
iv On the local paired unit, configure a service point on the Protocols port.
v On the remote paired unit, configure a service point on the Protocols port.
vi On the remote PTP 850E, configure a service point on the Protocols port.
vii On the remote PTP 850E, configure a service point on the Link Bonding group.

Note: The following three steps are unnecessary if the paired unit is a third-party device. Instead, you must configure OAM CCM to ensure that any traffic flow issues on the paired unit are reported to the main unit. See Procedure for Configuring Third-Party Devices for Operation in Link Bonding Configurations.

14 Configure Radio Bandwidth Notification on the PTP 850E by performing the following steps:

i Enter Link Bonding group view by entering the following command in root view:

```
root>ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

ii In group view, enter the following command to enter the view of the interface on the main unit transmitting traffic to the paired unit:

```
eth group [lbx]>ethernet link-bonding-member interface eth slot
1 port <port> vlan <1-4094|untag>
```

If the port is the PTP 850E Management port, use the following command syntax:

```
eth group [lbx]> ethernet link-bonding-member interface mng
slot 1 port 1 vlan <1-4094|untag>
```

iii In group member view, enter the following command to create the Radio Bandwidth Control entity.

- For single-cable configurations, the <port> parameter should be the same as the port transmitting traffic to the paired unit.
- For two-cable configurations, the <port> parameter should be the port on the main unit sending Protocols information to the paired unit.

```
lbg-member[eth|mngx/y]>bw-control add bw-ctrl-interface eth bw-
ctrl-slot 1 bw-ctrl-port <port> bw-ctrl-vlan <1-4094>bw-ctrl-port-
id
```

Note: The `bw-ctrl-vlan` parameter configures the VLAN used to transfer protocol information between the two units. You can use any available VLAN ID from 1 to 4090.

15 Configure Radio Bandwidth Notification on the paired unit by performing the following steps:

i Enter the following command in root view to create a Radio Bandwidth Notification entity:

```
root> ethernet abn abn-entity-create protocol-type-rbn abn-name
<name> monitored-group-on-slot enhanced-abc slot 1 group-id 1
vlan untag
```

Note: Once you configure the RBN entity, you cannot edit the name later. The only way to change the name is to delete and reconfigure the RBN entity.

To display information about the Radio Bandwidth Notification entity, enter the following command in root view:

```
root> ethernet abn abn-entity-show abn-name <name>
```

ii Enter the following command in root view to set the VLAN type to C-VLAN:

```
root> ethernet abn abn-vlan-type-set abn-name <name> vlan-type
c-vlan
```

iii Enter the following command in root view to set the VLAN ID:

- If the paired unit is an PTP 850C, select **the same VLAN you configured** for the main unit.
- If the paired unit is an PTP 820C or PTP 820C-HP, enter untagged.

```
root> ethernet abn abn-vlan-set abn-name <name> vlan <1-4094>
```

iv Enter the following command in root view to set the Admin status of the Radio Bandwidth Notification entity to Up:

```
root> ethernet abn abn-admin-set abn-name <name> admin up
```

16 On the paired units on both sides of the link, configure a point-to-point service for Radio Bandwidth Notification, with service points on the Multi-Carrier ABC group and on the interface connected to the main unit for L2 protocols data (the Protocols port). In single-cable configurations, this is the port used for the single traffic and protocols cable. In two-cable configurations, this is the port used for the Protocols cable.

The service points should be configured as follows:

- Create a service point on the paired unit' Multi-Carrier ABC group with the following parameters:
  - Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation:
    - If the paired unit is an PTP 850C, use the same VLAN you configured in the bw-ctrl-vlan parameter, in Step 14.
    - If the paired unit is an PTP 820C or PTP 820C-HP, use Untagged.

- Allow Flooding: Allow
- Learning Admin: Disable

- Create a service point on the paired unit's Protocols port with the following parameters:
  - Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation: use the same VLAN you configured in the bw-ctrl-vlan parameter, in Step 14.
  - Allow Flooding: Allow
  - Learning Admin: Disable

17 On the paired unit on both sides of the link, configure a point-to-point service for Link Bonding traffic, with service points on the radio or Multi-Carrier ABC group and on the interface connected to the main unit for traffic (the Traffic port).

The service points should be configured as follows:

i Create a service point on the Multi-Carrier ABC group with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation:
  - In configurations without Line Redundancy: Untagged
  - In configurations with Line Redundancy: Any VLAN
- Allow Flooding: Allow
- Learning Admin: Disable

ii Create a service point on the Traffic port with the following parameters:

- Type: SAP
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Untagged
- Allow Flooding: Allow
- Learning Admin: Disable

See Configuring Service Points (CLI).

For configurations with line redundancy, proceed to the instructions in Configuring Line Redundancy with Multiband and Link Bonding (CLI).

18.4.2 Configuring Line Redundancy with Multiband and Link Bonding (CLI)

For an overview of Line Redundancy with Multiband and Link Bonding, see Multiband with Layer 1 Link Bonding and Line Redundancy.

Before proceeding with the instructions below, perform the basic Link Bonding configurations described in Configuring Multiband with Layer 1 Link Bonding (CLI).

To configure Line Redundancy in a Multiband configuration with Link Bonding:

1. Verify that the port on the paired unit connected to the external switch is set to the same port speed as the port on the main unit connected to the external switch.
2. Make sure that QoS is configured on the paired unit the same as on the main unit. See Quality of Service (QoS) (CLI).
3. Enable and configure line protection on the main units on both sides of the link:

   i. Enter the following command in root view to select the interface connected to the external switch:

   ```
   root> platform management line-redundancy role set line
   interface eth slot 1 port 7
   ```

   To display the interface assigned as the role of line interface, that is, the interface connected to the external switch, enter the following command in root view:

   ```
   root> platform management line-redundancy role show line
   ```

   ii. Enter the following command in root view to configure the Link Bonding group as the radio interface:

   ```
   root> platform management line-redundancy role set radio group
   <lb1|lb2|lb3|lb4|lb5|lb6>
   ```

   To display the interface assigned as the role of radio interface, enter the following command in root view:

   ```
   root> platform management line-redundancy role show radio
   ```

   iii. Enter the following command in root view to select the interface connected to the paired unit:

   ```
   root> platform management line-redundancy role set data-share
   eth slot 1 port <3-7>
   ```

   To display the interface assigned as the role of data-share interface, that is, the interface commented to the paired unit, enter the following command in root view:

   ```
   root> platform management line-redundancy role show data-share
   ```

   iv. Enter the following command in root view to select the device as main unit:

   ```
   root> platform management line-redundancy set unit-role main
   ```

   Enter the following command in root view to display device's currently configured role:

   ```
   root> platform management line-redundancy show unit-role
   ```

   v. Enter the following command in root view to configure Revertive timer's WTR timer. When a failure condition is resolved after a switchover has taken place, the WTR timer is the time the system waits before restoring the system to its normal operational configuration. The default is 5 seconds.

```
root> platform management line-redundancy revertive-traffic set
wtr <0-84600
```

To display the WTR timer setting, enter the following command in root view:

```
root> platform management line-redundancy revertive-traffic show
wtr
```

vi Enter the following command in root view to enable line redundancy:

```
root> platform management line-redundancy set admin enable
```

To disable line redundancy, enter the following command:

```
root> platform management line-redundancy set admin disable
```

To display whether line redundancy is enabled, enter the following command:

```
root> platform management line-redundancy show admin
```

4 Enable and configure line protection on the paired units on both sides of the link:

i Enter the following command in root view to select the interface connected to the external switch:

```
root> platform management line-redundancy role set line
interface eth slot 1 port <3-4>
```

To display the interface assigned as the role of line interface, that is, the interface connected to the external switch, enter the following command in root view:

```
root> platform management line-redundancy role show line
```

ii Enter the following command in root view to configure the Multi-Carrier ABC group as the radio interface:

```
root> platform management line-redundancy role set radio group-
on-slot enhanced-abc 1 group-id <1-4>
```

To display the interface assigned as the role of radio interface, enter the following command in root view:

```
root> platform management line-redundancy role show radio
```

iii Enter the following command in root view to select the interface connected to the main unit:

```
root> platform management line-redundancy role set data-share
eth slot 1 port <3-4>
```

To display the interface assigned as the role of data-share interface, that is, the interface commented to the paired unit, enter the following command in root view:

```
root> platform management line-redundancy role show data-share
```

iv Enter the following command in root view to select the paired unit:

```
root> platform management line-redundancy set unit-role attach
```

Enter the following command in root view to display device's currently configured role:

```
root> platform management line-redundancy show unit-role
```

v Enter the following command in root view to configure Revertive timer's WTR timer. When a failure condition is resolved after a switchover has taken place, the WTR timer is the time the system waits before restoring the system to its normal operational configuration. The default is 5 seconds.

```
root> platform management line-redundancy revertive-traffic set
wtr <0-84600
```

To display the WTR timer setting, enter the following command in root view:

```
root> platform management line-redundancy revertive-traffic show
wtr
```

vi Enter the following command in root view to enable line redundancy:

```
root> platform management line-redundancy set admin enable
```

To disable line redundancy, enter the following command:

```
root> platform management line-redundancy set admin disable
```

To display whether line redundancy is enabled, enter the following command:

```
root> platform management line-redundancy show admin
```

5 On the paired unit on both sides of the link, create a point-to-point service for Link Bonding traffic, with service points on the port attached to the external switch and the Multi-Carrier ABC group or radio. Set the *service admin mode* of the service to operational.

Note: The Line Redundancy mechanism activates and deactivates these services based on the Line Redundancy operating state and role configurations, so they are not active during normal operation even though they are configured as operational. They are automatically activated in case of Line Redundancy switchover.

Both service points should be configured as follows:

- Type: PIPE
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Untagged
- Allow Flooding: Allow
- Learning Admin: Disable

6 For management, add service points on the management service on the following interfaces on the paired unit:

- The interface connected to the external switch.
- The Multi-Carrier ABC group.

7 If SyncE is configured on the link, add the interface on the paired unit connected to the external switch as a Sync Source, with priority 3. See Configuring an Ethernet Interface as a Synchronization Source (CLI).

To display the status of link redundancy, enter the following command in root view:

```
root> platform management line-redundancy show traffic state
```

Note: For an explanation of the Status parameters, see Line Redundancy with Multiband and Link Bonding – Status Parameters.

18.4.2.1 Line Redundancy with Link Bonding – Force-Switch and Lockout

To force the configuration to remain in its current state (lockout), enter the following command in root view. Lockout can be used to override Revertive mode and keep the configuration in switchover mode, should this be necessary.

```
root> platform management line-redundancy lockout set admin on
```

To end lockout, enter the following command in root view:

```
root> platform management line-redundancy lockout set admin off
```

To display the current lockout state, enter the following command in root view:

```
root> platform management line-redundancy lockout show admin
```

To force a switchover regardless of whether a failure state exists, enter the following command in root view:

```
root> platform management line-redundancy set force-switch
```

To prevent Revertive mode from operating to return the configuration to normal configuration, enter the lockout command described above after implementing the forced switchover.

18.4.3 Enabling Link Bonding Throughput Enhancement for Multiband with Layer 1 Link Bonding (CLI)

After configuring a Link Bonding node, it is recommended to enable Link Bonding Throughput Enhancement. Link Bonding Throughput Enhancement is available for both the main unit and the paired unit.

Note: In configurations with PTP 820N/PTP 820A, Link Bonding Throughput Enhancement can be used for the PTP 850C and PTP 850E as paired unit. For instructions, refer to the User Guide for PTP 820N and PTP 820A, System Release 12.1 and higher.

Link Bonding Throughput Enhancement can be enabled on the main unit's radio interface and/or on the attached unit's Multi-Carrier ABC group.

Link Bonding Throughput Enhancement affects the recommended L2 Header Compensation. Make sure to use the values listed in L1 and L2 Header Compensation Values.

The Link Bonding Throughput Enhancement and L2 Header Compensation settings must be the same for the main units on both sides of the link. Therefore, the changes should be applied in the following order to ensure that management is not lost:

Note: The settings on attached units do not affect management, and can be changed in any order.

1 Enable Link Bonding Throughput Enhancement on the remote unit (main and/or attached unit) by entering the following commands:

```
root> radio slot 1 port 1
radio [1/1]> lb-throughput-enhancement set admin enable
```

2 Enable Link Bonding Throughput Enhancement on the local unit (main and/or attached unit) by entering the following commands:

```
root> radio slot 1 port 1
radio [1/1]> lb-throughput-enhancement set admin enable
```

3 Modify the L2 Header Compensation on the remote unit (main and/or attached unit) by entering the following commands:

- For the main unit, enter the following commands to modify the L2 Header Compensation for the radio interface:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface radio
slot 1 port 1
lbg-member[radio1/1]> admin set disable
lbg-member[radio1/1]> l2-header-compensation edit l1-header-
compensation-enabled <yes|no> l2-header-compensation-value
<(-63)-63>
lbg-member[radio1/1]> admin set enable
```

To display the current parameter, enter the following command:

```
lbg-member[radio1/1]> l2-header-compensation show
```

- For the attached unit, enter the following commands to modify the L2 Header Compensation for the interface connected to the attached unit:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface eth
slot 1 port 4
lbg-member[eth4]>admin set disable
lbg-member[eth4]> l2-header-compensation edit l1-header-
compensation-enabled <yes|no> l2-header-compensation-value <(-
63)-63>
lbg-member[eth4]>admin set enable
```

To display the current parameter, enter the following command:

```
lbg-member[eth4]> l2-header-compensation show
```

Note: For recommended values, see L1 and L2 Header Compensation Values.

4 Modify the L2 Header Compensation on the local unit (main and/or attached unit) by entering the following commands:

- For the main unit, enter the following commands to modify the L2 Header Compensation for the radio interface:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface radio
slot 1 port 1
lbg-member[radio1/1]> admin set disable
lbg-member[radio1/1]> l2-header-compensation edit l1-header-
compensation-enabled <yes|no> l2-header-compensation-value
<(-63)-63>
lbg-member[radio1/1]> admin set enable
```

To display the current parameter, enter the following command:

```
lbg-member[radio1/1]> l2-header-compensation show
```

- For the attached unit, enter the following commands to modify the L2 Header Compensation for the interface connected to the attached unit:

```
root>ethernet interfaces group lb1
eth group [lb1]>
eth group [lb1]> ethernet link-bonding-member interface eth slot 1 port
4
lbg-member[eth4]>admin set disable
lbg-member[eth4]> l2-header-compensation edit l1-header-compensation-
enabled <yes|no> l2-header-compensation-value <(-63)-63>
lbg-member[eth4]>admin set enable
```

To display the current parameter, enter the following command:

```
lbg-member[eth4]> l2-header-compensation show
```

Note: For recommended values, see L1 and L2 Header Compensation Values.

18.4.4 Editing a Multiband Link Bonding Group or its Members (CLI)

To modify or display the parameters of the Link Bonding group, enter the following command to enter group view:

```
root>ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

To change the name of the Link Bonding group, enter the following command in group view:

```
eth group [lbx]> edit group-name <string>
```

To modify the attributes of a Link Bonding group member, you must first enter one of the following commands to enter the group member's view.

To enter the radio member's view, enter the following command in group view:

```
eth group [lbx]>ethernet link-bonding-member interface radio
slot 1 port 1
```

To enter the Ethernet member's view, enter the following command in group view:

```
eth group [lbx]>ethernet link-bonding-member interface eth
slot 1 port 7
```

To change the Admin Status of a group member, enter the following command in group member view:

```
lbg-member[radio/ethx/x]>admin set <enable|disable>
```

For example, to disable the radio interface in Link Bonding group 1, enter the following command in group view:

```
lbg-member[radio1/1]>admin set disable
```

To display the Admin Status of a group member, enter the following command in group member view:

```
lbg-member[radio/ethx/x]>admin state show
```

You can adjust the maximum shaper for either or both interfaces in the group. You should set this according to the maximum capacity of the radio interface, or

the maximum radio capacity of the paired connected to the Ethernet member. The default value is 30000 Mbps. To adjust this parameter, enter the following command in group member view:

```
lbg-member[ethx/y]>edit shaper-bit-rate <0-30000>
```

To display configuration of the group member, including its Admin Status and maximum shaper bit rate, enter the following command in group member view:

```
lbg-member[radio/ethx/x]> configuration show
```

To adjust the L1 Header Compensation, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l1-header-compensation edit l1-header-compensation-enabled <yes|no> l1-header-compensation-value <(-63)-63>
```

To adjust the L2 Header Compensation, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l2-header-compensation edit l1-header-compensation-enabled <yes|no> l2-header-compensation-value <(-63)-63>
```

Note: Before changing the `l2-header-compensation-enabled` parameter, the Admin status of the group member in the group must be set to `disable`. Otherwise, the change will have no effect. After changing the `l2-header-compensation-enabled` parameter, make sure to set the Admin status of the group member in the group back to `enable`.

For recommended values, see L1 and L2 Header Compensation Values.

To display the L1 Header Compression settings for the interface, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l1-header-compensation show
```

To display the L2 Header Compression settings for the interface, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l2-header-compensation show
```

18.4.5 Displaying Group Statistics for a Multiband Link Bonding Group (CLI)

Enter the group view by entering the following command in root view:

```
root>ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

To display the actual current traffic distribution between the main unit (the Multi-Carrier ABC group) and the paired unit (the Ethernet interface, enter the following command in group member view:

```
eth group [lb1]> lb-member status show all
```

For example:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

```
eth group [lb1]>lb-member status show all
Link Bonding members status Table:
```

```
-------------------------------------------------------------------------------
Member Location           VLAN ID    Group Location           Shaper actual bit rate
-------------------------------------------------------------------------------
Ethernet: Slot 1, Port 7  untagged   Link Bonding: Group #1   1898804
Radio: Slot 1, Port 1     untagged   Link Bonding: Group #1   9905046
```

To display statistics for overall traffic passing through the group, enter the following command in group member view:

```
eth group [lb1]> statistics show
```

For example:

```
eth group [lb1]>statistics show
         txPkts                          17304248327
         txOctets                        22885762312
         rxPkts                          0
         rxOctets                        0
         txUnicastPkts                   17304246993
         txMulticastPkts                 0
         txBroadcastPkts                 0
         txPkts64Octets                  0
         txPkts65to127Octets             0
         txPkts128to255Octets            17304248327
         txPkts256to511Octets            0
         txPkts512to1023Octets           0
         txPkts1024to1518Octets          0
         txPkts1519Octets                0
eth group [lb1]>
```

Note: The ability to clear member statistics is planned for future release.

You can also display and configure thresholds for throughput and utilization on both the group and the member levels. For further information, see Displaying Link Bonding PMs (CLI).

18.4.6 Deleting a Multiband Link Bonding Group (CLI)

To delete a Link Bonding group, you must first remove the members from the group:

1 Enter the group view by entering the following command in root view:

```
root>ethernet interfaces group lb<1-6>
```

2 Enter the following commands to remove the group members:

```
eth group [lb1]>lb-member delete interface radio slot 1 port 1
eth group [lb1]>lb-member delete interface eth slot 1 port 7
```

3 Exit group view.
4 Remove any service points on the Link Bonding group.
5 In root view, enter the following command to delete the group:

```
root>ethernet link-bonding delete group group_id <1-6>
```

18.5 Configuring XPIC (CLI)



Note

This section is only relevant for PTP 850C and PTP 850E.

For a general explanation of XPIC in PTP 850E, see XPIC Overview.

18.5.1 Configuring Layer 1 Link Bonding (Optional – PTP 850E Only) (CLI)

Note: You must configure the Link Bonding group *before* you configure the XPIC group.

To configure an XPIC node with Layer 1 Link Bonding:

1 Connect the external switch to the QSFP port (P4, Eth3) on the main unit. This port can be configured to operate in QSFP mode (40 Gbps) or SFP+ mode (10 Gbps).
2 In the Interface Manager, make sure the port used for passing traffic between the two units (Eth 7, P5) is set to **Admin** = **Down**.
3 Configure the speed of Eth 7 on both units to 10 Gbps.
4 Configure the speed of Eth 2 on both units to 2.5 Gbps.
5 Connect an optical cable between Eth 7 (P5) of each unit. This cable carries traffic between the two units.
6 Connect an optical cable between Eth 2 (P3) of each unit. This cable carries L2 protocol data between the two units.

Note: Special SFP+ modules must be used for both the inter-unit traffic ports (Eth 7/P5) and the Protocols ports (Eth 2/P3). For details and the marketing models of the required SFP+ modules, as well as the optical cables, see the Installation Guide for PTP 850E.

7 On the main unit only, configure a Link Bonding group that includes the radio interface and the Ethernet interface (Eth 7) connected to the paired unit:

Note: Before adding a group member, make sure that no shapers or service points are configured on the interface.

i Create the group by entering the following command in root view:

```
root> ethernet link-bonding create group group_id <1-6> group-
name <string>
```

Note: The `name` parameter is optional.

ii Enter the group view by entering the following command in root view:

```
root>ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

iii Add Eth 7 to the Link Bonding Group by entering the following command in group view. Eth 7 is the port connected to the PTP 850C.

```
eth group [lbx]> lb-member add interface eth slot 1 port 7
shaper-bit-rate <0-30000> vlan untag l1-header-compensation-
enabled no l1-header-compensation-value 20 l2-header-
compensation-enabled yes|no> l2-header-compensation-value 26
```

iv Add the radio interface to the Link Bonding Group by entering the following command in group view:

```
eth group [lbx]> lb-member add interface radio slot 1 port 1
shaper-bit-rate <0-30000> vlan untag l1-header-compensation-
enabled yes l1-header-compensation-value 20 l2-header-
compensation-enabled yes|no> l2-header-compensation-value 24
```

- The shaper-bit-rate parameter enables you to adjust the shaper for either or both interfaces in the group. This shaper controls the distribution of traffic between the main unit (the radio interface) and the paired unit (the Ethernet interface). Generally, there is no need to change this parameter from its default value of 30000 Mbps.
- The l1-header-compensation-enabled parameter should be set to no for the Ethernet member. For instructions on setting this parameter for the radio member.
- The l2-header-compensation-enabled parameter should be set to yes for both interfaces.
- The l2-header-compensation-value parameter should be set to their default values of 24 for the radio interface and 26 for the Ethernet interface.

8 In the Interface Manager, set the port connected to the paired unit for passing traffic between the two units to **Admin** = **Up**.

9 To ensure proper fault handling, configure Automatic State Propagation (ASP as follows:

i On the local and remote main units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The Link Bonding group
- Controlled Port: The port connected to the external switch (Eth 3).

ii On the local and remote paired units, configure ASP with **ASP trigger by remote fault** enabled, and the following settings:

- Monitored Port: The radio interface
- Controlled Port: The port connected to the main unit (Eth 7)

10 In-band management can be carried between the main unit and the paired unit via the Protocols cable that connects Eth 2 (P3) of each unit. To configure in-band management, you must enable in-band management on both units and define a management service that connects Eth 2 of both units, the Link Bonding groups, and the ingress port of the main unit:

i On the local main unit, configure a service point on the port connected to the external switch (Eth 3).
ii On the local main unit, configure a service point on Eth 2.
iii On the local main unit, configure a service point on the Link Bonding group.
iv On the local paired unit, configure a service point on Eth 2.
v On the remote paired unit, configure a service point on Eth 2.
vi On the remote main unit, configure a service point on Eth 2.
vii On the remote main unit, configure a service point on the Link Bonding group.

11 Configure Radio Bandwidth Notification on the main unit by performing the following steps:

i Enter Link Bonding group view by entering the following command in root view:

```
root>ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

ii In group view, enter the following command to enter the view of the interface on the main unit transmitting traffic to the paired unit:

```
eth group [lbx]>ethernet link-bonding-member interface eth slot
1 port <port> vlan <1-4094|untag>
```

iii In group member view, enter the following command to create the Radio Bandwidth Control entity. The <port> parameter should be the port on the main unit sending Protocols information to the paired unit.

```
lbg-member[ethx/y]>bw-control add bw-ctrl-interface eth bw-ctrl-
slot 1 bw-ctrl-port <port> bw-ctrl-vlan 4090 bw-ctrl-port-id
```

12 Configure Radio Bandwidth Notification on the paired unit by performing the following steps:

i Enter the following command in root view to create a Radio Bandwidth Notification entity:

```
root>ethernet abn abn-entity-create protocol-type-rbn abn-name
LB monitored-interface radio monitored-slot 1 monitored-port 1
vlan untag
```

To display information about the Radio Bandwidth Notification entity, enter the following command in root view:

```
root> ethernet abn abn-entity-show abn-name <name>
```

ii Enter the following command in root view to set the VLAN type to C-VLAN:

```
root> ethernet abn abn-vlan-type-set abn-name <name> vlan-type
c-vlan
```

iii Enter the following command in root view to set the VLAN ID to 4090:

```
root> ethernet abn abn-vlan-set abn-name <name> vlan 4090
```

iv Enter the following command in root view to set the Admin status of the Radio Bandwidth Notification entity to Up:

```
root> ethernet abn abn-admin-set abn-name <name> admin up
```

13 On the paired units on both sides of the link, configure a point-to-point service for Radio Bandwidth Notification, with service points on the radio interface and Eth 2. The service points should be configured as follows:

- Create a service point on the paired unit's radio interface with the following parameters:
  - Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation: 4090
  - Allow Flooding: Allow
  - Learning Admin: Disable
- Create a service point on Eth 2 of the paired unit with the following parameters:
  - Type: SAP
  - Attached Interface Type: dot1q
  - C-VLAN Encapsulation: 4090
  - Allow Flooding: Allow
  - Learning Admin: Disable

18.5.1.1 Configuring Synchronization in an XPIC Node with Layer 1 Link Bonding

SyncE and 1588 PTP can be used in XPIC nodes with Layer 1 Link Bonding. SyncE and 1588 PTP can be configured for both the main unit and the paired unit. Synchronization messages are passed between the units via the Protocols cable.

Configuring SyncE in an XPIC Node with Layer 1 Link Bonding

To configure SyncE on an XPIC node with Layer 1 Link Bonding:

- On the local main unit, configure the following:
  - Configure the port connected to the external switch (Eth 3) as a sync source with priority 1.
  - Configure the radio interface as a sync source with priority 2.
  - Configure Eth 2 as a sync source with priority 3.
- On the local paired unit, configure the following:
  - Configure Eth 2 as a sync source with priority 1.
  - Configure the radio interface as a sync source with priority 2.
- On the remote paired unit, configure the following:
  - Configure the radio interface as a sync source with priority 1.
  - Configure Eth 2 as a sync source with priority 2.
- On the remote main unit, configure the following:
  - Configure Eth 2 as a sync source with priority 1.
  - Configure the radio interface as a sync source with priority 2.
  - Configure the port connected to the external switch (Eth 3) as a sync source with priority 3.

All sync sources should be configured with Sync Interface Quality "Automatic".
For instructions on configuring SyncE.

Configuring 1588 PTP in an XPIC Node with Layer 1 Link Bonding

To use 1588 PTP on an XPIC node with Layer 1 Link Bonding, you must configure Boundary Clock on the main unit and Transparent Clock on all of the units, as described below. 1588 messages are generated by the Boundary Clock mechanism on the main unit and sent untagged to the paired unit via the Protocols cable. They receive VLAN tagging on the paired unit in order to separate them from user traffic.

Note: If the paired unit goes down, 1588 packets will not be transmitted to the other side of the link.

To configure 1588 PTP for the XPIC node with Layer 1 Link Bonding:

1. Configure SyncE following the instructions.
2. Enable 1588 PTP on each unit, including the main and paired units on both sides of the link, using the following command in each unit:

```
root> platform sync ptp set admin enable
```

3. On the main unit on both sides of the link, enable Boundary clock on:
    - The port connected to the external switch (Eth 3).
    - Eth 2.
4. On the paired unit on both sides of the link, enable Transparent Clock on the radio interface.
5. On the paired unit unit on both sides of the link, configure a point-to-point service with service points on the radio interface and Eth 2. The service points should be configured as follows:
    - Service point on the radio interface:
        - Service Point Type: SAP
        - Attached Interface Type: dot1q
        - C-VLAN Encapsulation: Per customer's choice
        - Allowing Flooding: Allow
        - Learning Admin: Disable
    - Service point on Eth 2:
        - Service Point Type: SAP
        - Attached Interface Type: dot1q
        - C-VLAN Encapsulation: Untagged
        - Allowing Flooding: Allow
        - Learning Admin: Disable

18.5.1.2 Editing a Link Bonding Group or its Members

To modify or display the parameters of the Link Bonding group, enter the following command to enter group view:

```
root>ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

To change the name of the Link Bonding group, enter the following command in group view:

```
eth group [lbx]> edit group-name <string>
```

To modify the attributes of a Link Bonding group member, you must first enter one of the following commands to enter the group member's view.

To enter the radio member's view, enter the following command in group view:

```
eth group [lbx]>ethernet link-bonding-member interface radio
slot 1 port 1
```

To enter the Ethernet member's view, enter the following command in group view:

```
eth group [lbx]>ethernet link-bonding-member interface eth
slot 1 port 7
```

To change the Admin Status of a group member, enter the following command in group member view:

```
lbg-member[radio/ethx/x]>admin set admin set <enable|disable>
```

For example, to disable the radio interface in Link Bonding group 1, enter the following command in group view:

```
lbg-member[radio1/1]>admin set admin set disable
```

To display the Admin Status of a group member, enter the following command in group member view:

```
lbg-member[radio/ethx/x]>admin state show
```

You can adjust the maximum shaper for either or both interfaces in the group. Generally, there is no need to change this parameter from its default value of 30000 Mbps. However, if you want to configure a different value in order to limit traffic distribution to either the main unit radio (the radio interface) or the paired unit (the Ethernet interface, through which traffic is sent to the paired unit), enter the following command in group member view:

```
lbg-member[ethx/y]>edit shaper-bit-rate <0-30000>
```

To display configuration of the group member, including its Admin Status and maximum shaper bit rate, enter the following command in group member view:

```
lbg-member[radio/ethx/x]> configuration show
```

In most cases, the `l1-header-compensation-enabled` parameter should be set to `no` for both interfaces. However, in some cases, it should be adjusted. See Step 11 in Configuring Layer 1 Link Bonding (Optional – PTP 850E Only).

If you did not set this parameter properly when configuring the group, or if you need to set it to a different value for any reason, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l1-header-compensation edit l1-header-
compensation-enabled <yes|no> l1-header-compensation-value <(-
63)-63>
```

The `l2-header-compensation-enabled` parameter should be set to `yes` for both interfaces in the group. The l2-header-compensation parameter should be set to its default value. If you did not set these parameters properly when configuring the group, or if you need to set them to a different value for any reason, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l2-header-compensation edit l1-header-
compensation-enabled <yes|no> l2-header-compensation-value <(-
63)-63>
```

Note: Before changing the `l2-header-compensation-enabled` parameter, the Admin status of the group member in the group must be set to `disable`. Otherwise, the change will have no effect. After changing the `l2-header-compensation-enabled` parameter, make sure to set the Admin status of the group member in the group back to `enable`.

To display the L1 Header Compression settings for the interface, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l1-header-compensation show
```

To display the L2 Header Compression settings for the interface, use the following command in group member view:

```
lbg-member[radio/ethx/x]> l2-header-compensation show
```

18.5.1.3 Displaying Group Statistics for a Link Bonding Group

Enter the group view by entering the following command in root view:

```
root>ethernet interfaces group lb<1-6>
```

For example, to enter group context for Link Bonding group 1, enter the following command:

To display the actual current traffic distribution between the main unit (the Multi-Carrier ABC group) and the paired unit (the Ethernet interface, enter the following command in group member view:

```
eth group [lb1]> lb-member status show all
```

For example:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

```
eth group [lb1]>lb-member status show all
Link Bonding members status Table:

--------------------------------------------------------------------------------
--------
Member Location           VLAN ID    Group Location           Shaper actual
bit rate
--------------------------------------------------------------------------------
--------
Ethernet: Slot 1, Port 7  untagged   Link Bonding: Group #1   1898804
Radio: Slot 1, Port 1     untagged   Link Bonding: Group #1   9905046
```

To display statistics for overall traffic passing through the group, enter the following command in group member view:

```
eth group [lb1]> statistics show
```

For example:

```
eth group [lb1]>statistics show
         txPkts                          17304248327
         txOctets                        22885762312
         rxPkts                          0
         rxOctets                        0
         txUnicastPkts                   17304246993
         txMulticastPkts                 0
         txBroadcastPkts                 0
         txPkts64Octets                  0
         txPkts65to127Octets             0
         txPkts128to255Octets            17304248327
         txPkts256to511Octets            0
         txPkts512to1023Octets           0
         txPkts1024to1518Octets          0
         txPkts1519Octets                0
eth group [lb1]>
```

Note: The ability to clear these statistics is planned for future release.

18.5.1.4 Deleting a Link Bonding Group

To delete a Link Bonding group, you must first remove the members from the group:

1 Enter the group view by entering the following command in root view:

```
root>ethernet interfaces group lb<1-6>
```

2 Enter the following commands to remove the group members:

```
eth group [lb1]>lb-member delete interface radio slot 1 port 1
eth group [lb1]>lb-member delete interface eth slot 1 port 7
```

3 Exit group view.
4 Remove any service points on the Link Bonding group.
5 In root view, enter the following command to delete the group:

```
root>ethernet link-bonding delete group group_id <1-6>
```

18.5.2 Configuring the Radio Carriers for XPIC (CLI)

For PTP 850C, you must create and enable a single AMCC (XPIC) group on both sides of the link. The group must include both carriers on the PTP 850C unit, with opposite polarizations.

For PTP 850E, you must create and enable an AMCC group on each PTP 850E. Each group must include that unit's radio carrier.

18.5.3 Configuring the Radio Carriers for XPIC an PTP 850C (CLI)

To configure the radio carriers for XPIC on an PTP 850C:

1 Configure the radio carrier in each unit on both ends of the link to the desired frequency channel. All radio carriers in the link must be configured to the same frequency channel.

2 Assign a script that supports XPIC to both radio carriers on both ends of the link. See Configuring the Radio (MRMC) Script(s) (CLI).

3 Create an AMCC (XPIC) group. To create an AMCC (XPIC) group, enter the following command:

```
root> amcc create group group_id 1
group_type xpic  group_sub_type external
```

The following should appear:

```
group_id 1, group_type xpic created
```

4 Attach the radio carrier to the AMCC (XPIC) group. To attach the radio carrier, enter the group view and attach the carrier using the following commands:

```
root>amcc group group_id 1 group_type xpic
xpic-group[1]>

xpic-group[1]>amcc attach slot 1 port 1 role <member-h|member-v>
```

The following should appear:

```
slot 1 port 1 role member h attached to group_id 1 group_type xpic
```

The **role** parameter can be `member-h` (Horizontal) or `member-v` (Vertical). Make sure the **role** you select matches the actual polarization of the PTP 850E unit, and that the **role** you configure in the paired unit is not the same as the role you configure here.

5 Enable the group. To enable the group, enter the following command in group view:

```
xpic-group[1]>set admin enable
```

The following should appear:

```
group_id 1 group_type xpic 'Admin Enabled'
```

Once you have configured XPIC on both units at both sides of the link, perform antenna alignment. For instructions, see Performing Antenna Alignment for XPIC.

18.5.4 Configuring the Radio Carriers for XPIC on an PTP 850E (CLI)

To configure the radio carriers for XPIC on an PTP 850E:

1 Configure the radio carrier in each unit on both ends of the link to the desired frequency channel. All radio carriers in the link must be configured to the same frequency channel.

2 Assign a script that supports XPIC to both radio carriers on both ends of the link. See *Configuring the Radio (MRMC) Script(s) (CLI)*.

3 Create an AMCC (XPIC) group. To create an AMCC (XPIC) group, enter the following command:

```
root> amcc create group group_id 1 group_type xpic
group_sub_type external
```

The following should appear:

```
group_id 1, group_type xpic created
```

4 Attach the radio carrier to the AMCC (XPIC) group. To attach the radio carrier, enter the group view and attach the carrier using the following commands:

```
root>amcc group group_id 1 group_type xpic
xpic-group[1]>

xpic-group[1]>amcc attach slot 1 port 1 role <member-h|member-v>
```

The following should appear:

```
slot 1 port 1 role member h attached to group_id 1 group_type xpic
```

The **role** parameter can be `member-h` (Horizontal) or `member-v` (Vertical). Make sure the **role** you select matches the actual polarization of the PTP 850E unit, and that the **role** you configure in the paired unit is not the same as the role you configure here.

5 Enable the group. To enable the group, enter the following command in group view:

```
xpic-group[1]>set admin enable
```

The following should appear:

```
group_id 1 group_type xpic 'Admin Enabled'
```

Once you have configured XPIC on both units at both sides of the link, perform antenna alignment. For instructions, see *Performing Antenna Alignment for XPIC*.

18.5.5 Deleting an AMCC (XPIC) Group

To delete an AMCC (XPIC) group:

1 Disable the group. To disable an AMCC (XPIC) group, enter the following command in group view:

```
xpic-group[1]>set admin disable
```

The following should appear:

```
group_id 1 group_type xpic 'Admin Disabled'
```

2 Remove the radio carrier from the group. To remove the radio carrier from the group, enter the following command in group view:

```
xpic-group[1]>amcc detach slot 1 port 1
```

The following should appear:

```
slot 1 port 1 detached from group_id 1 group_type xpic
```

3 1 Delete the group. To delete the group, enter the following command in root view:

```
root>amcc delete group group_id 1 group_type xpic
```

The following should appear:

```
group_id 1 group_type xpic deleted
```

18.5.6 Displaying XPIC Status (CLI)

To display basic information about an AMCC (XPIC) group, enter either of the following command in root view:

```
root>amcc show groups
```

If an XPIC group is configured on the unit, the following is displayed:

```
group_id 1 group_type xpic group_sub_type external
```

Alternatively, enter the following command in root view:

```
root>amcc show group_id 1 group_type xpic
```

If an XPIC group is configured on the unit, the following is displayed:

```
group_id 1 group_type xpic group_sub_type external
```

To display the Admin status of the XPIC group, enter the following command in group view:

```
xpic-group[1]>show admin
```

If the group is enabled, the following output is displayed:

```
group_id 1 group_type xpic 'Admin Enabled'
```

To display the role (polarization) assigned to the unit and the XPIC status of the unit, enter the following command in group view:

```
xpic-group[1]>show members
```

The following output indicates that the unit is assigned the Vertical role (v), and the status is normal:

```
slot 1 port 1 role member v state Idle
```

The following output indicates that the unit is assigned the Horizontal role (h), and the status is normal:

```
slot 1 port 1 role member h state Idle
```

To display the XPIC status of the unit, enter the following command in group view:

```
xpic-group[1]>show advanced-status
```

The following output indicates that the status is normal:

```
xpic state: IDLE
```

The following are the possible statuses:

- **IDLE** – XPIC is working properly.
- **INIT** – Indicates that the **Admin** state of the radio interface is **Down**. Go to the Interface Manager and set the **Admin** status of the radio interface to **Up**.

- **Configuration not supported** – Indicates that the MRMC script configured for the radio carrier does not support XPIC. See Configuring the Radio (MRMC) Script(s) (CLI).
- **Single Channel** – Indicates one of the following:
  - The Clock Sharing cable is not connected to one of the units, or is defective.
  - The XPIC cable is not connected to one of the units, or is defective.
  - One of the PTP 850E units in the XPIC pair is down.

If this status appears, make sure that both units are up and check that all the cables are properly connected.

18.6 Configuring Line Redundancy for Link Bonding Configurations (CLI)

For an overview of Line Redundancy with Multiband and Link Bonding, see Multiband with Layer 1 Link Bonding and Line Redundancy.

Before proceeding with the instructions below, perform the basic Link Bonding configurations.

To configure Line Redundancy in a configuration with Link Bonding:

1. Verify that the port on the attached unit connected to the external switch is set to the same port speed as the port on the main unit connected to the external switch.
2. Make sure that QoS is configured on the attached unit the same as on the main unit. See Quality of Service (QoS) (CLI).
3. Enable and configure line redundancy on the main units on both sides of the link:

   i. Enter the following command in root view to select the interface connected to the external switch:

   ```
   root> platform management line-redundancy role set line
   interface eth slot 1 port 7
   ```

   To display the interface assigned as the role of line interface, that is, the interface connected to the external switch, enter the following command in root view:

   ```
   root> platform management line-redundancy role show line
   ```

   ii. Enter the following command in root view to configure the Link Bonding group as the radio interface:

   ```
   root> platform management line-redundancy role set radio
   group <lb1|lb2|lb3|lb4|lb5|lb6>
   ```

   To display the interface assigned as the role of radio interface, enter the following command in root view:

   ```
   root> platform management line-redundancy role show radio
   ```

   iii. Enter the following command in root view to select the interface connected to the attached unit:

   ```
   root> platform management line-redundancy role set data-share
   eth slot 1 port <3-7>
   ```

   To display the interface assigned as the role of data-share interface, that is, the interface commented to the attached unit, enter the following command in root view:

```
root> platform management line-redundancy role show data-
share
```

iv If you want to configure external management redundancy, enter the following command in root view to select the management interface:

```
root> platform management line-redundancy role set management
mng slot 1 port 1
```

To display the external management redundancy configuration, enter the following command in root view:

```
root> platform management line-redundancy role show
management
```

v Enter the following command in root view to select the device as main unit:

```
root> platform management line-redundancy set unit-role main
```

Enter the following command in root view to display device's currently configured role:

```
root> platform management line-redundancy show unit-role
```

vi Enter the following command in root view to configure Revertive timer's WTR timer. When a failure condition is resolved after a switchover has taken place, the WTR timer is the time the system waits before restoring the system to its normal operational configuration. The default is 5 seconds.

```
root> platform management line-redundancy revertive-traffic
set wtr <0-84600
```

To display the WTR timer setting, enter the following command in root view:

```
root> platform management line-redundancy revertive-traffic
show wtr
```

Note: The Revertive timer only applies to traffic. Line redundancy for external management does not have a revertive timer.

vii Enter the following command in root view to enable line redundancy:

```
root> platform management line-redundancy set admin enable
```

To disable line redundancy, enter the following command:

```
root> platform management line-redundancy set admin disable
```

To display whether line redundancy is enabled, enter the following command:

```
root> platform management line-redundancy show admin
```

4 Enable and configure line redundancy on the attached units on both sides of the link:

i Enter the following command in root view to select the interface connected to the external switch:

```
root> platform management line-redundancy role set line
interface eth slot 1 port <3-4>
```

To display the interface assigned as the role of line interface, that is, the interface connected to the external switch, enter the following command in root view:

```
root> platform management line-redundancy role show line
```

ii Enter the following command in root view to configure the Multi-Carrier ABC group as the radio interface:

```
root> platform management line-redundancy role set radio
group-on-slot enhanced-abc 1 group-id <1-4>
```

To display the interface assigned as the role of radio interface, enter the following command in root view:

```
root> platform management line-redundancy role show radio
```

iii Enter the following command in root view to select the interface connected to the main unit:

```
root> platform management line-redundancy role set data-share
eth slot 1 port <3-4>
```

To display the interface assigned as the role of data-share interface, that is, the interface commented to the attached unit, enter the following command in root view:

```
root> platform management line-redundancy role show data-
share
```

iv If you want to configure external management redundancy, enter the following command in root view to select the management interface:

```
root> platform management line-redundancy role set management
mng slot 1 port 1
```

To display the external management redundancy configuration, enter the following command in root view:

```
root> platform management line-redundancy role show
management
```

v Enter the following command in root view to select the device as the attached unit:

```
root> platform management line-redundancy set unit-role
attach
```

Enter the following command in root view to display device's currently configured role:

```
root> platform management line-redundancy show unit-role
```

vi Enter the following command in root view to configure Revertive timer's WTR timer. When a failure condition is resolved after a switchover has taken place, the WTR timer is the time the system waits before restoring the system to its normal operational configuration. The default is 5 seconds.

```
root> platform management line-redundancy revertive-traffic
set wtr <0-84600
```

To display the WTR timer setting, enter the following command in root view:

```
root> platform management line-redundancy revertive-traffic
show wtr
```

vii Enter the following command in root view to enable line redundancy:

```
root> platform management line-redundancy set admin enable
```

To disable line redundancy, enter the following command:

```
root> platform management line-redundancy set admin disable
```

To display whether line redundancy is enabled, enter the following command:

```
root> platform management line-redundancy show admin
```

5 On the attached unit on both sides of the link, create a point-to-point service for Link Bonding traffic, with service points on the port attached to the external switch and the Multi-Carrier ABC group or radio. Set the *service admin mode* of the service to operational.

Note: The Line Redundancy mechanism activates and deactivates these services based on the Line Redundancy operating state and role configurations, so they are not active during normal operation even though they are configured as operational. They are automatically activated in case of Line Redundancy switchover.

Both service points should be configured as follows:

- Type: PIPE
- Attached Interface Type: dot1q
- C-VLAN Encapsulation: Untagged
- Allow Flooding: Allow
- Learning Admin: Disable

6 For management, add service points on the management service on the following interfaces on the attached unit:

- The interface connected to the external switch.
- The Multi-Carrier ABC group.

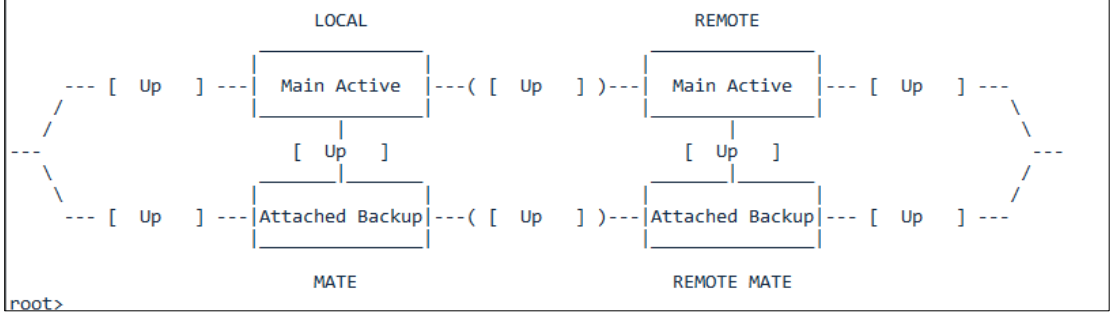
7 If SyncE is configured on the link, add the interface on the attached unit connected to the external switch as a Sync Source, with priority 3. See Configuring an Ethernet Interface as a Synchronization Source (CLI).

To display the status of link redundancy, enter the following command in root view:

```
root> platform management line-redundancy show traffic state
```

This command displays a graphical summary of the configuration's traffic state. For example:

```
root>platform management line-redundancy show traffic state
-------------------- Local Unit ----------------------
Local Line Traffic Interface:          Up
Local Radio Traffic Interface:         Up
Local Inter-Unit Interface:            Up
Local Unit State:                      Main Active
-------------------- Mate Unit -----------------------
Mate Line Traffic Interface:           Up
Mate Radio Traffic Interface:          Up
Mate Unit State:                       Attached Backup
-------------------- Remote Unit ---------------------
Remote Line Traffic Interface:         Up
Remote Inter-Unit Interface:           Up
Remote Unit State:                     Main Active
------------------ Remote Mate Unit --------------------
Remote Mate Line Traffic Interface:    Up
Remote Mate Unit State:                Attached Backup
```



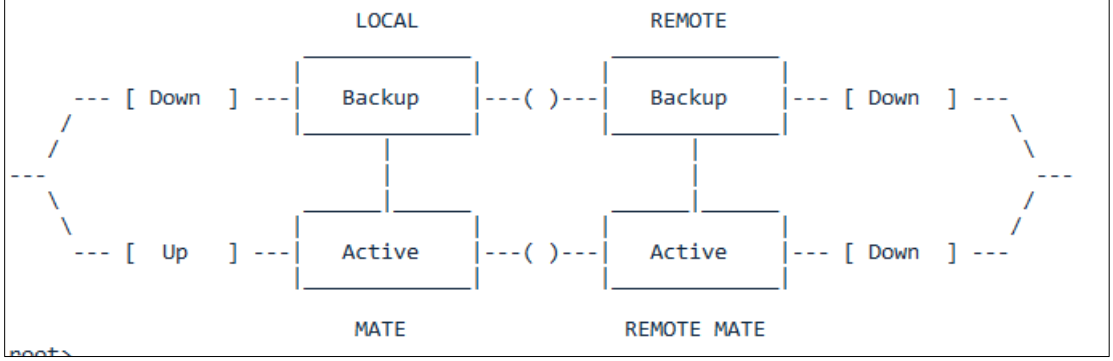

```
root>
```

If external management redundancy is enabled, enter the following command in root view to display the status of external management redundancy:

```
root> platform management line-redundancy show management state
```

This command displays a graphical summary of the configuration's management state. For example:

```
root>platform management line-redundancy show management state
---------------- Local Unit ------------------
Local Management Interface:             Down
Local Management State:          Backup
---------------- Mate Unit -------------------
Mate Management Interface:              Up
Mate Management State:           Active
---------------- Remote Unit -----------------
Remote Management Interface:            Down
Remote Management State:         Backup
------------- Remote Mate Unit --------------
Remote Mate Management Interface:               Down
Remote Mate Management State:    Active
```




```
root>
```

Note: For an explanation of the Status parameters, see Line Redundancy with Multiband and Link Bonding – Status Parameters.

18.6.1 Line Redundancy with Link Bonding – Force-Switch and Lockout (CLI)

To force the configuration to remain in its current state (lockout), enter the following command in root view. Lockout can be used to override Revertive mode and keep the configuration in switchover mode, should this be necessary.

```
root> platform management line-redundancy lockout set admin
on
```

To end lockout, enter the following command in root view:

```
root> platform management line-redundancy lockout set admin
off
```

To display the current lockout state, enter the following command in root view:

```
root> platform management line-redundancy lockout show admin
```

To force a switchover regardless of whether a failure state exists, enter the following command in root view:

```
root> platform management line-redundancy set force-switch
```

To prevent Revertive mode from operating to return the configuration to normal configuration, enter the lockout command described above after implementing the forced switchover.

The following commands are only relevant if you are using external management line redundancy. See Multiband with Layer 1 Link Bonding and Line Redundancy.

To force line redundancy for external management to remain in its current state (lockout), enter the following command in root view:

```
root>platform management line-redundancy lockout-mng set
admin <on|off> duration <60-3600>
```

The lockout remains in effect for the time configured in the duration parameter (in seconds). The default value is 600.

18.7 Configuring Unit Redundancy (CLI)

Note: This section is only relevant for PTP 850E.

This section includes:

- Configuring Ethernet Interface Protection (CLI)
- Configuring Unit Redundancy (CLI)
- Configuring Revertive Protection (CLI)
- Viewing the Configuration of the Standby Unit (CLI)
- Editing Standby Unit Settings (CLI)
- Viewing Link and Protection Status and Activity (CLI)
- Manually Switching to the Standby Unit (CLI)
- Disabling Automatic Switchover to the Standby Unit (CLI)
- Disabling Unit Redundancy (CLI)

For an overview of Unit Redundancy, see **Unit Redundancy Overview**.

To configure Unit Redundancy, you must perform the following steps:

1 Optionally, encrypt the external protection link using IPSec. See **Error! Reference source not found.**.
2 Configure Ethernet interface protection. See Configuring Ethernet Interface Protection (CLI).
3 Configure Unit Redundancy. See Configuring Unit Redundancy (CLI).
4 Optionally, you can configure revertive protection to ensure that the primary path is used whenever possible. See Configuring Revertive Protection (CLI).

18.7.1 Configuring Ethernet Interface Protection (CLI)

The Ethernet interfaces can be protected in either of two ways:

- **Split Protection Mode** – For Port 5 (SFP+, Eth 7), an optical splitter is used to route traffic to Port 5 on each PTP 850E unit. For Port 4 (QSFP, Eth 3-6), an optical splitter is used with MPO-MPO cables to route traffic to the QSFP splitter for each PTP 850E unit.

Note: For the QSFP port, Split Protection mode can only be used for 4x1/10Gbps configurations, not 1x40Gbps configurations. Support for Split Protection mode with 1x40Gbps is planned for future release.

- **Line Protection Mode** – Traffic is routed from two Ethernet ports on the external switch to a port on the active PTP 850E unit and a port on the standby PTP 850E unit. LACP protocol is used to determine which PTP 850E port is active and which port is standby, and traffic is only forwarded to the active port. Line Protection mode can be used with all PTP 850E Ethernet ports supported for traffic.

Notes: Line Protection mode is planned for future release.

For Line Protection mode, the external switch must support LACP.

18.7.1.1 Configuring Split Ethernet Interface Protection Mode (CLI)

To configure split Ethernet interface protection mode:

1 For each Ethernet link, use an optical splitter to route traffic between the Ethernet port on the external switch and an Ethernet port on each PTP 850E unit or each QSFP splitter.
2 Proceed to Configuring Unit Redundancy (CLI).

18.7.1.2 Configuring Line Protection Mode (CLI)

To configure line protection mode:

1 Configure the Ethernet ports on the external switch in LACP mode. The external switch must support LACP.

Note: PTP 850 supports a special LACP implementation for purposes of line protection only. This LACP implementation is configured on the logical interface level, as described below. Regular LACP is configured as part of the LAG configuration, and is not supported with unit redundancy. See Configuring Link Aggregation (LAG) and LACP (Optional) (CLI).

2 For each Ethernet link, connect one port on the external switch to an Ethernet port on the active PTP 850E (or QSFP splitter), and the other port on the external switch to an Ethernet port on the standby PTP 850E (or QSFP splitter).
3 Enable LACP on each Ethernet interface connected to the external switch on the active PTP 850E:

   i Go to interface view for the Ethernet interface connected to the external switch on the active PTP 850E.
   ii In interface view, enter the following command:

```
eth type eth [1/x]>interface-mode-set interface-mode LACP
```

To disable LACP mode, enter the following command in Ethernet interface view:

```
eth type eth [1/x]>interface-mode-set interface-mode NONE
```

To display an interface's current LACP setting, enter the following command in Ethernet interface view:

```
eth type eth [1/x]>interface-mode-show
```

18.7.2 Configuring Unit Redundancy (CLI)

To configure Unit Redundancy:

1 Optionally, encrypt the external protection link using IPSec. See Encrypting the External Protection Link (CLI).
2 Before enabling Unit Redundancy, you must:

   i Verify that both units have the same hardware part number (see Displaying Unit Inventory (CLI)) and the same software version (see Viewing Current Software Versions (CLI)). If the units do not have the same software version, upgrade each unit to the most recent software release (see Configuring a Software Download (CLI)).
   ii Assign an IP address to each unit. For instructions, see Changing the Management IP Address (CLI).
   iii Establish a management connection to one of the units. You can select either unit; once you enable Protection Administration, the system will determine which unit becomes the Active unit.

3 Before enabling Unit Redundancy, you must set the Management port to 100 Mbps and Auto Negotiation = Off. This should be done before connecting the management splitter cable (CBL-PTP 820-EXT-PROT+MGMT), since the cable will not work while the management port is set to its default settings of Auto Negotiation = On and Port Speed = 1000 Mbps.

   To configure the management port, enter the following commands:

```
root>platform management local-mngt autoneg state set off
port mng1

root>platform management local-mngt speed-and-duplex state
set 100fd port mng1
```

To display the current management port settings, enter the following command:

```
root>platform management local-mngt speed-and-duplex state
show port mng1
```

When you enable Unit Redundancy and perform copy-to-mate, these settings will be copied to the Standby unit.

Note that if at any time you disable Unit Redundancy and wish to change the settings of the management port, you should do so only after changing the management cable to a regular RJ-45 cable. The following is the full syntax for the management port setting commands:

```
root> platform management local-mngt autoneg state set
<off|on> port mng1

root> platform management local-mngt speed-and-duplex state
set <1000fd|100fd|100hd|10fd|10hd> port <all | mng1 | mng2>
```

4 To enable Unit Redundancy, enter the following command in root view:

```
root> platform management protection set admin enable
```

The system configures itself for Unit Redundancy:

- The system determines which unit is the Active unit based on a number of pre-defined criteria.
- When the system returns online, all management must be performed via the Active unit using the IP address you defined for that unit.
- The IP address you defined for the unit which is now the Standby unit is no longer valid, and the management port of the Standby unit becomes non-operational.
- Management of the Standby unit is performed via the Active unit, via the cable between the two Protection ports connecting the two units.
- Unit Redundancy is enabled on both units.

5 Once you have enabled Protection Admin:

i Perform all necessary radio configurations on the Active unit, such as setting the frequency, assigning MRMC scripts, and unmuting the radio.
ii Perform all necessary Ethernet configurations on the Active unit, such as defining Ethernet services.
iii Enter the following command in root view to copy the configuration of the Active unit to the Standby unit:

```
root> platform management protection copy-to-mate
```

Note: While the system is performing the copy-to-mate operation, a temporary loss of management connection will occur.

To keep the Standby unit up-to-date, after any change to the configuration of the Active unit enter the `copy-to-mate` command to copy the configuration to the Standby unit.

If you are unsure whether the Standby unit's configuration matches that of the Active unit, enter the following command in root view. The command output displays the list of mismatched parameters.

```
root> platform management protection show mismatch details
```

User profiles and user accounts are copied to the Standby unit dynamically, without the need to perform a Copy-to-Mate operation. This includes both new user profiles and user accounts and changes to existing user profiles and user accounts.

Note that it may take up to a minute for new user profile or user account and changes to existing user profiles and accounts to be copied to the Standby unit. Therefore, if an unexpected switchover takes place less than one minute after adding or modifying a user profile or account:

- Check that the user profile or account is configured in the new Active unit. If it is not, reconfigure the user profile or account and make sure at least one minute passes before another switchover occurs.
- If the user profile or account is configured in the new Active unit, check that you can successfully log into the unit with that user. If you cannot, delete the user profile or account and re-configure it in the new Active unit.

18.7.3 Configuring Revertive Protection (CLI)

To configure revertive mode, enter the following command in root view:

```
root> platform management protection revertive set admin
<enable|disable>
```

To set the active unit to be the primary unit, enter the following command in root view:

```
root> platform management protection revertive set primary
yes
```

If you set the active unit to be the primary unit, you must enter the following command in the standby unit:

```
root> platform management protection revertive set primary no
```

See Editing Standby Unit Settings (CLI).

Note: You can also set the standby unit to be the primary unit by entering the `primary yes` command in the standby unit and the `primary no` command in the active unit.

To configure the revertive mode wait-to-restore timer (in seconds), enter the following command in root view:

```
root> platform management protection revertive set wtr <10-
600>
```

To display the revertive mode settings, enter the following command in root view:

```
root> platform management protection revertive show
```

18.7.4 Viewing the Configuration of the Standby Unit (CLI)

You can view the settings of the standby unit any time.

To view the settings of the standby unit, you can run show commands in the standby unit. To do so, first enter the mate/root context, as described in Performing CLI operations on the Standby Unit (CLI), then run the relevant show command, and then switch back to the active unit.

18.7.5 Editing Standby Unit Settings (CLI)

Almost all settings of the standby unit are view-only. However, several settings are editable on the Standby unit. They must be configured separately for the Standby unit, and are not copied via copy-to-mate, nor do they trigger a configuration mismatch in the CLI.

In the Web EMS, failure to synchronize these configuration settings causes a configuration mismatch alarm.

The following settings must be configured separately on the standby unit:

- Revertive Mode – If Revertive Mode is enabled, you must set the platform management protection revertive set primary command in the standby unit to the opposite setting as the active unit. See Configuring Revertive Protection (CLI).
- Setting the Unit Name. See Configuring Unit Parameters (CLI).
- Disabling/enabling Radio TX-mute.
- Clearing the Radio and RMON counters. See Displaying General Modem Status and Defective Block PMs (CLI).
- Setting the activation key configuration. See Configuring the Activation Key (CLI) and Activating a Demo Activation Key (CLI).
- Defining user accounts. See Configuring User Accounts (CLI).
- Setting synchronization settings.

To configure these settings in the standby unit, first enter the mate/root context, as described in Performing CLI operations on the Standby Unit (CLI), then run the relevant commands, and then switch back to the active unit.

18.7.5.1 Performing CLI operations on the Standby Unit (CLI)

You can run CLI commands in the standby unit.

To run CLI commands in the standby unit:

1 Use the following command to enter view context for the standby unit:

```
root> switch-to mate

mate/root>
```

2 Enter the specific CLI command you want to run in mate/root context.
3 To switch back to the active unit, enter the following command:

```
mate/root> switch-back

root>
```

18.7.6 Viewing Link and Protection Status and Activity (CLI)

You can view link and protection status and activity any time.

- To view whether Unit Redundancy is enabled or disabled, enter the following command in root view:

```
root> platform management protection show admin
```

- To view whether Unit Redundancy is functional (available in practice), enter the following command in root view. Note that Unit Redundancy is not functional if MIMO is configured, or if the management connection to the mate is down.

```
root> platform management protection show operational-state
```

- To view protection activity, enter the following command in root view:

```
root> platform management protection show activity-state
```

- To view the status of the protection link to the mate, enter the following command in root view:

```
root> platform management protection show link-status
```

- To view the status of the last copy-to-mate operation, enter the following command in root view:

```
root> platform management protection show copy-to-mate status
```

18.7.7 Manually Switching to the Standby Unit (CLI)

At any point, you can manually switch to the Standby unit, provided that the highest protection fault level in the Standby unit is no higher than the highest protection fault level on the Active unit.

To manually switchover to the Standby unit enter the following in root view:

```
root> platform management protection set manual-switch
```

18.7.8 Disabling Automatic Switchover to the Standby Unit (CLI)

At any point, you can perform lockout, which disables automatic switchover to the standby unit.

To disable automatic switchover to the Standby unit, use the following command in root view:

```
root> platform management protection lockout set admin on
```

To re-enable automatic switchover to the standby unit, use the following command in root view:

```
root> platform management protection lockout set admin off
```

18.7.9 Disabling Unit Redundancy (CLI)

You can disable Unit Redundancy at any time. If you disable Unit Redundancy, on the active unit, the standby unit retains its IP address and remains in standby mode, with its radio muted. To restore the standby unit to normal operation as a standalone unit, reboot the unit. When the unit comes back up, it will no longer be in standby mode, and the radio will no longer be muted. The unit will retain all its other configuration parameters, including its IP address.

To disable Unit Redundancy, enter the following command in root view.

```
root> platform management protection set admin disable
```

18.8 Configuring Link Aggregation (LAG) and LACP (Optional) (CLI)

Link aggregation (LAG) enables you to group several physical Ethernet or radio interfaces into a single logical interface bound to a single MAC address. This logical interface is known as a LAG group. Traffic sent to the interfaces in a LAG group is distributed by means of a load balancing mechanism. PTP 850 uses a distribution function of up to Layer 4 in order to generate the most efficient distribution among the LAG physical ports.

This section explains how to configure LAG and includes the following topics:

- Configuring a LAG Group (CLI)
- Configuring LACP (CLI)
- Viewing LAG Details (CLI)
- Editing and Deleting a LAG Group (CLI)

- Enabling and Disabling the LAG Group Shutdown in Case of Degradation Event Option (CLI)
- Configuring Enhanced LAG Distribution (CLI)
- Displaying LACP Parameters and Statistics (CLI)

18.8.1 Configuring a LAG Group (CLI)

To create a LAG:

1. Go to interface view for the first interface you want to assign to the LAG and enter the following command:

```
eth type eth [x/x]> static-lag add lagid <lagid>
```

2. Repeat this process for each interface you want to assign to the LAG.
3. To enter interface view for a LAG, enter the following command in root view:

```
root> ethernet interfaces group <lag1|lag2|lag3|lag4>
```

18.8.2 Configuring LACP (CLI)

To enable LACP on a LAG group, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> lacp admin set enable
```

To disable LACP on a LAG group, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> lacp admin set disable
```

To display whether or not LACP is enabled on a LAG group, go to interface view for the LAG and enter the following command:

```
eth group [lagx]>lacp admin show
```

The following commands enable LACP for LAG group 1:

```
root> ethernet interfaces group lag1
eth group [lag1]>lacp admin set enable
eth group [lag1]>
```

18.8.3 Configuring Multi-Homing (CLI)

To enable Multi-Homing for ETH-BN and CSF messages on the LAG, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> static-lag set lag-multi-homing admin
enable
```

To disable Multi-Homing for ETH-BN and CSF messages on the LAG, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> static-lag set lag-multi-homing admin
disable
```

To display whether Multi-Homing for ETH-BN and CSF messages is enabled or disabled on the LAG, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> static-lag show lag-multi-homing-admin
```

18.8.4 Viewing LAG Details (CLI)

To display the name of a LAG to which an interface belongs, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> static-lag show name
```

To enter interface view for a LAG, enter the following command in root view:

```
root> ethernet interfaces group <lagid>
```

To display details about a LAG, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> summary show
```

To display a LAG's operational state, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> operational state show
```

To display a list of interfaces that belong to a LAG, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> port static-lag show members
```

18.8.5 Editing and Deleting a LAG Group (CLI)

Note: Before deleting a LAG group, make sure that all members of the LAG group are set to **Admin** = **Down**.

To remove a member Ethernet interface from a LAG, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> port static-lag remove member interface eth
slot <slot> port <port>
```

To remove a member radio interface from a LAG, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> port static-lag remove member interface
radio slot <slot> port <port>
```

To delete a LAG, go to interface view for the LAG and simply remove all the members, as described above.

Table 105: LAG Group CLI Parameters

Parameter	Input Type	Permitted Values	
lagid	Variable	lag1 lag2 lag3 lag4	
slot	Number	Ethernet: 1 Radio: 1	
Port	Number	Ethernet interface on PTP 850C: 1-4	

Parameter	Input Type	Permitted Values	
		Ethernet interface on PTP 850E: 1-7 Radio interface on an PTP 850C: 1-2 Radio interface on an PTP 850E: 1Management: 1	

For PTP 850E, the following commands create a LAG with the ID lag1. The LAG includes Ethernet interfaces 3, 4, and 7 and the radio. Multi Homing for ETH-BN and CSF messages is enabled on the LAG.

```
root> platform if-manager set interface-type ethernet slot 1
port 3 admin down
root> ethernet interfaces eth slot 1 port 3
eth type eth [1/3]>
eth type eth [1/3]> static-lag add lagid lag1
eth type eth [1/3]> exit
root>
root> platform if-manager set interface-type ethernet slot 1
port 4 admin down
root> ethernet interfaces eth slot 1 port 4
eth type eth [1/4]>
eth type eth [1/4]> static-lag add lagid lag1
eth type eth [1/4]> exit
root> platform if-manager set interface-type ethernet slot 1
port 7 admin down
root> ethernet interfaces eth slot 1 port 7
eth type eth [1/7]>
eth type eth [1/7]> static-lag add lagid lag1
eth type eth [1/7]> exit
root> ethernet interfaces radio slot 1 port 1
eth type radio[1/1]>
eth type radio[1/1]> static-lag add lagid lag1
eth type radio[1/1]> exit
root> platform if-manager set interface-type ethernet slot 1
port 3 admin up
root> platform if-manager set interface-type ethernet slot 1
port 4 admin up
root> platform if-manager set interface-type ethernet slot 1
port 7 admin up
root> ethernet interfaces group lag1
eth group [lag1]>
eth group [lag1]> static-lag set lag-multi-homing admin
enable
eth group [lag1]> exit
root>
```

For PTP 850C, the following commands create a LAG with the ID lag1. The LAG includes Ethernet interfaces 3 and 4 and radio carrier 1. Multi Homing for ETH-BN and CSF messages is not enabled on the LAG.

```
root> platform if-manager set interface-type ethernet slot 1
port 3 admin down
root> ethernet interfaces eth slot 1 port 3
eth type eth [1/3]>
eth type eth [1/3]> static-lag add lagid lag1
eth type eth [1/3]> exit
root>
root> platform if-manager set interface-type ethernet slot 1
port 4 admin down
root> ethernet interfaces eth slot 1 port 4
eth type eth [1/4]>
eth type eth [1/4]> static-lag add lagid lag1
eth type eth [1/4]> exit
root> ethernet interfaces radio slot 1 port 1
eth type radio[1/1]>
eth type radio[1/1]> static-lag add lagid lag1
eth type radio[1/1]> exit
root> platform if-manager set interface-type ethernet slot 1
port 3 admin up
root> platform if-manager set interface-type ethernet slot 1
port 4 admin up
```

The following command displays the name of the LAG to which Ethernet port 1 belongs:

```
eth type eth [1/1]> static-lag show name

Static-lag group name: lag2
```

The following commands display details about the LAG:

```
root> ethernet interfaces group lag2

eth group [lag2]>

eth group [lag2]> port static-lag show members

Static-lag members

-------------------

Eth#[1/1]
Eth#[1/2]
Radio#[2/1]

eth group [lag2]> summary show

Group lag2 Summary:    Value
Port Description:
Port Admin state:     enable
Port Operational state:  down
Port Edge state:     non-edge-port
Member Port#(1)      1/1
Member Port#(2)      1/2
Member Port#(3)      1/1

eth group [lag2]> operational state show

Port operational state: up.
```

```
eth group [lag2]>
```

The following commands remove port 2 on slot 1 from the LAG:

```
root> platform if-manager set interface-type ethernet slot 1
port 2 admin down

root> ethernet interfaces group lag2

eth group [lag2]>

eth group [lag2]> port static-lag remove member interface eth
slot 1 port 2
```

18.8.6 Enabling and Disabling the LAG Group Shutdown in Case of Degradation Event Option (CLI)

Note: LAG Group Shutdown in Case of Degradation Event cannot be used with LACP.

A LAG group can be configured to be automatically closed in the event of LAG degradation. This option is used if you want traffic from the switch to be re-routed during such time as the link is providing less than a certain capacity.

By default, the LAG group shutdown in case of degradation event option is disabled. When enabled, the LAG is automatically closed in the event that any one or more ports in the LAG fail. When all ports in the LAG are again operational, the LAG is automatically re-opened.

Note: Failure of a port in the LAG also triggers a lag-degraded alarm, Alarm ID 100.

To enable the LAG group shutdown in case of degradation event option, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> static-lag set lag-degrade-admin admin
enable
```

To disable the LAG group shutdown in case of degradation event option , go to interface view for the LAG and enter the following command:

```
eth group [lagx]> static-lag set lag-degrade-admin admin
disable
```

To display the current LAG group shutdown in case of degradation event option setting, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> static-lag show lag-degrade-admin
```

The following commands enable the LAG group shutdown in case of degradation event option for LAG group 1:

```
root> ethernet interfaces group lag1
eth group [lag1]>static-lag set lag-degrade-admin admin
enable
eth group [lag1]>
```

18.8.7 Configuring Enhanced LAG Distribution (CLI)

You can change the distribution function by selecting from ten pre-defined LAG distribution schemes. The feature includes a display of the TX throughput for each interface in the LAG, to help you identify the best LAG distribution scheme for the specific link.

Note: Enhanced LAG distribution is only available for LAG groups that consist of exactly two interfaces. It cannot be used with LACP. It is not user-configurable for PTP 850C and PTP 850E.

To configure enhanced LAG distribution, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> static-lag set df-pattern df <1-10>
```

The following commands set the LAG distribution scheme for LAG group 1 as distribution pattern 3.

```
root> ethernet interfaces group lag1
eth group [lag1]>static-lag set df-pattern df 3
```

The default LAG distribution pattern is 1.

To display the current LAG distribution scheme, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> static-lag show df-pattern
```

It is recommended to experiment with the various schemes by monitoring the TX port PMs for each interface in the LAG for each LAG distribution scheme. In the Web EMS, the page in which you configure enhanced LAG distribution also displays TX throughput PMs per interface. For information on monitoring Ethernet port PMs via the CLI, see Displaying Ethernet Port PMs (CLI).

18.8.8 Displaying LACP Parameters and Statistics (CLI)

You can display the following LACP parameters and statistics:

- LACP Aggregation (per LAG)
- LACP Port Status
- LACP Port Statistics
- LACP Port Debug Statistics

18.8.8.1 Displaying LACP Aggregation Status Parameters (CLI)

To display LACP aggregation status parameters, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> lacp show status
```

```
root> ethernet interfaces group lag1
eth group [lag1]>lacp show status
=============================================
|   LACP LAG Configuration                  |
=============================================
Admin key :                         0
System ID :                         0:0:0:0:0:0
System Priority :                   0
Aggregate or Individual :           0
Actor Oper Key:                     0
Agg MAC address :                   0:0:0:0:0:0
Partner System ID :                 0:0:0:0:0:0
Partner System Priority :           0
Partner Oper Key :                  0
Collector Max Delay :               0
eth group [lag1]>
```

Table 106 describes the LACP aggregation status parameters.

Table 106: LACP Aggregation Status Parameters (CLI)

Parameter	Definition
Admin Key	The current administrative value of the key for the Aggregator.
System ID	The MAC address value used as a unique identifier for the system that contains this Aggregator.
System Priority	The priority value associated with the Actor's System ID.
Aggregate or Individual	Indicates whether the Aggregator represents an aggregate or an individual link.
Actor Oper Key	The current operational value of the Key for the Aggregator.
Agg MAC Address	The individual MAC address assigned to the Aggregator.
Partner System ID	The MAC address value consisting of the unique identifier for the current protocol Partner of this Aggregator.
Partner System Priority	The priority value associated with the Partner's System ID.
Partner Oper Key	The current operational value of the Key for the Aggregator's current Protocol partner.

Parameter	Definition
Collector Max Delay	The maximum delay, in tens of microseconds.

18.8.8.2 Displaying LACP Port Status Parameters (CLI)

To display LACP port status parameters, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> lacp show ports status
```

```
root> ethernet interfaces group lag1
eth group [lag1]>lacp show ports status
=========================================
|   LACP LAG Ports Configuration          |
=========================================

-----------------------------------------
        Ethernet: Slot 1, Port 1
-----------------------------------------

Port :            11                    Partner Oper Port :            0
System Priority : 32768                 Partner Oper System Priority : 0
Admin Key :       1                     Partner Oper Key :             0
System ID :       0:a:25:40:1f:8c       Partner Oper System ID :       0:0:0:0:0:0
Port Priority :   32768                 Partner Oper Port Priority :   0

Actor State :   Active+Aggregatable+Defaulted
Partner State : None
Last RX Time:   0 seconds
Age:             382 seconds
RX State :      Defaulted
MUX State :     Detached
MUX reason:   Selected = False

-----------------------------------------
        Ethernet: Slot 1, Port 2
-----------------------------------------

Port :            12                    Partner Oper Port :            0
System Priority : 32768                 Partner Oper System Priority : 0
Admin Key :       1                     Partner Oper Key :             0
System ID :       0:a:25:40:1f:8c       Partner Oper System ID :       0:0:0:0:0:0
Port Priority :   32768                 Partner Oper Port Priority :   0

Actor State :   Active+Aggregatable+Defaulted
Partner State : None
Last RX Time:   0 seconds
Age:             382 seconds
RX State :      Defaulted
MUX State :     Detached
MUX reason:   Selected = False
eth group [lag1]>
```

Table 107: LACP Port Status Parameters (CLI)

Parameter	Definition
System Priority	The priority value associated with the Actor's System ID.
Admin Key	The current administrative value of the Key for the Aggregation Port.

Parameter	Definition
System ID	The MAC Address value that defines the value of the System ID for the system that contains this Aggregation Port.
Port Priority	The priority value assigned to this Aggregation Port.
Actor State	The current operational values of the Actor's state as transmitted by the Actor via LACPDUs.
Partner State	The current values of Actor State in the most recently received LACPDU transmitted by the protocol Partner.
Last RX Time	The value of a TimeSinceSystemReset (F.2.1) when the last LACPDU was received by this Aggregation port.
RX State	The state of the receive state machine for the Aggregation port. Possible values are: • Current – An LACPDU was received before expiration of the most recent timeout period. • Expired – No LACPDU was received before expiration of the most recent timeout period. • Defaulted – No LACPDU was received during the two most recent timeout periods.
Mux State	The state of the Mux state machine for the Aggregation port. Possible values are Collecting, Distributing, Attached, and Detached.
Mux Reason	A text string indicating the reason for the most reason change in the state of the Mux machine.
Partner Oper Port	The operational port number assigned to this Aggregation port by the Aggregation port's port Partner.
Partner Oper System Priority	The operational value of priority associated with the Partner's System ID.
Partner Oper Key	The current operational value of the Key for the protocol Partner.

Parameter	Definition
Partner Oper System ID	The MAC Address value representing the current value of the Aggregation Port's protocol Partner's System ID.
Partner Oper Port Priority	The Priority value assigned to this Aggregation port by the Partner.

18.8.8.3 Displaying LACP Port Statistics (CLI)

To display LACP port statistics, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> lacp show ports statistics
```

```
eth group [lag1]>lacp show ports statistics
==========================================
|   LACP LAG Ports Statistics            |
==========================================

------------------------------------------
        Ethernet: Slot 1, Port 1
------------------------------------------
LACPDU Rx : 0
LACPDU Tx : 192
Illegal Rx: 0
Unknown Rx: 0

------------------------------------------
        Ethernet: Slot 1, Port 2
------------------------------------------
LACPDU Rx : 0
LACPDU Tx : 58
Illegal Rx: 0
Unknown Rx: 0
eth group [lag1]>
```

Table 108 describes the LACP port statistics.

Table 108: LACP Port Statistics (CLI)

Parameter	Definition
LACPDU RX	The number of LACPDUs that this port has received.
LACPDU TX	The number of LACPDUs that this port has transmitted.
Illegal RX	The number of illegal protocol frames that this port has received.
Unknown RX	The number of unknown protocol frames that this port has received.

19. Unit Management (CLI)

This section includes:

- Defining the IP Protocol Version for Initiating Communications (CLI)
- Configuring the Remote Unit's IP Address (CLI)
- Configuring SNMP (CLI)
- Configuring the Internal Ports for FTP or SFTP (CLI)
- Upgrading the Software (CLI)
- Backing Up and Restoring Configurations (CLI)
- Setting the Unit to the Factory Default Configuration (CLI)
- Performing a Unit Reset (CLI)
- Configuring Unit Parameters (CLI)
- Configuring NTP (CLI)
- Displaying Unit Inventory (CLI)
- Displaying SFP DDM and Inventory Information (CLI)

Related topics:

- Setting the Time and Date (Optional) (CLI)
- Uploading Unit Info (CLI)
- Changing the Management IP Address (CLI)

19.1 Defining the IP Protocol Version for Initiating Communications (CLI)

You can specify which IP protocol the unit will use when initiating communications, such as downloading software, sending traps, pinging, or exporting configurations. The options are IPv4 or IPv6.

To define which IP protocol the unit will use when initiating communications, enter the following command in root view:

```
root> platform management ip set ip-address-family
<ipv4|ipv6>
```

To show the IP protocol version the unit will use when initiating communications, enter the following command in root view:

```
root> platform management ip show ip-address-family
```

19.2 Configuring the Remote Unit's IP Address (CLI)

You can configure the remote unit's IP address, subnet mask and default gateway in IPv4 format and/or in IPv6 format. The remote unit will receive communications whether they were sent to its IPv4 address or its IPv6 address.



Note

Release 10.6 does not support the ability to configure the remote IP address.

19.2.1 Configuring the Remote Radio's IP Address in IPv4 format (CLI)

To set the remote radio's IP Address, enter the following command in radio view:

```
radio[x/x]>remote-unit set ip-address <ipv4-address>
```

To display the remote radio's IP Address, enter the following command in radio view:

```
radio[x/x]>remote-unit show ip-address
```

To set the remote radio's subnet mask, enter the following command in radio view:

```
radio[x/x]>remote-unit set subnet-mask IP <subnet-mask>
```

To display the remote radio's subnet mask, enter the following command in radio view:

```
radio[x/x]>remote-unit show subnet-mask
```

To set the remote radio's default gateway, enter the following command in radio view:

```
radio[x/x]>remote-unit set default-gateway IP <ipv4-address>
```

To display the remote radio's default gateway, enter the following command in radio view:

```
radio[x/x]>remote-unit show default-gateway
```

Table 109 Remote Unit IP Address (IPv4) CLI Parameters

Parameter	Input Type	Permitted Values	Description
ipv4-address	Dotted decimal format.	Any valid IPv4 address.	Sets the default gateway or IP address of the remote radio.
subnet-mask	Dotted decimal format.	Any valid subnet mask.	Sets the subnet mask of the remote radio.

The following command sets the default gateway of the remote radio as 192.168.1.20:

```
radio[1/1]>remote-unit set default-gateway IP 192.168.1.20
```

The following commands set the IP address of the remote radio as 192.168.1.1, with a subnet mask of 255.255.255.255.

```
radio[1/1]>remote-unit set ip-address 192.168.1.1
radio[1/1]>remote-unit set subnet-mask IP 255.255.255.255
```

19.2.2 Configuring the Remote Radio's IP Address in IPv6 format (CLI)

To set the remote radio's IP Address, enter the following command in radio view:

```
radio[x/x]>remote-unit set ip-address-ipv6 <ipv6-address>
```

To display the remote radio's IP Address, enter the following command in radio view:

```
radio[x/x]>remote-unit show ip-address-ipv6
```

To set the remote radio's prefix length , enter the following command in radio view:

```
radio[x/x]>remote-unit set prefix-length <prefix-length >
```

To display the remote radio's prefix-length, enter the following command in radio view:

```
radio[x/x]>remote-unit show prefix-length
```

To set the remote radio's default gateway, enter the following command in radio view:

```
radio[x/x]>remote-unit set default-gateway-ipv6 IPv6 <ipv6-address>
```

To display the remote radio's default gateway, enter the following command in radio view:

```
radio[x/x]>remote-unit show default-gateway-ipv6
```

Table 110 Remote Unit IP Address (IPv6) CLI Parameters

Parameter	Input Type	Permitted Values	Description
ipv6-address	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	Sets the default gateway or IP address of the remote radio.
prefix-length	Number	1-128	Sets the prefix length of the remote radio. It should be different for each RADIUS client.

The following command sets the default gateway of the remote radio as The following command sets the default gateway of the remote radio as FE80:0000:0000:0000:0202:B3FF:FE1E:8329:

```
radio[1/1]>remote-unit set default-gateway-ipv6 IPv6
FE80:0000:0000:0000:0202:B3FF:FE1E:8329
```

The following commands set the IP address of the remote radio as FE80:0000:0000:0000:0202:B3FF:FE1E:8329, with a prefix length of 64:

```
radio[1/1]>remote-unit set ip-address-ipv6
FE80:0000:0000:0000:0202:B3FF:FE1E:8329
radio[1/1]>remote-unit set prefix-length 64
```

19.3 Configuring SNMP (CLI)

PTP 850 supports SNMP v1, V2c, and v3. You can set community strings for access to PTP 850 units.

PTP 850Eupports the following MIBs:

- RFC-1213 (MIB II).
- RMON MIB.
- Proprietary MIB.

Access to the unit is provided by making use of the community and context fields in SNMPv1 and SNMPv2c/SNMPv3, respectively.

This section includes:

- Configuring Basic SNMP Settings (CLI)
- Configuring SNMPv3 (CLI)
- Displaying the SNMP Settings (CLI)
- Configuring Trap Managers (CLI)

19.3.1 Configuring Basic SNMP Settings (CLI)

By default, SNMP is enabled with SNMPv3, and SNMPv1 and SNMPv2 are blocked. The following commands enable you to change these settings and configure the other SNMP parameters.

To enable SNMP, enter the following command in root view:

```
root> platform security protocols-control snmp admin set
<admin>
```

To specify the SNMP version, enter the following command in root view:

```
root> platform security protocols-control snmp version set
<version>
```

To specify the SNMP read and write communities, enter the following command in root view:

```
root> platform security protocols-control snmpv1v2 set read-
community <read-community> write-community <write-community>
```

Table 111 Basic SNMP CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin	Variable	enable disable	Select **enable** to enable SNMP monitoring, or **disable** to disable SNMP monitoring.
version	Variable	v1 v2 v3	Specifies the SNMP version.

Parameter	Input Type	Permitted Values	Description
ead-community	Text String	Any valid SNMP read community.	The community string for the SNMP read community.
write-community	Text String	Any valid SNMP write community.	The community string for the SNMP write community.
set-block	Variable	yes no	yes – SNMPv1 and SNMPv2 access is blocked. no – SNMPv1 and SNMPv2 access is not blocked.

The following commands enable SNMP v2 on the unit, and set the read community to "public" and the write community to "private":

```
root> platform security protocols-control snmp admin set
enable

root> platform security protocols-control snmp version set v2

root> platform security protocols-control snmpv1v2 set read-
community public write-community private
```

19.3.2 Configuring SNMPv3 (CLI)

The following commands are relevant for SNMPv3.

To block SNMPv1 and SNMPv2 access so that only SNMPv3 access will be enabled, enter the following command in root view:

```
root> platform security protocols-control snmp v1v2-block set
<set-block>
```

To add an SNMPv3 user, enter the following command in root view:

```
root> platform security protocols-control snmp v3-
authentication add v3-user-name <v3-user-name> v3-user-
password <v3-user-password> v3-security-mode <v3-security-
mode> v3-encryption-mode <v3-encryption-mode> v3-auth-
algorithm <v3-auth-algorithm> v3-access-mode <v3-access-mode>
```

To remove an SNMP v3 user, enter the following command in root view:

```
root> platform security protocols-control snmp v3-
authentication remove v3-user-name <v3-user-name>
```

To display all SNMP v3 users and their authentication parameters, enter the following command in root view:

```
root> platform security protocols-control snmp v3-
authentication show
```

Table 112 SNMPv3 CLI Parameters

Parameter	Input Type	Permitted Values	Description
v3-user-name	Text String		A SNMPv3 user name.

Parameter	Input Type	Permitted Values	Description
v3-user-password	Text String	Must be at least eight characters.	An SNMPv3 user password.
v3-security-mode	Variable	authNoPriv authPriv noAuthNoPriv	Defines the security mode to be used for this user.
v3-encryption-mode	Variable	Non DES AES	Defines the encryption (privacy) protocol to be used for this user.
v3-auth-algorithm	Variable	None SHA MD5	Defines the authentication algorithm to be used for this user.
v3-access-mode	Variable	readWrite readOnly	Defines the access permission level for this user.

The following commands enable SNMP v3 on the unit, block SNMP v1 and SNMP v2 access, and define an SNMPv3 user with User Name=Geno, Password=abcdefgh, security mode authPriv, encryption mode DES, authentication algorithm SHA, and read-write access:

```
root> platform security protocols-control snmp admin set enable
root> platform security protocols-control snmp version set v3
root> platform security protocols-control snmp v1v2-block set yes
root> platform security protocols-control snmp v3-authentication add v3-user-name geno v3-user-password abcdefgh v3-security-mode authPriv v3-encryption-mode DES v3-auth-algorithm SHA v3-access-mode readWrite
```

19.3.3 Displaying the SNMP Settings (CLI)

To display the general SNMP parameters, enter the following command in root view:

```
root> platform security protocols-control snmp show-all
```

To display all SNMP v3 users and their authentication parameters, enter the following command in root view:

```
root> platform security protocols-control snmp v3-authentication show
```

To display the current MIB version used in the system, enter the following command in root view:

```
root> platform security protocols-control snmp show-mib-version
```

To display details about the current MIB version used in the system, enter the following command in root view:

```
root> platform security protocols-control snmp show-mib-version-table
```

To display the SNMP read and write communities, enter the following command in root view:

```
root> platform security protocols-control snmpv1v2 show
```

19.3.4 Configuring Trap Managers (CLI)

To display the current SNMP trap manager settings, enter the following command in root view:

```
root> platform security protocols-control snmp trap-manager show
```

To modify the settings of an SNMP trap manger, enter the following command in root view:

```
root> platform security protocols-control snmp trap-manager set manager-id <manager-id> manager-admin <manager-admin> manager-ipv4 <manager-ipv4> manager-ipv6<manager-ipv6> manager-port <manager-port> manager-community <manager-community> manager-v3-user <manager-v3-user> manager-description <manager-description>
```

To enable an SNMP trap manger without modifying its parameters, enter the following command in root view:

```
root> platform security protocols-control snmp trap-manager admin manager-id <manager-id> manager-admin <manager-admin>
```

To specify the number of minutes between heartbeat traps, enter the following command in root view:

```
root> platform security protocols-control snmp trap-manager heartbeat manager-id <manager-id> manager-heartbeat <manager-heartbeat>
```

Table 113 Trap Managers CLI Parameters

Parameter	Input Type	Permitted Values	Description
manager-id	Number.	1 – 4	Enter the Manager ID of the trap manager you want to modify.
manager-admin	Variable.	enable disable	Enter **enable** or **disable** to enable or disable the trap manager.
manager-ipv4	Dotted decimal format.	Any valid IPv4 address.	If the IP protocol selected in platform management ip set ip-address-family is IPv4, enter the destination IPv4 address. Traps will be sent to this IP address.

Parameter	Input Type	Permitted Values	Description
manager-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	If the IP protocol selected in platform management ip set ip-address-family is IPv6, enter the destination IPv6 address. Traps will be sent to this IP address.
manager-port	Number.	70 – 65535	Enter the number of the port through which traps will be sent.
manager-community	Text String.	Any valid SNMP read community.	Enter the community string for the SNMP read community.
manager-v3-user	Text String.	The name of a V3 user defined in the system.	If the SNMP Trap version selected in platform security protocols-control snmp version set is V3, enter the name of a V3 user defined in the system. **Note**: Make sure that an identical V3 user is also defined on the manager's side
manager-description	Text String.		Enter a description of the trap manager (optional).
manager-heartbeat	Number.	0 – 1440	Specifies the number of minutes between heartbeat traps. If you enter 0, no heartbeat traps will be sent. **Note**: To reduce unnecessary traffic, heartbeat traps are only sent if no other trap was sent during the Heartbeat Period.

The following commands enable trap manager 2, and assign it IP address 192.168.1.250, port 164, and community “private”, with a heartbeat of 12 minutes.

```
root> platform security protocols-control snmp trap-manager
set manager-id 2 manager-admin enable manager-
ip 192.168.1.250 manager-port 164 manager-community private
manager-description text

root> platform security protocols-control snmp trap-manager
heartbeat manager-id 2 manager-heartbeat 12
```

19.4 Configuring the Internal Ports for FTP or SFTP (CLI)

By default, the following PTP 850 ports are used for FTP and SFTP when the PTP 850 unit is acting as an FTP or SFTP client (e.g., software downloads, configuration file backup and restore operations):

FTP – 21

SFTP – 22

To change the port for either protocol, enter the following command in root view:

```
root> platform management file-transfer port-config protocol
<ftp|sftp> port-number <0-65535>
```

To display the ports that are currently configured for FTP and SFTP, enter the following command in root view:

```
root> platform management file-transfer port-show
```

These ports are configured globally, rather than per specific operation.

The following sequence of commands displays the current (default) FTP and SFTP port settings, changes the FTP port to 125 and the SFTP port to 126, and shows the new FTP and SFTP port settings.

```
root>platform management file-transfer port-show

Port config table:
==================
File transfer   File transfer port

protocol        number
====================================
ftp             21
sftp            22

root> platform management file-transfer port-config protocol
ftp port-number 125

root> platform management file-transfer port-config protocol
sftp port-number 126

root>platform management file-transfer port-show

Port config table:
==================
File transfer   File transfer port

protocol        number
====================================

ftp             125
sftp            126

root>
```

19.5 Upgrading the Software (CLI)

PTP 850 software and firmware releases are provided in a single bundle that includes software and firmware for all components in the system. Software is first downloaded to the system, then installed. After installation, a reset is automatically performed on all components whose software was upgraded.

This section includes:

- Software Upgrade Overview (CLI)
- Viewing Current Software Versions (CLI)
- Configuring a Software Download (CLI)
- Downloading a Software Package (CLI)
- Installing and Upgrading Software (CLI)

19.5.1 Software Upgrade Overview (CLI)

The PTP 850 software installation process includes the following steps:

1. **Download** – The files required for the installation or upgrade are downloaded from a remote server.
2. **Installation** – The downloaded software and firmware files are installed in all modules and components of the PTP 850 that are currently running an older version.
3. **Reset** – The PTP 850 is restarted in order to boot the new software and firmware versions.

Software and firmware releases are provided in a single bundle that includes software and firmware for all components in the system. When you download a software bundle, the system verifies the validity of the bundle. The system also compares the files in the bundle to the files currently installed in the PTP 850 and its components, so that only files that need to be updated are actually downloaded. A message is displayed for each file that is actually downloaded.



Note

When downloading an older version, all files in the bundle may be downloaded, including files that are already installed.

Software bundles can be downloaded via HTTP, HTTPS, FTP or SFTP. After the software download is complete, you can initiate the installation.



Note

Before performing a software upgrade, it is important to verify that the system date and time are correct. See Setting the Time and Date (Optional) (CLI).

When upgrading a node with unit protection, upgrade the standby unit first, then the active unit.

19.5.2 Viewing Current Software Versions (CLI)

To display all current software versions, enter the following command in root view:

```
root> platform software show versions
```

19.5.3 Configuring a Software Download (CLI)

You can download software using HTTP, HTTPS, FTP, or SFTP.

When downloading software via HTTP or HTTPS, the PTP 850 functions as the server, and you can download the software directly to the PTP 850 unit.



Note

HTTP/HTTPS software download is only supported using the Web EMS. For instructions, see Downloading and Installing Software.

When downloading software, the IDU functions as an FTP or SFTP client. You must install FTP or SFTP server software on the PC or laptop you are using to perform the software upgrade. For details, see Installing and Configuring an FTP or SFTP Server.

To set the file transfer protocol you want to use (FTP or SFTP), enter the following command:

```
root> platform software download version protocol <ftp|sftp>
```

If the IP protocol selected in platform management ip set ip-address-family is IPv4, enter the following command:

```
root> platform software download channel server set server-ip
<server-ipv4> directory <directory> username <username>
password <password>
```

If the IP protocol selected in platform management ip set ip-address-family is IPv6, enter the following command:

```
root> platform software download channel server-ipv6 set
server-ip <server-ipv6> directory <directory> username
<username> password <password>
```

To display the software download channel configuration, enter one of the following commands:

```
root> platform software download channel server show
root> platform software download channel server-ipv6 show
```

Table 114 Software Download CLI Parameters

Parameter	Input Type	Permitted Values	Description
server-ipv4	Dotted decimal format.	Any valid IPv4 address.	The IPv4 address of the PC or laptop you are using as the FTP server.
server-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The IPv6 address of the PC or laptop you are using as the FTP server.

Parameter	Input Type	Permitted Values	Description
directory	Text String.		The directory path from which you are downloading the files. Enter the path relative to the FTP user's home directory, not the absolute path. To leave the path blank, enter //. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
server-username	Text String.		The user name you configured in the FTP server.
server-password	Text String.		The password you configured in the FTP server. If you did not configure a password for your FTP user, simply omit this parameter.

The following command configures a download from IP address 192.168.1.242, in the directory “current”, with user name “anonymous” and password “12345.”

```
root> platform software download channel server set server-
ip 192.168.1.242 directory \current username anonymous
password 12345
```

19.5.4 Downloading a Software Package (CLI)

To initiate a software download, enter the following command in root view:

```
root> platform software download version protocol ftp
```

The following prompt appears:

```
You are about to perform a software management operation.
This may cause a system reset.

Are you sure? (yes/no)
```

Enter `Yes` at the prompt. When the prompt appears again, enter the following command to check the download status:

```
root> platform software download status show
```

Once the following message appears, proceed with the installation:

```
DOWNLOAD VERSION status: download success, process
percentage: 100
```

If the software version on the FTP or SFTP server has already been downloaded to the unit, the following message appears:

```
DOWNLOAD VERSION status: all components exist, process
percentage: 0
```

19.5.5 Installing and Upgrading Software (CLI)

To install or upgrade the software, enter the following command in root view after downloading the software bundle:

```
root> platform software install version
```

If you wish to delay the start of installation, enter instead the following command. The time you enter in HH:MM format is the amount of time to delay until the start of the installation process:

```
root> platform software install version timer-countdown <hh:mm>
```

The following prompt appears:

```
Software version to be installed:

Are you sure? (yes/no)
```

To display the status of a software installation or upgrade, enter the following command:

```
root> platform software install status show
```

Important Notes:

DO NOT reboot the unit during software installation process. As soon as the process is successfully completed, the unit will reboot itself.

Sometimes the installation process can take up to 30 minutes.

Only in the event that software installation was not successfully finished and more than 30 minutes have passed can the unit be rebooted.

If you configured delayed installation, you can do any of the following:

Abort the current delayed installation. To do so, enter the following command:

```
root> platform software install abort-timer
```

Show the time left until the installation process begins. To do so, enter the following command:

```
root> platform software install time-to-install
```

Show the original timer as configured for a delayed installation. To do so, enter the following command:

```
root> platform software install show-time
```

19.6 Backing Up and Restoring Configurations (CLI)

You can import and export PTP 850 configuration files. This enables you to copy the system configuration to multiple PTP 850 units. You can also backup and save configuration files.

Configuration files can only be copied between units of the same type, i.e., PTP 850E to PTP 850E to PTP 850E.

Note that you can also write CLI scripts that will automatically execute a series of commands when the configuration file is restored. For information, refer to Editing CLI Scripts (CLI).

This section includes:

- Configuration Management Overview (CLI)

- Setting the Configuration Management Parameters (CLI)
- Backing up and Exporting a Configuration File (CLI)
- Importing and Restoring a Configuration File (CLI)
- Editing CLI Scripts (CLI)

19.6.1 Configuration Management Overview (CLI)

System configuration files consist of a zip file that contains three components:

A binary configuration file used by the system to restore the configuration.

A text file which enables users to examine the system configuration in a readable format. The file includes the value of all system parameters at the time of creation of the backup file.

An additional text file which enables you to write CLI scripts in order to make desired changes in the backed-up configuration. This file is executed by the system after restoring the configuration.

The system provides three restore points to manage different configuration files. Each restore point contains a single configuration file. Files can be added to the restore points by creating backups of the current system state or by importing them from an external server. For example, you may want to use one restore point to keep a last good configuration, another to import changes from an external server, and the third to store the current configuration.

You can apply a configuration file to the system from any of the restore points.

You must configure from 1 to 3 restore points:

When you import a configuration file, the file is saved to the selected restore point, and overwrites whichever file was previously held in that restore point.

When you export a configuration file, the file is exported from the selected restore point.

When you backup the current configuration, the backup configuration file is saved to the selected restore point, and overwrites whichever file was previously held in that restore point.

When you restore a configuration, the configuration file in the selected restore point is the file that is restored.

19.6.2 Setting the Configuration Management Parameters (CLI)

When importing and exporting configuration files, the PTP 850 functions as an FTP or SFTP client. You must install FTP or SFTP server software on the PC or laptop you are using to perform the import or export. For details, see Installing and Configuring an FTP or SFTP Server.



Note

Before importing or exporting a configuration file, you must verify that the system date and time are correct. See Setting the Time and Date (Optional) (CLI).

To set the FTP or SFTP parameters for configuration file import and export, enter one of the following commands in root view:

If the IP protocol selected in platform management ip set ip-address-family is IPv4, enter the following command:

```
root> platform configuration channel server set ip-
address <server-ipv4> directory <directory> filename <filename>
username <username> password <password>
```

If the IP protocol selected in platform management ip set ip-address-family is IPv6, enter the following command:

```
root> platform configuration channel server-ipv6 set ip-
address <server-ipv6> directory <directory> filename <filename>
username <username> password <password>
```

To set the file transfer protocol you want to use (FTP or SFTP), enter the following command:

```
root>platform configuration channel set protocol <ftp|sftp>
```

To display the FTP channel parameters for importing and exporting configuration files, enter one of the following commands in root view:

```
root> platform configuration channel server show

root> platform configuration channel server-ipv6 show
```

Table 115 Configuration Management CLI Parameters

Parameter	Input Type	Permitted Values	Description
server-ipv4	Dotted decimal format.	Any valid IPv4 address.	The IPv4 address of the PC or laptop you are using as the FTP server.
server-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The IPv6 address of the PC or laptop you are using as the FTP server.
directory	Text String.		The location of the file you are downloading or uploading. If the location is the root shared folder, it should be left empty. If the location is a sub-folder under the root shared folder, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".

Parameter	Input Type	Permitted Values	Description
filename	Text String.		The name of the file you are importing, or the name you want to give the file you are exporting. **Note**: You must add the suffix .zip to the file name. Otherwise, the file import may fail. You can export the file using any name, then add the suffix .zip manually.
username	Text String.		The user name you configured in the FTP server.
password	Text String.		The password you configured in the FTP server. If you did not configure a password for your FTP user, simply omit this parameter.

The following command configures the FTP channel for configuration file import and export to IP address 192.168.1.99, in the directory “current”, with file name “version_8_backup.zip”, user name “anonymous”, and password “12345.”

```
root> platform configuration channel server set server-ip
192.168.1.99 directory \current filename version_8_backup.zip
username anonymous password 12345
```

19.6.3 Backing up and Exporting a Configuration File (CLI)

To save the current configuration as a backup file to one of the restore points, enter the following command in root view:

```
root> platform configuration configuration-file add <restore-
point>
```

To export a configuration from a restore point to the external server location, enter the following command in root view:

```
root> platform configuration configuration-file export <restore-
point>
```

Table 116 Configuration Backup and Restore CLI Parameters

Parameter	Input Type	Permitted Values	Description
restore-point	Variable	restore-point-1 restore-point-2 restore-point-3	Identifies the restore point to or from which to perform the backup operation.

The following commands save the current configuration as a configuration at Restore Point 1, and export the file to the external server location:

```
root> platform configuration configuration-file add restore-point-1

root> platform configuration configuration-file export restore-point-1
```

19.6.4 Importing and Restoring a Configuration File (CLI)

You can import a configuration file from an external PC or laptop to one of the restore points. Once you have imported the file, you can restore the configuration. Restoring a saved configuration does not change the unit's FIPS mode.



Note

In order to import a configuration file, you must configure the FTP channel parameters and restore points, as described in Setting the Configuration Management Parameters and Backing up and Exporting a Configuration File.

To import a configuration file, enter the following command in root view:

```
root> platform configuration configuration-file import <restore-point>
```

To restore a configuration from a restore point to become the active configuration file, enter the following command in root view:

```
root> platform configuration configuration-file restore <restore-point>
```

Table 117 Configuration Import and Restore CLI Parameters

Parameter	Input Type	Permitted Values	Description
restore-point	Variable	restore-point-1 restore-point-2 restore-point-3	Identifies the restore point to or from which to perform the backup operation.

The following commands import a configuration file from an external PC or laptop to Restore Point 2 on the PTP 850, and restore the file to be the system configuration file for the PTP 850:

```
root> platform configuration configuration-file import restore-point-2

root> platform configuration configuration-file restore restore-point-2
```

19.6.5 Editing CLI Scripts (CLI)

The configuration file package includes a text file that enables you to write CLI scripts in a backed-up configuration that are executed after restoring the configuration.

To edit a CLI script:

1. Back up the current configuration to one of the restore points. See Backing up and Exporting a Configuration File (CLI).
2. Export the configuration from the restore point to a PC or laptop. See Backing up and Exporting a Configuration File (CLI).
3. On the PC or laptop, unzip the file *Configuration_files.zip*.
4. Edit *the cli_script.txt* file using clish commands, one per line.
5. Save and close the *cli_script.txt* file, and add it back into the *Configuration_files.zip* file.
6. Import the updated *Configuration_files.zip* file back into the unit. See Importing and Restoring a Configuration File (CLI).
7. Restore the imported configuration file. See Importing and Restoring a Configuration File (CLI). The unit is automatically reset. During initialization, the CLI script is executed, line by line.



Note

If any specific command in the CLI script requires reset, the unit is reset when that that command is executed. During initialization following the reset, execution of the CLI script continues from the following command.

19.7 Setting the Unit to the Factory Default Configuration (CLI)

To restore the unit to its factory default configuration, while retaining the unit's IP address settings and logs, enter the following commands in root view:

```
root> platform management set-to-default
```

The following prompt appears:

```
WARNING: All database and configuration will be lost, unit will be
restart.
Are you sure? (yes/no):yes
```

At the prompt, type `yes`.



Note

This does not change the unit's IP address or FIPS configuration.

19.8 Performing a Unit Reset (CLI)

You can reset the unit. You can also use a timer to schedule a unit reset at a later time.

To initiate an immediate reset on the unit, enter the following command in root view:

```
root> platform shelf-manager chassis reset
```

The following prompt appears:

```
You are about to reset the shelf
Are you sure? :(yes/no):
```

Enter `yes`. The unit is reset.

To configure a timed reset of the unit, in seconds, enter the following command in root view:

```
root> platform shelf-manager chassis reset-with-timeout timeout
set <2147483647>
```

To display the current status of the timer, enter the following command in root view:

```
root> platform shelf-manager chassis reset-with-timeout timeout
show
```

To cancel a timed reset, enter the following command in root view:

```
root> platform shelf-manager chassis reset-with-timeout timeout
set 0
```

19.9 Resetting the Remote Unit (CLI)

To initiate a reset on the remote unit, go to radio view and enter the following command:

```
radio [x/1]>remote-unit reset unit
```

The following prompt appears:

```
Are you sure you want to reset the remote unit
Are you sure? (yes/no):
```

Enter `yes`. The unit is reset.

You can also create a Unit Info file on the remote unit. This is useful in the event that management to the remote unit has been lost or the remote unit is not broadcasting but is still able to receive on the radio link. In these scenarios, the request to create a Unit Info file can be transmitted via the local-remote radio link, and the file can be retrieved later to help with troubleshooting.

To create a Unit Info file on the remote unit, go to radio view and enter the following command:

```
radio [x/1]>remote-unit create unit info
```

If you wish to reset the remote unit after creating the Unit Info file, make sure to wait about one minute after performing this command in order to provide time for the Unit Info file to be created on the remote unit. Then, you can perform the reset command described above, and retrieve the Unit Info file from the remote unit after management has been restored.

19.10 Configuring Unit Parameters (CLI)

You can view and configure system information:

To configure a name for the unit, enter the following command in root view:

```
root> platform management system-name set name <name>
```

To define a location for the unit, enter the following command in root view:

```
root> platform management system-location set name <name>
```

To define a contact person for questions pertaining to the unit, enter the following command in root view:

```
root> platform management system-contact set name <name>
```

To define the unit's latitude coordinates, enter the following command in root view:

```
root> platform management system-latitude set <latitude>
```

To define the unit's longitude coordinates, enter the following command in root view:

```
root> platform management system-longitude set <longitude>
```

To define the type of measurement unit you want the system to use, enter the following command in root view:

```
root> platform management set unit_measure_format
<unit_measure_format>
```

To display the type of measurement unit used by the system, enter the following command in root view:

```
root> platform management show unit_measure_format
```

Table 118 Unit Parameters CLI Parameters

Parameter	Input Type	Permitted Values	Description
name	Text	Up to 64 characters.	Defines the name of the unit.
latitude	Text	Up to 256 characters.	Defines the latitude coordinates of the unit.
longitude	Text	Up to 256 characters.	Defines the longitude coordinates of the unit.
unit_measure_format	Variable	metric imperial	Defines the measurement units of the unit.

The following commands configure a name, location, contact person, latitude coordinates, longitude coordinates, and units of measurements for the PTP 850:

```
root> platform management system-name set name "My-System-Name"
root> platform management system-location set name "My-System-
Location"
root> platform management system-contact set name "John Doe"
root> platform management system-latitude set 40
root> platform management system-longitude set 73
root> platform management set unit_measure_format metric
```

19.11 Configuring NTP (CLI)

PTP 850 supports Network Time Protocol (NTP). NTP distributes Coordinated Universal Time (UTC) throughout the system, using a jitter buffer to neutralize the effects of variable latency.

You can configure up to four NTP servers. Each server can be configured using IPv4 or IPv6. When multiple servers are configured, the unit chooses the best server according to the implementation of Version 4.2.6p1 of the NTPD (Network Time Protocol Daemon). The servers are continually polled. The polling interval is determined by the NTPD, to achieve maximum accuracy consistent with minimum network overhead.

Optionally, for extra security you can enable NTP authentication, as defined in the NTP specification (IETF RFC 5905). NTP authentication enables the client to verify the authenticity of the NTP server before synchronizing its clock with the server's time. This can help prevent man-in-the-middle attacks and other types of threats that could manipulate the client's clock by providing it with false time information.

NTP authentication requires the client and server to have a shared secret key that is used to authenticate the NTP messages exchanged between them. You can define the shared key for the client on the device, as described below.

To configure an NTP server, enter the following commands in root view:

```
root> platform management ntp set admin index <index> admin
<admin> authentication-admin <authentication> Key-Identifier <key>
auth-type <auth-type> shared-secret <secret>
```

To specify the server's IP address, use one of the following commands.

Note: For each NTP server you configure, you can define an IPv4 address or an IPv6 address, but not both.

- To configure the NTP server with an IPv4 address, enter the following command in root view:

  ```
  root> platform management ntp set server ipv4 index <index> ipv4
  <ipv4> ntp-version <ntp-version>
  ```

- To configure the NTP server with an IPv6 address, enter the following command in root view:

  ```
  root> platform management ntp set server ipv4 index <index> ipv4
  <ipv6> ntp-version <ntp-version>
  ```

To display the current configuration of all the defined NTP servers, enter the following command in root view:

```
root> platform management ntp show status
```

To display the current configuration and status of all the defined NTP servers, including details that can be used for debugging, enter the following command in root view:

```
root> platform management ntp show status all
```

For example:

```
root>platform management ntp show status
Id      IP                                      Lock status   Admin    Version   Auth-admin   Key-id   Auth-type   Shared-secret
=============================================================================================================================
1       192.168.1.18                            candidate     enable   4         enable       1        SHA2        ********
2       192.168.1.130                           n/a           enable   4         enable       2        MD5         ********
3       192.168.1.166                           locked        enable   4         enable       3        MD5         ********
4       192.168.1.250                           n/a           enable   4         enable       4        MD5         ********
root>
```

The following shows an example of the output of this command. For an explanation of the status fields, see Table 35.

```
root>platform management ntp show status all
Id      IP                                      Lock status   Admin    Version Refid              Stratum Peer type Last poll Poll interval Reach Delay Offset   Jitter
=============================================================================================================================================================
1       192.168.1.18                            candidate     enable   4       162.159.200.123    4       unicast   104       256           377   0.611 +1.143   0.747
2       192.168.1.130                           n/a           enable   4       .INIT.             16      unicast   -         1024          0     0.000 +0.000   0.000
3       192.168.1.166                           locked        enable   4       193.226.12.21      3       unicast   40        256           377   0.661 +0.001   0.368
4       192.168.1.250                           n/a           enable   4       .INIT.             16      unicast   -         1024          0     0.000 +0.000   0.000
root>_
```

Table 119: NTP CLI Parameters

Parameter	Input Type	Permitted Values	D
index	Number	1-4	D th b c Y c to s
admin	Variable	enable disable	E o e d N
authentication	Variable	enable disable	E o e d a B N a is

Parameter	Input Type	Permitted Values	D
key	Number	1-65535	C n y e a T id in c a th s c fo a
auth-type	Variable	md5 sha1 sha2-256	C n y e a T a c N a T v
secret	Number	Depends on the *auth-type*: • **md5** – 8-32 characters • **sha1 (default)** – 8-40 characters • **sha2-256** – 8-64 characters	C n y e a T s a
ipv4	Dotted decimal format.	Any valid IPv4 address.	E a N

Parameter	Input Type	Permitted Values	D
ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	E a N
ntp-version	Variable	ntpv3 ntpv4	E v w N p ir w a S

The following commands configure NTP server 3, enable the server using NTP v4, and set the IP address of the NTP server as 62.90.139.210.

```
root> platform management ntp set admin index 3 admin enable

root> platform management ntp set server ipv4 index 3 ipv4
62.90.139.210 ntp-version ntpv4
```

19.12 Displaying Unit Inventory (CLI)

To view inventory information, such as the part number and serial number of the unit hardware, enter the following command in root view:

```
root> platform management inventory show info
```

For example:

```
root> platform management inventory show info


System information:

card-name : PTP 850

Subtype : 350

part number : 22-0001-0|

serial number : F493606212

company name : Cambium Networks

product name : AODU DC, All-outdoor, dual radio carriers in one
product

product description : AODU DC, All-outdoor, dual radio carriers in
one product

root>
```

19.13 Displaying SFP DDM and Inventory Information (CLI)

Static and dynamic monitoring is available for SFP, SFP+, and QSFP modules used in ports P3 (Eth2), P4 (Eth3, Eth4, Eth5, Eth6), and P5 (Eth7).

Dynamic monitoring (DDM) PMs are also available.



Note

DDM parameters are not relevant for electrical SFPs.

Several alarms are available in connection with SFP DDM and inventory monitoring. See SFP DDM Alarms.

19.13.1 Displaying Static Information about an SFP Transceiver (CLI)

To display static information about an SFP transceiver, enter the following command in root view:

```
root> platform interfaces sfp-inventory show
```

For example:

```
root>platform interfaces sfp-inventory show

SFP Transceiver Inventory and DDM :
===================================

Interface Location        Transceiver Present  Connector Type  Transceiver Type                Vendor Name  Vendor Part Number  Vendor Serial Number  Vendor Revision  Laser Wavelength (nm)  Link Length SM Fiber (km)  Link Length OM1 Fiber (m)  Link Length OM2 Fiber (m)  Link Length OM3 Fiber (m)  Optical Diagnostics Supported
=========================================================================================================================================================================================================================================
Ethernet: Slot 1, Port 2  yes                  LC              I/SN/M6                         AVAGO        AFBR-57J7APZ        AA1243A4T39                                850                    0                          30                         80                         200                        yes
Ethernet: Slot 1, Port 7  yes                  LC              1000BASE-LX/L/LC/SM/100MBps     LINKTEL      LX1023IDR-CER       1170822524            1.0              1310                   40                         0                          0                          0                          yes
root>
```

Table 120 SFP Inventory Parameters (CLI)

Parameter	Description
Transceiver Present	Indicates whether an SFP transceiver is attached to the interface.
Connector Type	Always displays LC.
transceiver Type	Displays a description of the SFP transceiver.
Vendor Name	Displays the name of the SFP's vendor.
Vendor Part Number	Displays the vendor's part number for the SFP transceiver.
Vendor Serial Number	Displays the vendor's serial number for the SFP transceiver.
Vendor Revision	Displays the revision number of the serial number provided by the vendor for the SFP transceiver.
Laser Wavelength (nm)	Display's the SFP module's laser wavelength. For CSFP transceiver, two wavelengths are displayed. This parameters is not relevant for copper SFPs.
Link Length SM Fiber (km)	The maximum length of the cable (in km) for single mode fiber cables.
Link Length OM1 Fiber (m)	The maximum length of the cable (in meters) for OM1 multi-mode fiber cables.
Link Length OM2 Fiber (m)	The maximum length of the cable (in meters) for OM2 multi-mode fiber cables.

Link Length OM3 Fiber	The maximum length of the cable (in meters) for OM3 multi-mode fiber cables.
Optical Diagnostics Supported	Displays whether the SFP transceiver supports DDM monitoring. For modules that do not support DDM monitoring, the parameters described in Table 90 are not available.

19.13.2 Displaying Dynamic (DDM) Information about an SFP Transceiver (CLI)

To display dynamic information about an SFP transceiver, enter the following command in root view:

```
root> platform interfaces sfp-diagnostic show
```

For example:

```
root>platform interfaces sfp-diagnostic show

SFP Transceiver Inventory and DDM :
===================================

Interface Location          Transceiver     Optical         RX Power Level  TX Power Level  Bias Current    Temperature     Voltage
                            Present         Diagnostics     (dBm)           (dBm)           (mA)
                                            Supported
-------------------------------------------------------------------------------------------------------------------------------
Ethernet: Slot 1, Port 2    yes             yes             -2.49           -4.09           6               57C / 134F      3.227
Ethernet: Slot 1, Port 3    yes             yes             -4.36           -2.18           7               58C / 136F      3.248
root>_
```

Table 121 SFP Digital Diagnostic Monitoring (DDM) Parameters (CLI)

Parameter	Description
Transceiver Present	Indicates whether an SFP transceiver is attached to the interface.
RX Power Level (dBm)	The SFP transceiver current RX power signal strength (in dBm).
TX Power Level (dBm)	The SFP transceiver current TX power signal strength (in dBm).
Bias Current (mA)	The laser bias current of the SFP transceiver (in mA)
Temperature	The current temperature of the SFP transceiver (displayed in both C° and F°).
Voltage (V)	The supply voltage (VCC) currently being received by the SFP transceiver (if available).

Note

Tx Power level DDM is not supported for QSFP (P4) – not part of the standard.

If no signal is being received, RX Power Level is displayed as -40 dBm.

If the Admin status of the port is Down, the TX Power Level is displayed as -40 DBm and the Bias Current is displayed as 0 mA.

The Temperature is always shown as long as the SFP transceiver is inserted in the port.

19.13.3 Displaying DDM PMs about an SFP Transceiver (CLI)

DDM PMs can be displayed for 15-minute and 24-hour intervals. For each interval, the following PMs are displayed:

- Minimum RX power during the interval (dBm)
- Average RX power during the interval (dBm)
- Maximum RX power during the interval (dBm)
- Minimum TX power during the interval (dBm)
- Average TX power during the interval (dBm)
- Maximum TX power during the interval (dBm)
- Minimum voltage received by the SFP transceiver during the interval (VCC).
- Average voltage received by the SFP transceiver during the interval (VCC).
- Maximum voltage received by the SFP transceiver during the interval (VCC).

To display DDM PMs, enter the following command in root view:

```
root> platform interfaces sfp-pm show slot <slot> port <port>
interface eth interval <15min|24h|all>
```

For example:

```
root>platform interfaces sfp-pm show slot 1 port 3 interface eth interval all

SFP Devices PM Table:
=====================
```

SFP ifindex	PM interval	Integrity	Interval time stamp	Min RX power (dBm)	Avg RX power (dBm)	Max RX power (dBm)	Min TX power (dBm)	Avg TX power (dBm)	Max TX power (dBm)	Min Voltage	Avg Voltage	Max Voltage
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 14:30:00	-4.69	-4.56	-4.46	-0.31	-0.31	-0.31	3.244	3.245	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 14:30:00	-4.76	-4.54	-4.16	-0.31	-0.31	-0.31	3.244	3.245	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 14:15:00	-5.11	-4.67	-4.46	-0.31	-0.31	-0.31	3.244	3.245	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 14:00:00	-5.11	-4.58	-4.25	-0.31	-0.31	-0.31	3.244	3.246	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 13:45:00	-4.94	-4.58	-4.49	-0.31	-0.31	-0.31	3.244	3.246	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 13:30:00	-5.11	-4.68	-4.47	-0.31	-0.31	-0.31	3.244	3.246	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 13:15:00	-4.76	-4.57	-4.16	-0.31	-0.31	-0.31	3.244	3.245	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 13:00:00	-4.76	-4.57	-4.46	-0.31	-0.31	-0.31	3.244	3.246	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 12:45:00	-5.11	-4.63	-4.47	-0.31	-0.31	-0.31	3.246	3.246	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 12:30:00	-5.11	-4.68	-4.47	-0.31	-0.31	-0.31	3.244	3.246	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 12:15:00	-5.11	-4.61	-4.46	-0.31	-0.31	-0.31	3.245	3.246	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 12:00:00	-5.11	-4.69	-4.47	-0.35	-0.30	-0.03	3.246	3.246	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 11:45:00	-5.11	-4.77	-4.47	-0.35	-0.30	-0.08	3.246	3.246	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 11:30:00	-5.11	-4.70	-4.47	-0.35	-0.28	-0.03	3.245	3.246	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 11:15:00	-5.11	-4.64	-4.47	-0.31	-0.30	-0.08	3.244	3.246	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 11:00:00	-5.11	-4.64	-4.47	-0.31	-0.31	-0.31	3.244	3.245	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 10:45:00	-5.11	-4.63	-4.47	-0.31	-0.31	-0.31	3.244	3.246	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 10:30:00	-5.04	-4.74	-4.47	-0.31	-0.31	-0.31	3.244	3.246	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025, 10:15:00	-5.11	-4.66	-4.47	-0.35	-0.29	-0.03	3.246	3.246	3.247
Ethernet: Slot 1, Port 3	15min	0	02-02-2025,	-5.11	-4.80	-4.47	-0.35	-0.30	-0.05	3.245	3.246	3.247

The Integrity column indicates whether the PM is valid:

- 0 indicates a valid entry.
- 1 indicates an invalid entry. This can be caused by any of the following events that occurred during the interval
  - LOC alarm
  - Changing the Admin status of the interface
  - Unit reset



Note

No entries are displayed if the SFP device does not support DDM, or if the Admin status of the interface is Down.

DDM PMs are not persistent, which means they are not saved in the event of unit reset. RX and TX power levels are collected five times per 15-minute interval. 15-minute PM data is saved for 24 hours. 24-hour PM data, which is updated every 15 minutes, is saved for 30 days.

19.13.4 Configuring SFP Tccransceiver Voltage Thresholds (CLI)

You can configure high and low SFP RX power thresholds for each interface with an SFP. If these thresholds are exceeded, an alarm is raised. For details, see SFP DDM Alarms.

To set the high and low SFP RX power thresholds, enter the following command in root view:

```
root> platform interfaces sfp-config set slot 1 port <port> rx_thr_low
<text> rx_thr_high <text>
```

The following are the value ranges and defaults for these thresholds:

- `rx_thr_low` – -40 dBm to +10 dBm. Default value: -25 dBm.
- `rx_thr_high` – -40 dBm to +10 dBm. Default value: 0 dBm.

For example, the following command sets the low threshold to -25 dBm and the high threshold to 0 dBm.

root>platform interfaces sfp-config set slot 1 port 2 rx_thr_low -25 rx_thr_high 0

20. Radio Configuration (CLI)

This section includes:

- Viewing the Radio Status and Settings (CLI)
- To display the radio status, enter the following command in radio view:

```
radio[x/x]>rf module status show
```

This command is entered per radio carrier.

The following commands display the status of the radio on an PTP 850E:

```
root>radio slot 1 port 1
radio [1/1]>rf module status show
RF module status:
 TX Frequency: 73500000
 RX Frequency: 83500000
 Tx Rx frequency separation: 10000000
| TX level: 3
 RX level: -38
 Mute configuration: disabled
 Mute status: disabled
radio [1/1]>
```

The following commands display the status of the second radio on an PTP 850C:

```
root>radio slot 1 port 2
radio [1/2]>rf module status show
RF module status:
 TX Frequency: 18350000
 RX Frequency: 19380000
 Tx Rx frequency separation: 1030000
 TX level: 20
 RX level: -28
 Mute configuration: disabled
 Mute status: disabled
radio [1/2]>
```

To display the radio capabilities, enter the following command in radio view:

```
radio[x/x]>rf module capabilities show
```

The following commands display the radio capabilities of an PTP 850E:

```
radio [1/1]>rf module capabilities show

  Type: RFU-50E
  Part Number: 32-0002-0D
  Serial Number: F420T20798

  Band: 80
  Last Band: 80
  Max bandwidth(KHz): 2000000
  Min bandwidth(KHz): 62500
  Max RX frequency(KHz): 85875000
  Min RX frequency(KHz): 81125000
  Max TX frequency(KHz): 75875000
  Min TX frequency(KHz): 71125000

  Max Available TX Power(dBm): 20
  Min Available TX Power(dBm): -2
  XPIC Support: yes

  IF Combiner support: 3
radio [1/1]>
```

The following commands display the radio capabilities of the first radio carrier of an PTP 850C:

```
  Type: RFU-50C
  Part Number: 33-0018L-0C
  Serial Number: E431N29623

  Band: 18
  Last Band: 18
  Max bandwidth(KHz): 224000
  Min bandwidth(KHz): 3500
  Max RX frequency(KHz): 19588000
  Min RX frequency(KHz): 19272000
  Max TX frequency(KHz): 18578000
  Min TX frequency(KHz): 18238000

  Max Available TX Power(dBm): 20
  Min Available TX Power(dBm): 1
  XPIC Support: yes

  IF Combiner support: 3

radio [1/1]>
```

- Viewing and Configuring the Remote Radio Parameters (CLI)
- Configuring and Viewing Radio PMs and Statistics (CLI)

Related topics:

- Entering Radio View (CLI)
- Muting and Unmuting a Radio (CLI)
- Configuring the Transmit (TX) Level (CLI)
- Configuring the Transmit (TX) Frequency (CLI)
- Configuring the Radio (MRMC) Script(s) (CLI)
- System Configurations (CLI)

- Configuring 1+1 HSB Unit Protection (CLI)
- Configuring Multiband (CLI)
- Configuring Multiband with Layer 1 Link Bonding (CLI)
- Configuring Multi-Carrier ABC (CLI)
- Configuring XPIC (CLI)
- Configuring Link Aggregation (LAG) and LACP (Optional) (CLI)



Note

For convenience, this User Guide generally shows the radio prompt as `radio[1/1]>`.

20.1 Viewing the Radio Status and Settings (CLI)

To display the radio status, enter the following command in radio view:

```
radio[x/x]>rf module status show
```

This command is entered per radio carrier.

The following commands display the status of the radio on an PTP 850E:

```
root>radio slot 1 port 1
radio [1/1]>rf module status show
RF module status:
 TX Frequency: 73500000
 RX Frequency: 83500000
 Tx Rx frequency separation: 10000000
| TX level: 3
 RX level: -38
 Mute configuration: disabled
 Mute status: disabled
radio [1/1]>
```

The following commands display the status of the second radio on an PTP 850C:

```
root>radio slot 1 port 2
radio [1/2]>rf module status show
RF module status:
 TX Frequency: 18350000
 RX Frequency: 19380000
 Tx Rx frequency separation: 1030000
 TX level: 20
 RX level: -28
 Mute configuration: disabled
 Mute status: disabled
radio [1/2]>
```

To display the radio capabilities, enter the following command in radio view:

```
radio[x/x]>rf module capabilities show
```

The following commands display the radio capabilities of an PTP 850E:

```
radio [1/1]>rf module capabilities show

  Type: RFU-50E
  Part Number: 32-0002-0D
  Serial Number: F420T20798

  Band: 80
  Last Band: 80
  Max bandwidth(KHz): 2000000
  Min bandwidth(KHz): 62500
  Max RX frequency(KHz): 85875000
  Min RX frequency(KHz): 81125000
  Max TX frequency(KHz): 75875000
  Min TX frequency(KHz): 71125000

  Max Available TX Power(dBm): 20
  Min Available TX Power(dBm): -2
  XPIC Support: yes

  IF Combiner support: 3
radio [1/1]>
```

The following commands display the radio capabilities of the first radio carrier of an PTP *850C*:

```
  Type: RFU-50C
  Part Number: 33-0018L-0C
  Serial Number: E431N29623

  Band: 18
  Last Band: 18
  Max bandwidth(KHz): 224000
  Min bandwidth(KHz): 3500
  Max RX frequency(KHz): 19588000
  Min RX frequency(KHz): 19272000
  Max TX frequency(KHz): 18578000
  Min TX frequency(KHz): 18238000

  Max Available TX Power(dBm): 20
  Min Available TX Power(dBm): 1
  XPIC Support: yes

  IF Combiner support: 3

radio [1/1]>
```

20.2 Viewing and Configuring the Remote Radio Parameters (CLI)

This section includes:

- Displaying Communication Status with the Remote Radio (CLI)
- Displaying Remote Radio's Location (CLI)
- Muting and Unmuting the Remote Radio (CLI)
- Displaying the Remote Radio's RX Level (CLI)
- Configuring the Remote Radio's TX Level (CLI)
- Displaying the Remote Unit's Most Severe Alarm (CLI)

Related topics:

Configuring the Remote Unit's IP Address (CLI)

20.2.1 Displaying Communication Status with the Remote Radio (CLI)

To display the communication status with the remote radio, enter the following command:

```
radio[x/x]>remote-unit communication status show
```

20.2.2 Displaying Remote Radio's Location (CLI)

To display the remote radio's slot ID (location in the chassis), enter the following command in radio view. The slot ID of the remote radio will generally be 1, unless there is no communication with the remote unit. In that case, it will be -1.

```
radio[1/1]>remote-unit show slot-id
```

20.2.3 Muting and Unmuting the Remote Radio (CLI)

To mute or unmute the remote radio, enter the following command in radio view:

```
radio[1/1]>remote-unit mute set admin <admin> timeout-value
<timeout-value>
```

To display the mute status of the remote radio, enter the following command in radio view:

```
radio[1/1]>remote-unit mute show status
```

The output of this command indicates whether the remote unit is muted. If the remote unit is muted with a timer, the output of this command also indicates the length of the configured timeout and the time remaining until expiration of the timeout.

In the following example, the remote radio is muted with a timer set for 15 minutes, with 12 minutes remaining on the timer at the time of the command.

```
radio [1/1]>remote-unit mute show status
remote mute admin is: on-with-timer
remote mute configured timeout: 15 minutes
remote mute current timeout: 12 minutes
```

Table 122 Remote Radio Mute/Unmute CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin	Variable	on off on-with-timer	Mutes (on) or unmutes (off) the remote unit. Note that if AES-256 is enabled, you *must* set a timeout (*on-with-timer*). If you set a remote mute with a timer and then want to modify the timer, you must disable the mute by setting the admin value to off, then enter a new command with the desired timer.
timeout-value	Number	1-1440	Only use this parameter is the value of the *admin* parameter is set to *on-with-timer*. Sets the amount of time after which the remote radio will automatically be unmuted. The default value is 10 minutes. If you set the *admin* parameter to *on-with-timer* without adding this parameter, the timer will be set to 10 minutes.

The following command mutes the remote radio:

```
radio[2/1]>remote-unit mute set admin on
```

The following command unmutes the remote radio:

```
radio[2/1]>remote-unit mute set admin off
```

20.2.4 Displaying the Remote Radio's RX Level (CLI)

To display the remote radio's RX level, enter the following command in radio view:

```
radio[x/x]>remote-unit show rx-level
```

20.2.5 Configuring the Remote Radio's TX Level (CLI)

To set the transmit (TX) level of the remote radio, enter the following command in radio view:

```
radio[x/x]>remote-unit set tx-level <tx-level>
```

To display the transmit (TX) level of the remote radio, enter the following command in radio view:

```
radio[x/x]>remote-unit show tx-level
```

Table 123 Remote Radio TX Level CLI Parameters

Parameter	Input Type	Permitted Values	Description
tx-level	Number	Depends on the frequency and unit type.	The desired TX signal level (TSL), in dBm.

The following command sets the TX level of the remote radio to 10 dBm:

```
radio[2/1]>remote-unit set tx-level 10
```

20.2.6 Configuring Remote ATPC (CLI)

To set the RX reference level for ATPC on the remote radio, enter the following command in radio view:

```
radio[x/1]>remote-unit atpc set ref-level <ref-level>
```

To display the RX reference level for ATPC on the remote radio, enter the following command in radio view:

```
radio[x/1]>remote-unit atpc show ref-level
```

Table 124 Remote Radio ATPC CLI Parameters

Param	InputT	Permit	Description

et er	y p e	e d V al u e s	
re f- le v el	N u m b e r	- 7 0 - - 3 0	Th e RX ref ere nc e lev el for the AT PC me ch ani sm .

The following command sets the ATPC RX reference level of the remote radio to -55:

```
radio[2/1]>remote-unit atpc set ref-level -55
```

20.2.7 Displaying the Remote Unit's Most Severe Alarm (CLI)

To display the most severe alarm currently raised in the unit, enter the following command in radio view:

```
radio[x/x]>remote-unit show most-severe-alarm
```

20.3 Configuring ATPC and ATPC Override Timer (CLI)



Note

This section is only relevant for PTP 850S.

ATPC is a closed-loop mechanism by which each carrier changes the TX power according to the indication received across the link, in order to achieve a desired RSL on the other side of the link.

With ATPC, if the radio increases its TX power up to the configured TX power, it can lead to a period of sustained transmission at maximum power, resulting in unacceptable interference with other systems.

In order to minimize interference, PTP 850S provides an ATPC override mechanism. When ATPC override is enabled, a timer begins when ATPC raises the TX power to

its maximum. When the timer expires, the radio enters ATPC override state. In ATPC override state, the radio transmits no higher than the pre-determined ATPC override TX level, and an ATPC override alarm is raised. The radio remains in ATPC override state until the ATPC override state is manually cancelled by the user (or until the unit is reset). The radio then returns to normal ATPC operation.

In a configuration with unit protection, the ATPC override state is propagated to the standby unit in the event of switchover.



Note

When canceling an ATPC override state, you should ensure that the underlying problem has been corrected. Otherwise, ATPC may be overridden again.

To enable or disable ATPC, enter the following command in radio view:

```
radio[x/1]>atpc set admin <admin>
```

To display whether or not ATPC is enabled, enter the following command in radio view:

```
radio[x/1]>atpc show admin
```

To set the RX reference level for ATPC, enter the following command in radio view

```
radio[x/1]>atpc set rx-level atpc_ref_rx_level <rx-level>
```

To display the RX reference level for ATPC, enter the following command in radio view:

```
radio[x/1]>atpc show rx-level
```

To set an ATPC override timer, enter the following command in radio view:

```
radio[x/1]>atpc set override timeout <timeout>
```



Note

The next command actually enables ATPC override. However, it is recommended to set the timer before enabling ATPC override. Failure to do so can lead to unexpected reduction of the TX power with corresponding loss of capacity if TX override is enabled with the timer set to a lower-than-desired value.

To enable ATPC override, enter the following command in radio view. ATPC must be enabled before you enable ATPC override.

```
radio[x/1]>atpc override set admin <override admin>
```

To display whether or not ATPC override is enabled, enter the following command in radio view:

```
radio[x/1]>atpc override show admin
```

To display the ATPC override timeout, enter the following command in radio view:

```
radio[x/1]>atpc show override timeout
```

To set the TX power to be used when the unit is in an ATPC override state, enter the following command in radio view:

```
radio[x/1]>atpc set override-tx-level <override-tx-level>
```

To display the ATPC override TX power, enter the following command in radio view:

```
radio[x/1]>atpc show override tx-level
```

To display the current ATPC override state, enter the following command in radio view:

```
radio[x/1]>atpc show override
```

Possible values are:

Normal – ATPC override is enabled, and there is no override.

Disabled – ATPC override is not enabled.

Override – ATPC override has been activated.

To cancel ATPC override, enter the following command in radio view:

```
radio[x/x]>atpc set override-cancel
```

Table 125 Radio ATPC CLI Parameters

Parameter	Input Type	Permitted Values	Description
adm	Var	ena	Enabl
rx-level	Number	-70-	The RSL ref
timeout	Number	0-1800	The amount of

o v er	V a r	e n a	En abl es
o v er ri d e-	N u m b e r	- 5 0 - 5 0	Th e TX po we r,

The following commands enable ATPC mode and ATPC override, with an RSL reference level of -55, an ATPC override timeout of 15 minutes, and an override TX level of 18 dBm:

```
radio[2/1]>atpc set admin enable

radio[2/1]>atpc set rx-level atpc_ref_rx_level -55
radio[2/1]>atpc set override timeout 900
radio[2/1]>atpc override set admin enable
radio[2/1]> atpc set override tx-level 18
```

20.4 Configuring Header De-Duplication (CLI)

Note: This section is only relevant for PTP 850S.

Header De-Duplication identifies traffic flows and replaces header fields with a flow ID. The Header De-Duplication module includes an algorithm for learning each new flow, and implements compression on the flow type starting with the next frame of that flow type.

You can determine the depth to which the compression mechanism operates, from Layer 2 to Layer 4. You must balance the depth of compression against the number of flows in order to ensure maximum efficiency. Multi-Layer (Enhanced) compression supports up to 256 flow types.

The Header De-Duplication configuration must be identical on both

To configure Header De-Duplication, enter the following command in radio view:

```
radio[2/1]> compression header-compression set <mode>
```

To clear Ethernet port counters, including both Frame Cut-Through and Header De-Duplication counters, enter the following command in radio view:

```
radio[x/x]>clear-ethernet-port-counters
```

Table 126 Header De-Duplication CLI Parameters

Parameter	Input Type	Permitted Values	Description

mode	Variable	Disabled Layer2 MPLS Layer3 Layer4 Tunnel Tunnel-Layer3 Tunnel-Layer4	Disabled - Header De-Duplication is disabled. Layer2 - Header De-Duplication operates on the Ethernet level. MPLS - Header De-Duplication operates on the Ethernet and MPLS levels. Layer3 - Header De-Duplication operates on the Ethernet and IP levels. Layer4 - Header De-Duplication operates on all supported layers up to Layer 4. Tunnel - Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel layer for packets carrying GTP or GRE frames. Tunnel-Layer3 - Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel and T-3 layers for packets carrying GTP or GRE frames. Tunnel-Layer4 - Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel, T-3, and T- 4 layers for packets carrying GTP or GRE frames.

The following command enables Layer 2 Header De-Duplication on the radio:

```
root> radio slot 2 port 1

radio[2/1]> compression header-compression set Layer2
```

20.4.1 Displaying Header De-Duplication Information (CLI)

To display the current Header De-Duplication configuration, enter the following command in radio view:

```
radio[x/1]> compression show-configuration
```

To display counters for Header De-Duplication, enter the following command in radio view:

```
radio[x/1]> compression header-compression show-counters
```

The following counters are displayed:

- TX in octet count - Bytes on the TX side before Header De-Duplication.
- TX out octet count - Bytes on the TX side that were compressed by Header De- Duplication.
- TX frame in count - Frames on the TX side before Header De-Duplication.
- TX frame out compressed count - Frames on the TX side that were compressed by Header De-Duplication.
- TX frame uncompressed count - The number of frames on the TX side that were not compressed due to exclusion rules.

> The use of exclusion rules for Header De-Duplication is planned for future release.

- TX frame uncompressed other count - Frames on the TX side that were not compressed for reasons other than the use of exclusion rules.
- TX out frame learning count - The number of frames that have been used to learn unique data flows. Once a particular flow type has been learned, subsequent frames with that flow type are compressed by Header De-Duplication.
- TX out number of active flows in count - The number of Header De-Duplication flows that are active on the TX side.

20.5 Configuring Frame Cut-Through (CLI)

> **Note:** This section is only relevant for PTP 850S.

Using the Frame Cut-Through feature, frames assigned to queues with 4th priority pre-empt frames already in transmission over the radio from other queues. After the 4th queue frames have been transmitted, transmission of the pre-empted frames resumes.

The Frame Cut-Through configuration must be identical on both sides

of the link.

Frame Cut-Through cannot be used together with 1588

To enable Frame Cut-Through, enter the following command in radio view:

```
radio[x/1]> cut-through mode yes
```

To disable Frame Cut-Through, enter the following command in radio view:

```
radio[x/1]> cut-through mode no
```

To display whether Frame Cut-Through is currently enabled or disabled, enter the following command in radio view:

```
radio[x/1]> cut-through show-mode
```

To display the number of frames and bytes that have been transmitted via Frame Cut-Through, enter the following command in radio view:

```
radio[x/1]> cut-through show-counters
```

20.6 Configuring AES-256 Payload Encryption (CLI)

This feature is only relevant for PTP 850E units.

This feature is not supported with 2+0 XPIC and Multiband links

This feature requires:

- Requires an activation key. If no valid AES activation key has been applied to the unit, AES will not operate on the unit. See *Configuring the Activation Key (CLI)*.

In order for the AES activation key to become active, you must reset

the unit after configuring a valid AES activation key. Until the unit is reset, an alarm will be present if you enable AES. This is not the case for other activation keys.

PTP 850E supports AES-256 payload encryption, using a dual-key encryption mechanism:

- The user provides a master key. The master key can also be generated by the system upon user command. The master key is a 32-byte symmetric encryption key. The same master key must be manually configured on both ends of the encrypted link.
- The session key is a 32-byte symmetric encryption key used to encrypt the actual data. Each link uses two session keys, one for each direction. For each

direction, the session key is generated by the transmit side unit and propagated automatically, via a Key Exchange Protocol, to the other side of the link. The Key Exchange Protocol exchanges session keys by encrypting them with the master key, using the AES-256 encryption algorithm. Session keys are regenerated at user-configured intervals.

The first KEP exchange that takes place after a new master key is configured causes traffic to be blocked for up to one minute, until the Crypto Validation State becomes Valid. Subsequent KEP exchanges that take place when a session key expires do not affect traffic. KEP exchanges have no effect upon ACM, RSL, and MSE.

To display the current payload encryption status for all available radio links on the unit, enter the following command in root view:

```
root> payload encryption status show
```

The following is a sample output of this command in which payload encryption is enabled but not operational.

```
root>payload encryption status show
Traffic Crypto configuration table:
=========================================
| Interface      | Interface      | Admin          | Master                          | Session        |
| slot           | port           | mode           | Key                             | Key            |
|                |                |                |                                 | Period         |
=============================================================================================================
| 1              | 1              | AES-256        | {w,2Gsf_\R]]Jl;)+U{Pp;omJkS_*ycm | 12:00          |
Traffic Crypto status table:
============================
| Interface      | Interface      | Crypto         |
| slot           | port           | Validation     |
|                |                | State          |
=================================================
| 1              | 1              | not-valid      |
root>
```

Note

The Crypto Validation State field indicates whether the interface is functioning properly, with AES-256 encryption. In order for this field to display Valid, both the interface itself and AES-256 encryption must be enabled, the hardware must be in place and functioning properly, initialization must be finished, and AES-256 encryption must be functioning properly, with no loopback on the interface.

To configure payload encryption:

1. Verify that both the local and remote units are running with no alarms. If any alarm is present, take corrective actions to clear the alarms before proceeding.
2. If the link is using in-band management, identify which unit is local and which unit is remote from the management point of view.
3. To configure AES on a radio carrier, you must first enter traffic enc`ryption view for the specific radio. To enter Payload Encryption view, enter the following command in root view:

```
root> payload encryption slot 1 port 1
```

To display the payload encryption mode of the radio interface, enter the following command in Payload Encryption view:

```
Payload Encryption [1/1]> payload encryption mode show
```

The following display indicates that payload encryption is enabled on radio interface 1:

```
Payload Encryption [1/1]> payload encryption mode show
Admin Mode: AES-256
```

The following display indicates that payload encryption is disabled:

```
Payload Encryption [1/1]> payload encryption mode show
Admin Mode: Disable
```

4 Configure the master key on the remote unit by doing one of the following:

- Enter a master key manually.
- Generate the master key automatically.

You must use the same master key on both sides of the link. This means that if you generate a master key automatically on one side of the link, you must copy that key and for use on the other side of the link. Once payload encryption has been enabled on both sides of the link, the Key Exchange Protocol periodically verifies that both ends of the link have the same master key. If a mismatch is detected, an alarm is raised and traffic transmission is stopped for the mismatched carrier at both sides of the link. The link becomes non-valid and traffic stops being forwarded.

To define the master key manually, enter the following command in Payload Encryption view:

```
Payload Encryption [1/1]> payload encryption mkey
```

When you press **<Enter>**, the following prompt appears:

```
Please enter key:
```

Enter the master key and press **<Enter>.** The master key must be between 8 and 32 ASCII characters. The characters *do not* appear as you type them. To display the master key and verify that you typed it correctly, enter the `payload encryption status show` command described above. You can copy the master key from the output of this command.

To generate the master key automatically, enter the following command in Payload Encryption view:

```
Payload Encryption [1/1]> master key generate
```

A random master key is generated. You must copy and paste this key to the other end of the link to ensure that both sides of the link have the same master key. To display and copy the master key, enter the `traffic encryption status show` command described above. You can copy the master key from the output of this command.

5 On the local unit, follow the procedure described in Step 4 to configure the same master key configured on the remote unit also on the local unit.

6 Enable payload encryption on the remote unit:

i Enter the following command in Payload Encryption view:

```
Payload Encryption [1/1]> payload encryption mode admin AES-256
```

This step will cause the link status to be Down until payload encryption is successfully enabled on the local unit. However, the RSL measured on the link should remain at an acceptable level.

To disable payload encryption, enter the following command in Payload Encryption view:

```
Payload Encryption [1/1]> payload encryption mode admin Disable
```

ii The session key is automatically regenerated at defined intervals. To set the session key regeneration interval, enter the following command in Payload Encryption view:

```
Payload Encryption [x/x]> payload encryption session-key period
set <00:03-12:00>
```

Enter the regeneration interval in hours and minutes (HH:MM). For example, the following command configures radio interface 1 to regenerate the session key every 4 hours and 15 minutes:

```
Payload Encryption [1/1]> payload encryption session-key period
set 04:15
```

To display the session key regeneration interval, enter the following command in Payload Encryption view:

```
Payload Encryption [1/1]> payload encryption session-key period
show
```

7 Enable payload encryption on the local unit by following the procedure described in Step 6. Verify that on both the local and remote active units, the link status returns to Up and user traffic is restored. In links using in-band management, verify also that in-band management returns.

8 Verify that there are no alarms on the link.

You can set all master keys defined on the unit to zero value. To zeroize the master keys, enter the following command in root view:

```
root> payload encryption key zeroize
```

Any time payload encryption fails, the Operational status of the link is Down until payload encryption is successfully restored.

20.7 Configuring and Viewing Radio PMs and Statistics (CLI)

This section includes:

- Displaying General Modem Status and Defective Block PMs (CLI)
- Displaying Excessive BER (Aggregate) PMs (CLI)
- Displaying BER Level and Configuring BER Parameters (CLI)

- Configuring RSL Thresholds (CLI)
- Configuring TSL Thresholds (CLI)
- Displaying RSL and TSL Levels (CLI)
- Configuring the Signal Level Threshold (CLI)
- Configuring the MSE Thresholds and Displaying the MSE PMs (CLI)
- Configuring the XPI Thresholds and Displaying the XPI PMs (CLI)
- Displaying ACM PMs and Configuring ACM Profile Thresholds (CLI)

20.7.1 Displaying General Modem Status and Defective Block PMs (CLI)

To display the general status of the modem, enter the following command in radio view:

```
radio[x/x]>modem show status
```

The following is a sample output of the `modem show status` command:

```
MSE[db]: -99.00
Defective Blocks count: 0

Current Tx profile: 0
Current Tx QAM: 4
Current Tx rate(Kbps): 43389
Current Rx profile: 0
Current Rx QAM: 4
Current Rx rate(Kbps): 43389
```

A value of 0 in the MSE (Db) field means that the modem is not locked.

To clear all radio PMs in the system, enter the following command in root view:

```
root> radio pm clear all
```

To clear defective blocks counters for a radio, enter the following command in radio view:

```
radio[x/x]>modem clear counters
```

20.7.2 Displaying Excessive BER (Aggregate) PMs (CLI)

You can display modem BER (Bit Error Rate) PMs in either 15-minute or daily intervals.

To display modem BER PMs in 15-minute intervals, enter the following command in radio view:

```
radio [x/x]>framer pm-aggregate show interval 15min
```

The following is a partial sample output of the `framer pm-aggregate show interval 15min` command:

```
radio [2/1]>framer pm-aggregate show interval 15min
Modem BER PM table:
===================

Interval    Integrity    ES      SES       UAS        BBE
=========================================================
0           1            0       0         333         0
1           1            0       0         900         0
2           1            0       0         900         0
3           1            0       0         900         0
4           1            0       0         900         0
5           1            0       0         900         0
6           1            0       0         900         0
7           1            0       0         900         0
8           1            0       0         900         0

radio [2/1]>
```

To display modem BER PMs in daily intervals, enter the following command:

```
radio [x/x]>framer pm-aggregate show interval 24hr
```

The following is a sample output of the `framer pm-aggregate show interval 24hr` command:

```
radio [2/1]>framer pm-aggregate show interval 24hr

Modem BER PM table:
===================

Interval    Integrity    ES          SES          UAS       BBE
=============================================================
0           1            0           0            53843     0
4           1            0           0            37061     0
5           1            0           0            4034       0
6           1            0           0            85971     0
8           1            0           0            46171     0
11          1            0           0            24184     0
15          1            0           0            85978     0
17          1            0           0            54979     0

radio [2/1]>
```

Table 127 Aggregate PMs (CLI)

Parameter	Description
Interval	The number of the interval: 1-30 for daily PM reports, and 1-96 for 15 minute PM reports.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. "1" in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.

Parameter	Description
ES	Indicates the number of seconds in the measuring interval during which errors occurred.
SES	Indicates the number of severe error seconds in the measuring interval.
UAS	Indicates the Unavailable Seconds value of the measured interval. The value can be between 0 and 900 seconds (15 minutes).
BBE	Indicates the number of background block errors during the measured interval.

20.7.3 Displaying BER Level and Configuring BER Parameters (CLI)

To display the current BER level, enter the following command:

```
radio [x/x]>modem show ber
```

The `excessive-ber` parameter determines whether or not excessive BER is propagated as a fault and considered a system event. For example, if `excessive-ber` is enabled, excessive BER can trigger a protection switchover.

To enable or disable Excessive BER Admin, enter the following command in root view:

```
root> radio excessive-ber set admin <admin>
```

To display the current setting for `excessive-ber`, enter the following command in root view:

```
root> radio excessive-ber show admin
```

To set the level above which an excessive BER alarm is issued for errors detected over the radio link, enter the following command:

```
radio [x/x]>modem excessive-ber set threshold <threshold>
```

To display the excessive BER threshold, enter the following command:

```
radio [x/x]>modem excessive-ber show threshold
```

Table 128 Excessive BER CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin	Variable	enable disable	Enables or disables propagation of excessive BER as a fault.
threshold	Variable	1e -3 1e -4 1e -5	The level above which an excessive BER alarm is issued for errors detected over the radio link.

The following command enables `excessive-ber`:

```
root> radio excessive-ber set admin enable
```

The following command sets the excessive BER threshold to 1e-5:

```
radio [2/1]>modem excessive-ber set threshold 1e-5
```

20.7.4 Configuring RSL Thresholds (CLI)

You can set two RSL (RX Signal Level) thresholds. The number of seconds during which the RSL exceeds these thresholds are counted as RSL Exceed Threshold Seconds. See Displaying RSL and TSL Levels (CLI).

To set the RSL thresholds, enter the following command:

```
radio [x/x]>rf pm-rsl set threshold1 <threshold1> threshold2
<threshold2>
```

Table 129 RSL Thresholds CLI Parameters

Parameter	Input Type	Permitted Values	Description
threshold1	Number	-75 - -15	The first RSL threshold (dBm).
threshold2	Number	-75 - -15	The second RSL threshold (dBm).

The following command sets the RSL thresholds to -30 dBm and -60 dBm, respectively.

```
radio [2/1]>rf pm-rsl set threshold1 -30 threshold2 -60
```

20.7.5 Configuring TSL Thresholds (CLI)

The number of seconds during which the TX Signal Level exceeds the TSL threshold are counted as TSL Exceed Threshold Seconds. See Displaying RSL and TSL Levels (CLI).

To set the TSL threshold, enter the following command:

```
radio [x/x]>rf pm-tsl set threshold -15
```

Table 130 TSL Thresholds CLI Parameters

Parameter	Input Type	Permitted Values	Description
threshold	Number	-10 - 34	The TSL threshold (dBm).

The following command sets the TSL threshold to 10 dBm:

```
radio [2/1]>rf pm-tsl set threshold 10
```

20.7.6 Displaying RSL and TSL Levels (CLI)

You can display the RSL (RX Signal Level) and TSL (TX Signal Level) PMs in either 15-minute or daily intervals.

To display RSL and TSL PMs in 15-minute intervals, enter the following command:

```
radio [x/x]>rf pm-rsl-tsl show interval 15min
```

To display RSL and TSL PMs in daily intervals, enter the following command:

```
radio [x/x]>rf pm-rsl-tsl show interval 24hr
```

The following is the output format of the `rf pm-rsl-tsl show` commands:

```
radio [1/1]>rf pm-rsl-tsl show interval 15min

RF PM table:
============

Interval   Integrity  Min RSL (dBm)  Max RSL (dBm)  Min TSL (dBm)  Max TSL (dBm) TSL exceed   RSL exceed   RSL exceed
                                                                                 threshold    threshold1   threshold2
                                                                                 seconds      seconds      seconds
=============================================================================================================================
0          0          -72            -71            -20            -20           0            294          294
1          0          -72            -71            -20            -20           0            900          900
2          0          -72            -71            -20            -20           0            900          900
3          0          -72            -71            -20            -20           0            900          900
4          0          -72            -71            -20            -20           0            900          900
5          0          -72            -71            -20            -20           0            900          900
6          0          -72            -71            -20            -20           0            900          900
7          0          -72            -71            -20            -20           0            900          900
8          0          -73            -71            -20            -20           0            900          900
9          0          -73            -72            -20            -20           0            900          900
10         0          -74            -72            -20            -20           0            900          900
11         1          -85            -15            -20            -20           0            381          381
72         0          -72            -71            -20            -20           0            900          900
73         0          -72            -71            -20            -20           0            900          900
74         0          -73            -71            -20            -20           0            900          900
75         1          -84            -14            -20            -20           0            586          586
78         0          -72            -71            -20            -20           0            900          900
79         0          -72            -71            -20            -20           0            900          900
80         0          -72            -71            -20            -20           0            900          900
81         0          -72            -71            -20            -20           0            900          900
82         0          -72            -71            -20            -20           0            900          900
83         0          -72            -71            -20            -20           0            900          900
84         0          -72            -71            -20            -20           0            900          900
85         0          -73            -71            -20            -20           0            900          900
86         0          -73            -72            -20            -20           0            900          900
87         1          -84            -11            -20            -20           0            447          447
90         0          -72            -71            -20            -20           0            900          900
91         0          -72            -71            -20            -20           0            900          900
92         0          -72            -71            -20            -20           0            900          900
93         0          -72            -71            -20            -20           0            900          900
94         0          -72            -71            -20            -20           0            900          900
radio [1/1]>
```

Table 131 RSL and TSL PMs (CLI)

Parameter	Description
Interval	The number of the interval: 1-30 for daily PM reports, and 1-96 for 15 minute PM reports.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. "1" in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.
Min RSL (dBm)	The minimum RSL (Received Signal Level) that was measured during the interval.
Max RSL (dBm)	The maximum RSL (Received Signal Level) that was measured during the interval.
Min TSL (dBm)	The minimum TSL (Transmit Signal Level) that was measured during the interval.
Max TSL (dBm)	The maximum TSL (Transmit Signal Level) that was measured during the interval.
TSL exceed threshold seconds	The number of seconds the measured TSL exceeded the threshold during the interval. See Configuring TSL Thresholds (CLI).
RSL exceed threshold1 seconds	The number of seconds the measured RSL exceeded RSL threshold 1 during the interval. See Configuring RSL Thresholds (CLI).
RSL exceed threshold2 seconds	The number of seconds the measured RSL exceeded RSL threshold 2 during the interval. See Configuring RSL Thresholds (CLI).

20.7.7 Configuring the Signal Level Threshold (CLI)

To set the BER (Bit Error Rate) level above which a Signal Degrade alarm is issued for errors detected over the radio link, enter the following command:

```
radio [x/x]>modem signal-degrade set threshold 1e-7
```

To display the Signal Degrade BER threshold, enter the following command:

```
radio [x/x]>modem signal-degrade show threshold
```

Table 132 Signal Level Threshold CLI Parameters

Parameter	Input Type	Permitted Values	Description
threshold	Variable	1e -6 1e -7 1e -8 1e -9 1e -10	The BER level above which a Signal Degrade alarm is issued for errors detected over the radio link.

The following command sets the Signal Degrade threshold at 1e-7:

```
radio [2/1]>modem signal-degrade set threshold 1e-7
```

20.7.8 Configuring the MSE Thresholds and Displaying the MSE PMs (CLI)

To configure the MSE (Mean Square Error) threshold, enter the following command:

```
radio [x/x]>modem set mse-exceed threshold <threshold>
```

To display the currently configured MSE threshold, enter the following command:

```
radio [x/x]>modem show threshold-mse-exceed
```

Table 133 MSE CLI Parameters

Parameter	Input Type	Permitted Values	Description
threshold	Number	-99 - -1	The MSE threshold.

To display MSE (Mean Square Error) PMs in 15-minute intervals, enter the following command:

```
radio [x/x]>modem pm-mse show interval 15min
```

The following is a partial sample output of the `modem pm-mse show interval 15min` command:

```
radio [2/1]>modem pm-mse show interval 15min


Modem MSE PM Table:
===================

Interval   Integrity    Min MSE (dB)   Max MSE (dB)   Exceed
                                                      threshold
                                                      seconds
============================================================
0          1            0.00           0.00           708
1          1            0.00           0.00           900
2          1            0.00           0.00           900
3          1            0.00           0.00           900
4          1            0.00           0.00           900
5          1            0.00           0.00           900
6          1            0.00           0.00           900
7          1            0.00           0.00           900
8          1            0.00           0.00           900
9          1            0.00           0.00           900
10         1            0.00           0.00           900


radio [2/1]>
```

To display MSE (Mean Square Error) PMs in daily intervals, enter the following command:

```
radio [x/x]>modem pm-mse show interval 24hr
```

The following is sample output of the `modem pm-mse show interval 24hr` command:

```
radio [2/1]>modem pm-mse show interval 24hr

Modem MSE PM Table:
===================

Interval   Integrity    Min MSE (dB)   Max MSE (dB)   Exceed
                                                      threshold
                                                      seconds
============================================================
0          1            0.00           0.00           63745
4          1            0.00           0.00           37062
5          1            0.00           0.00           3495
6          1            0.00           0.00           85976
8          1            0.00           0.00           46173
11         1            0.00           0.00           24185
15         1            0.00           0.00           85988
17         1            0.00           0.00           54981

radio [2/1]>modem
```

Table 134 MSE PMs (CLI)

Parameter	Description
Interval	The number of the interval: 1-30 for daily PM reports, and 1-96 for 15 minute PM reports.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. "1" in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time. A 1 and a 0 value in the **Max MSE** field may also indicate that the modem was unlocked.
Min MSE (dB)	Indicates the minimum MSE in dB, measured during the interval. A 0 in this field and a 1 in the **Integrity** field may also indicate that the modem was unlocked during the entire interval.
Max MSE (dB)	Indicates the maximum MSE in dB, measured during the interval. A 0 in this field and a 1 in the **Integrity** field may also indicate that the modem was unlocked.
Exceed Threshold Seconds	Indicates the number of seconds the MSE exceeded the MSE PM threshold during the interval.

The following command sets the MSE threshold to -30:

```
radio [2/1]>modem set mse-exceed threshold -30
```

Configuring the XPI Thresholds and Displaying the XPI PMs (CLI)

Note: This section is only relevant for PTP 850C and PTP 850E.

To configure the modem XPI threshold for calculating XPI Exceed Threshold seconds, enter the following command in radio view:

```
radio[x/x]>modem set threshold-xpi-exceed threshold <threshold>
```

To display the currently configured XPI threshold, enter the following command in radio view:

```
radio[x/x]>modem show threshold-xpi-below
```

Table 143: XPI Threshold CLI Parameters

Parame	Input Type	Permitted	Description
threshol	Number	0-99	The XPI threshold.

To display XPI PMs in 15-minute intervals, enter the following command in radio view:

```
radio[x/x]>modem pm-xpi show interval 15min
```

The following is a partial sample output of the modem pm-xpi show interval 15min command:

```
radio [x/x]>modem pm-xpi show interval 15min

Modem XPI PM Table:
==================

Interval   Integrity   Min XPI (dB)   Max XPI (dB)   XPI below
                                                     threshold
                                                     seconds
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5          0
                5
                .          0
                0          0
```

To display XPI PMs in daily intervals, enter the following command in radio view:

```
radio[x/x]>modem pm-xpi show interval 24hr
```

The following is a partial sample output of the `modem pm-xpi show interval 24hr` command:

```
radio [x/x]>modem pm-xpi show interval 24hr

Modem XPI PM Table:
===================

Interval     Integrity      Min XPI (dB)   Max XPI (dB)
  XPI below

                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5          (
                5
```

Table 144: XPI PMs (CLI)

Parameter	Description
Interval	The number of the interval: 1-30 for daily PM reports, and 1-96 for 15 minute PM reports.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. "1" in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.

Min XPI (dB)	Indicates the lowest XPI value in dB, measured during the interval.
Max XPI (dB)	Indicates the highest XPI value in dB, measured during the interval.
XPI Below Threshold Seconds	Indicates the number of seconds the XPI value was lower than the XPI threshold during the interval.

The following command sets the XPI threshold to 15:

```
radio[x/x]>modem set threshold-xpi-below threshold 15
```

Displaying ACM PMs and Configuring ACM Profile Thresholds (CLI)

For each radio carrier, you can display the minimum and maximum ACM profile and the minimum and maximum bitrate (throughput) per 15-minute or daily intervals.

You can also define two ACM profile thresholds for each radio carrier, and display the number of seconds per interval that the radio's ACM profile was below each of these thresholds. These thresholds trigger the following alarms:

- **Threshold 1** – When the ACM profile goes beneath this threshold, Alarm ID 1313 (Major) is raised. The alarm is cleared when the ACM profile is at or above this threshold.
- **Threshold 2** – When the ACM profile goes beneath this threshold, Alarm ID 1314 (Critical) is raised. The alarm is cleared when the ACM profile is at or above this threshold.

To define the ACM thresholds, enter the following command in radio view:

```
radio [x/x]>mrmc pm-acm set threshold1 <threshold1> threshold2
<threshold2>
```

To display the ACM thresholds, enter the following command in radio view:

```
radio [x/x]>mrmc pm-acm get thresholds
```

To display ACM PMs in 15-minute intervals, enter the following command in radio view:

```
radio [x/x]>mrmc pm-acm show interval 15min
```

The following is a partial sample output of the `modem pm-acm show interval 15min` command:

```
radio [1/1]>mrmc pm-acm show interval 15min

MRMC PM Table:
==============
```

Interval	Integrity	Min profile	Max profile	Min bitrate	Max bitrate	Seconds above Threshold 1	Seconds below Threshold 1	Seconds below Threshold 2
0	0	10	10	223353	223353	263	0	0
1	0	10	10	223353	223353	900	0	0
2	0	10	10	223353	223353	900	0	0
3	0	10	10	223353	223353	900	0	0
4	0	10	10	223353	223353	900	0	0
5	1	0	10	18662	223353	215	0	0
6	1	10	10	223353	223353	507	0	0
7	1	1	10	38830	223353	410	47	2
8	1	10	10	223353	223353	1	0	0
9	1	10	10	223353	223353	310	0	0
10	1	10	10	223353	223353	1	0	0
11	1	10	10	223353	223353	448	0	0
12	1	10	10	223353	223353	1	0	0
13	1	10	10	223353	223353	72	0	0
14	1	7	10	179364	223353	541	1	0
15	1	10	10	223353	223353	1	0	0
16	1	10	10	223353	223353	373	0	0
17	1	10	10	223353	223353	1	0	0
18	1	10	10	223353	223353	879	0	0
19	0	10	10	223353	223353	900	0	0
20	0	10	10	223353	223353	900	0	0
21	0	10	10	223353	223353	900	0	0
22	0	10	10	223353	223353	900	0	0
23	0	10	10	223353	223353	900	0	0
24	0	10	10	223353	223353	900	0	0

To display ACM PMs in daily intervals, enter the following command in radio view:

```
radio [x/x]>mrmc pm-acm show interval 24hr
```

The following is sample output of the modem pm-acm show interval 24hr command:

```
radio [1/1]>mrmc pm-acm show interval 24hr

MRMC PM Table:
==============
```

Interval	Integrity	Min profile	Max profile	Min bitrate	Max bitrate	Seconds above Threshold 1	Seconds below Threshold 1	Seconds below Threshold 2
0	1	0	10	18662	223353	3422	0	0
1	1	1	10	38830	223353	411	47	2
2	1	10	10	223353	223353	311	0	0
3	1	10	10	223353	223353	449	0	0
4	1	7	10	179364	223353	614	1	0
5	1	10	10	223353	223353	1253	0	0
6	1	10	10	223353	223353	73583	0	0
7	0	10	10	223353	223353	86400	0	0
8	0	10	10	223353	223353	86400	0	0
9	1	0	10	18662	223353	23913	1	0
10	0	11	11	240534	240534	39599	0	0
11	1	0	11	18662	240534	86334	0	0
12	1	0	11	18662	460075	79901	0	0
13	1	0	10	18662	460075	49419	0	158
14	0	10	10	223353	223353	36900	0	0
15	1	0	10	18662	223353	85829	0	0
16	0	10	10	223353	223353	86400	0	0
17	1	0	10	18662	223353	86373	0	0
18	1	0	10	18662	223353	33981	0	0
19	1	0	0	20512	43535	1812	0	0
20	1	0	11	43535	529505	42585	0	0
21	1	0	11	43535	529505	31611	0	0
22	1	0	11	43535	529505	52184	0	0
23	1	0	12	20512	544920	84037	128	63
24	1	0	12	43535	544920	85276	0	424
25	0	12	12	544920	544920	86400	0	0
26	0	12	12	544920	544920	86400	0	0
27	0	12	12	544920	544920	86400	0	0
28	1	12	12	544920	544920	36882	0	0

Table 145: ACM PMs and ACM Profile Thresholds (CLI)

Parameter	Description
Interval	The number of the interval: 1-30 for daily PM reports, and 1-96 for 15 minute PM reports.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. "1" in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.
Min profile	Indicates the minimum ACM profile that was measured during the interval.
Max profile	Indicates the maximum ACM profile that was measured during the interval.
Min bitrate	Indicates the minimum total radio throughput (Mbps), delivered during the interval.
Max bitrate	Indicates the maximum total radio throughput (Mbps), delivered during the interval.

Parameter	Description
Seconds above Threshold 1	Displays the number of seconds the radio was above both ACM profile thresholds during the interval.
Seconds below Threshold 1	Displays the number of seconds the radio was below ACM profile threshold 1 during the interval.
Seconds below Threshold 2	Displays the number of seconds the radio was below ACM profile threshold 2 during the interval.
Profile X	A column is displayed for each ACM profile. For each interval, this column displays the number of seconds during which the radio operated at that ACM profile during that interval.

20.7.9 Displaying Traffic PMs (CLI)

This section includes:

- Displaying Capacity PMs (CLI)
- Displaying Throughput PMs (CLI)
- Displaying Utilization PMs and Configuring Utilization Thresholds (CLI)

20.7.9.1 Displaying Capacity PMs (CLI)

You can display capacity PMs for a radio or Multi-Carrier ABC group, based on the total Layer 1 bandwidth (payload plus overheads) sent through the radio or group, in Mbps.

You can also configure a threshold for capacity PMs. The number of seconds during which this threshold is exceeded are among the displayed PMs.

Peak counters display the maximum data rate for each interval, with a resolution of one second. This means the PM mechanism records the number of bytes sent during each second of the interval and displays the number of bytes for the highest one-second period during that interval. So, for example, when measuring 15-minute intervals, the PM mechanism chooses the peak value from 900 recorded values in that interval (60 seconds multiplied by 15 60-second record periods).

Average counters display the average number of bytes received on the interface measured with a resolution of one second. This means the PM mechanism divides the total number of bytes received during the interval by the total number of seconds in the interval. So, for example, when measuring 15-minute intervals, the PM mechanism divides the total number of bytes received during the 15-minute interval by 900.

To display capacity PMs per radio or Multi-Carrier ABC group in 15-minute intervals, enter the following command interface view:

```
radio [x/x]> traffic capacity show pm interval 15min
```

To display capacity PMs per radio or Multi-Carrier ABC group in daily intervals, enter the following command in interface view:

```
radio [x/x]> traffic capacity show pm interval 24hr
```

The following is the output format for the capacity show command in 15-minute intervals:

```
Radio Ethernet capacity PM:
===========================

Time interval   Integrity       Peak capacity   Average         Seconds
index                           (Mbps)          capacity (Mbps) exceeding
                                                                threshold
=============================================================================
0               0               243             242             361
1               0               243             242             900
2               0               243             242             900
3               0               243             242             900
4               0               243             242             900
5               0               243             242             900
6               0               243             242             900
7               0               243             242             900
8               0               243             242             900
9               0               243             242             900
10              0               243             242             900
11              0               243             242             900
12              0               243             242             900
13              0               243             242             900
14              0               243             242             900
15              0               243             242             900
16              0               243             242             900
```

The following is the output format for the capacity show command in 24-hour intervals:

```
Radio Ethernet capacity PM:
===========================

Time interval   Integrity       Peak capacity   Average         Seconds
index                           (Mbps)          capacity (Mbps) exceeding
                                                                threshold
=============================================================================
0               0               243             242             45000
1               0               243             141             49843
2               0               363             30              11671
3               0               0               0               0
4               0               0               0               0
5               0               0               0               0
6               0               0               0               0
7               0               0               0               0
8               0               0               0               0
9               0               0               0               0
10              0               0               0               0
11              0               0               0               0
12              0               0               0               0
13              0               0               0               0
14              0               0               0               0
15              0               363             64              33220
16              1               363             161             57650
17              0               243             242             86400
18              0               243             242             86399
19              0               243             241             86393
20              0               243             242             86400
21              0               243             242             86399
22              0               243             242             86400
23              0               243             242             86399
24              0               243             242             86399
25              0               243             242             86400
26              1               243             240             85650
27              0               243             242             86400
28              0               243             241             86399
29              0               243             242             86399
```

To set the threshold for capacity PMs, enter the following command in radio view. The capacity threshold is set in Mbps. The default threshold is 1000 Mbps.

```
radio [x/x]> traffic capacity set pm-threshold <0-4294967295>
```

To display the threshold for capacity PMs, enter the following command in radio view:

```
radio [x/x]> traffic capacity show pm-threshold
```

Table 135 describes the capacity PMs.

Table 135: Capacity/Throughput PMs (CLI)

Parameter	Definition
Time interval index	Identifies the interval.
Integrity	Indicates whether the values received at time and date of the measured interval are reliable. "1" in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.
Peak capacity (Mbps)	Displays the highest L1 bandwidth, in Mbps, sent through the selected radio during the measured time interval.
Average capacity (Mbps)	Displays the average L1 bandwidth, in Mbps, during the measured time interval.
Seconds exceeding Threshold	Displays the number of seconds during the measured time interval during which the L1 bandwidth exceeded the configured capacity threshold.

20.7.9.2 Displaying Throughput PMs (CLI)

You can display throughput PMs for a radio or Multi-Carrier ABC group, based on the total effective Layer 2 traffic sent through the radio or group, in Mbps.

You can also configure a threshold for throughput PMs. The number of seconds during which this threshold is exceeded are among the displayed PMs.

Peak counters display the maximum data rate for each interval, with a resolution of one second. This means the PM mechanism records the number of bytes sent during each second of the interval and displays the number of bytes for the highest one-second period during that interval. So, for example, when measuring 15-minute intervals, the PM mechanism chooses the peak value from 900 recorded values in that interval (60 seconds multiplied by 15 60-second record periods).

Average counters display the average number of bytes received on the interface measured with a resolution of one second. This means the PM mechanism divides the total number of bytes received during the interval by the total number of seconds in the interval. So, for example, when measuring 15-minute intervals, the PM mechanism divides the total number of bytes received during the 15-minute interval by 900.

To display throughput PMs per radio or Multi-Carrier ABC group in 15-minute intervals, enter the following command in radio view:

```
radio [x/x]> traffic throughput show pm interval 15min
```

To display throughput PMs per radio or Multi-Carrier ABC group in daily intervals, enter the following command in radio view:

```
radio [x/x]> traffic throughput show pm interval 24hr
```

The following is the output format for the throughput show command in 15-minute intervals:

```
Radio Ethernet throughput PM:
=============================

Time interval   Integrity       Peak            Average         Seconds
index                           throughput      throughput      exceeding
                                (Mbps)          (Mbps)          threshold
================================================================================
0               0               238             237             489
1               0               238             237             900
2               0               238             237             900
3               0               238             237             900
4               0               238             237             900
5               0               238             237             900
6               0               238             237             900
7               0               238             237             900
8               0               238             237             900
9               0               238             237             900
10              0               238             237             900
11              0               238             237             900
12              0               238             237             900
13              0               238             237             900
14              0               238             237             900
15              0               238             237             900
16              0               238             237             900
```

The following is the output format for the throughput show command in 24-hour intervals:

```
Radio Ethernet throughput PM:
=============================

Time interval   Integrity       Peak            Average         Seconds
index                           throughput      throughput      exceeding
                                (Mbps)          (Mbps)          threshold
================================================================================
0               0               238             237             45000
1               0               238             138             49843
2               0               354             29              11671
3               0               0               0               0
4               0               0               0               0
5               0               0               0               0
6               0               0               0               0
7               0               0               0               0
8               0               0               0               0
9               0               0               0               0
10              0               0               0               0
11              0               0               0               0
12              0               0               0               0
13              0               0               0               0
14              0               0               0               0
15              0               354             63              33220
16              1               354             158             57650
17              0               238             237             86400
18              0               238             237             86399
19              0               238             236             86393
20              0               238             237             86400
21              0               238             237             86399
22              0               238             237             86400
23              0               238             237             86399
24              0               238             237             86399
25              0               238             237             86400
26              1               238             235             85650
27              0               238             237             86400
28              0               238             236             86399
29              0               238             237             86399
```

To set the threshold for throughput PMs, enter the following command in radio view. The throughput threshold is set in Mbps. The default threshold is 1000 Mbps.

```
radio [x/x]> traffic throughput set pm-threshold <0-4294967295>
```

To display the threshold for capacity PMs, enter the following command in radio view:

```
radio [x/x]> traffic throughput show pm-threshold
```

Table 136 describes the throughput PMs.

Table 136: Throughput PMs (CLI)

Parameter	Definition
Time interval index	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Integrity	Indicates whether the values received at time and date of the measured interval are reliable. "1" in the column indicates that the values are not reliable due to a possible

	power surge or power failure that occurred at that time.
Peak throughput (Mbps)	Displays the highest throughput, in Mbps, that occurred for the selected radio or group during the measured time interval.
Average throughput (Mbps)	Displays the average throughput, in Mbps, for the selected radio or group during the measured time interval.
Seconds exceeding Threshold	Displays the number of seconds during the measured time interval during which the throughput exceeded the configured throughput threshold.

20.7.9.3 Displaying Utilization PMs and Configuring Utilization Thresholds (CLI)

You can configure three radio capacity utilization thresholds, in percentage. The Utilization PM Report displays the number of seconds in which a radio or Multi-Carrier ABC group exceeded each threshold during each interval. It also displays the peak and average utilization, in percentage, per interval.

To display radio utilization PMs per radio or Multi-Carrier ABC group in 15-minute intervals, enter the following command in radio view:

```
radio [x/x]> traffic utilization show pm interval 15min
```

To display radio utilization PMs per radio or Multi-Carrier ABC group in daily intervals, enter the following command in radio view:

```
radio [x/x]> traffic utilization show pm interval 24hr
```

The following is the output format for the radio utilization show command in 15-minute intervals:

```
Radio Ethernet utilization PM:
==============================

Time interval   Integrity       Peak            Average         Seconds         Seconds         Seconds         Seconds below
index                           utilization     utilization     exceeding       exceeding       exceeding       Threshold 3
                                (percent)       (percent)       Threshold 1     Threshold 2     Threshold 3
=============================================================================================================================
0               0               56              56              0               631             0               0
1               0               56              56              0               900             0               0
2               0               56              56              0               900             0               0
3               0               56              56              0               900             0               0
4               0               56              56              0               900             0               0
5               0               56              56              0               900             0               0
6               0               56              56              0               900             0               0
7               0               56              56              0               900             0               0
8               0               56              56              0               900             0               0
9               0               56              56              0               900             0               0
10              0               56              56              0               900             0               0
11              0               56              56              0               900             0               0
12              0               56              56              0               900             0               0
13              0               56              56              0               900             0               0
14              0               56              56              0               900             0               0
15              0               56              56              0               900             0               0
16              0               56              56              0               900             0               0
```

The following is the output format for the radio utilization show command in 24-hour intervals:

```
Radio Ethernet utilization PM:
==============================

Time interval   Integrity       Peak            Average         Seconds         Seconds         Seconds         Seconds below
index                           utilization     utilization     exceeding       exceeding       exceeding       Threshold 3
                                (percent)       (percent)       Threshold 1     Threshold 2     Threshold 3
=============================================================================================================================
0               0               56              56              0               45000           0               0
1               0               56              32              0               49843           0               36556
2               0               100             6               0               11669           0               74731
3               0               0               0               0               0               0               86399
4               0               0               0               0               0               0               86400
5               0               0               0               0               0               0               86399
6               0               0               0               0               0               0               86399
7               0               0               0               0               0               0               86400
8               0               0               0               0               0               0               86399
9               0               0               0               0               0               0               86400
10              0               0               0               0               0               0               86399
11              0               0               0               0               0               0               86400
12              0               0               0               0               0               0               86399
13              0               0               0               0               0               0               86400
14              0               0               0               0               0               0               86399
15              0               100             14              0               33219           0               53180
16              1               83              37              0               57650           0               28284
17              0               56              56              0               86400           0               0
18              0               56              56              0               86399           0               0
19              0               56              55              0               86393           0               6
20              0               56              56              0               86400           0               0
21              0               56              56              0               86399           0               0
22              0               56              56              0               86400           0               0
23              0               56              56              0               86399           0               0
24              0               56              56              0               86399           0               0
25              0               56              56              0               86400           0               0
26              1               56              55              0               85650           0               92
27              0               56              56              0               86400           0               0
28              0               56              55              0               86399           0               0
29              0               56              56              0               86399           0               0
```

To set the thresholds for radio utilization PMs, enter the following command in radio view. You can define three thresholds, in percentage (1-100). *utilization-threshold-1* and *utilization-threshold-3* should be the lowest. The default value for *utilization-threshold-1* is 100%. The default value for *utilization-threshold-2* and *utilization-threshold-3* is 0%.

```
radio [x/x]> traffic utilization set utilization-threshold-1 <0-
100> utilization-threshold-2 <0-99> utilization-threshold-3 <0-98>
```

To display the thresholds for radio utilization PMs, enter the following command in radio view:

```
radio [x/x]> traffic utilization show pm-thresholds
```

Table 137 describes the utilization PMs.

Table 137: Utilization PMs (CLI)

Parameter	Definition
Time interval index	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Integrity	Indicates whether the values received at time and date of the measured interval are reliable. "1" in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.
Peak utilization (percent)	Indicates the highest utilization of the radio capacity that occurred for the selected

	radio or group during the measured time interval.
Average utilization (percent)	Indicates the average utilization of the radio capacity for the selected radio or group during the measured time interval.
Seconds exceeding Threshold 1	Displays the number of seconds during the measured time interval during which the L1 bandwidth exceeded Threshold 1 (the highest threshold).
Seconds exceeding Threshold 2	Displays the number of seconds during the measured time interval during which the L1 bandwidth exceeded Threshold 2.
Seconds exceeding Threshold 3	Displays the number of seconds during the measured time interval during which the L1 bandwidth exceeded Threshold 3 (the lowest threshold).
Seconds below Threshold 3	Displays the number of seconds during the measured time interval during which the L1 bandwidth was less than Threshold 3 (the lowest threshold).

21. Ethernet Services and Interfaces (CLI)

This section includes:

- Configuring Ethernet Services (CLI)
- Setting the MRU Size and the S-VLAN Ethertype (CLI)
- Configuring Ethernet Interfaces (CLI)
- Configuring Automatic State Propagation and Link Loss Forwarding (CLI)
- Viewing Ethernet PMs and Statistics (CLI)

Related topics:

- Configuring Link Aggregation (LAG) and LACP (Optional) (CLI)
- Performing Ethernet Loopback (CLI)
- Ethernet Protocols (CLI)

21.1 Configuring Ethernet Services (CLI)

This section includes:

- Ethernet Services Overview (CLI)
- General Guidelines for Provisioning Ethernet Services (CLI)
- Defining Services (CLI)
- Configuring Service Points (CLI)
- Defining the MAC Address Forwarding Table for a Service (CLI)

21.1.1 Ethernet Services Overview (CLI)

Users can define the following number of Ethernet services:

- PTP 850C and PTP 850E: Up to 1024.
- PTP 850S: Up to 64.

Each service constitutes a virtual bridge that defines the connectivity between logical ports in the PTP 850 network element.

This version of PTP 850 supports the following service types:

-



Note

In release 10.6, only P2P and MNG services are supported. In release 10.9, Multipoint services are also supported.

In addition to user-defined services, PTP 850 contains a pre-defined management service (Service ID 257). By default, this service is operational.



Note

You can use the management service for in-band management. For instructions on configuring in-band management, see Mate Management Access (IP Forwarding) (CLI)

A service point is a logical entity attached to a physical or logical interface. Service points define the movement of frames through the service. Each service point includes both ingress and egress attributes. A Point-to-Point or Multipoint service can hold up to 32 service points. A Management service can hold up 30 service points.

For a more detailed overview of the PTP 850 service-oriented Ethernet switching engine, refer to the Technical Description for the PTP 850 product type you are using.

21.1.2 General Guidelines for Provisioning Ethernet Services (CLI)

When provisioning Ethernet services, it is recommended to follow these guidelines:

- Use the same Service ID for all service fragments along the path of the service.
- Do not re-use the same Service ID within the same region. A region is defined as consisting of all PTP 850 devices having Ethernet connectivity between them.
- Use meaningful EVC IDs.

Give the same EVC ID (service name) to all service fragments along the path of the service.

Do not reuse the same EVC ID within the same region.

It is recommended to follow these guidelines for creating service points:

Always use SNP service points on NNI ports and SAP service points on UNI ports.

For each logical interface associated with a specific service, there should never be more than a single service point.

The transport VLAN ID should be unique per service within a single region. That is, no two services should use the same transport VLAN ID.

21.1.3 Defining Services (CLI)

Use the commands described in the following sections to define a service and its parameters. After defining the service, you must add service points to the service in order for the service to carry traffic.

21.1.3.1 Adding a Service (CLI)

To add a service, enter the following command in root view:

```
root> ethernet service add type <service type> sid <sid> admin
<service admin mode> evc-id <evc-id> description <evc-description>
```

Table 138 Adding Ethernet Service CLI Parameters

Parameter	Input Type	Permitted Values	Description
service type	Variable	p2p mp	Defines the service type: p2p - Point-to-Point mp - Multipoint
sid	Number	350C and PTP 850E: Any unused value from 1- 4095 PTP 850S: Any unused value from 1-256	A unique ID for the service. Once you have added the service, you cannot change the Service ID. Service ID 257 is reserved for a pre-defined management service.
service admin mode	Variable	Operational reserved	The administrative state of the service: operational - The service is functional. reserved - The service is disabled until this parameter is changed to operational. In this mode, the service occupies system resources but is unable to receive and transmit data.
evc-id	Text String	Up to 20 characters.	Defines an Ethernet Virtual Connection (EVC) ID. This parameter does not affect the network element's behavior, but is used by the NMS for topology management.
evc-description	Text String	Up to 64 characters.	A text description of the service. This parameter does not affect the network element's behavior, but is used by the NMS for topology management.

The following command adds a Multipoint service with Service ID 18.

```
root> ethernet service add type mp sid 18 admin operational evc-id
Ring_1 description east_west
```

The following command adds a Point-to-Point service with Service ID 10.

```
root> ethernet service add type p2p sid 10 admin operational evc-
id Ring_1 description east_west
```

These services are immediately enabled, although service points must be added to the services in order for the services to carry traffic.

Entering Service View (CLI)

To view service details and set the service's parameters, you must enter the service's view level in the CLI.

To enter a service's view level:

```
root> ethernet service sid <sid>
```

Table 139 Entering Ethernet Service View CLI Parameters

Parameter	Input Type	Permitted Values	Description
sid	Number	Any unused value from 1-256	A unique ID for the service. Once you have added the service, you cannot change the Service ID. Service ID 257 is reserved for a pre-defined management service.

The following command enters service view for the service with Service ID 10:

```
root> ethernet service sid 10
```

The following prompt appears:

```
service[10]>
```

Showing Service Details (CLI)

To display the attributes of a service, go to service view for the service and enter the following command:

```
service[SID]>service info show
```

For example:

```
service[1]>service info show
   service info:
   service id: 1
   service type: p2p
   service admin: operational
   Maximal MAC address learning entries: 131072
   default cos: 0
   cos mode: preserve-sp-cos-decision
   EVC id: N.A.
   EVC description: N.A.
   split horizon group: disable
   configured multicast grouping: no
service[1]>
```

To display the attributes of a service and its service points, go to service view for the service and enter the following command:

```
service[SID]>service detailed-info show
```

For example:

```
service[1]>service detailed-info show
   service info:
   service id: 1
   service type: p2p
   service admin: operational
   Maximal MAC address learning entries: 131072
   default cos: 0
   cos mode: preserve-sp-cos-decision
   EVC id: PIPE
   EVC description: sid1
   split horizon group: disable
   configured multicast grouping: no
service-points info:
+----------+------------+------------+--------------------+----------------------+-------------+------------+-------
|Service ID|Service Type|List of SP's|Attached to Interface|Attached Interface Type|Service Admin|STP Instance|SP name|
+----------+------------+------------+--------------------+----------------------+-------------+------------+-------
|1         |p2p         |pipe     \1 |sfp              1/2|dot1q                 |operational  |0           | N.A.  |
|1         |p2p         |pipe     \2 |radio            2/1|dot1q                 |operational  |0           | N.A.  |
+----------+------------+------------+--------------------+----------------------+-------------+------------+----- -+
service[1]>
```

To display a list of service points and their attributes, enter the following command in root view:

```
root>ethernet service show info sid <sid>
```

Table 140 Displaying Ethernet Service Details CLI Parameters

Parameter	InputType	Permitted Values	Description
sid	Number	Any defined Service ID.	None

For example:

```
root>ethernet service show info sid 1
service-points info:

+----------+------------+------------+--------------------+----------------------+-------------+------------+-------
|Service ID|Service Type|List of SP's|Attached to Interface|Attached Interface Type|Service Admin|STP Instance|SP name|
+----------+------------+------------+--------------------+----------------------+-------------+------------+-------
|1         |p2p         |pipe     \1 |sfp              1/2|dot1q                 |operational  |0           | sp1   |
|1         |p2p         |pipe     \2 |radio            2/1|dot1q                 |operational  |0           | sp2   |
+----------+------------+------------+--------------------+----------------------+-------------+------------+----- -+
root>
```

Configuring a Service's Operational State (CLI)

To change the operational state of a service, go to service view for the service and enter the following command:

```
service[SID]>service admin set <service admin mode>
```

To display a service's admin mode, go to service view for the service and enter the following command:

```
Service[SID]> service admin show state
```

Table 141 Ethernet Service Operational State CLI Parameters

Parameter	Input Type	Permitted Values	Description
service admin mode	Variable	Operational reserved	The administrative state of the service: operational - The service is functional. reserved - The service is disabled until this parameter is changed to Operational. In this mode, the service occupies system resources but is unable to receive and transmit data.

The following command sets Service 10 to be operational:

```
service[10]>service admin set operational
```

Configuring a Service's CoS Mode and Default CoS (CLI)

The CoS mode determines whether or not frames passing through the service have their CoS modified at the service level. The CoS determines the priority queue to which frames are assigned.

The CoS of frames traveling through a service can be modified on the interface level, the service point level, and the service level. The service level is the highest priority, and overrides CoS decisions made at the interface and service point levels. Thus, by configuring the service to apply a CoS value to frames in the service, you can define a single CoS for all frames traveling through the service.

To set a service's CoS mode, go to service view for the service and enter the following command:

```
service[SID]>service cos-mode set cos-mode <cos-mode>
```

If the CoS mode is set to `default-cos`, you must define the Default CoS. Use the following command to define the Default CoS:

```
service[SID]>service default-cos set cos <cos>
```

Table 142 Ethernet Service CoS Mode CLI Parameters

Parameter	Input Type	Permitted Values	Description
cos-mode	Variable	default-cos preserve-sp-cos-decision	**default cos** - Frames passing through the service are assigned the default CoS defined below. This CoS value overrides whatever CoS may have been assigned at the service point or interface level. **preserve-sp-cos-decision** - The CoS of frames passing through the service is not modified by the service.
cos	Number	0 – 7	This value is assigned to frames at the service level if cos-mode is set to default-cos. Otherwise, this value is not used, and frames retain whatever CoS value they were assigned at the service point or logical interface level.

The following commands configure Service 10 to assign a CoS value of 7 to frames traversing the service:

```
service[10]>service cos-mode set cos-mode default-cos
service[10]>service default-cos set cos 7
```

The following command configures Service 10 to preserve the CoS decision made at the interface or service point level for frames traveling through the service:

```
service[10]>service cos-mode set cos-mode preserve-sp-cos-decision
```

Configuring a Service's EVC ID and Description (CLI)

To add or change the EVC ID of a service, go to service view for the service and enter the following command:

```
service[SID]>service evcid set <evcid>
```

To display a service's EVC ID, go to service view for the service and enter the following command:

```
service[SID]>service evcid show
```

To add or change the EVC description of a service, go to service view for the service and enter the following command:

```
service[SID]>service description set <evc description>
```

To display a service's EVC description, go to service view for the service and enter the following command:

```
service[SID]>service description show
```

Table 143 Ethernet Service EVC CLI Parameters

Parameter	Input Type	Permitted Values	Description
evcid	Text String	Up to 20 characters.	Defines an Ethernet Virtual Connection (EVC) ID. This parameter does not affect the network element's behavior, but is used by the NMS for topology management.
evc descripti on	Text String	Up to 64 characters.	A text escription of the service. This parameter does not affect the network element's behavior, but is used by the NMS for topology management.

The following commands add the EVC ID "East_West" and the EVC description "Line_to_Radio" to Service 10:

```
service[10]>service evcid set East_West
service[10]>service description set Line_to_Radio
```

Deleting a Service (CLI)

Before deleting a service, you must first delete any service points attached to the service (refer to Deleting a Service Point (CLI)).

Use the following command to delete a service:

```
root>ethernet service delete sid <sid>
```

Use the following command to delete a range of services:

```
root>ethernet service delete sid <sid> to <sid>
```

Table 144 Deleting Ethernet Service CLI Parameters

Parameter	Input Type	Permitted Values	Description
sid	Number	Any defined Service ID.	The Service ID.

The following command deletes Service 10:

```
root>ethernet service delete sid 10
```

The following command deletes Services 10 through 15:

```
root>ethernet service delete sid 10 to 15
```

21.1.4 Configuring Service Points (CLI)

This section includes:

- Service Points Overview (CLI)
- Service Point Classification (CLI)
- Adding a Service Point (CLI)
- Configuring Service Point Ingress Attributes (CLI)
- Configuring Service Point Egress Attributes (CLI)
- Displaying Service Point Attributes (CLI)
- Deleting a Service Point (CLI)

21.1.4.1 Service Points Overview (CLI)

Service points are logical interfaces within a service. A service point is a logical entity attached to a physical or logical interface. Service points define the movement of frames through the service. Each service point includes both ingress and egress attributes.

Each service point for a Point-to-Point or Multipoint service can be either a Service Access Point (SAP) or a Service Network Point (SNP). A Point-to-Point service can also use Pipe service points.

An SAP is equivalent to a UNI in MEF terminology and defines the connection of the user network with its access points. SAPs are used for Point-to-Point and Multipoint traffic services.

An SNP is equivalent to an NNI or E-NNI in MEF terminology and defines the connection between the network elements in the user network. SNPs are used for Point-to-Point and Multipoint traffic services.

A Pipe service point is used to create traffic connectivity between two ports in a port-based manner (Smart Pipe). In other words, all the traffic from one port passes to the other port.

Management services utilize Management (MNG) service points.

A Point-to-Point or Multipoint service can hold up to 32 service points. A management service can hold up to 30 service points.

Table 145 summarizes the service point types available per service type.

Table 145 Service Points per Service Type

		Service Point Type			
		MNG	**SAP**	**SNP**	**Pipe**
Service Type	Management	Yes	No	No	No
	Point-to-Point	No	Yes	Yes	Yes
	Multipoint	No	Yes	Yes	No

Table 146 shows which service point types can co-exist on the same interface.

Table 146 Service Point Types per Interface

	MNG	**Pipe**
MNG	Only one MNG SP is allowed per interface.	Yes
SAP	Yes	No
SNP	Yes	No
PIPE	Yes	Only one Pipe SP is allowed per interface.

Service Point Classification (CLI)

This section includes:

- Overview of Service Point Classification (CLI)
- SAP Classification (CLI)
- SNP Classification (CLI)
- Pipe Service Point Classification (CLI)
- MNG Service Point Classification (CLI)

Overview of Service Point Classification (CLI)

Service points connect the service to the network element interfaces. It is crucial that the network element have a means to classify incoming frames to the proper service point. This classification process is implemented by means of a parsing encapsulation rule for the interface associated with the service point. This rule is called the Interface Type, and is based on a key consisting of:

The Interface ID of the interface through which the frame entered.

The frame's C-VLAN and/or S-VLAN tags.

The Interface Type provides a definitive mapping of each arriving frame to a specific service point in a specific service. Since more than one service point may be associated with a single interface, frames are assigned to the earliest defined service point in case of conflict.

SAP Classification (CLI)

SAPs can be used with the following Interface Types:

- All to one – All C-VLANs and untagged frames that enter the interface are classified to the same service point.
- Dot1q – A single C-VLAN is classified to the service point.
- QinQ – A single S-VLAN and C-VLAN combination is classified to the service point.
- Bundle C-Tag – A set of multiple C-VLANs is classified to the service point.
- Bundle S-Tag – A single S-VLAN and a set of multiple C-VLANs are classified to the service point.

SNP Classification (CLI)

- SNPs can be used with the following Attached Interface Types:
- Dot1q – A single C-VLAN is classified to the service point.
- S-Tag – A single S-VLAN is classified to the service point.

Pipe Service Point Classification (CLI)

- Pipe service points can be used with the following Attached Interface Types:
- Dot1q – All C-VLANs and untagged frames that enter the interface are classified to the same service point.
- S-Tag – All S-VLANs and untagged frames that enter the interface are classified to the same service point.

MNG Service Point Classification (CLI)

- Management service points can be used with the following Interface Types:
- Dot1q – A single C-VLAN is classified to the service point.
- S-Tag – A single S-VLAN is classified to the service point.
- QinQ – A single S-VLAN and C-VLAN combination is classified to the service point.

Table 147 and Table 148 show which service point – Interface Type combinations can co-exist on the same interface.

Table 147 Legal Service Point – Interface Type Combinations per Interface – SAP and SNP

	SP Type	SAP				SNP	
SP Type	**Attached Interface Type**	**802.1q**	**Bundle -C**	**Bundle -S**	**All to One**	**802.1q**	**S-Tag**
SAP	**802.1q**	Yes	Yes	No	No	No	No
	Bundle-C	Yes	Yes	No	No	No	No
	Bundle-S	No	No	Yes	No	No	No
	All to One	No	No	No	Only 1 All to One SP Allowed	No	No
	Q in Q	No	No	Yes	No	No	No
SNP	**802.1q**	No	No	No	No	Yes	No
	S-Tag	No	No	No	No	No	Yes
Pipe	**802.1q**	No	No	No	No	No	No
	S-Tag	No	No	No	No	No	No
MNG	**802.1q**	Yes	Yes	No	No	Yes	No
	Q in Q	No	No	Yes	No	No	No
	S-Tag	No	No	No	No	No	Yes

Table 148 Legal Service Point – Interface Type Combinations per Interface – Pipe and MNG

	SP Type	Pipe		MNG		
SP Type	**Attached Interface Type**	**802.1q**	**S-Tag**	**802.1q**	**Q in Q**	**S-Tag**
	802.1q	No	No	Yes	No	No
	Bundle-C	No	No	Yes	No	No

	SP Type	Pipe		MNG		
SP Type	**Attached Interface Type**	**802.1q**	**S-Tag**	**802.1q**	**Q in Q**	**S-Tag**
	Bundle-S	No	No	No	Yes	No
	All to One	No	No	No	No	No
	Q in Q	No	No	No	Yes	No
SNP	**802.1q**	No	No	Yes	No	No
	S-Tag	No	No	No	No	Yes
	802.1q	Only one Pipe SP Allowed	No	Yes	No	No
	S-Tag	No	Only one Pipe SP Allowed	No	No	Yes
MNG	**802.1q**	Yes	No	Only 1 MNG SP Allowed	No	No
	Q in Q	No	No	No	Only 1 MNG SP Allowed	No
	S-Tag	No	Yes	No	No	Only 1 MNG SP Allowed

Adding a Service Point (CLI)

The command syntax for adding a service point depends on the interface type of the service point. The interface type determines which frames enter the service via this service point.

Note: The service-bundle-id parameter is optional. If you do not use this parameter, Service Bundle ID 1 is assigned to the service point.Once a service point has been created, you cannot edit the Service Bundle ID. Instead, you must delete the service point and create a new service point with the desired Service Bundle ID. In the case of the management service point, in-band management must be disabled in order to delete the management service point.

To add a service point with an All-to-One interface type, go to service view for the service and enter the following command:

```
service[SID]>sp add sp-type <sp-type> int-type all-to-
one spid <sp-id> [interface|group] <interface|group> slot <slot>
port <port> sp-name <sp-name> service-bundle-id <service-bundle-
id>
```

To add a service point with a Dot1q interface type, go to service view for the service and enter the following command:

```
service[SID]>sp add sp-type <sp-type> int-type dot1q spid <sp-id>
[interface|group] <interface|group> slot <slot> port
<port> vlan <vlan> sp-name <sp-name> service-bundle-id <service-
bundle-id>
```

To add a service point with an S-Tag interface type, go to service view for the service and enter the following command:

```
service[SID]>sp add sp-type <sp-type> int-type s-tag spid <sp-id>
[interface|group] <interface|group> slot <slot> port
<port> vlan <vlan> sp-name <sp-name> service-bundle-id <service-
bundle-id>
```

To add a service point with a Bundle-C interface type, go to service view for the service and enter the following command:

```
service[SID]>sp add sp-type <sp-type> int-type bundle-c spid <sp-
id> [interface|group] <interface|group> slot <slot> port <port>
sp-name <sp-name> service-bundle-id <service-bundle-id>
```

To add a service point with a Bundle-S interface type, go to service view for the service and enter the following command:

```
service[SID]>sp add sp-type <sp-type> int-type bundle-s spid <sp-
id> [interface|group] <interface|group> slot <slot> port <port>
[outer-vlan <outer-vlan>|vlan <vlan>] sp-name <sp-name> service-
bundle-id <service-bundle-id>
```

Note: In SAP service points, use the parameter `outer-vlan`. In SP service points, use the parameter `vlan`.

To add a service point with a Q-in-Q interface type, go to service view for the service and enter the following command:

```
service[SID]>sp add sp-type <sp-type> int-type qinq spid <sp-id>
[interface|group] <interface|group> slot <slot> port <port> outer-
vlan <outer-vlan> inner-vlan <inner-vlan> sp-name <sp-name>
service-bundle-id <service-bundle-id>
```

To add a Pipe service point, go to service view for the service and enter the following command:

```
service[SID]>sp add sp-type pipe int-type <int-type> spid <sp-id>
[interface|group] <interface|group> slot <slot> port <port> sp-
name <sp-name> service-bundle-id <service-bundle-id>
```

Table 149 Add Service Point CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-type	Variable	sap snp pipe mng	SAP - Service Access Point SNP - Service Network Point PIPE - Pipe service point MNG - Management service point
int-type	Variable	all-to-one dot1q s-tag bundle-c-tag bundle-s-tag qinq	Determines which frames enter the service via this service point, based on the frame's VLAN tagging. Since more than one service point may be associated with a single interface, frames are assigned to the earliest defined service point in case of conflict. all-to-one - All C-VLANs and untagged frames that enter the interface are classified to the service point. Only valid for SAP service point types. dot1q - A single C-VLAN is classified to the service point. Valid for all service point types. s-tag - A single S- VLAN is classified to the service point. Valid for SNP and MNG service point types. bundle-c-tag - A set of multiple C-VLANs is classified to the service point. Only valid for SAP service point types. bundle-s-tag - A single S-VLAN and a set of multiple C-VLANs are classified to the service point. Only valid for SAP service point types. qinq - A single S-VLAN and C-VLAN combination is classified to the service point. Valid for SAP and MNG service point types.
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	This ID is unique within the service.

Parameter	Input Type	Permitted Values	Description
interface	Variable	eth radio	The Interface type for the service point: eth - An Ethernet interface. radio - A radio interface. When you are defining the service point on a group, such as a LAG, use the group parameter instead of the interface parameter.
group	Variable	rp1 rp2 rp3 rp4 lag1 lag2 lag3 lag4 mc-abc1 mc-abc2 mc-abc3 mc-abc4	When you are defining the service point on an HSB group (rp1 - rp-4), a LAG (lag1 - lag4), or a Multi-Carrier ABC group (mc-abc1 - mc-abc4), use this parameter instead of the interface parameter to identify the group. The group must be defined before you add the service point. **Note**: Multi-Carrier ABC and HSB protection are only relevant for PTP 850E units.
slot	Number	Ethernet: 1 Radio: 2	
port	Number	For an Ethernet interface: 1-3 For a radio interface in PTP 850E units: 1-2 For a radio interface in PTP 850E: 1	The port or radio carrier on which the service point is located.

Parameter	Input Type	Permitted Values	Description
vlan	Number or Variable	1-4094 (except 4092 which is reserved for the default management service), or Untagged	Defines the VLAN classified to the service point. This parameter should not be included for service points with an interface type of bundle-C-tag. For instructions on attaching a bundled VLAN, refer to Attaching a VLAN Bundle to a Service Point (CLI). This parameter is also not relevant for: Service points with an interface type of qinq and all-to-one. Pipe service points.
outer-vlan	Number	1-4094 (except 4092, which is reserved for the default management service), or Untagged	Defines the S-VLAN classified to the service point. This parameter is only relevant for service points with the interface type bundle-s-tag or qinq.
inner-vlan	Number	1-4094 (except 4092, which is reserved for the default management service), or Untagged	Defines the C-VLAN classified to the service point. This parameter is only relevant for service points with the interface type qinq.
sp-name	Text string	Up to 20 characters.	A descriptive name for the service point (optional).

Parameter	Input Type	Permitted Values	Description
service-bundle-id	Number	If H-QoS is enabled on the interface to which the service bundle is assigned, the range is 1-6. Otherwise, the only available service bundle ID is 1. See Enabling Hierarchical QoS (H-QoS) (CLI). In System Release 11.9, H-QoS is only available with PTP 850C. For PTP 850E, H-QoS is planned for future release.	The service bundle assigned to the service point. This parameter is optional. If you do not include this parameter in the command, Service Bundle ID 1 is assigned to the service point.

The following command adds an SAP service point with Service Point ID 10 to Service 37, with interface type dot1q. This service point is located on radio carrier 1. VLAN ID 100 is classified to this service point.

```
service[37]>sp add sp-type sap int-type dot1q spid 10 interface
radio slot 2 port 1 vlan 100 sp-name Radio
```

The following command adds an SAP service point with Service Point ID 10 to Service 37, with interface type bundle-s-tag. This service point is located on radio carrier 2 in a PTP 850E unit. S-VLAN 100 is classified to the service point.

```
service[37]>sp add sp-type sap int-type bundle-s-tag spid 10
interface radio slot 2 port 2 outer-vlan 100 sp-name Radio
```

The following command adds an SAP service point with Service Point ID 10 to Service 37, with interface type qinq. This service point is located on radio carrier 2 in a PTP 850E unit. S-VLAN 100 and C-VLAN 200 are classified to the service point.

```
service[37]>sp add sp-type sap int-type qinq spid 10 interface
radio slot 2 port 2 outer-vlan 100 inner-vlan 200 sp-name Radio
```

The following command adds an SAP service point with Service Point ID 10 to Service 37, with interface type all-to-one. This service point is located on radio carrier 1. All traffic entering the system from that port is classified to the service point.

```
service[37]>sp add sp-type sap int-type all-to-one spid 10
interface radio slot 2 port 1 sp-name "all-to-one"
```

The following command adds an SNP service point with Service Point ID 10 to Service 37, with interface type s-tag. This service point is located on radio carrier 1. S-VLAN 100 is classified to the service point.

```
service[37]>sp add sp-type snp int-type s-tag spid 10 interface
radio slot 2 port 1 vlan 100 sp-name Radio
```

The following command adds an SAP service point with Service Point ID 7 to Service 36, with interface type dot1q. This service point is connected to HSB group 1 (rp1). VLAN ID 100 is classified to the service point.

```
service[36]>sp add sp-type sap int-type dot1q spid 7 group
rp1 vlan 100 sp-name test1
```

The following command adds a Pipe service point with Service Point ID 1 to Service 1, with interface type dot1q. This service point is connected to Eth1.

```
service[1]>sp add sp-type pipe int-type dot1q spid 1 interface eth
slot 1 port 1 sp-name pipe_dot1q
```

The following commands create a Smart Pipe service between Eth1 and radio carrier 1. This service carries S-VLANs and untagged frames between the two interfaces:

```
root> ethernet service add type p2p sid 10 admin operational evc-
id test description east_west

root>

root> ethernet service sid 10

service[10]>

service[10]>sp add sp-type pipe int-type s-tag spid 1 interface
eth slot 1 port 1 sp-name test1

service[10]>

service[10]>sp add sp-type pipe int-type s-tag spid 2 interface
radio slot 2 port 1 sp-name test2

service[10]>
```

Configuring Service Point Ingress Attributes (CLI)

A service point's ingress attributes are attributes that operate upon frames ingressing via the service point. This includes how the service point handles the CoS of ingress frames and how the service point forwards frames to their next destination within the service.

This section includes:

- Enabling and Disabling Broadcast Frames (CLI)
- CoS Preservation and Modification on a Service Point (CLI)
- Enabling and Disabling Flooding (CLI)

Enabling and Disabling Broadcast Frames (CLI)

To determine whether frames with a broadcast destination MAC address are allowed to ingress the service via this service point, go to service view for the service and enter the following command:

```
service[SID]>sp broadcast set spid <sp-id> state <state>
```

Table 150 Enable/Disable Broadcast Frames CLI Parameters

Parameter	InputType	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
state	Variable	allow disable	Determines whether frames with a broadcast destination MAC address are allowed to ingress the service via this service point.

The following command allows frames with a broadcast destination MAC address to ingress Service 37 via Service Point 1.

```
service[37]>sp broadcast set spid 1 state allow
```

The following command prevents frames with a broadcast destination MAC address from ingressing Service 37 via Service Point 1.

```
service[37]>sp broadcast set spid 1 state disable
```

CoS Preservation and Modification on a Service Point (CLI)

The CoS of frames traversing a service can be modified on the logical interface, service point, and service level. The service point can override the CoS decision made at the interface level. The service, in turn, can modify the CoS decision made at the service point level.

To determine whether the service point modifies CoS decisions made at the interface level, go to service view for the service and enter the following command:

```
service[SID]> sp cos-mode set spid <sp-id> mode <cos mode>
```

If you set cos-mode to `sp-def-cos`, you must then configure a default CoS. This CoS is applied to frames that ingress the service point, but can be overwritten at the service level.
To configure the default CoS, go to service view for the service and enter the following command:

```
service[SID]>sp sp-def-cos set spid <sp-id> cos <cos>
```

Table 151 Service Point CoS Preservation CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.

Parameter	Input Type	Permitted Values	Description
cos mode	Variable	sp-def-cos interface-decision	sp-def-cos - The service point re-defines the CoS of frames that pass through the service point, according to the Default CoS (below). This decision can be overwritten on the service level. interface-decision - The service point preserves the CoS decision made at the interface level. This decision can still be overwritten at the service level.
cos	Number	0 – 7	If cos-mode is sp-def-cos, this is the CoS assigned to frames that pass through the service point. This decision can be overwritten on the service level.

The following commands configure Service Point 1 in Service 37 to apply a CoS value of 5 to frames that ingress the service point:

```
service[37]>sp cos-mode set spid 1 mode sp-def-cos
service[37]>sp sp-def-cos set spid 1 cos 5
```

The following command configures Service Point 1 in Service 37 to preserve the CoS decision made at the interface level for frames that ingress the service point:

```
service[37]>sp cos-mode set spid 1 mode interface-decision
```

Enabling and Disabling Flooding (CLI)

The ingress service point for a frame can forward the frame within the service by means of flooding or dynamic MAC address learning in the service.
To enable or disable forwarding by means of flooding for a service point, go to service view for the service and enter the following command:

```
service[SID]>sp flooding set spid <sp-id> state <flooding state>
```

Table 152 Service Point Enable/Disable Flooding CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
state	Variable	Allow disable	Determines whether incoming frames with unknown MAC addresses are forwarded to other service points via flooding.

The following command configures Service Point 1 in Service 37 to flood incoming frames with unknown MAC addresses to other service points:

```
service[37]>sp flooding set spid 1 state allow
```

The following command configures Service Point 1 in Service 37 not to flood incoming frames with unknown MAC addresses to other service points:

```
service[37]>sp flooding set spid 1 state disable
```

Configuring Service Point Egress Attributes (CLI)

A service point's egress attributes are attributes that operate upon frames ingressing via the service point. This includes VLAN preservation and marking attributes.

This section includes:

- Configuring VLAN and CoS Preservation (CLI)
- Configuring Service Bundles (CLI)
- Attaching a VLAN Bundle to a Service Point (CLI)

Configuring VLAN and CoS Preservation (CLI)

CoS and VLAN preservation determines whether the CoS and/or VLAN IDs of frames egressing the service via the service point are restored to the values they had when the frame entered the service.

This section includes:

- Configuring C-VLAN CoS Preservation (CLI)
- Configuring C-VLAN Preservation (CLI)
- Configuring S-VLAN CoS Preservation (CLI)

21.1.4.2 Configuring C-VLAN CoS Preservation (CLI)

To configure CoS preservation for C-VLAN-tagged frames, go to service view for the service and enter the following command:

```
service[SID]>sp cvlan-cos-preservation-mode set spid <sp-id> mode
<c-vlan cos preservation mode>
```

Table 153 C-VLAN CoS Preservation Mode CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
c-vlan cos preservation mode	Variable	enable disable	Select enable or disable to determine whether the original C-VLAN CoS value is preserved or restored for frames egressing the service point. enable - the C-VLAN CoS value of frames egressing the service point is the same as the value when the frame entered the service. disable - the C-VLAN CoS value of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking (see Configuring Marking (CLI)).

The following command enables C-VLAN CoS preservation for Service Point 1 on Service 37:

```
service[37]>sp cvlan-cos-preservation-mode set spid 1 mode enable
```

The following command disables C-VLAN CoS preservation for Service Point 1 on Service 37:

```
service[37]>sp cvlan-cos-preservation-mode set spid 1 mode disable
```

21.1.4.3 Configuring C-VLAN Preservation (CLI)

To configure VLAN preservation for C-VLAN-tagged frames, go to service view for the service and enter the following command:

```
service[SID]>sp cvlan-preservation-mode set spid <sp-id> mode <c-
vlan preservation mode>
```

Table 154 C-VLAN Preservation CLI Parameters

Parameter	InputType	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.

Parameter	InputType	Permitted Values	Description
c-vlan preservation mode	Variable	enable disable	Determines whether the original C-VLAN ID is preserved or restored for frames egressing from the service point. enable - The C-VLAN ID of frames egressing the service point is the same as the C-VLAN ID when the frame entered the service. disable - The C-VLAN ID of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking (see Configuring Marking (CLI)).

The following command enables C-VLAN preservation for Service Point 1 on Service 37:

```
service[37]>sp cvlan-preservation-mode set spid 1 mode enable
```

The following command disables C-VLAN preservation for Service Point 1 on Service 37:

```
service[37]>sp cvlan-preservation-mode set spid 1 mode disable
```

21.1.4.4 Configuring S-VLAN CoS Preservation (CLI)

To configure CoS preservation for S-VLAN-tagged frames, go to service view for the service and enter the following command:

```
service[SID]>sp svlan-cos-preservation-mode set spid <sp-id> mode
<s-vlan cos preservation mode>
```

Table 155 S-VLAN CoS Preservation CLI Parameters

Parameter	Input Type	PermittedValues	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
s-vlan cos preservation mode	Variable	enable disable	Select enable or disable to determine whether the original S-VLAN CoS value is preserved or restored for frames egressing the service point. enable - the S-VLAN CoS value of frames egressing the service point is the same as the value when the frame entered the service. disable - the S-VLAN CoS value of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking (see Configuring Marking (CLI)).

The following command enables S-VLAN CoS preservation for Service Point 1 on Service 37:

```
service[37]>sp svlan-cos-preservation-mode set spid 1 mode enable
```

The following command disables S-VLAN CoS preservation for Service Point 1 on Service 37:

```
service[37]>sp svlan-cos-preservation-mode set spid 1 mode disable
```

Configuring Service Bundles (CLI)

You can use service bundles to personalize common sets of egress queue attributes that can be applied to multiple service points. In this version only one service bundle is supported.
To assign a service point to a service bundle, go to service view for the service and enter the following command:

```
service[SID]>sp egress-service-bundle set spid 1 service-bundle-id
<service-bundle-id>
```

Table 156 Service Bundle CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
service-bundle-id	Number	1 – 63 **Note**: In the current release, only Service Bundle 1 is supported.	The service bundle assigned to the service point.

The following command assigns Service Bundle 1 to Service Point 1 in Service 37.

```
service[37]>sp egress-service-bundle set spid 1 service-bundle-id
1
```

Attaching a VLAN Bundle to a Service Point (CLI)

For service points with an interface type of bundle-C-tag or bundle-S-tag, you must classify a group of VLANs (VLAN Bundle) to the service point.
To classify a VLAN Bundle to a bundle-c-tag or bundle s-tag service point, go to service view for the service and enter the following command:

```
service[SIP]>sp bundle cvlan attach spid <sp-id> vlan <vlan> to-
vlan <to-vlan>
```

To remove a VLAN Bundle from a bundle-c-tag or bundle-s-tag service point, go to service view for the service and enter the following command:

```
service[SIP]>sp bundle cvlan remove spid <sp-id> vlan <vlan> to-
vlan <to-vlan>
```

To remove untagged frames from a bundle-c-tag or bundle s-tag service point, go to service view for the service and enter the following command:

```
service[SIP]>sp bundle remove untagged spid <sp-id>
```

To display a service point's attributes, including the VLANs classified to a bundle service point, go to service view for the service to which the service point belongs and enter the following command:

```
service[SID]>sp service-point-info show spid <sp-id>
```

Table 157 VLAN Bundle to Service Point CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
vlan	Number	1-4094 (except 4092, which is reserved for the default management service)	The C-VLAN at the beginning of the range of the VLAN Bundle.
to-vlan	Number	1-4094 (except 4092, which is reserved for the default management service)	The C-VLAN at the end of the range of the VLAN Bundle.

The following command classifies C-VLANs 100 through 200 to Service Point 1 in Service 37:

```
service[37]>sp bundle cvlan attach spid 1 vlan 100 to-vlan 200
```

The following command removes C-VLANs 100 through 200 from Service Point 1 in Service 37:

```
service[37]>sp bundle cvlan remove spid 1 vlan 100 to-vlan 200
```

Displaying Service Point Attributes (CLI)

To display a service point's attributes, go to service view for the service to which the service point belongs and enter the following command:

```
service[SID]>sp service-point-info show spid <sp-id>
```

Table 158 Display Service Point Attributes CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.

The following command displays the attributes of Service Point 1 in Service 37:

```
service[37]>sp service-point-info show spid 1
```

Deleting a Service Point (CLI)

You can only delete a service point if no VLAN bundles are attached to the service point. This is only relevant if the interface type of the service point is bundle-c-tag or bundle-s-tag. For more information, refer to Attaching a VLAN Bundle to a Service Point (CLI).

To delete a service point from a service, go to service view for the service and enter the following command:

```
service[SID]>sp delete spid <sp-id>
```

Table 159 Delete Service Point Attributes CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.

The following command deletes Service Point 10 from Service 37:

```
service[37]>sp delete spid 10
```

21.1.5 Defining the MAC Address Forwarding Table for a Service (CLI)

This section includes:

- MAC Address Forwarding Table Overview (CLI)
- Setting the Maximum Size of the MAC Address Forwarding Table (CLI)
- Setting the MAC Address Forwarding Table Aging Time (CLI)
- Adding a Static MAC Address to the Forwarding Table (CLI)
- Displaying the MAC Address Forwarding Table (CLI)
- There are two options for displaying the MAC address forwarding table:
  - **Current** – When the display command is given, data is collected directly from the device hardware. This provides an up-to-date version of the table but may take a few seconds. In a network with numerous devices, this delay could become significant.
  - **Saved** – The MAC address forwarding table is cached at least once per day and up to four times per day (user configurable, as described below). Up to 1,000 learned MAC addresses along with their VLANs can be cached. When the display command is given, the latest cached version is displayed. This may not be as up-to-date as the current version, but it is displayed much more quickly.

Every time you display the MAC address forwarding table, you can use a command parameter to determine whether to display the **Current** or **Saved** version.

The following command determines how many times per day the MAC forwarding table is cached. By default, the table is cached once per day, at midnight. Using the following command, you can configure the table to be cached one, two, three, or four times daily.

```
root>ethernet generalcfg mac-learning-table updates-per-day set
updates <1-4>
```

The MAC forwarding table is also cached every time the device is rebooted, between 15 and 30 minutes after the reboot.

To display the current number of updates configured, enter the following command:

```
root>ethernet generalcfg mac-learning-table updates-per-day show
```

The MAC address forwarding table includes the following columns:

Number – The position of the MAC address in the table.

Service ID – The Ethernet Service on which the MAC address was learned.

C-VLAN – The C-VLAN on which the MAC address was learned, if any. This column can be hidden using the detailed-vlan no parameter.

S-VLAN – The S-VLAN on which the MAC address was learned, if any. This column can be hidden using the detailed-vlan no parameter.

Note: For Bundle-C and Bundle-S service points, the table lists the MAC addresses in duplicate rows, one for each VLAN in the bundle range.

Port – The interface on which the MAC address was learned.

MAC – The MAC address.,

Entry Type – Dynamic or Static.

To display the MAC address forwarding table for the entire unit, enter the following command:

root> ethernet generalcfg mac-learning-table show mac-type <static|dynamic|all> collection-type <saved|current> detailed-vlan <yes|no>

To display the MAC address forwarding table for a service, go to service view for the service and enter the following command:

```
service[SID]>service mac-learning-table show mac-type
<static|dynamic|all> collection-type <saved|current> detailed-vlan
<yes|no>
```

To display the MAC address forwarding table for an interface, go to interface view for the interface and enter the following command:

eth type xxx[1/x]>mac-learning-table show mac-type <static|dynamic|all> collection-type <saved|current> detailed-vlan <yes|no>

For example, to display the latest cached record of all dynamic entries in the MAC address forwarding table for Eth 3, enter the following commands:

```
root> ethernet interfaces eth slot 1 port 3
eth type eth[1/1]mac-learning-table show mac-type dynamic
collection-type saved detailed-vlan yes
```

To display the most up-to-date version of the complete MAC address forwarding table for the entire unit, enter the following command:

root> ethernet generalcfg mac-learning-table show mac-type all collection-type current detailed-vlan yes

If the mac-type parameter is not specified, all entries are displayed.

If the collection-type parameter is not specified, the cached (saved) table is displayed.

If the detailed-vlan parameter is not specified, the VLAN columns are displayed.

The following is an example of the command output for the entire unit:

```
root>ethernet generalcfg mac-learning-table show mac-type all collection-type saved detailed-vlan yes
=============================================================================================================
| Number# | Service| Service    | Port          | S-Vlan      | C-Vlan      | MAC               | Entry    |
|         |   ID#  | Point ID#  |               |             |             |                   | Type     |
=============================================================================================================
|       1|       1|          2|lagl           |100          |3            |d4:6f:bc:89:10:d3| dynamic  |
|       2|       1|          2|lagl           |100          |4            |d4:6f:bc:89:10:d3| dynamic  |
|       3|       1|          2|lagl           |100          |3            |e4:ef:bc:89:10:d3| dynamic  |
|       4|       1|          2|lagl           |100          |4            |e4:ef:bc:89:10:d3| dynamic  |
|       5|       1|          2|lagl           |100          |3            |da:3f:bc:89:10:d3| dynamic  |
|       6|       1|          2|lagl           |100          |4            |da:3f:bc:89:10:d3| dynamic  |
|       7|       1|          2|lagl           |100          |3            |d2:0c:bc:89:10:d3| dynamic  |
|       8|       1|          2|lagl           |100          |4            |d2:0c:bc:89:10:d3| dynamic  |
|       9|       1|          2|lagl           |100          |3            |e4:39:bc:89:10:d3| dynamic  |
|      10|       1|          2|lagl           |100          |4            |e4:39:bc:89:10:d3| dynamic  |
|      11|       1|          1|enhanced-abc  1/1|N.A.         |3            |00:00:bb:00:00:02| static   |
|      12|       1|          1|enhanced-abc  1/1|N.A.         |5            |00:00:bb:00:00:02| static   |
|      13|       1|          2|lagl           |100          |3            |da:2d:bc:89:10:d3| dynamic  |
|      14|       1|          2|lagl           |100          |4            |da:2d:bc:89:10:d3| dynamic  |
|      15|       1|          2|lagl           |100          |3            |de:80:bc:89:10:d3| dynamic  |
|      16|       1|          2|lagl           |100          |4            |de:80:bc:89:10:d3| dynamic  |
|      17|       1|          2|lagl           |100          |3            |dc:84:bc:89:10:d3| dynamic  |
|      18|       1|          2|lagl           |100          |4            |dc:84:bc:89:10:d3| dynamic  |
|      19|       1|          2|lagl           |100          |3            |e2:4d:bc:89:10:d3| dynamic  |
|      20|       1|          2|lagl           |100          |4            |e2:4d:bc:89:10:d3| dynamic  |
|      21|       1|          2|lagl           |100          |3            |d2:41:bc:89:10:d3| dynamic  |
|      22|       1|          2|lagl           |100          |4            |d2:41:bc:89:10:d3| dynamic  |
|      23|       1|          2|lagl           |100          |3            |e0:af:bc:89:10:d3| dynamic  |
|      24|       1|          2|lagl           |100          |4            |e0:af:bc:89:10:d3| dynamic  |
|      25|       1|          2|lagl           |100          |3            |d2:45:bc:89:10:d3| dynamic  |
|      26|       1|          2|lagl           |100          |4            |d2:45:bc:89:10:d3| dynamic  |
|      27|       1|          2|lagl           |100          |3            |e4:68:bc:89:10:d3| dynamic  |
|      28|       1|          2|lagl           |100          |4            |e4:68:bc:89:10:d3| dynamic  |
|      29|       1|          2|lagl           |100          |3            |de:fb:bc:89:10:d3| dynamic  |
|      30|       1|          2|lagl           |100          |4            |de:fb:bc:89:10:d3| dynamic  |
|      31|       1|          2|lagl           |100          |3            |d0:f2:bc:89:10:d3| dynamic  |
|      32|       1|          2|lagl           |100          |4            |d0:f2:bc:89:10:d3| dynamic  |
|      33|       1|          2|lagl           |100          |3            |de:62:bc:89:10:d3| dynamic  |
|      34|       1|          2|lagl           |100          |4            |de:62:bc:89:10:d3| dynamic  |
|      35|       1|          2|lagl           |100          |3            |d8:a2:bc:89:10:d3| dynamic  |
|      36|       1|          2|lagl           |100          |4            |d8:a2:bc:89:10:d3| dynamic  |
|      37|       1|          2|lagl           |100          |3            |b6:6e:bc:89:10:d3| dynamic  |
|      38|       1|          2|lagl           |100          |4            |b6:6e:bc:89:10:d3| dynamic  |
|      39|       1|          2|lagl           |100          |3            |d6:0b:bc:89:10:d3| dynamic  |
|      40|       1|          2|lagl           |100          |4            |d6:0b:bc:89:10:d3| dynamic  |
|      41|       1|          2|lagl           |100          |3            |e2:38:bc:89:10:d3| dynamic  |
|      42|       1|          2|lagl           |100          |4            |e2:38:bc:89:10:d3| dynamic  |
```

Note that if a flush is performed on the MAC address forwarding table (see Error! Not a valid bookmark self-reference., the cached table is not flushed and is inaccurate until the next caching takes place.

In a configuration with TCC Redundancy, in the event of switchover the cached table in the newly active TCC is empty until the next caching takes places.

However, if you attempt to display the cached (saved) table at a time when the cache is empty, the device will automatically display the current table rather than the saved table.

- Flushing the MAC Address Forwarding Table (CLI)
- Enabling MAC Address Learning on a Service Point (CLI)

MAC Address Forwarding Table Overview (CLI)

PTP 850 performs MAC address learning per service. PTP 850 can learn up to 131,072 MAC addresses.

If necessary due to security issues or resource limitations, you can limit the size of the MAC address forwarding table. The maximum size of the MAC address forwarding table is configurable per service in granularity of 16 entries.

When a frame arrives via a specific service point, the learning mechanism checks the MAC address forwarding table for the service to which the service point belongs to determine whether that MAC address is known to the service. If the MAC address is not found, the learning mechanism adds it to the table.

In parallel with the learning process, the forwarding mechanism searches the service's MAC forwarding table for the frame's MAC address. If a match is found, the frame is forwarded to the service point associated with the MAC address. If not, the frame is flooded to all service points in the service.

Setting the Maximum Size of the MAC Address Forwarding Table (CLI)

To limit the size of the MAC address forwarding table for a specific service, go to service view for the service and enter the following command:

```
service[SID]>service mac-limit-value set <mac limit>
```

Table 160 MAC Address Forwarding Table Maximum Size CLI Parameters

Parameter	Input Type	Permitted Values	Description
mac limit	Number	16 to 131,072, in multiples of 16	The maximum MAC address table size for the service. This maximum only applies to dynamic, not static, MAC address table entries.

The following command limits the number of dynamic MAC address forwarding table entries for Service 10 to 128:

```
service[10]>service mac-limit-value set 128
```

Setting the MAC Address Forwarding Table Aging Time (CLI)

You can configure a global aging time for dynamic entries in the MAC address forwarding table. Once this aging time expires for a specific table entry, the entry is erased from the table.

To set the global aging time for the MAC address forwarding table, enter the following command:

```
root> ethernet service learning-ageing-time set time <time>
```

To display the global aging time for the MAC address forwarding table, enter the following command:

```
root> ethernet service learning-ageing-time show
```

Table 161 MAC Address Forwarding Table Aging Time CLI Parameters

Parameter	Input Type	Permitted Values	Description
time	Number	15 - 3825	The global aging time for the MAC address forwarding table, in seconds.

The following command sets the global aging time to 2500 seconds:

```
root> ethernet service learning-ageing-time set time 2500
```

Adding a Static MAC Address to the Forwarding Table (CLI)

You can add static entries to the MAC forwarding table. The global aging timer does not apply to static entries, and they are not counted with respect to the maximum size of the MAC address forwarding table. It is the responsibility of the user not to use all the entries in the table if the user also wants to utilize dynamic MAC address learning.

To add a static MAC address to the MAC address forwarding table, go to service view for the service to which you want to add the MAC address and enter the following command:

```
service[SID]>service mac-learning-table set-static-
mac <static mac> spid <sp-id>
```

To delete a static MAC address from the MAC address forwarding table, go to service view for the service from which you want to delete the MAC address and enter the following command:

```
service[SID]>service mac-learning-table del-static-
mac <static mac> spid <sp-id>
```

Table 162 Adding Static Address to MAC Address Forwarding Table CLI Parameters

Parameter	Input Type	Permitted Values	Description
static mac	Six groups of two hexadecimal digits		The MAC address.
sp-id	Number	1-32	The Service Point ID of the service point associated with the MAC address.

The following command adds MAC address 00:11:22:33:44:55 to the MAC address forwarding table for Service 10, and associates the MAC address with Service Point ID 1 on Service 10:

```
service[10]>service mac-learning-table set-static-
mac 00:11:22:33:44:55 spid 1
```

The following command deletes MAC address 00:11:22:33:44:55, associated with Service Point 1, from the MAC address forwarding table for Service 10:

```
service[10]>service mac-learning-table del-static-
mac 00:11:22:33:44:55 spid 1
```

Displaying the MAC Address Forwarding Table (CLI)

You can display the MAC address forwarding table for an interface, a service, or for the entire unit.

There are two options for displaying the MAC address forwarding table:

- **Current** – When the display command is given, data is collected directly from the device hardware. This provides an up-to-date version of the table but may take a few seconds. In a network with numerous devices, this delay could become significant.
- **Saved** – The MAC address forwarding table is cached at least once per day and up to four times per day (user configurable, as described below). Up to 1,000 learned MAC addresses along with their VLANs can be cached. When the display command is given, the latest cached version is displayed. This may not be as up-to-date as the current version, but it is displayed much more quickly.

Every time you display the MAC address forwarding table, you can use a command parameter to determine whether to display the **Current** or **Saved** version.

The following command determines how many times per day the MAC forwarding table is cached. By default, the table is cached once per day, at midnight. Using the following command, you can configure the table to be cached one, two, three, or four times daily.

```
root>ethernet generalcfg mac-learning-table updates-per-day set updates
<1-4>
```

The MAC forwarding table is also cached every time the device is rebooted, between 15 and 30 minutes after the reboot.

To display the current number of updates configured, enter the following command:

```
root>ethernet generalcfg mac-learning-table updates-per-day show
```

The MAC address forwarding table includes the following columns:

- **Number** – The position of the MAC address in the table.
- **Service ID** – The Ethernet Service on which the MAC address was learned.
- **C-VLAN** – The C-VLAN on which the MAC address was learned, if any. This column can be hidden using the detailed-vlan no parameter.
- **S-VLAN** – The S-VLAN on which the MAC address was learned, if any. This column can be hidden using the detailed-vlan no parameter.

Note: For Bundle-C and Bundle-S service points, the table lists the MAC addresses in duplicate rows, one for each VLAN in the bundle range.

- **Port** – The interface on which the MAC address was learned.
- **MAC** – The MAC address.,
- **Entry Type** – Dynamic or Static.

To display the MAC address forwarding table for the entire unit, enter the following command:

```
root> ethernet generalcfg mac-learning-table show mac-type
<static|dynamic|all> collection-type <saved|current> detailed-vlan
<yes|no>
```

To display the MAC address forwarding table for a service, go to service view for the service and enter the following command:

```
service[SID]>service mac-learning-table show mac-type
<static|dynamic|all> collection-type <saved|current> detailed-vlan
<yes|no>
```

To display the MAC address forwarding table for an interface, go to interface view for the interface and enter the following command:

```
eth type xxx[1/x]>mac-learning-table show mac-type <static|dynamic|all>
collection-type <saved|current> detailed-vlan <yes|no>
```

For example, to display the latest cached record of all dynamic entries in the MAC address forwarding table for Eth 3, enter the following commands:

```
root> ethernet interfaces eth slot 1 port 3
eth type eth[1/1]mac-learning-table show mac-type dynamic collection-type
saved detailed-vlan yes
```

To display the most up-to-date version of the complete MAC address forwarding table for the entire unit, enter the following command:

```
root> ethernet generalcfg mac-learning-table show mac-type all
collection-type current detailed-vlan yes
```

If the `mac-type` parameter is not specified, all entries are displayed.

If the `collection-type` parameter is not specified, the cached (saved) table is displayed.

If the `detailed-vlan` parameter is not specified, the VLAN columns are displayed.

The following is an example of the command output for the entire unit:

```
root>ethernet generalcfg mac-learning-table show mac-type all collection-type saved detailed-vlan yes
=============================================================================================================
| Number# | Service| Service    | Port          | S-Vlan      | C-Vlan      | MAC               | Entry    |
|         |   ID#  | Point ID# |               |             |             |                   | Type     |
=============================================================================================================
|       1|       1|          2|lagl           |100          |3            |d4:6f:bc:89:10:d3| dynamic  |
|       2|       1|          2|lagl           |100          |4            |d4:6f:bc:89:10:d3| dynamic  |
|       3|       1|          2|lagl           |100          |3            |e4:ef:bc:89:10:d3| dynamic  |
|       4|       1|          2|lagl           |100          |4            |e4:ef:bc:89:10:d3| dynamic  |
|       5|       1|          2|lagl           |100          |3            |da:3f:bc:89:10:d3| dynamic  |
|       6|       1|          2|lagl           |100          |4            |da:3f:bc:89:10:d3| dynamic  |
|       7|       1|          2|lagl           |100          |3            |d2:0c:bc:89:10:d3| dynamic  |
|       8|       1|          2|lagl           |100          |4            |d2:0c:bc:89:10:d3| dynamic  |
|       9|       1|          2|lagl           |100          |3            |e4:39:bc:89:10:d3| dynamic  |
|      10|       1|          2|lagl           |100          |4            |e4:39:bc:89:10:d3| dynamic  |
|      11|       1|          1|enhanced-abc  1/1|N.A.         |3            |00:00:bb:00:00:02| static   |
|      12|       1|          1|enhanced-abc  1/1|N.A.         |5            |00:00:bb:00:00:02| static   |
|      13|       1|          2|lagl           |100          |3            |da:2d:bc:89:10:d3| dynamic  |
|      14|       1|          2|lagl           |100          |4            |da:2d:bc:89:10:d3| dynamic  |
|      15|       1|          2|lagl           |100          |3            |de:80:bc:89:10:d3| dynamic  |
|      16|       1|          2|lagl           |100          |4            |de:80:bc:89:10:d3| dynamic  |
|      17|       1|          2|lagl           |100          |3            |dc:84:bc:89:10:d3| dynamic  |
|      18|       1|          2|lagl           |100          |4            |dc:84:bc:89:10:d3| dynamic  |
|      19|       1|          2|lagl           |100          |3            |e2:4d:bc:89:10:d3| dynamic  |
|      20|       1|          2|lagl           |100          |4            |e2:4d:bc:89:10:d3| dynamic  |
|      21|       1|          2|lagl           |100          |3            |d2:41:bc:89:10:d3| dynamic  |
|      22|       1|          2|lagl           |100          |4            |d2:41:bc:89:10:d3| dynamic  |
|      23|       1|          2|lagl           |100          |3            |e0:af:bc:89:10:d3| dynamic  |
|      24|       1|          2|lagl           |100          |4            |e0:af:bc:89:10:d3| dynamic  |
|      25|       1|          2|lagl           |100          |3            |d2:45:bc:89:10:d3| dynamic  |
|      26|       1|          2|lagl           |100          |4            |d2:45:bc:89:10:d3| dynamic  |
|      27|       1|          2|lagl           |100          |3            |e4:68:bc:89:10:d3| dynamic  |
|      28|       1|          2|lagl           |100          |4            |e4:68:bc:89:10:d3| dynamic  |
|      29|       1|          2|lagl           |100          |3            |de:fb:bc:89:10:d3| dynamic  |
|      30|       1|          2|lagl           |100          |4            |de:fb:bc:89:10:d3| dynamic  |
|      31|       1|          2|lagl           |100          |3            |d0:f2:bc:89:10:d3| dynamic  |
|      32|       1|          2|lagl           |100          |4            |d0:f2:bc:89:10:d3| dynamic  |
|      33|       1|          2|lagl           |100          |3            |de:62:bc:89:10:d3| dynamic  |
|      34|       1|          2|lagl           |100          |4            |de:62:bc:89:10:d3| dynamic  |
|      35|       1|          2|lagl           |100          |3            |d8:a2:bc:89:10:d3| dynamic  |
|      36|       1|          2|lagl           |100          |4            |d8:a2:bc:89:10:d3| dynamic  |
|      37|       1|          2|lagl           |100          |3            |b6:6e:bc:89:10:d3| dynamic  |
|      38|       1|          2|lagl           |100          |4            |b6:6e:bc:89:10:d3| dynamic  |
|      39|       1|          2|lagl           |100          |3            |d6:0b:bc:89:10:d3| dynamic  |
|      40|       1|          2|lagl           |100          |4            |d6:0b:bc:89:10:d3| dynamic  |
|      41|       1|          2|lagl           |100          |3            |e2:38:bc:89:10:d3| dynamic  |
|      42|       1|          2|lagl           |100          |4            |e2:38:bc:89:10:d3| dynamic  |
```

Note that if a flush is performed on the MAC address forwarding table (see **Error! Not a valid bookmark self-reference.**, the cached table is not flushed and is inaccurate until the next caching takes place.

In a configuration with TCC Redundancy, in the event of switchover the cached table in the newly active TCC is empty until the next caching takes places.

However, if you attempt to display the cached (saved) table at a time when the cache is empty, the device will automatically display the current table rather than the saved table.

Flushing the MAC Address Forwarding Table (CLI)

You can perform a global flush on the MAC address forwarding table. This erases all dynamic entries for all services. Static entries are not erased.



Note

The ability to flush the MAC address forwarding table per-service and per-interface is planned for future release.

	To perform a global flush of the MAC address forwarding table, enter the following command:

```
root> ethernet service mac-learning-table set global-flush
```

Enabling MAC Address Learning on a Service Point (CLI)

You can enable or disable MAC address learning for specific service points. By default, MAC learning is enabled.

To enable or disable MAC address learning for a service point, go to service view for the service and enter the following command:

```
service[SID]>sp learning-state set spid <sp-id> learning
<learning>
```

Table 163 Enabling MAC Address Learning CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32	The Service Point ID of the service point associated with the MAC address.
learning	Variable	Enable disable	Select enable or disable to enable or disable MAC address learning for frames that ingress via the service point. When enabled, the service point learns the source MAC addresses of incoming frames and adds them to the MAC address forwarding table.

The following command enables MAC address learning for Service Point 1 on Service 37:

```
service[37]>sp learning-state set spid 1 learning enable
```

The following command disables MAC address learning for Service Point 1 on Service 37:

```
service[37]>sp learning-state set spid 1 learning disable
```

21.2 Setting the MRU Size and the S-VLAN Ethertype (CLI)

The following parameters are configured globally for the PTP 850 switch:

- S- VLAN Ethertype – Defines the ethertype recognized by the system as the S-VLAN ethertype.
- C-VLAN Ethertype – Defines the ethertype recognized by the system as the C-VLAN ethertype. PTP 850 supports 0x8100 as the C-VLAN ethertype.

- MRU – The maximum segment size defines the maximum receive unit (MRU) capability and the maximum transmit capability (MTU) of the system. You can configure a global MRU for the system.



Note

The MTU is determined by the receiving frame and editing operation on the frame.

This section includes:

- Configuring the S-VLAN Ethertype (CLI)
- Configuring the C-VLAN Ethertype (CLI)
- Configuring the MRU (CLI)

21.2.1 Configuring the S-VLAN Ethertype (CLI)

To configure the S-VLAN Ethertype, enter the following command in root view:

```
root> ethernet generalcfg ethertype set svlan-value <ethertype>
```

To display the system S-VLAN ethertype, enter the following command in root view:

```
root> ethernet generalcfg ethertype show svlan
```

Table 164 Configure S-VLAN Ethertype CLI Parameters

Parameter	Input Type	Permitted Values	Description
ethertype	Hexadecimal	0x8100 0x88a8 0x9100 0x9200	Defines the ethertype recognized by the system as the S-VLAN ethertype.

Example

For example, the following command sets the system S-VLAN ethertype to 0x88a8:

```
root> ethernet generalcfg ethertype set svlan-value 0x88a8
```

21.2.2 Configuring the C-VLAN Ethertype (CLI)

The system C-VLAN Ethertype is set by the system as 0x8100.

To display the system C-VLAN ethertype, enter the following command in root view:

```
root> ethernet generalcfg ethertype show cvlan
```

21.2.3 Configuring the MRU (CLI)

To define the global size (in bytes) of the Maximum Receive Unit (MRU), enter the following command in root view:

```
root> ethernet generalcfg mru set size <size>
```

To display the system MRU, enter the following command in root view:

```
root> ethernet generalcfg mru show
```

Table 165 Configure MRU CLI Parameters

Parameter	Input Type	Permitted Values	Description
size	Number	64 to 9612	Defines the global size (in bytes) of the Maximum Receive Unit (MRU). Frames that are larger than the global MRU will be discarded.

Example

For example, the following command sets the system MRU to 9612:

```
root> ethernet generalcfg mru set size 9612
```

21.3 Configuring Ethernet Interfaces (CLI)

Related Topics:

- Enabling the Interfaces (CLI)
- Performing Ethernet Loopback (CLI)
- Configuring Ethernet Services (CLI)
- Quality of Service (QoS) (CLI)

PTP 820's switching fabric distinguishes between physical interfaces and logical interfaces. Physical and logical interfaces serve different purposes in the switching fabric. In some cases, a physical interface corresponds to a logical interface on a one-to-one basis. For some features, such as LAG, a group of physical interfaces can be joined into a single logical interface.

The basic interface characteristics, such as media type, port speed, duplex, and auto-negotiation, are configured on the physical interface level. Ethernet services, QoS, and OAM characteristics are configured on the logical interface level.



Note

You cannot change the configuration of the Management interface. By default, the Management interface has the following configuration:

- Auto negotiation ON
- Full Duplex
- RJ45 - 100Mbps

This section includes:

- Entering Interface View (CLI)
- Displaying the Operational State of the Interfaces in the Unit (CLI)
- Viewing Interface Attributes (CLI)
- Configuring an Interface's Speed and Duplex State (CLI)
- Configuring an Interface's Auto Negotiation State (CLI)
- Configuring an Interface's IFG (CLI)
- Configuring an Interface's Preamble (CLI)
- Adding a Description for the Interface (CLI)

21.3.1 Entering Interface View (CLI)

To view interface details and set the interface's parameters, you must enter the interface's view level in the CLI.

Use the following command to enter an Ethernet interface's view level:

```
root> ethernet interfaces eth slot <slot> port <port>
```

Use the following command to enter the radio interface's view level:

```
root> ethernet interfaces radio slot <slot> port <port>
```

Use the following command to enter the view level of a group, such as a Multi-Carrier ABC group, an HSB protection group, or a LAG:

```
root> ethernet interfaces group <group>
```

Table 166 Entering Interface View CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	1	
port	Number	Ethernet: 1-7 Radio: 1	The port number of the interface.



Note

In release 10.6, only Ethernet 7 is supported, along with the radio interface. In release 10.9, Ethernet Slot 1, Ports 4 through 7 are also supported.

The QSFP port (Port 4), is displayed as follows.

In a 4x1/10G configuration the QSFP port can provide four Ethernet interfaces: Eth3, Eth4, Eth 5, and Eth6. In this configuration, a QSFP transceiver is attached to the QSFP port, and an MPO-MPO cable is connected between the transceiver and a splitter on the other side of the link. The splitter splits the traffic between four Ethernet cables connecting the splitter to the customer equipment.

The following command enters interface view for Ethernet 7:

```
root> ethernet interfaces eth slot 1 port 7
```

The following prompt appears:

```
eth type eth [1/7]>
```

The following command enters interface view for the radio interface:

```
root> ethernet interfaces radio slot 1 port 1
```

The following prompt appears:

```
radio [1/1]>
```



Note

For simplicity, the examples in the following sections show the prompt for an Ethernet interface.

21.3.2 Displaying the Operational State of the Interfaces in the Unit (CLI)

To display a list of all interfaces in the unit and their operational states, enter the following command:

```
root> platform if-manager show interfaces
```

The following is a sample output of this command:

```
root>platform if-manager show interfaces
|=============================================================================================================================================================================================|
|  Interface          |  Type|  Description |  Admin  |  Operational |  Secondary                  |  Last change          |  Connector|  Speed (bps)|  MTU  |  MAC          | Minimum Bandwidth |
| type       |slot|port |      |              |  status |  status      |  operational-status         |                       |  Present  |             |       |  address      | admin             |
|=============================================================================================================================================================================================|
| ethernet   | 1  | 1   | 6    | Ethernet     | down    | down         | RX LOS/LOC                  | 01-01-1970,00:00:01   | false     | 1000000000  | 2000  | 0:a:25:0:0:c  | disable           |
|            |    |     |      |              |         |              | Interface not ready         |                       |           |             |       |               |                   |
|            |    |     |      |              |         |              | IF admin disabled           |                       |           |             |       |               |                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ethernet   | 1  | 2   | 6    | Ethernet     | down    | down         | RX LOS/LOC                  | 01-01-1970,00:00:01   | false     | 2500000000  | 2000  | 0:a:25:0:0:d  | disable           |
|            |    |     |      |              |         |              | Interface not ready         |                       |           |             |       |               |                   |
|            |    |     |      |              |         |              | IF admin disabled           |                       |           |             |       |               |                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ethernet   | 1  | 3   | 6    | Ethernet     | down    | down         | RX LOS/LOC                  | 01-01-1970,00:00:01   | false     | 10000000000 | 2000  | 0:a:25:0:0:4  | disable           |
|            |    |     |      |              |         |              | Interface not ready         |                       |           |             |       |               |                   |
|            |    |     |      |              |         |              | IF admin disabled           |                       |           |             |       |               |                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ethernet   | 1  | 4   | 6    | Ethernet     | down    | down         | RX LOS/LOC                  | 01-01-1970,00:00:01   | false     | 10000000000 | 2000  | 0:a:25:0:0:5  | disable           |
|            |    |     |      |              |         |              | Interface not ready         |                       |           |             |       |               |                   |
|            |    |     |      |              |         |              | IF admin disabled           |                       |           |             |       |               |                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ethernet   | 1  | 5   | 6    | Ethernet     | down    | down         | RX LOS/LOC                  | 01-01-1970,00:00:01   | false     | 10000000000 | 2000  | 0:a:25:0:0:6  | disable           |
|            |    |     |      |              |         |              | Interface not ready         |                       |           |             |       |               |                   |
|            |    |     |      |              |         |              | IF admin disabled           |                       |           |             |       |               |                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ethernet   | 1  | 6   | 6    | Ethernet     | down    | down         | RX LOS/LOC                  | 01-01-1970,00:00:01   | false     | 10000000000 | 2000  | 0:a:25:0:0:7  | disable           |
|            |    |     |      |              |         |              | Interface not ready         |                       |           |             |       |               |                   |
|            |    |     |      |              |         |              | IF admin disabled           |                       |           |             |       |               |                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ethernet   | 1  | 7   | 6    | Ethernet     | up      | down         | RX LOS/LOC                  | 01-01-1970,00:00:01   | false     | 10000000000 | 2000  | 0:a:25:0:0:26 | disable           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| radio      | 1  | 1   | 1    | Radionet     | up      | down         | Rx LOF/LOP                  | 01-01-1970,00:00:01   | false     | 1337000000  | 2000  | 0:a:25:0:0:c  | disable           |
|            |    |     |      |              |         |              | Rx only                     |                       |           |             |       |               |                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| management | 1  | 1   | 6    | Management   | up      | up           | Clear                       | 02-04-2000,06:50:03   | false     | 100000000   | 1632  | 0:0:0:0:0:0   | disable           |
```

21.3.3 Viewing Interface Attributes (CLI)

To display an interface's attributes, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>summary show
```

To display an interface's current operational state (up or down), go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>operational state show
```

The following command shows the attributes of Eth 7:

```
eth type eth [1/7]>summary show
```

The following command shows the operational state of Eth 7:

```
eth type eth [1/7]>operational state show
```

21.3.4 Configuring the QSFP Interface on an PTP 850E (CLI)

The QSFP interface (P4) on an PTP 850E requires special configuration of the QSFP mode before configuring the normal physical interface parameters. Before changing the **QSFP Expected** parameter, you must verify that:

- The **Admin** status of Eth3, Eth4, Eth5, and Eth6 is **Down**. See *Enabling the Interfaces (CLI)*.

If the QSFP interface is already set to **40Gbps Ethernet**, Eth4, Eth5, and

- No service point is attached to the interface. See *Configuring Service Points (CLI)*.
- No ASP pair is assigned to the interface. See *Configuring Automatic State Propagation and Link Loss Forwarding (CLI)*.
- No Policer is attached to the interface. See *Attaching a Rate Meter (Policer) to an Interface (CLI)*.
- No Shaper is attached to the interface. See *Configuring Shapers (CLI)*.
- The interface is not part of a LAG group. See *Configuring Link Aggregation (LAG) and LACP (Optional) (CLI)*.
- No synchronization is configured on the interface. See *Synchronization (CLI)*Synchronization.

To configure the QSFP interface, enter the following command in root view:

```
root> platform qsfp expected set slot 1 id 1 type <type>
```

To display the current parameters of the QSFP interface, enter the following command in root view:

```
root> platform qsfp expected show
```

The type parameter can be any of the following:

- **ETH** – Use this for 4x1/10 and 1x1/10 Gbps configurations. After entering the command, proceed to the following sections to configure the regular parameters of the interface or interfaces.
- **CPRI** – Reserved for future use.
- **ETH-40G** – Use this for 1x40 Gbps configurations. There is no need to configure the regular interface parameters because they are set:
  - Auto Negotiation is Off
  - Speed is 40 Gbps
  - Full Duplex

Note: The option **CPRI** is reserved for future use.

21.3.5 Configuring an Interface's Media Type (CLI)

The Media Type attribute defines the physical interface Layer 1 media type. Permitted values are RJ-45 and SFP.

Note

In System release 11.3,

For PTP 850C, Ethernet Slot 1, Ports 1, 2, 3, and 4 are supported.

For PTP 850E, Ethernet Slot 1, Ports 2 through 7 are supported. Port 2 can only be used in Multiband configurations to connect the PTP 850E with the paired unit.

To configure an Ethernet interface's Media Type, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>media-type state set <media type>
```

Table 167 Interface Media Type CLI Parameters

Parameter	Input Type	Permitted Values	Description
media type	Variable	rj45 sfp	Select the physical interface layer 1 media type: **RJ45** - An electrical (RJ-45) Ethernet interface. **SFP** - An optical (SFP) Ethernet interface.

21.3.6 Configuring an Interface's Speed and Duplex State (CLI)

To configure an Ethernet interface's maximum speed and duplex state, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>speed-and-duplex state set <speed-and-duplex
state>
```

Table 168 Interface Speed and Duplex State CLI Parameters

Parameter	InputType	Permitted Values	Description
speed-and-duplex state	Variable	'10hd' '10fd' '100hd' '100fd' '1000fd' ‘10000fd’	This parameter sets the maximum speed and the duplex state of the interface. For RJ-45 interfaces, any of the permitted values except 10000fd can be configured. For SFP interfaces, only '1000fd' is supported. **Note:** In relase 10.6, only Ethernet 7 (SFP+) is supported. In release 10.9, Ethernet Slot 1, Ports 4 through 7 are also supported.



Note

To use an SFP+ interface in 10G mode, the third-party switch must be running Pause Frame Flow Control, as defined in IEEE 802.3x. It is also recommended to configure shapers on the third-party switch so as to limit the packet flow from the switch to the PTP 850E unit to 2.5 Gbps.

After changing the speed of an SFP+ interface to or from 10000fd, you must reset the unit in order for the change to take effect.

21.3.7 Configuring an Interface’s Auto Negotiation State (CLI)

To configure an Ethernet interface’s auto-negotiation state, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>autoneg state set <autoneg state>
```

Table 169 Interface Auto Negotiation State CLI Parameters

Parameter	Input Type	Permitted Values	Description
autoneg state	Variable	On off	Enables or disables auto-negotiation on the physical interface. The default value is off. For Ports 3 to 6 (the QSFP ports), Auto Negotiation is not available, and the setting must remain off. For Port 7, if the Speed is set to 10000 (10G), Auto Negotiation is not available, and the setting must remain off. If the speed is set to 1000 (1G), Auto negotiation can be set to off (default) or on.

The following command enables auto negotiation for GbE 2:

```
eth type eth [1/2]>autoneg state set on
```

21.3.8 Configuring an Interface's IFG (CLI)

The IFG attribute represents the physical port Inter-frame gap. Although you can modify the IFG field length, it is strongly recommended not to modify the default value of 12 bytes without a thorough understanding of how the modification will impact traffic.

To configure an Ethernet interface's IFG, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>ifg set <ifg>
```

Table 170 Interface IFG CLI Parameters

Parameter	Input Type	Permitted Values	Description
ifg	Number	6 - 15	Sets the interface's IFG (in bytes).

The following command sets the ifg for GbE 1 to 12:

```
eth type eth [1/1]>ifg set 12
```

The following displays the currently configured ifg for GbE 1:

```
eth type eth [1/1]>ifg get
```

21.3.9 Configuring an Interface's Preamble (CLI)

Although you can modify an Ethernet interface's preamble, it is strongly recommended not to modify the default value of 8 bytes without a thorough understanding of how the modification will impact traffic.

To configure an Ethernet interface's preamble, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>preamble set <preamble>
```

Table 171 Interface Preamble CLI Parameters

Parameter	Input Type	Permitted Values	Description
preamble	Number	6 - 15	Sets the interface's preamble (in bytes).

The following command sets the preamble for GbE 1 to 8:

```
eth type eth [1/1]>preamble set 8
```

The following command displays the current preamble for GbE 1:

```
eth type eth [1/1]>preamble get
```

21.3.10 Adding a Description for the Interface (CLI)

You can add a text description for an interface. To add a description, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>description set <description>
```

To delete a description, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>description delete
```

To display an interface's description, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>description show
```

Table 172 Interface Description CLI Parameters

Parameter	Input Type	Permitted Values	Description
description	Text String	Up to 40 characters	Adds a text description to the interface.

The following command adds the description "Line" to GbE 1:

```
eth type eth [1/1]>description set Line
```

21.4 Configuring Automatic State Propagation and Link Loss Forwarding (CLI)

Automatic state propagation enables propagation of radio failures back to the Ethernet port. You can also configure Automatic State Propagation to close the Ethernet port based on a radio failure at the remote carrier.

Automatic state propagation is configured as pairs of interfaces. Each interface pair includes one Monitored Interface and one Controlled Interface.

Automatic state propagation is configured as pairs of interfaces. Each interface pair includes one Monitored Interface and one Controlled Interface. You can create multiple pairs using the same Monitored Interface and multiple Controlled Interfaces.

The Monitored Interface is a radio interface, a radio protection, or Multi-Carrier ABC group. The Controlled Interface is an Ethernet interface or LAG. An Ethernet interface can only be assigned to one Monitored interface.

Each Controlled Interface is assigned an LLF ID. If **ASP trigger by remote fault** is enabled on the remote side of the link, the ASP state of the Controlled Interface is propagated to the Controlled Interface with the same LLF ID at the remote side of the link. This means if ASP is triggered locally, it is propagated to the remote side of the link, but only to Controlled Interfaces with LLF IDs that match the LLF IDs of the affected Controlled Interfaces on the local side of the link.



Note

LLF requires an activation key. Without this activation key, only LLF ID 1 is available. See Configuring the Activation Key (CLI).

The following events in the Monitored Interface trigger ASP:

- Radio LOF
- Radio Excessive BER
- Radio LOC
- Remote Radio LOF
- Remote Excessive BER
- Remote LOC

The user can also configure the ASP pair so that Radio LOF, Radio Excessive BER, or loss of the Ethernet connection at the remote side of the link will also trigger ASP.

In addition, ASP is triggered if the Controlled Interface is a LAG, and the physical interfaces that belong to the LAG are set to **Admin** = **Down** in the Interface Manager.

When a triggering event takes place:

- If the Controlled Interface is an electrical GbE port, the port is closed.
- If the Controlled Interface is an optical GbE port, the port is muted.

The Controlled Interface remains closed or muted until all triggering events are cleared.

In addition, when a local triggering event takes place, the ASP mechanism sends an indication to the remote side of the link. Even when no triggering event has taken place, the ASP mechanism sends periodic update messages indicating that no triggering event has taken place.

A trigger delay time can be configured, so that when a triggering event takes place, the ASP mechanism does not propagate the event until this delay time has elapsed. A trigger delay from 0 to 10,000 ms can be set per LLD ID.



Note

It is recommended to configure both ends of the link to the same Automatic State Propagation configuration.

To configure propagation of a radio interface failure to an Ethernet port, use the following command:

```
root> auto-state-propagation add eth-port-to-radio eth-slot 1 eth-
port <eth-port> radio-slot 1 radio-port 1 llf-id <llf-id>
```

To enable automatic state propagation on an Ethernet port, determine whether remote interface failures are also propagated, enable ASP Management Safe (CSF) mode (optional), and set a trigger delay (optional), use the following command:

```
root> auto-state-propagation configure eth-port eth-slot 1 eth-
port <eth-port> asp-admin <asp-admin> remote-fault-trigger-admin
<remote-fault-trigger-admin> csf-mode-admin <csf-mode-admin>
trigger-delay <trigger-delay> llf-id <llf-id>
```



Note

In this command, the llf-id command is used optionally to change the LLF ID of the Ethernet port.

To delete automatic state propagation on an Ethernet port, use the following command:

```
root> auto-state-propagation delete eth-port eth-slot 1 eth-port
<eth-port>
```

To display all automatic state propagation configurations on the unit, use the following command:

```
root> auto-state-propagation show-config all
```

To display the automatic state propagation configuration for a specific Ethernet port, use the following command:

```
root> auto-state-propagation show-config eth-port eth-slot <eth-
slot> eth-port <eth-port>
```

Table 173: Automatic State Propagation to an Ethernet Port CLI Parameters

Parameter	Input Type	Permitted Values	Description
eth-port	Number	PTP 850S: 1-3 PTP 850E: 3-7	The interface to which you want to propagate faults from the selected radio or group.

llf-id	Number	1-31	An ID for Link Loss Forwarding (LLF). When **remote-fault-trigger-admin** is set to **enable**, ASP events at the other side of the link are propagated to Controlled Interfaces with LLF

			IDs that match the LLF IDs of affected Controlled Interfaces at the other side of the link. LLF IDs are unique per Monitored Interface. That is, if LLF ID 1 has been used for a Controlled Inter

			face that is grouped with radio interface 1, that ID cannot be used again for another Controlled Interface grouped with radio interface 1. However, it *can* be used for Controlled Interface grouped

Parameter	InputType	PermittedValues	Description
			with radio interface 2.
asp-admin	Variable	enable|disable	Enables or disables automatic state propagation on the Ethernet interface.

Parameter	InputType	PermittedValues	Description
remote-fault-trigger-admin	Variable	enable disable	Determines whether faults on the remote radio interface or group are propagated to the local Ethernet interface.

csf-mode-admin	Variable	enabled disable	Enables or disables ASP Management Safe (CSF) mode. In ASP Management Safe mode, the ASP mechanism does not physically shutdown the Controlled Interface when ASP is trigg

			ered. Instead, the ASP mechanism sends a failure indication message. This message is used to propagate the failure indication to external equipment.
trigger-del	Number	0-10000	Sets a trigger delay time, in

a y			milli sec ond s. Whe n a trigg erin g eve nt take s plac e, the ASP mec hani sm doe s not pro pag ate the eve nt until this dela y time has elap sed. By defa ult, the trigg er- dela y is 0 (no dela y

Parameter	Input Type	Permitted Values	Description
			time). In XPIC configurations, it is recommended to configure a trigger-delay of 100 ms.

The following commands configure and enable automatic state propagation to propagate faults from radio interface 1 to Ethernet ports 1 and 2, and from radio interface 2 to Ethernet port 3. CSF mode is disabled. Faults on the remote carrier are propagated to the local Ethernet ports as follows:

A failure on the remote side of the link is propagated to any of local Ethernet ports 3 or 4 that share an LLF ID with an Ethernet interface in an ASP pair with the remote radio.

The trigger delay for Ethernet port 3 is 100 ms. There is no trigger delay for Ethernet port 4.

```
root> auto-state-propagation add eth-port-to-radio eth-slot 1 eth-port 1 radio-slot 2 radio-port 1 llf-id 1
```

```
root> auto-state-propagation add eth-port-to-radio eth-slot 1 eth-port 2 radio-slot 2 radio-port 2 llf-id 2

root> auto-state-propagation configure eth-port eth-slot 1 eth-port 1 asp-admin enable remote-fault-trigger-admin enable csf-mode-admin disable trigger-delay 100

root> auto-state-propagation configure eth-port eth-slot 1 eth-port 2 asp-admin enable remote-fault-trigger-admin enable csf-mode-admin disable trigger-delay 5000

root> auto-state-propagation add eth-port-to-radio eth-slot 1 eth-port 3 radio-slot 1 radio-port 2 llf-id 1

root> auto-state-propagation configure eth-port eth-slot 1 eth-port 3 asp-admin enable remote-fault-trigger-admin enable csf-mode-admin disable
```

21.5 Configuring Receipt of CSF PDUs (CLI)

When ASP Management Safe mode (CSF) is configured, the peer unit must be configured to receive CSF PDUs. To enable the unit to receive CSF PDUs, enter the following command in root view:

```
root> ethernet soam csf receive set admin enable ifc-down <yes|no>
```

CSF receive must be enabled in order for G.8032 ERPI topology changes to be initiated upon receipt of a CSF PDU.

To disable this setting, enter the following command

```
root> ethernet soam csf receive set admin disable
```

The ifc-down parameter should usually be set to Yes. This means that all network protocols, LAG, and other unit modules will treat the interface on which the CSF PDU was received as Operation Status = Down. Also, a soam-csf-rdi-alarm will be raised to indicate that that relevant port is set to Operational Status = Down due to ASP triggered by the remote unit.

To display the current setting of this parameter, enter the following command:

```
root> ethernet soam csf receive show
```

21.6 Viewing Ethernet PMs and Statistics (CLI)

PTP 850 stores and displays statistics in accordance with RMON and RMON2 standards. You can display various peak TX and RX rates (in seconds) and average TX and RX rates (in seconds), both in bytes and in packets, for each measured time interval. You can also display the number of seconds in the interval during which TX and RX rates exceeded the configured threshold.

This section includes:

- Displaying Ethernet Port PMs (CLI)
- Clearing Ethernet Port PMs (CLI)

- Displaying RMON Statistics (CLI)
- Displaying Ethernet Port PMs (CLI)
- Clearing Ethernet Port PMs (CLI)
- Displaying Link Bonding PMs (CLI)

21.6.1 Displaying RMON Statistics (CLI)

PTP 850E stores and displays statistics in accordance with RMON and RMON2 standards.

RMON counters per frame size are not available for individual radio interfaces and radio groups. For Link Bonding groups, TX counters are available but not RX counters. For radio members of Link Bonding groups, all counters are available.

In Multiband (non-Link Bonding) and Layer 1 Link Aggregation configurations, there is no distinction between regular and idle packets in RMON statistics for the Ethernet interface connected to the attached unit (the Traffic interface). Therefore, it is recommended to rely on Capacity, Throughput, and Utilization PMs for the Traffic interface. See Displaying Traffic PMs (CLI).

To display RMON statistics for a physical interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rmon statistics show clear-on-read <clear-on-read> layer-1 <layer-1>
```

Table 174 RMON Statistics CLI Parameters

Parameter	Input Type	Permitted Values	Description
clear-on-read	Boolean	yes no	If you enter yes, the statistics are cleared once you display them.
layer-1	Boolean	yes no	yes – Statistics are represented as Layer 1 statistics, including preamble and IFG. no – Statistics are represented as Layer 2 statistics.

The following commands bring you to interface view for Ethernet port 1, and clears the statistics after displaying them.

```
root> ethernet interfaces eth slot 1 port 1

eth type eth [1/1]>rmon statistics show clear-on-read yes layer-1 yes
```

The following commands bring you to interface view for radio interface 2, without clearing the statistics.

```
root> ethernet interfaces radio slot 2 port 1

eth type radio[2/2]>rmon statistics show clear-on-read no layer-1 no
```

21.6.2 Configuring Ethernet Port PMs and PM Thresholds (CLI)

To enable the gathering of PMs for an Ethernet interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm set admin <enable|disable>
```

You can configure thresholds and display the number of seconds these thresholds were exceeded during a specified interval.

To configure interface PM thresholds, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm set thresholds rx-layer1-rate-threshold <0-
4294967295> tx-layer1-rate-threshold <0-4294967295>
```

To display whether or not PM gathering is enabled for an Ethernet interface, as well as the configured thresholds, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show configuration
```

Table 175 Port PM Thresholds CLI Parameters

Parameter	Input Type	Permitted Values	Description
rx-layer1-rate-thershold	Number	0-4294967295	The exceed threshold for port RX PMs, in bytes per second.
tx-layer1-rate-thershold	Number	0-4294967295	The exceed threshold for port TX PMs, in bytes per second.

The following commands bring you to interface view for Ethernet port 1, enable PM gathering, and set the thresholds for RX and TX PMs at 850,000,000 bytes per second:

```
root> ethernet interfaces eth slot 1 port 1

eth type eth [1/1]>pm set admin enable

eth type eth [1/1]>pm set thresholds rx-layer1-rate-threshold
850000000 tx-layer1-rate-threshold 850000000
```

21.6.3 Displaying Ethernet Port PMs (CLI)



Note

The port PM results may be several pages long. Remember:
To view the next results page, press the space bar.
To end the list and return to the most recent prompt, press the letter q.

To display RX packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-packets interval 15min
```

To display RX packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-packets interval 24hr
```

To display RX broadcast packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bcast-packets interval 15min
```

To display RX broadcast packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bcast-packets interval 24hr
```

To display RX multicast packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-mcast-packets interval 15min
```

To display RX multicast packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-mcast-packets interval 24hr
```

To display Layer 1 RX PMs, in bytes per second, in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bytes-layer1 interval 15min
```

To display Layer 1 RX PMs, in bytes per second, in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bytes-layer1 interval 24hr
```

To display Layer 2 RX PMs, in bytes per second, in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bytes-layer2 interval 15min
```

To display Layer 2 RX PMs, in bytes per second, in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bytes-layer2 interval 24hr
```

To display TX packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-packets interval 15min
```

To display TX packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-packets interval 24hr
```

To display TX broadcast packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bcast-packets interval 15min
```

To display TX broadcast packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bcast-packets interval 24hr
```

To display TX multicast packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-mcast-packets interval 15min
```

To display TX multicast packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-mcast-packets interval 24hr
```

To display Layer 1 TX PMs, in bytes per second, in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bytes-layer1 interval 15min
```

To display Layer 1 TX PMs, in bytes per second, in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bytes-layer1 interval 24hr
```

To display Layer 2 TX PMs, in bytes per second, in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bytes-layer2 interval 15min
```

To display Layer 2 TX PMs, in bytes per second, in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bytes-layer2 interval 24hr
```

Table 176 Ethernet Port PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Invalid data flag	Indicates whether the values received during the measured interval are valid. An x in the column indicates that the values are not valid (for example, because of a power surge or power failure that occurred during the interval).
Peak RX Packets	The peak rate of RX packets per second for the measured time interval.
Average RX Packets	The average rate of RX packets per second for the measured time interval.
Peak RX Broadcast Packets	The peak rate of RX broadcast packets per second for the measured time interval.
Average RX Broadcast Packets	The average rate of RX broadcast packets per second for the measured time interval.
Peak RX Multicast Packets	The peak rate of RX multicast packets per second for the measured time interval.

Parameter	Definition
Average RX Multicast Packets	The average rate of RX multicast packets per second for the measured time interval.
Peak RX Bytes in Layer1	The peak RX rate, in bytes per second, for the measured time interval (including preamble and IFG).
Average RX Bytes in Layer1	The average RX rate, in bytes per second, for the measured time interval (including preamble and IFG).
RX Bytes Layer1 Exceed Threshold (sec)	The number of seconds during the measured time interval that the RX rate exceeded the configured threshold.
Peak RX Bytes in Layer2	The peak RX rate, in bytes per second, for the measured time interval (excluding preamble and IFG).
Average RX Bytes in Layer2	The average RX rate, in bytes per second, for the measured time interval (excluding preamble and IFG).
Peak TX Packets	The peak rate of TX packets per second for the measured time interval.
Average TX Packets	The average rate of TX packets per second for the measured time interval.
Peak TX Broadcast Packets	The peak rate of TX broadcast packets per second for the measured time interval.
Average TX Broadcast Packets	The average rate of TX broadcast packets per second for the measured time interval.
Peak TX Multicast Packets	The peak rate of TX multicast packets per second for the measured time interval.
Average TX Multicast Packets	The average rate of TX multicast packets per second for the measured time interval.
Peak TX Bytes in Layer1	The peak TX rate, in bytes per second, for the measured time interval (including preamble and IFG).
Average TX Bytes in Layer1	The average TX rate, in bytes per second, for the measured time interval (including preamble and IFG).
TX Bytes Layer1 Exceed Threshold (sec)	The number of seconds during the measured time interval that the TX rate exceeded the configured threshold.
Peak TX Bytes in Layer2	The peak TX rate, in bytes per second, for the measured time interval (excluding preamble and IFG).

Parameter	Definition
Average TX Bytes in Layer2	The average TX rate, in bytes per second, for the measured time interval (excluding preamble and IFG).

21.6.4 Clearing Ethernet Port PMs (CLI)

To clear all PMs for an Ethernet interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm clear-all
```

21.6.5 Displaying Link Bonding PMs (CLI)

You can display PMs for L2 user traffic throughput and utilization for Link Bonding groups and their individual members. Group-level PMs exclude Link Bonding overhead. Member-level PMs include Link Bonding overhead.

You can also configure thresholds for the throughput and utilization PMs. The number of seconds during which these thresholds are exceeded are among the displayed PMs.

Peak counters display the maximum data rate and utilization percentage for each interval, with a resolution of one second. This means the PM mechanism records the number of bytes sent during each second of the interval and displays the number of bytes and utilization percentage for the highest one-second period during that interval. So, for example, when measuring 15-minute intervals, the PM mechanism chooses the peak value from 900 recorded values in that interval (60 seconds multiplied by 15 60-second record periods).

Average counters display the average data rate and utilization percentage for each interval, with a resolution of one second. For throughput, this means the PM mechanism divides the total number of bytes received during the interval by the total number of seconds in the interval. So, for example, when measuring 15-minute intervals, the PM mechanism divides the total number of bytes received during the 15-minute interval by 900.

Note: For Link Bonding group members with Throughput Enhancement enabled, the utilization percentage may at times exceed 100%. This is because the actual throughput over the radio is greater than the calculated maximum throughput because the radio is reducing Link Bonding overhead, allowing for additional user throughput.

Link Bonding PMs are displayed and configured from the Link Bonding group or member.

To go into group view, use the following command:

```
root>ethernet interfaces group lb<1-6>
eth group [lbx]>
```

For example, the following command accesses group view for Link Bonding group 1:

```
root>ethernet interfaces group lb1
eth group [lb1]>
```

To go into member view for an Ethernet interface, use the following command in group view:

```
eth group [lbx]> ethernet link-bonding-member interface eth slot
<slot> port <port>
```

For example, the following commands access member view for Eth 3, belonging to Link Bonding group 1:

```
root> ethernet interfaces group lb1
eth group [lb1]> ethernet link-bonding-member interface eth slot 1
port 3
lbg-member[eth1/3]>
```

To go into member view for a radio interface, use the following command in group view:

```
eth group [lbx]> ethernet link-bonding-member interface radio slot
1 port <port>
```

For example, the following commands access member view for radio interface 1, belonging to Link Bonding group 1:

```
root> ethernet interfaces group lb1
eth group [lb1]> ethernet link-bonding-member interface radio slot
1 port 1
lbg-member[radio1/1]>
```

To go into member view for a Multi-Carrier ABC group, use the following command in group view:

```
eth group [lb1]>ethernet link-bonding-member group-on-slot
enhanced-abc slot 1 group-id <1-4>
```

For example, the following commands access member view for Multi-Carrier ABC group 1, belonging to Link Bonding group 1:

```
root> ethernet interfaces group lb1
eth group [lb1]> ethernet link-bonding-member group-on-slot
enhanced-abc slot 1 group-id 1
lbg-member[enhanced-abc1/1]>
```

By default, Link Bonding PMs are disabled on all Link Bonding groups and group members. To enable (or disable) Link Bonding PMs on a group or member, go to interface view for the group or member and enter the following command:

```
pm-link-bonding set admin <enable|disable>
```

To display the current Link Bonding PMs configuration for a Link Bonding group or member, go to interface view for the group or member and enter the following command:

```
pm-link-bonding show configuration
```

To display Link Bonding PMs for a Link Bonding group or member, go to interface view for the group or member and enter the following command:

```
pm-link-bonding show counters-period interval <15min|24hr>
```

To set the utilization threshold for a Link Bonding group or member, go to interface view for the group or member and enter the following command:

```
pm-link-bonding set threshold utilization <0-100>
```

To set the throughput threshold for a Link Bonding group or member, in Mbps, go to interface view for the group or member and enter the following command:

```
pm-link-bonding set threshold throughput <0-30000>
```

The following is a sample output for 15-minute intervals.

```
Link Bonding PM Table:
======================

PM interval     Interval        Integrity       Peak            Average         Seconds         Peak            Average         Seconds
                                                Utilization     Utilization     Exceeding       Throughput      Throughput      Exceeding
                                                (percent)       (percent)       Utilization     (Mbps)          (Mbps)          Throughput
                                                                                Threshold                                       Threshold
================================================================================================================================================
15min           0               0               54              54              121             2354            2352            121
15min           1               0               54              54              900             2355            2352            900
15min           2               0               54              54              900             2355            2352            900
15min           3               0               54              54              900             2355            2352            900
15min           4               0               54              54              900             2355            2352            900
15min           5               0               54              54              900             2355            2352            900
15min           6               0               54              54              900             2355            2352            900
15min           7               0               54              54              900             2355            2352            900
15min           8               0               54              54              900             2355            2352            900
15min           9               0               54              54              900             2355            2352            900
15min           10              0               54              54              900             2355            2352            900
15min           11              0               54              54              900             2355            2352            900
15min           12              0               54              54              900             2355            2352            900
15min           13              0               54              54              900             2355            2352            900
15min           14              0               54              54              900             2355            2352            900
15min           15              0               54              54              900             2355            2352            900
15min           16              0               54              54              900             2355            2352            900
15min           17              0               54              54              900             2355            2352            900
15min           18              0               54              54              900             2355            2352            900
15min           19              0               54              54              900             2359            2352            900
15min           20              0               54              53              895             2355            2339            895
15min           21              0               54              32              540             2355            1416            540
15min           22              0               54              54              900             2355            2352            900
15min           23              0               54              54              900             2355            2352            900
15min           24              0               54              54              900             2355            2352            900
15min           25              0               54              54              900             2355            2352            900
15min           26              0               87              48              900             3790            2092            900
15min           27              0               96              63              899             966             921             899
15min           28              0               96              95              900             966             965             900
15min           29              0               96              95              900             966             965             900
15min           30              0               96              95              900             966             965             900
15min           31              0               96              95              900             966             965             900
15min           32              0               96              95              900             966             965             900
15min           33              0               96              95              900             966             965             900
15min           34              0               96              95              900             966             965             900
15min           35              0               96              95              900             966             965             900
15min           36              0               96              95              900             966             965             900
15min           37              0               96              95              900             966             965             900
15min           38              0               96              95              900             966             965             900
15min           39              0               96              95              900             966             965             900
15min           40              0               96              95              900             966             965             900
```

The following is a sample output for 24-hour intervals.

```
Link Bonding PM Table:
======================

PM interval     Interval        Integrity       Peak            Average         Seconds         Peak            Average         Seconds
                                                Utilization     Utilization     Exceeding       Throughput      Throughput      Exceeding
                                                (percent)       (percent)       Utilization     (Mbps)          (Mbps)          Throughput
                                                                                Threshold                                       Threshold
================================================================================================================================================
24hr            0               0               96              77              59034           3790            1500            59034
24hr            1               0               96              95              86400           968             965             86400
24hr            2               1               106             56              73847           1069363         503976          73847
24hr            3               0               22              21              84123           908331          905662          84123
24hr            4               0               22              21              84122           910694          905662          84122
24hr            5               1               111             43              81588           4160002         1889938         81588
24hr            6               1               110             84              80959           4159144         3675354         80959
24hr            7               1               104             68              46988           3520152         2941921         46988
24hr            9               1               94              80              28261           3521873         3515341         28261
24hr            10              1               94              53              68210           3527603         2253716         74159
24hr            11              1               64              46              35749           1735597         1729739         35749
```

Table 177 describes the capacity and throughput PMs.

Table 177: Link Bonding PMs (CLI)

Parameter	Definition
PM Interval	Displays the type of interval (15min or 24hr).
Interval	An index to identify the interval. **Note:** Interval dates and times are only available via the Web EMS.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. A “1” in the column indicates that the values are not reliable due to a

	possible power surge or power failure that occurred at that time.
Peak Utilization (percent)	Displays the highest L2 user traffic utilization percentage during the interval. This includes Link Bonding overhead for individual members and excludes Link Bonding overhead for Link Bonding groups.
Average Utilization (percent)	Displays the average L2 user traffic utilization percentage per interval. This includes Link Bonding overhead for individual members and excludes Link Bonding overhead for Link Bonding groups.
Seconds exceeding Utilization Threshold	Displays the number of seconds during the interval during which the L2 user traffic utilization percentage for the Link Bonding group or member exceeded the configured utilization threshold.
Peak Throughput (Mbps)	Displays the highest L2 user traffic throughput, in Mbps, during the interval. This includes Link Bonding overhead for individual members and excludes Link Bonding overhead for Link Bonding groups.
Average Throughput (Mbps)	Displays the average L2 user traffic throughput, in Mbps, per interval. This includes Link Bonding overhead for individual members and excludes Link Bonding overhead for Link Bonding groups.
Seconds Exceeding Throughput Threshold	Displays the number of seconds during the interval during which the L2 user traffic throughput for the Link Bonding group or member exceeded the configured throughput threshold.

22. Quality of Service (QoS) (CLI)

This section includes:

- Configuring Classification (CLI)
- Configuring Policers (Rate Metering) (CLI)
- Configuring Marking (CLI)
- Configuring WRED (CLI)
- Configuring Shapers (CLI)
- Configuring Scheduling (CLI)
- Enabling Hierarchical QoS (H-QoS) (CLI)
- Displaying Ingress Statistics (CLI)
- Displaying Egress PMs and Statistics (CLI)

22.1 Configuring Classification (CLI)

This section includes:

- Classification Overview (CLI)
- Configuring Ingress Path Classification on a Logical Interface (CLI)
- Configuring VLAN Classification and Override (CLI)
- Configuring DSCP Classification (CLI)
- Configuring MPLS Classification (CLI)
- Configuring Ingress Path Classification on a Service Point (CLI)
- Configuring Ingress Path Classification on a Service (CLI)

22.1.1 Classification Overview (CLI)

PTP 850 supports a hierarchical classification mechanism. The classification mechanism examines incoming frames and determines their CoS and Color. The benefit of hierarchical classification is that it provides the ability to “zoom in” or “zoom out”, enabling classification at higher or lower levels of the hierarchy. The nature of each traffic stream defines which level of the hierarchical classifier to apply, or whether to use several levels of the classification hierarchy in parallel.

The hierarchical classifier consists of the following levels:

Logical interface-level classification

Service point-level classification

Service level classification

22.1.2 Configuring Ingress Path Classification on a Logical Interface (CLI)

Logical interface-level classification enables you to configure classification on a single interface or on a number of interfaces grouped tougher, such as a LAG group.

The classifier at the logical interface level supports the following classification methods, listed from highest to lowest priority. A higher level classification method supersedes a lower level classification method:

- VLAN ID
- MPLS EXP field
- DSCP bits (only considered if MPLS is not present, regardless of trust setting)
- 802.1p bits
- Default CoS

PTP 850 performs the classification on each frame ingressing the system via the logical interface. Classification is performed step by step from the highest priority to the lowest priority classification method. Once a match is found, the classifier determines the CoS and Color decision for the frame for the logical interface-level.

You can disable some of these classification methods by configuring them as un-trusted. For example, if MPLS classification is configured as un-trusted for a specific interface, the classification mechanism does not perform classification according to the MPLS EXP bits. This is useful, for example, if classification is based on 802.1p bits.

If no match is found at the logical interface level, the default CoS is applied to incoming frames at this level. In this case, the Color of the frame is assumed to be Green.

22.1.3 Configuring VLAN Classification and Override (CLI)

You can specify a specific CoS and Color for a specific VLAN ID. In the case of double-tagged frames, the match must be with the frame's outer VLAN. Permitted values are CoS 0 to 7 and Color Green or Yellow per VLAN ID. This is the highest classification priority on the logical interface level, and overrides any other classification criteria at the logical interface level.

To configure CoS and Color override based on VLAN ID, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>vlan-cos-override set outer-vlan-id <outer-
vlan-id> inner-vlan-id <inner-vlan-id> use-cos <use-cos> use-
color <use-color>
```

To display configured VLAN-based CoS and Color override values, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>vlan-cos-override show outer-vlan-id
<outer-vlan-id> inner-vlan-id <inner-vlan-id>
```

To delete a set of VLAN-based CoS and Color override values, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>vlan-cos-override delete outer-vlan-id
<outer-vlan-id> inner-vlan-id <inner-vlan-id>
```

Table 178 VLAN Classification and Override CLI Parameters

Parameter	Input Type	Permitted Values	Description
outer-vlan-id	Number	1 – 4094	For double-tagged frames, the S-VLAN value mapped to the CoS and Color values defined in the command. For single-tagged frames, the VLAN value mapped to the CoS and Color values defined in the command.
inner-vlan-id	Number	1 – 4094	Optional. Include this parameter when you want to map double-tagged frames to specific CoS and Color values. When this parameter is included in the command, both the S-VLAN and the C-VLAN IDs must match the configured `outer-vlan-id` and `inner-vlan-id` values, respectively, in order for the defined CoS and Color values to be applied to the frame.
use-cos	Number	0 – 7	The CoS value applied to matching frames.
use-color	Variable	green yellow	The Color applied to matching frames.

The following command configures the classification mechanism on GbE 1 to override the CoS and Color values of frames with S-VLAN ID 10 and C-VLAN ID 30 with a CoS value of 6 and a Color value of Green:

```
eth type eth [1/1]>vlan-cos-override set outer-vlan-id 10
inner-vlan-id 30 use-cos 6 use-color green
```

The following command configures the classification mechanism on GbE 2 to override the CoS and Color values of frames with VLAN ID 20 with a CoS value of 5 and a Color value of Green:

```
eth type eth [1/2]>vlan-cos-override set outer-vlan-id 20 use-
cos 5 use-color green
```

The following command displays the CoS and Color override values for frames that ingress on GbE 1, with S-VLAN ID 10 and C-VLAN ID 20:

```
eth type eth [1/1]>vlan-cos-override show outer-vlan-id 10
inner-vlan-id 20
```

The following command displays all CoS and Color override values for frames that ingress on GbE 2:

```
eth type eth [1/2]>vlan-cos-override show all
```

The following command deletes the VLAN to CoS and Color override mapping for frames that ingress on GbE 1, with S-VLAN ID 10 and C-VLAN ID 20:

```
eth type eth [1/1]>vlan-cos-override delete outer-vlan-id 10
inner-vlan-id 20
```

22.1.4 Configuring DSCP Classification (CLI)

When DSCP classification is set to Trust mode, the interface performs QoS and Color classification according to a user-configurable DSCP to CoS and Color classification table. 802.1p classification has priority over DSCP Trust Mode, so that if a match is found on the 802.1p level, DSCP is not considered.

This section includes:

- Configuring Trust Mode for DSCP Classification (CLI)
- Modifying the DSCP Classification Table (CLI)

Configuring Trust Mode for DSCP Classification (CLI)

To define the trust mode for DSCP classification, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>classification set ip-dscp <ip-dscp>
```

To display the trust mode for DSCP classification, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>classification show 802.1p state
```

Parameter	Input Type	Permitted Values	Description
ip-dscp	Variable	trust un-trust	Select the interface's trust mode for DSCP classification: `trust` – The interface performs QoS and color classification according to a user-configurable table for DSCP to CoS and color classification. DSCP classification has priority over MPLS classification, so that if a match is found with the DSCP value of the ingressing frame, MPLS bits are not considered. `un-trust` – The interface does not consider DSCP during classification.

The following command enables DSCP trust mode for GbE 1:

```
eth type eth [1/1]>classification set ip-dscp trust
```

The following command disables DSCP trust mode for GbE 1:

```
eth type eth [1/1]>classification set ip-dscp un-trust
```

Modifying the DSCP Classification Table (CLI)

PTP 850 units have a DSCP classification table with 24 pre-defined entries.
Each entry includes the following criteria:

- **DSCP** – The DSCP value to be mapped.
- **Binary** – The binary representation of the DSCP value.
    - **Description** – A description of the DSCP value.
- **CoS** – The CoS assigned to frames with the designated DSCP value.

- **Color** – The Color assigned to frames with the designated DSCP value.

You can modify the Description, CoS, and Color for any of the pre-defined entries. You can also add and delete entries. The maximum number of entries is:

- PTP 850C and PTP 850E: 64.
- PTP 850S: 32

The following table shows the default values for the DSCP classification table.

Table 179 DSCP Classification Table Default Values

DSCP	DSCP (bin)	Description	CoS (Configurable)	Color (Configurable)
0 (default)	000000	BE (CS0)	0	Green
10	001010	AF11	1	Green
12	001100	AF12	1	Yellow
14	001110	AF13	1	Yellow
18	010010	AF21	2	Green
20	010100	AF22	2	Yellow
22	010110	AF23	2	Yellow
26	011010	AF31	3	Green
28	011100	AF32	3	Yellow
30	011110	AF33	3	Yellow
34	100010	AF41	4	Green
36	100100	AF42	4	Yellow
38	100110	AF43	4	Yellow
46	101110	EF	7	Green
8	001000	CS1	1	Green
16	010000	CS2	2	Green
24	011000	CS3	3	Green
32	100000	CS4	4	Green
40	101000	CS5	5	Green
48	110000	CS6	6	Green
56	111000	CS7	7	Green

DSCP	DSCP (bin)	Description	CoS (Configurable)	Color (Configurable)
51	110011	DSCP_51	6	Green
52	110100	DSCP_52	6	Green
54	110110	DSCP_54	6	Green
56	111000	CS7	7	Green

To modify the DSCP classification table, enter the following command:

```
root> ethernet qos dscp-mapping-tbl set dscp <dscp> cos <cos>
color <color>
```

To display the DSCP classification table, enter the following command:

```
root> ethernet qos dscp-mapping-tbl show
```

Table 180 Modify DSCP Classification Table CLI Parameters

Parameter	Input Type	Permitted Values	Description
dscp	Number	0-63	The DSCP value to be mapped.
cos	Number	0 – 7	The CoS assigned to frames with the designated DSCP value.
color	Variable	green yellow	The Color assigned to frames with the designated DSCP value.

Example

The following command maps frames with DSCP value of 10 to CoS 1 and Green color:

```
root> ethernet qos dscp-mapping-tbl set dscp 10 cos 1 color green
```

22.1.5 Configuring MPLS Classification (CLI)

When MPLS classification is set to Trust mode, the interface performs QoS and Color classification according to a user-configurable MPLS EXP bit to CoS and Color classification table. Both 802.1p and DSCP classification have priority over MPLS Trust Mode, so that if a match is found on either the 802.1p or DSCP levels, MPLS bits are not considered.

This section includes:

- Configuring Trust Mode for MPLS Classification (CLI)
- Modifying the MPLS EXP Bit Classification Table (CLI)

Configuring Trust Mode for MPLS Classification (CLI)

To define the trust mode for MPLS classification, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>classification set mpls <mpls>
```

Note

For PTP 850C and PTP 850E, if you change the trust mode for MPLS, the trust mode for DSCP is automatically changed to the same setting.

To display the trust mode for MPLS classification, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>classification show mpls state
```

Table 181 Trust Mode for MPLS CLI Parameters

Parameter	Input Type	Permitted Values	Description
mpls	Variable	Trust un-trust	Select the interface's trust mode for MPLS bits: `trust` – The interface performs QoS and color classification according to a user-configurable table for MPLS EXP to CoS and color classification. `un-trust` – The interface does not consider MPLS bits during classification.

The following command enables MPLS trust mode for GbE 1:

```
eth type eth [1/1]>classification set mpls trust
```

The following command disables MPLS trust mode for GbE 1:

```
eth type eth [1/1]>classification set mpls un-trust
```

Modifying the MPLS EXP Bit Classification Table (CLI)

The following table shows the default values for the MPLS EXP bit classification table.

Table 182 MPLS EXP Bit Classification Table Default Values

MPLS EXP bits	CoS (Configurable)	Color (Configurable)
0	0	Yellow
1	1	Green
2	2	Yellow
3	3	Green
4	4	Yellow
5	5	Green
6	6	Green
7	7	Green

To modify the MPLS EXP bit classification table, enter the following command:

```
root> ethernet qos mpls-exp-bits-mapping-tbl set mpls-exp
<mpls-exp> cos <cos> color <color>
```

To display the MPLS EXP bit classification table, enter the following command:

```
root> ethernet qos mpls-mapping-tbl show
```

Table 183 MPLS EXP Bit Classification Table Modification CLI Parameters

Parameter	Input Type	Permitted Values	Description
mpls-exp	Number	0 – 7	The MPLS EXP bit to be mapped.
cos	Number	0 – 7	The CoS assigned to frames with the designated MPLS EXP bit value.
color	Variable	green yellow	The Color assigned to frames with the designated MPLS EXP bit value.

The following command maps frames with MPLS EXP bit value of 4 to CoS 4 and Yellow color:

```
root> ethernet qos mpls-exp-bits-mapping-tbl set mpls-exp 4
cos 4 color yellow
```

22.1.6 Configuring 802.1p Classification (CLI)

When 802.1p classification is set to Trust mode, the interface performs QoS and Color classification according to user-configurable tables for 802.1q UP bit (C-VLAN frames) or 802.1AD UP bit (S-VLAN frames) to CoS and Color classification.

This section includes:

- Configuring Trust Mode for 802.1p Classification (CLI)
- Modifying the C-VLAN 802.1 UP and CFI Bit Classification Table (CLI)
- Modifying the S-VLAN 802.1 UP and DEI Bit Classification Table (CLI)

Configuring Trust Mode for 802.1p Classification (CLI)

To define the trust mode for 802.1p classification, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>classification set 802.1p <802.1p>
```

To display the trust mode for 802.1p classification, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>classification show 802.1p state
```

Table 184: 802.1p Trust Mode CLI Parameters

Parameter	InputType	PermittedValues	Description
802.1p	Variable	trust un-trust	Enter the interface's trust mode for user priority (UP) bits: • **trust** – The interface performs QoS and color classification according to UP and CFI/DEI bits according to user-configurable tables for 802.1q UP bits (C-VLAN frames) or 802.1AD UP bits (S-VLAN frames). MPLS and DSCP classification have priority over 802.1p classification, so that if a match is found on the MPLS or DSCP level, 802.1p bits are not considered. • **un-trust** – The interface does not consider 802.1 UP bits during classification.

The following command enables 802.1p trust mode for Eth 7:

```
eth type eth [1/7]>classification set 802.1p trust
```

The following command disables 802.1p trust mode for GbE 1:

```
eth type eth [1/7]>classification set 802.1p un-trust
```

Modifying the C-VLAN 802.1 UP and CFI Bit Classification Table (CLI)

The following table shows the default values for the C-VLAN 802.1 UP and CFI bit classification table.

Table 185: C-VLAN 802.1 UP and CFI Bit Classification Table Default Values

802.1UP	CFI	CoS (configurable)	Color (configurable)
0	0	0	Green
0	1	0	Yellow
1	0	1	Green
1	1	1	Yellow
2	0	2	Green
2	1	2	Yellow
3	0	3	Green
3	1	3	Yellow
4	0	4	Green
4	1	4	Yellow
5	0	5	Green
5	1	5	Yellow
6	0	6	Green
6	1	6	Yellow
7	0	7	Green
7	1	7	Yellow

To modify the C-VLAN 802.1 UP and CFI bit classification table, enter the following command:

```
root> ethernet qos 802.1q-up-bits-mapping-tbl set 802.1p
<802.1p> cfi <cfi> cos <cos> color <color>
```

To display the C-VLAN 802.1 UP and CFI bit classification table, enter the following command:

```
root> ethernet qos 802.1q-up-bits-mapping-tbl show
```

Table 186: C-VLAN 802.1 UP and CFI Bit Classification Table CLI Parameters

Parameter	InputType	PermittedValues	Description
802.1p	Number	0–7	The User Priority (UP) bit to be mapped.

Parameter	InputType	PermittedValues	Description
cfi	Number	0–1	The CFI bit to be mapped.

cos	Number	0–7	The CoS assigned to frames with the designated UP and CFI.
color	Variable	Greenyellow	The Color assigned to

Parameter	Input Type	Permitted Values	Description
			frames with the designated UP and CFI.

The following command maps frames with an 802.1p UP bit value of 1 and a CFI bit value of 0 to CoS 1 and Green color:

```
root> ethernet qos 802.1q-up-bits-mapping-tbl set 802.1p 1 cfi 0 cos 1
color green
```

Modifying the S-VLAN 802.1 UP and DEI Bit Classification Table (CLI)

The following table shows the default values for the S-VLAN 802.1 UP and DEI bit classification table.

Table 187: S-VLAN 802.1 UP and DEI Bit Classification Table Default Values

802.1UP	DEI	CoS (Configurable)	Color (Configurable)
0	0	0	Green
0	1	0	Yellow
1	0	1	Green
1	1	1	Yellow
2	0	2	Green
2	1	2	Yellow
3	0	3	Green
3	1	3	Yellow
4	0	4	Green
4	1	4	Yellow
5	0	5	Green
5	1	5	Yellow
6	0	6	Green
6	1	6	Yellow
7	0	7	Green
7	1	7	Yellow

To modify the S-VLAN 802.1 UP and DEI bit classification table, enter the following command:

```
root> ethernet qos 802.1ad-up-bits-mapping-tbl set 802.1p
<802.1p> dei <dei> cos <cos> color <color>
```

To display the S-VLAN 802.1 UP and CFI bit classification table, enter the following command:

```
root> ethernet qos 802.1ad-up-bits-mapping-tbl show
```

Table 188: S-VLAN 802.1 UP and DEI Bit Classification Table CLI Parameters

Parameter	InputType	PermittedValues	Description
802.1p	Number	0–7	The User Priority (UP) bit to be mapped.

Parameter	InputType	PermittedValues	Description
dei	Number	0-1	The DEI bit to be mapped.

cos	Number	0–7	The CoS assigned to frames with the designated UP and CFI.
color	Variable	greenyellow	The Color assigned to

Parameter	InputType	PermittedValues	Description
			frameswiththedesignatedUPandCFI.

The following command maps frames with an 802.1ad UP bit value of 7 and a DEI bit value of 0 to CoS 7 and Green color:

```
root> ethernet qos 802.1ad-up-bits-mapping-tbl set 802.1p 7
dei 0 cos 7 color green
```

Configuring MAC DA Classification (CLI)

Note: This section is only relevant for PTP 850S.

You can determine whether classification is performed by MAC DA in the service point's **CoS Mode** parameter. See *Classification Overview*.

To add an entry to the MAC DA classification table, enter the following command in root view:

```
root>ethernet generalcfg mac-da add mac <MAC address> color
<green|yellow>
```

To edit an entry to the MAC DA classification table, enter the following command in root view:

```
root>ethernet generalcfg mac-da edit mac <MAC address> color
<green|yellow>
```

To delete an entry to the MAC DA classification table, enter the following command in root view:

```
root>ethernet generalcfg mac-da delete mac <MAC address>
```

The following command adds MAC address 00:11:22:33:44:55 to the MAC DA classification table, with a CoS of 7 and the Color green.

```
root>ethernet generalcfg mac-da add mac 00:11:22:33:44:55 cos 7
color green
```

The following command changes the CoS assigned to this MAC address to 6.

```
root>ethernet generalcfg mac-da edit mac 00:11:22:33:44:55 cos
6 color green
```

The following command deletes this MAC address.

```
root>ethernet generalcfg mac-da delete mac 00:11:22:33:44:55
```

22.1.7 Configuring a Default CoS (CLI)

You can define a default CoS value for frames passing through the interface. This value can be overwritten on the service point and service level. The Color is assumed to be Green.

To define a default CoS value for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>classification set default-cos <default-
cos>
```

To display the default CoS value for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>classification show default-cos
```

Table 189 Default CoS CLI Parameters

Parameter	Input Type	Permitted Values	Description
default-cos	Number	0 – 7	Enter the default CoS value for frames passing through the interface. This value can be overwritten on the service point and service level.

The following command sets the default CoS for GbE 1 as 7:

```
eth type eth [1/1]>classification set default-cos 7
```

22.1.8 Configuring Ingress Path Classification on a Service Point (CLI)

For instruction on configuring ingress path classification on a service point, see CoS Preservation and Modification on a Service Point (CLI).

22.1.9 Configuring Ingress Path Classification on a Service (CLI)

For instruction on configuring ingress path classification on a service, see Configuring a Service's CoS Mode and Default CoS (CLI).

22.2 Configuring Policers (Rate Metering) (CLI)

This section includes:

- Overview of Rate Metering (Policing) (CLI)
- Configuring Rate Meter (Policer) Profiles (CLI)
- Displaying Rate Meter Profiles (CLI)
- Deleting a Rate Meter Profile (CLI)
- Attaching a Rate Meter (Policer) to an Interface (CLI)

22.2.1 Overview of Rate Metering (Policing) (CLI)

The PTP 850 switching fabric supports hierarchical policing on the logical interface level. You can define up to 250 rate meter (policer) profiles.



Note

Policing on the service point level, and the service point and CoS level, is planned for future release.

The PTP 850's policer mechanism is based on a dual leaky bucket mechanism (TrTCM). The policers can change a frame's color and CoS settings based on CIR/EIR + CBS/EBS, which makes the policer mechanism a key tool for implementing bandwidth profiles and enabling operators to meet strict SLA requirements.

The output of the policers is a suggested color for the inspected frame. Based on this color, the queue management mechanism decides whether to drop the frame or to pass it to the queue.

22.2.2 Configuring Rate Meter (Policer) Profiles (CLI)

To add a rate meter (policer) profile, enter the following command:

```
root> ethernet qos rate-meter add profile-id <profile-id> cir <cir> cbs
<cbs> eir <eir> ebs <ebs> color-mode <color-mode> coupling-flag <coupling-
flag> rate-meter-profile-name <rate-meter-profile-name>
```

To edit an existing rate meter (policer) profile, enter the following command:

```
root> ethernet qos rate-meter edit profile-id <profile-id> cir <cir> cbs
<cbs> eir <eir> ebs <ebs> color-mode <color-mode> coupling-flag <coupling-
flag> rate-meter-profile-name <rate-meter-profile-name>
```

Table 190 Rate Meter Profile CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 – 256	A unique ID for the rate meter (policer) profile.
cir	Number	0, or 64,000 - 1,000,000,000	The Committed Information Rate (CIR) defined for the rate meter (policer), in bits per second. If the value is 0, all incoming CIR traffic is dropped.
cbs	Number	0 - 4096	The Committed Burst Size (CBS) for the rate meter (policer), in Kbytes.
eir	Number	0, or 64,000 - 1,000,000,000	The Excess Information Rate (EIR) for the rate meter (policer), in bits per second. If the value is 0, all incoming EIR traffic is dropped.
ebs	Number	0 - 4096	The Excess Burst Size (EBR) for the rate meter (policer), in Kbytes.
color-mode	Variable	color-blind color-aware	Determines how the rate meter (policer) treats frames that ingress with a CFI or DEI field set to 1 (yellow). Options are: `color aware` – All frames that ingress with a CFI/DEI field set to 1 (yellow) are treated as EIR frames, even if credits remain in the CIR bucket. `color blind` – All ingress frames are treated as green regardless of their CFI/DEI value. A color-blind policer discards any former color decisions.
coupling-flag	Variable	enable disable	When enabled, frames that ingress as yellow may be converted to green when there are no available yellow credits in the EIR bucket. Only relevant in `color-aware` mode.
rate-meter-profile-name	Text string	Up to 20 characters.	A description of the rate meter (policer) profile.

The following command creates a rate meter (policer) profile with Profile ID 50, named “64k.”

```
root> ethernet qos rate-meter add profile-id 50 cir 64000 cbs 5 eir 64000
ebs 5 color-mode color-blind coupling-flag disable rate-meter-profile-name
64k
```

This profile includes the following parameters:

- CIR – 64,000 bps
- CBS – 5 Kbytes
- CBS – 5 Kbytes
- EIR – 64,000 bps
- EBS – 5 Kbytes
- Color Blind mode
- Coupling Flag disabled

The following command edits the rate meter (policer) profile with Profile ID 50, and changes its name to “256 kBytes.”

```
root> ethernet qos rate-meter edit profile-id 50 cir 128000 cbs 5 eir
128000 ebs 5 color-mode color-aware coupling-flag enable rate-meter-
profile-name 256 kBytes
```

This edited profile includes the following parameters:

- CIR – 128,000 bps
- CBS – 5 Kbytes
- EIR – 128,000 bps
- EBS – 5 Kbytes
- Color Aware mode
- Coupling Flag enabled

22.2.3 Displaying Rate Meter Profiles (CLI)

You can display all configured rate meter (policer) profiles or a specific profile.

To display a specific profile, enter the following command:

```
root> ethernet qos rate-meter show profile-id <profile-id>
```

To display all configured profiles, enter the following command:

```
root> ethernet qos rate-meter show profile-id all
```

The following command displays the parameters of Rate Meter Profile 50:

```
root> ethernet qos rate-meter show profile-id 50
```

22.2.4 Deleting a Rate Meter Profile (CLI)

You cannot delete a rate meter (policer) profile that is attached to a logical interface. You must first remove the profile from the logical interface, then delete the profile.

To delete a rate meter (policer) profile, use the following command:

```
root> ethernet qos rate-meter delete profile-id <profile-id>
```

The following command deletes Rate Meter Profile 50:

```
root> ethernet qos rate-meter delete profile-id 50
```

22.2.5 Attaching a Rate Meter (Policer) to an Interface (CLI)

On the logical interface level, you can assign rate meter (policer) profiles as follows:

Per frame type (unicast, multicast, and broadcast)

Per frame ethertype

This section includes:

- Assigning a Rate Meter (Policer) for Unicast Traffic (CLI)
- Assigning a Rate Meter (Policer) for Unknown Multicast Traffic (CLI)
- Assigning a Rate Meter (Policer) per Ethertype (CLI)

Assigning a Rate Meter (Policer) for Unicast Traffic (CLI)

To assign a rate meter (policer) profile for unicast traffic to the interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter unicast add capability admin-state
<admin-state> profile-id <profile-id>
```

To change the rate meter (policer) profile for unicast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter unicast edit admin-state <admin-state>
profile-id <profile-id>
```

To display the current unicast rate meter (policer) profile for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter unicast show configuration
```

To delete the rate meter (policer) profile for unicast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter unicast delete
```

Table 191 Assigning Rate Meter for Unicast Traffic CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin-state	Variable	enable disable	Enables or disables rate metering on unicast traffic flows from the logical interface.
profile-id	Number	1 – 250	Select from the rate meter profiles defined in the system.

The following command assigns Rate Meter Profile 1 to unicast traffic on GbE 1, and enables rate metering on the port:

```
eth type eth [1/1]>rate-meter unicast add capability admin-
state enable profile-id 1
```

The following command changes the rate meter (policer) profile for unicast traffic on GbE 1 to 4:

```
eth type eth [1/1]>rate-meter unicast edit admin-state enable
profile-id 4
```

22.2.5.1 Assigning a Rate Meter (Policer) for Unknown Unicast Traffic (CLI)

Unknown unicast packets are unicast packets with unknown destination MAC addresses To assign a rate meter (policer) profile for unknown unicast traffic to the interface, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>rate-meter unknown-unicast add capability
admin-state <admin-state> profile-id <profile-id>
```

To change the rate meter (policer) profile for unicast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>rate-meter unknown-unicast edit admin-state
<admin-state> profile-id <profile-id>
```

To display the current unicast rate meter (policer) profile for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>rate-meter unknown-unicast show
configuration
```

To delete the rate meter (policer) profile for unicast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>rate-meter unknown-unicast delete
```

Table 192: Assigning Rate Meter for Unknown Unicast Traffic CLI Parameters

Parameter	InputType	PermittedValues	Description

admin-state	Variable	enabled disable	Enables or disables rate metering on unknown unicast traffic flows from the logical inte

Parameter	InputType	PermittedValues	Description
			rface.
profile-id	Number	1–250	Select from the rate meter profiles defined in the system.

The following command assigns Rate Meter Profile 1 to unknown unicast traffic on Eth 7, and enables rate metering on the port:

```
eth type eth [1/7]>rate-meter unknown-unicast add capability
admin-state enable profile-id 1
```

The following command changes the rate meter (policer) profile for unknown unicast traffic on Eth 7 to 4:

```
eth type eth [1/7]>rate-meter unknown-unicast edit admin-state
enable profile-id 4
```

Assigning a Rate Meter (Policer) for Multicast Traffic (CLI)

To assign a rate meter (policer) profile for multicast traffic to the interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter multicast add capability admin-state <admin-
state> profile-id <profile-id>
```

To change the rate meter (policer) profile for multicast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter multicast edit admin-state <admin-state>
profile-id <profile-id>
```

To display the current multicast rate meter (policer) profile for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter multicast show configuration
```

To delete the rate meter (policer) profile for multicast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter multicast delete
```

Table 193 Assigning Rate Meter for Multicast Traffic CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin-state	Variable	enable disable	Enables or disables rate metering on multicast traffic flows from the logical interface.
profile-id	Number	1 – 250	Select from the rate meter profiles defined in the system.

The following command assigns Rate Meter Profile 1 to multicast traffic on GbE 1, and enables rate metering on the port.

```
eth type eth [1/1]>rate-meter multicast add capability admin-state enable
profile-id 1
```

The following command changes the rate meter (policer) profile for multicast traffic on GbE 1 to 4:

```
eth type eth [1/1]>rate-meter multicast edit admin-state enable profile-id
4
```

22.2.5.2 Assigning a Rate Meter (Policer) for Unknown Multicast Traffic (CLI)

Unknown multicast packets are multicast packets with unknown destination MAC addresses. To assign a rate meter (policer) profile for unknown multicast traffic to the interface, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>rate-meter unknown-multicast add capability admin-state
<admin-state> profile-id <profile-id>
```

To change the rate meter (policer) profile for multicast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>rate-meter unknown-multicast edit admin-state <admin-
state> profile-id <profile-id>
```

To display the current multicast rate meter (policer) profile for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>rate-meter unknown-multicast show configuration
```

To delete the rate meter (policer) profile for multicast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>rate-meter unknown-multicast delete
```

Table 194*:* Assigning Rate Meter for Multicast Traffic CLI Parameters

Parameter	InputType	PermittedValues	Description

admin-state	Variable	enable disable	Enables or disables rate metering on unknown multicast traffic flows from the logical in

Parameter	InputType	PermittedValues	Description
			terface.
profile-id	Number	1–250	Select from the rate meter profiles defined in the system.

The following command assigns Rate Meter Profile 1 to unknown multicast traffic on Eth 7, and enables rate metering on the port.

```
eth type eth [1/7]>rate-meter unknown-multicast add capability admin-state
enable profile-id 1
```

The following command changes the rate meter (policer) profile for unknown multicast traffic on Eth 7 to 4:

```
eth type eth [1/7]>rate-meter unknown-multicast edit admin-state enable
profile-id 4
```

Assigning a Rate Meter (Policer) for Broadcast Traffic (CLI)

To assign a rate meter (policer) profile for broadcast traffic to the interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter broadcast add capability admin-state <admin-
state> profile-id <profile-id>
```

To change the rate meter (policer) profile for broadcast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter broadcast edit admin-state <admin-state>
profile-id <profile-id>
```

To display the current broadcast rate meter (policer) settings for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter broadcast show configuration
```

To delete the rate meter (policer) profile for broadcast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter broadcast delete
```

Table 195 Assigning Rate Meter for Broadcast Traffic CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin-state	Variable	enable disable	Enables or disables rate metering on broadcast traffic flows from the logical interface.
profile-id	Number	1 – 250	Select from the rate meter profiles defined in the system.

The following command assigns Profile 1 to broadcast traffic on GbE 1, and enables rate metering on the port.

```
eth type eth [1/1]>rate-meter broadcast add capability admin-state enable
profile-id 1
```

The following command changes the rate meter (policer) profile for broadcast traffic on GbE 1 to 4:

```
eth type eth [1/1]>rate-meter broadcast edit admin-state enable profile-id
4
```

Assigning a Rate Meter (Policer) per Ethertype (CLI)

You can define up to three policers per Ethertype value.

To assign a rate meter (policer) profile for a specific Ethertype to an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter <ethertype#> add capability ethertype-value
<ethertype-value> admin-state <admin-state> profile-id <profile-id>
```

To change the rate meter (policer) profile for a specific Ethertype, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter <ethertype#> edit ethertype-
value <ethertype-value> admin-state <admin-state> profile-id
<profile-id>
```

To display the current Ethertype rate meter (policer) settings for an interface, go to interface view for the interface and enter the following commands:

```
eth type eth [x/x]>rate-meter ethertype1 show configuration
eth type eth [x/x]>rate-meter ethertype2 show configuration
eth type eth [x/x]>rate-meter ethertype3 show configuration
```

To delete the rate meter (policer) profile for an Ethertype, go to interface view for the interface and enter one or more of the following commands:

```
eth type eth [x/x]>rate-meter ethertype1 delete
eth type eth [x/x]>rate-meter ethertype2 delete
eth type eth [x/x]>rate-meter ethertype3 delete
```

Table 196 Assigning Rate Meter per Ethertype CLI Parameters

Parameter	Input Type	Permitted Values	Description
ethertype#	Variable	ethertype1 ethertype2 ethertype3 I	Identifies which of three possible policer-per-Ethertype combinations you are defining.
ethertype-value	Hexadecimal	1-65535	Identifies the Ethertype to which the profile applies.
admin-state	Variable	enable disable	Enables or disables policing on broadcast traffic flows from the logical interface.
profile-id	Number	1 – 250	Select from the policer profiles defined in the system. For instructions on defining rate meter (policer) profiles, refer to Configuring Rate Meter (Policer) Profiles (CLI).

The following commands assign Rate Meter Profiles 1, 2, and 3 to Ethertypes 0x8000, 0x8100, and 0x9100, respectively, on GbE 1, and enable rate metering on the port.

```
eth type eth [1/1]>rate-meter ethertype1 add capability ethertype-
value 0x8000 admin-state enable profile-id 1

eth type eth [1/1]>rate-meter ethertype2 add capability ethertype-
value 0x8100 admin-state enable profile-id 2

eth type eth [1/1]>rate-meter ethertype3 add capability ethertype-
value 0x9100 admin-state enable profile-id 3
```

The following commands change the rate meter (policer) profiles assigned in the examples above to 4, 5, and 6, respectively.

```
eth type eth [1/1]>rate-meter ethertype1 edit ethertype-value 0x8000 admin-
state enable profile-id 4

eth type eth [1/1]>rate-meter ethertype2 edit ethertype-value 0x8100 admin-
state enable profile-id 5

eth type eth [1/1]>rate-meter ethertype3 edit ethertype-value 0x9100 admin-
state enable profile-id 6
```

22.2.6 Attaching a Rate Meter (Policer) to a Service Point and CoS (CLI)

To assign a rate meter (policer) profile to a service point, go to service view for the service and enter the following commands:

```
service[x]>sp rate-meter add capability spid <spid>

service[x]>sp rate-meter edit spid <spid> admin-state
<admin-  state> profile-id <profile-id>
```

To change the rate meter (policer) profile for a service point, go to service view for the service and enter the following command:

```
service[x]>sp rate-meter edit spid <spid> admin-state <admin-
state> profile-id <profile-id>
```

To display the current rate meter (policer) profile for a service point, go to service view for the service and enter the following command:

```
service[x]>sp rate-meter show configuration spid <spid>
```

To assign a rate meter (policer) profile to a service point and CoS, go to service view for the service and enter the following commands:

```
service[x]>sp rate-meter add capability spid <spid>

service[x]>sp rate-meter edit spid <spid> cos <cos> admin-state
<admin-state> profile-id <profile-id>
```

To change the rate meter (policer) profile for a service point and CoS, go to service view for the service and enter the following command:

```
service[x]>sp rate-meter edit spid <spid> cos <cos> admin-state
<admin-state> profile-id <profile-id>
```

To display the current rate meter (policer) profile for a service point and CoS, go to service view for the service and enter the following command:

```
service[x]>sp rate-meter show configuration spid <spid> cos
<cos>
```

To delete the rate meter (policer) profile for a service point or service point/CoS combination, go to service view for the service and enter the following command:

```
service[x]>sp rate-meter delete spid <spid>
```

Table 202: Assigning Rate Meter for Service Point and Service Point/CoS CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
admin-state	Variable	enable disable	Enables or disables rate metering on unicast traffic flows from the logical
profile-id	Number	1 – 250	Select from the rate meter profiles defined in
cos	Number	0 – 7	The CoS value to which you are assigning the

The following commands assign Rate Meter Profile 2 to service point 10 on service 5:

```
root> ethernet service sid 5

service[5]> sp rate-meter add capability spid 10

service[5]>sp rate-meter edit spid 10 admin-state enable
profile-id 2
```

The following commands assign Rate Meter Profile 4 to service point 10 and CoS 6 on service 5:

```
root> ethernet service sid 5

service[5]> sp rate-meter add capability spid 10

service[5]>sp rate-meter edit spid 10 cos 6 admin-state enable
profile-id 4
```

22.2.7 Configuring the Line Compensation Value for a Rate Meter (Policer) (CLI)

A rate meter can measure CIR and EIR at Layer 1 or Layer 2 rates. Layer 1 capacity is equal to Layer 2 capacity plus 20 additional bytes for each frame due to the preamble and Inter Frame Gap (IFG). In most cases, the preamble and IFG equals 20 bytes, but other values are also possible. Line compensation defines the number of bytes to be added to each frame for purposes of CIR and EIR calculation. When Line Compensation is 20, the rate meter operates as Layer 1. When Line Compensation is 0, the rate meter operates as Layer 2. This parameter is very important to users that want to distinguish between Layer 1 and Layer 2 traffic.

To configure the rate meter (policer) line compensation value for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter-compensation-value set <value>
```

To display the rate meter (policer) line compensation value for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter-compensation-value get
```

Table 197 Assigning Line Compensation Value for Rate Meter CLI Parameters

Parameter	Input Type	Permitted Values	Description
value	Number	0 – 32	Policers attached to the interface use this value to compensate for Layer 1 non-effective traffic bytes.

The following command sets the line compensation value for policers attached to GbE 1 to 20:

```
eth type eth [1/1]>rate-meter-compensation-value set 20
```

22.2.8 Displaying Rate Meter Statistics for an Interface (CLI)

Note: This section is only relevant for PTP 850S.

For the rate meter (policer) at the logical interface level, you can display the following statistics counters:

- Green Frames
- Green Bytes
- Yellow Frames
- Yellow Bytes
- Red Frames
- Red Bytes

Note: Rate meter (policer) counters are displayed in granularity of 64 bits.

The following commands display rate meter counters for the available frame types and Ethertypes:

```
eth type eth [x/x]>rate-meter unicast show statistics clear-on- read
<clear-on-read> layer-1 <layer-1>

eth type eth [x/x]>rate-meter multicast show statistics clear- on-read
<clear-on-read> layer-1 <layer-1>

eth type eth [x/x]>rate-meter broadcast show statistics clear- on-read
<clear-on-read> layer-1 <layer-1>

eth type eth [x/x]>rate-meter ethertype1 show statistics clear- on-read
<clear-on-read> layer-1 <layer-1>

eth type eth [x/x]>rate-meter ethertype2 show statistics clear- on-read
<clear-on-read> layer-1 <layer-1>

eth type eth [x/x]>rate-meter ethertype3 show statistics clear- on-read
<clear-on-read> layer-1 <layer-1>
```

Table 204: Displaying Rate Meter Statistics CLI Parameters

Parameter	Input Type	Permitted Values	Description
clear-on-read	Boolean	yes no	If you enter yes, the statistics are cleared once you display them.
layer 1	Boolean	yes no	yes – Statistics are represented as Layer 1 statistics, including preamble and IFG. no – Statistics are

			represented as Layer 2 statistics.

The following commands display rate meter counters for GbE 1, for each of the available frame types and Ethertypes. These commands clear the counters after displaying them.

```
eth type eth [1/1]>rate-meter unicast show statistics clear-on-  read yes layer-1
no

eth type eth [1/1]>rate-meter multicast show statistics clear-  on-read yes layer-
1 no

eth type eth [1/1]>rate-meter broadcast show statistics clear-  on-read yes layer-
1 no

eth type eth [1/1]>rate-meter ethertype1 show statistics clear-  on-read yes layer-
1 no

eth type eth [1/1]>rate-meter ethertype2 show statistics clear-  on-read yes layer-
1 no

eth type eth [1/1]>rate-meter ethertype3 show statistics clear-  on-read yes layer-
1 no
```

22.3 Configuring Marking (CLI)

This section includes:

- Marking Overview (CLI)
- Configuring Marking Mode on a Service Point (CLI)
- Marking Table for C-VLAN UP Bits (CLI)
- Marking Table for S-VLAN UP Bits (CLI)

22.3.1 Marking Overview (CLI)

When enabled, PTP 850's marking mechanism modifies each frame's 802.1p UP bit and CFI/DEI bits according to the classifier decision. The CFI/DEI (color) field is modified according to the classifier and policer decision. The color is first determined by a classifier and may be later overwritten by a policer. Green color is represented by a CFI/DEI value of 0, and Yellow color is represented by a CFI/DEI value of 1. Marking is performed on egress frames that are VLAN-tagged.

The marking is performed according to global marking tables that describe the 802.1p UP bits and the CFI bits (for C-VLAN tags) or DEI bits (for S VLAN tags). The marking mode attribute in the service point egress attributes determines whether the frame is marked as Green or Yellow according to the calculated color.



Note

The calculated color is sent to the queue manager regardless of whether the marking bit is set.

Regular marking is only performed when:

The outer frame is S-VLAN, and S-VLAN CoS preservation is disabled

The outer frame is C-VLAN, and C-VLAN CoS preservation is disabled

If marking and CoS preservation for the relevant outer VLAN are both disabled, special marking is applied. Special marking means that marking is performed, but only according to the values defined for Green frames in the 802.1Q and 802.1AD marking tables.

When marking is performed, the C-VLAN or S-VLAN 802.1p UP bits are re-marked according to the calculated CoS and Color.

22.3.2 Configuring Marking Mode on a Service Point (CLI)

To enable or disable marking mode on a service point, go to service view for the service and enter the following command:

```
service[SID]>sp marking set spid <sp-id> mode <mode>
```

Table 198 Marking Mode on Service Point CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.

Parameter	Input Type	Permitted Values	Description
mode	Variable	enable disable	Determines whether re-marking of the outer VLAN (C-VLAN or S-VLAN) of tagged frames that pass through the service point is enabled. If `mode` is set to `enable`, and CoS preservation for the relevant outer VLAN is set to `disable`, the service point re-marks the C-VLAN or S-VLAN 802.1p UP bits of egress frames according to the calculated CoS and Color, and the user-configurable 802.1Q and 802.1AD marking tables. If `mode` is set to `enable` and CoS preservation for the relevant outer VLAN is also set to `enable`, re-marking is not performed. If `mode` is set to `disable` and CoS preservation for the relevant outer VLAN is also set to `disable`, re-marking is applied, but only according to the values defined for Green frames in the 802.1Q and 802.1AD marking tables. For information about configuring CoS Preservation, refer to CoS Preservation and Modification on a Service Point (CLI).

Examples

The following command enables marking mode on Service Point 3 on Service 2:

```
service[2]>sp marking set spid 3 mode enable
```

The following command disables marking mode on Service Point 3 on Service 2:

```
service[2]>sp marking set spid 3 mode disable
```

22.3.3 Marking Table for C-VLAN UP Bits (CLI)

When marking is performed, the following table is used by the marker to decide which CoS and Color to use as the egress CoS and Color bits for C-VLAN-tagged frames.

Table 199 Marking Table for C-VLAN UP Bits

CoS	Color	802.1q (Configurable)	CFI Color (Configurable)
0	Green	0	0

CoS	Color	802.1q (Configurable)	CFI Color (Configurable)
0	Yellow	0	1
1	Green	1	0
1	Yellow	1	1
2	Green	2	0
2	Yellow	2	1
3	Green	3	0
3	Yellow	3	1
4	Green	4	0
4	Yellow	4	1
5	Green	5	0
5	Yellow	5	1
6	Green	6	0
6	Yellow	6	1
7	Green	7	0
7	Yellow	7	1

To modify the 802.1q CoS and Color to UP and CFI bit mapping table, enter the following command in root view:

```
root> ethernet qos 802.1q-up-bits-marking-tbl set cos <cos>
color <color> 802.1p <802.1p> cfi <cfi>
```

To display the 802.1q CoS and Color to UP and CFI bit mapping table, enter the following command in root view:

```
root> ethernet qos 802.1q-up-bits-marking-tbl show
```

Table 200 802.1q CoS and Color to UP and CFI Bit Mapping Table CLI Parameters

Parameter	Input Type	Permitted Values	Description
cos	Number	0 – 7	The CoS value to be mapped.
color	Variable	green yellow	The Color to be mapped.

Parameter	Input Type	Permitted Values	Description
802.1p	Number	0 – 7	The UP bit value assigned to matching frames.
cfi	Number	0 – 1	The CFI bit value assigned to matching frames.

Example

The following command maps CoS 0, Green, to 802.1p UP bit 0, and CFI bit 0:

```
root> ethernet qos 802.1q-up-bits-marking-tbl set cos 0 color green
      802.1p 0 cfi 0
```

22.3.4 Marking Table for S-VLAN UP Bits (CLI)

When marking is performed, the following table is used by the marker to decide which CoS and Color to use as the egress CoS and Color bits for S-VLAN-tagged frames.

Table 201 802.1ad UP Marking Table (S-VLAN)

CoS	Color	802.1ad UP (Configurable)	DEI Color (Configurable)
0	Green	0	0
0	Yellow	0	1
1	Green	1	0
1	Yellow	1	1
2	Green	2	0
2	Yellow	2	1
3	Green	3	0
3	Yellow	3	1
4	Green	4	0
4	Yellow	4	1
5	Green	5	0
5	Yellow	5	1
6	Green	6	0
6	Yellow	6	1
7	Green	7	0

CoS	Color	802.1ad UP (Configurable)	DEI Color (Configurable)
7	Yellow	7	1

To modify the 802.1ad CoS and Color to UP and DEI bit mapping table, enter the following command in root view:

```
root> ethernet qos 802.1ad-up-bits-marking-tbl set cos
<cos> color <color> 802.1p <802.1p> dei <dei>
```

To display the 802.1q CoS and Color to UP and CFI bit mapping table, enter the following command in root view:

```
root> ethernet qos 802.1ad-up-bits-marking-tbl show
```

Table 202 802.1ad UP Marking Table (S-VLAN) CLI Parameters

Parameter	Input Type	Permitted Values	Description
cos	Number	0 – 7	The CoS value to be mapped.
color	Variable	green yellow	The Color to be mapped.
802.1p	Number	0 – 7	The UP bit value assigned to matching frames.
dei	Number	0 – 1	The DEI bit value assigned to matching frames.

Example

The following command marks CoS 5, Yellow, to 802.1p UP bit 5, and DEI bit 1:

```
root> ethernet qos 802.1ad-up-bits-marking-tbl set cos 5 color yellow
              802.1p 5 dei 1
```

22.4 Configuring WRED (CLI)

This section includes:

- WRED Overview (CLI)
- Configuring WRED Profiles (CLI)
- Assigning a WRED Profile to a Queue (CLI)

22.4.1 WRED Overview (CLI)

Weighted Random Early Detection (WRED) enables differentiation between higher and lower priority traffic based on CoS. You can define up to 30 WRED profiles. Each profile contains a green traffic curve and a yellow traffic curve. These curves describe the probability of randomly dropping frames as a function of queue occupancy.

The system also includes two pre-defined read-only profiles. These profiles are assigned WRED profile IDs 31 and 32.

Profile number 31 defines a tail-drop curve and is configured with the following values:

100% Yellow traffic drop after 64kbytes occupancy.

100% Green traffic drop after 128kbytes occupancy.

Yellow maximum drop is 100%

Green maximum drop is 100%

Profile number 32 defines a profile in which all will be dropped. It is for internal use and should not be applied to traffic.

A WRED profile can be assigned to each queue. The WRED profile assigned to the queue determines whether or not to drop incoming frames according to the occupancy of the queue. As the queue occupancy grows, the probability of dropping each incoming frame increases as well. As a consequence, statistically more TCP flows will be restrained before traffic congestion occurs.

22.4.2 Configuring WRED Profiles (CLI)

To configure a WRED profile, enter the following command in root view:

```
root> ethernet qos wred-profile-tbl add profile-id <profile-id> green-min-
threshold <green-min-threshold> green-max-threshold <green-max-threshold>
green-max-drop <green-max-drop> yellow-min-threshold <yellow-min-threshold>
yellow-max-threshold <yellow-max-threshold> yellow-max-drop <yellow-max-
drop>
```

To edit an existing WRED profile, enter the following command in root view:

```
root> ethernet qos wred-profile-tbl edit profile-id <profile-id> green-min-
threshold <green-min-threshold> green-max-threshold <green-max-threshold>
green-max-drop <green-max-drop> yellow-min-threshold <yellow-min-threshold>
yellow-max-threshold <yellow-max-threshold> yellow-max-drop <yellow-max-
drop>
```

To display a WRED profile, enter the following command in root view:

```
root> ethernet qos wred-profile-tbl show profile-id <profile-
id>
```

To delete a WRED profile, enter the following command in root view:

```
root> ethernet qos wred-profile-tbl delete profile-id <profile
id>
```

You cannot delete a WRED profile that is assigned to a queue. You must first remove the WRED profile from the queue by replacing it with a different WRED profile. You can then delete the WRED profile.



Note

Each queue always has a WRED profile assigned to it. By default, WRED Profile 31 is assigned to every queue until a different profile is assigned.

Table 203 WRED Profile CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 - 30	A unique ID to identify the profile.

Parameter	Input Type	Permitted Values	Description
green-min-threshold	Number	24 - 8192	The minimum number of green frames for queues with this profile, in Kbytes. When this value is reached, the system begins dropping green frames in the queue.
green-max-threshold	Number	24 - 8192	The maximum number of green frames for queues with this profile, in Kbytes. When this value is reached, all green frames in the queue are dropped.
green-max-drop	Number	1 - 100	The maximum percentage of dropped green frames for queues with this profile.
yellow-min-threshold	Number	24 - 8192	The minimum number of yellow frames for queues with this profile, in Kbytes. When this value is reached, the system begins dropping yellow frames in the queue.
yellow-max-threshold	Number	0 - 8192	The maximum number of yellow frames for queues with this profile, in Kbytes. After this value is reached, all yellow frames in the queue are dropped.
yellow-max-drop	Number	1 - 100	The maximum percentage of dropped yellow frames for queues with this profile.

Examples

The following command adds a WRED profile.

```
root> ethernet qos wred-profile-tbl add profile-id 2 green-
min-threshold 8000 green-max-threshold 8000 green-max-drop 100
yellow-min-threshold 8000 yellow-max-threshold 8000 yellow-
max-drop 100
```

The new profile has the following parameters:

profile-id – 2

green-min-threshold – 8000 Kbytes

green-max-threshold – 8000 Kbytes

green-max-drop – 100%

yellow-min-threshold – 8000 Kbytes

yellow-max-threshold – 8000 Kbytes

yellow-max-drop – 100%

The following command edits the WRED profile created by the previous command:

```
root> ethernet qos wred-profile-tbl edit profile-id 2 green-min-
threshold 8000 green-max-threshold 8000 green-max-drop 100 yellow-
min-threshold 4000 yellow-max-threshold 4000 yellow-max-drop 100
```

The edited profile has the following parameters:

green-min-threshold – 8000 Kbytes

green-max-threshold – 8000 Kbytes

green-max-drop – 100%

yellow-min-threshold – 4000 Kbytes

yellow-max-threshold –4000 Kbytes

yellow-max-drop – 100%

22.4.3 Assigning a WRED Profile to a Queue (CLI)

To assign a WRED profile to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> wred set service-bundle-id <service-bundle-id>
cos <cos> profile-id <profile-id>
```

To display the WRED profile assigned to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> wred show profile-id service-bundle-id <service-bundle-
id> cos <cos>
```

Table 204 Assigning WRED Profile to Queue CLI Parameters

Parameter	Input Type	Permitted Values	Description
service-bundle-id	Number	1	QoS is not relevant for WRED configuration.
cos	Number	0 – 7	Assigns the WRED profile to a queue in the designated service bundle.
profile-id	Number	1 – 32	A unique ID that identifies the profile.

Examples

The following command assigns WRED Profile 2 to the CoS 0 queue in Service Bundle 1, on GbE 1:

```
eth type eth [1/1]> wred set service-bundle-id 1 cos 0
profile-id 2
```

The following command displays the WRED profile assigned to the CoS 0 queue in Service Bundle 1, on GbE 1:

```
eth type eth [1/1]> wred show profile-id service-bundle-id
1 cos 0
```

22.5 Configuring Shapers (CLI)

Egress shaping abilities differ between PTP 850C and PTP 850E, on one hand, and PTP 850S, on the other. Therefore, it is presented separately for each product group:

- Configuring Queue Shapers for PTP 850C and PTP 850E (CLI)
- Configuring Shapers for PTP 850S (CLI)

22.5.1 Configuring Queue Shapers for PTP 850C and PTP 850E (CLI)

This section includes:

- Overview of Egress Queue Shaping for PTP 850C and PTP 850E (CLI)
- Configuring Egress Line Compensation for Shaping for PTP 850C and PTP 850E (CLI)

Overview of Egress Queue Shaping for PTP 850C and PTP 850E (CLI)

Egress shaping determines the traffic profile for each queue. PTP 850 can perform queue shaping on the queue level, using dual leaky bucket shaping. On the queue level, you can configure up to 32 single leaky bucket shaper profiles. If no profile is attached to the queue, no egress shaping is performed on that queue.

Note: You can enter any value within the permitted range. Based on the value you enter, the software automatically rounds off the setting according to the granularity. If you enter a value below the lowest granular value (except 0), the software adjusts the setting to the minimum.

You can attach one of the configured queue shaper profiles to each priority queue. If no profile is attached to the queue, no egress shaping is performed on that queue.

This section includes:

- Configuring Queue Shaper Profiles for PTP 850C and PTP 850E (CLI)
- Attaching a Shaper Profile to a Queue for PTP 850C and PTP 850E (CLI)

Configuring Queue Shaper Profiles (CLI)

To configure a queue shaper profile, enter the following command in root view:

```
root> ethernet qos queue-shaper-profile-tbl-broadband add profile-id
<profile-id> cir <cir> shaper-profile-name <shaper-profile-name> cbs <cbs>
eir <eir> ebs <ebs> burst-type <burst-type>
```

To edit the parameters of an existing queue shaper profile, enter the following command in root view:

```
root> ethernet qos queue-shaper-profile-tbl-broadband edit profile-id
<profile-id> cir <cir> shaper-profile-name <shaper-profile-name> cbs <cbs>
eir <eir> ebs <ebs> burst-type <burst-type>
```

Table 205: Queue Shaper Profiles CLI Parameters

Parameter	InputType	PermittedValues	Description
profile-id	Number	1-32	A unique ID that identifies the profile.
cir	Number	0–4000000000	The Committed Information Rate (CIR) assigned to the profile (in kbps). If the value is 0, all incoming CIR traffic

Parameter	InputType	PermittedValues	Description
			is dropped. Granularity is 81 kbps. The default value is 40000000 kbps.
shaper-profile-name	TextString	Upto20characters.	Granularity is 81 kbps. The default value is 40000000 kbps. A description of the profile.

Parameter	InputType	PermittedValues	Description
cbs	Number	1–32	The Committed Burst Size (CBR) for the shaper, in Kbytes. Permitted values are 1-32 KB. The default value is 16 KB.
eir	Number	4000000	The Excess Information Rate (EIR) for the shaper (in

Parameter	InputType	PermittedValues	Description
			kbps). If the value is 0, all incoming EIR traffic is dropped. Granularity is 162 kbps. The default value is 40000000 kbps.
ebs	Number	1–32	The Excess Burst Size (EBR) for the shaper, in Kbyt

Parameter	InputType	PermittedValues	Description
			es. Permitted values are 1-32 KB. The default value is 16 KB.
burst-type	Variable	short long	Only **short** is supported.

The following command creates Queue Shaper 1, named “p1,” with a CIR value of 16000 kbps, CBS of 16 KB, EIR of 16000 kbps, and EBS of 1:

```
root> ethernet qos queue-shaper-profile-tbl-broadband add
profile-id 1 cir 16000 shaper-profile-name p1 cbs 16 eir 16000
ebs 1 burst-type short
```

The following command changes the CIR value of the profile created above from 16000 to 32000, and changes the profile name to p3:

```
root> ethernet qos queue-shaper-profile-tbl-broadband add
profile-id 1 cir 32000 shaper-profile-name p3 cbs 16 eir 16000
ebs 1 burst-type short
```

To display the parameters of a queue shaper profile, enter the following command in root view:

```
root> ethernet qos queue-shaper-profile-tbl-broadband show
profile-id <profile-id>
```

To delete a queue shaper profile, enter the following command in root view:

```
root> ethernet qos queue-shaper-profile-tbl-broadband delete
profile-id <profile id>
```

You cannot delete a queue shaper profile if it is attached to a queue. You must first remove the profile from the queue. You can then delete the profile.

Attaching a Shaper Profile to a Queue (CLI)

You can attach one of the configured queue shaper profiles to each priority queue. If no profile is attached to the queue, no egress shaping is performed on that queue. Shapers are attached to queues based on the logical interface and service bundle to which the queue belongs, and the queue's CoS value.

To attach a queue shaper profile to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> queue-shaper add capability service-bundle-id
<service-bundle-id> cos <cos> admin-state <admin-state> profile-id
<profile-id>
```

To change the queue shaper profile attached to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> queue-shaper edit service-bundle-id
<service-bundle-id> cos <cos> admin-state <admin-state>
profile-id <profile-id>
```

To display the queue shaper profile attached to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> queue-shaper show configuration service-
bundle-id <service-bundle-id> cos <cos>
```

To remove a queue shaper profile from a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> queue-shaper delete service-bundle-id
<service-bundle-id> cos <cos>
```

Table 206 Attaching Shaper Profile to Queue CLI Parameters

Parameter	Input Type	Permitted Values	Description
service-bundle-id	Number	1 – 63 **Note:** In the current release, only Service Bundle 1 is supported.	The service bundle to which you are attaching the queue shaper profile.
cos	Number	0 – 7	The CoS queue ID of the queue to which you want to assign the shaper. Queues are numbered according to CoS value.

Parameter	Input Type	Permitted Values	Description
admin-state	Variable	enable disable	Select `enable` to enable egress queue shaping on the queue, or `disable` to disable egress queue shaping on the queue. If you set shaping to `disable`, the shaper profile remains attached to the queue, but does not affect traffic.
profile-id	Number	1 – 32	Enter the ID of one of the configured queue shaper profiles.

The following command adds Queue Shaper Profile 5 to queues with CoS 0, on Service Bundle 1, on GbE 1, and enables shaping on these queues.

```
eth type eth [1/1]> queue-shaper add capability service-
bundle-id 1 cos 0 admin-state enable profile-id 5
```

The following command changes the Queue Shaper Profile assigned in the previous command to Queue Shaper Profile 2:

```
eth type eth [1/1]> queue-shaper edit service-bundle-id
1 cos 0 admin-state enable profile-id 2
```

22.5.2 Configuring Egress Line Compensation for Shaping for PTP 850C and PTP 850E (CLI)

You can configure a line compensation value for all the shapers under a specific logical interface. This value is used to compensate for Layer 1 non-effective traffic bytes on egress.

To set the egress line compensation value, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>shaping-compensation-value set <value>
```

To display the egress line compensation value, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>shaping-compensation-value get
```

Table 207 Egress Line Compensation for Shaping CLI Parameters

Parameter	Input Type	Permitted Values	Description
value	Number	0 – 26 (even numbers only)	Shapers attached to the interface use this value to compensate for Layer 1 non-effective traffic bytes on egress.

The following command sets the egress line compensation value to 0 on GbE 1:

```
eth type eth [1/1]>shaping-compensation-value set 0
```

22.5.3 Configuring Service Bundle Shapers for PTP 850C (CLI)

Note: This section is only relevant if H-QoS is enabled on at least one interface. In System Release 11.9, H-QoS is only supported with PTP 850C. For PTP 850E, H-QoS is planned for future release.

Configuring Service Bundle Shaper Profiles (CLI)

To configure a service bundle shaper profile, enter the following command in root view:

```
root> ethernet qos service-bundle-shaper-profile-tbl-broadband
add profile-id <2-32> cir <0-10000000> pir <0-20000000>
shaper-profile-name <string> cbs <1-32> pbs <1-32>
```

Note: Profile 1 is pre-defined and read-only.

To edit the parameters of an existing service bundle shaper profile, enter the following command in root view:

```
root> ethernet qos service-bundle-shaper-profil-id <2-32> cir
<0-10000000> pir <0-20000000> shaper-profile-name <string> cbs
<1-32> pbs <1-32>
```

To display the parameters of a service bundle shaper profile, enter the following command in root view:

```
root> ethernet qos service-bundle-shaper-profile-tbl-broadband
show profile-id <1-32|all>
```

To delete a service bundle shaper profile, enter the following command in root view:

```
root> ethernet qos service-bundle-shaper-profile-tbl-broadband
delete profile-id <1-32>
```

You cannot delete a service bundle shaper profile if it is attached to an interface. You must first remove the profile from the service bundle. You can then delete the profile.

Parameter	InputType	PermittedValues	Description
profil	Number	1–32	Auniqu

Parameter	InputType	PermittedValues	Description
e-id			eID that identifies the profile.1 is a pre-define

Parameter	InputType	PermittedValues	Description
			dservicebundleshapeprprofileandcannotbee

Parameter	InputType	PermittedValues	Description
			ditedd.
cir	Number	0–100000000	TheCommittedInformationRate(CIR)as

Parameter	InputType	PermittedValues	Description
			signed to the profile, in kbps. Permitted value

Parameter	InputType	PermittedValues	Description
			sare:0–32000,withgranularityof16.32000–

Parameter	InputType	PermittedValues	Description
			1000000000, with granularity of 64.
pir	Number	0 – 2000000000	ThePeakInf

Parameter	InputType	PermittedValues	Description
			ormationRate(PIR)forthesshaper,inkbps.Per

Parameter	InputType	PermittedValues	Description
			mittedvaluesare:16–32000,withgranularity

Parameter	InputType	PermittedValues	Description
			of16.320000–2000000000,withgranularityof6

Parameter	InputType	PermittedValues	Description
			4.
shaper-profile-name	TextString	Upto20characters.	Adescriptionofthepprofile.
cbs	Number	1–32	TheCommittedBu

Parameter	InputType	PermittedValues	Description
			rstSize(CBS)forthesshaper,inKBytes.Permit

Parameter	InputType	PermittedValues	Description
			tedvaluesare1-32.Thedefaultvalueis16.

Parameter	InputType	PermittedValues	Description
pbs	Number	1–64	ThePeakBurstSize(PBS)fortheshaper,inKB

Parameter	InputType	PermittedValues	Description
			ytes.Permittedvaluesare1-32.Thedefaultva

Parameter	Input Type	Permitted Values	Description
			lue is 32.

Attaching a Service Bundle Shaper Profile to an Interface and Service Bundle (CLI)

You can attach one of the configured service bundle shaper profiles to an interface and service bundle.

Note: H-QoS must be configured on the interface in order to assign a service bundle shaper profile to the interface. Otherwise, an error message will appear when you attempt to assign the profile.

To attach a service bundle shaper profile to an interface and service bundle, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> service-bundle-shaper add capability service-bundle-id <1-6> admin-state <enable|disable> profile-id <1-32>
```

To change the service bundle shaper profile attached to a service bundle, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> service-bundle-shaper edit service-bundle-id <1-6> admin-state <enable|disable> profile-id <1-32>
```

To display the service bundle shaper profile attached to a service bundle, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> service-bundle-shaper show configuration service-bundle-id <1-6>
```

To remove a service bundle shaper profile from a service bundle, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> service-bundle-shaper delete service-bundle-id <1-6>
```

The following command assigns Service Bundle Shaper Profile 5 to Ethernet port 1 for Service Bundle 3, and enables shaping on this interface and service bundle:

```
eth type eth [1/1]> service-bundle-shaper add capability
service-bundle-id 3 admin-state enable profile-id 5
```

The following command changes the Service Bundle Shaper Profile assigned in the previous command to Service Bundle 3, from 5 to 4:

eth type eth [1/1]> service-bundle-shaper edit service-bundle-id 3 admin-state enable profile-id 4

22.5.4 Configuring Shapers for PTP 850S (CLI)

This section includes:

- Overview of Egress Shaping for PTP 850S (CLI)
- Configuring Queue Shapers for PTP 850S (CLI)
- Configuring Service Bundle Shapers for PTP 850S (CLI)
- Configuring Egress Line Compensation for Shaping for PTP 850S (CLI)

Overview of Egress Shaping for PTP 850S (CLI)

Egress shaping determines the traffic profile for each queue. PTP 850 performs egress shaping on the following levels:

- Queue level – Single leaky bucket shaping
- Service Bundle level – Dual leaky bucket shaping

> Single leaky bucket shaping on the interface level is planned for future

Configuring Queue Shapers for PTP 850S (CLI)

You can configure up to 32 single leaky bucket queue shaper profiles. The CIR value can be set to the following values:

- 16,000 – 32,000,000 bps – granularity of 16,000 bps
- 32,000,000 – 131,008,000 bps – granularity of 64,000 bps

> You can enter any value within the permitted range. Based on the
>
> value you enter, the software automatically rounds off the setting according to the granularity. If you enter a value below the lowest granular value (except 0), the software adjusts the setting to the minimum.

You can attach one of the configured queue shaper profiles to each priority queue. If no profile is attached to the queue, no egress shaping is performed on that queue.

This section includes:

- Configuring Queue Shaper Profiles for PTP 850S (CLI)
- Attaching a Shaper Profile to a Queue for PTP 850S (CLI)

Configuring Queue Shaper Profiles for PTP 850S (CLI)

To configure a queue shaper profile, enter the following command in root view:

```
root> ethernet qos queue-shaper-profile-tbl add profile-id
<profile-id> cir <cir> shaper-profile-name <shaper-profile-
```

To edit the parameters of an existing queue shaper profile, enter the following command in root view:

```
root> ethernet qos queue-shaper-profile-tbl edit profile-id
<profile-id> cir <cir> shaper-profile-name <shaper-profile-
```

The burst-type parameter is reserved for future use. However, you

To display the parameters of a queue shaper profile, enter the following command in root view:

```
root> ethernet qos queue-shaper-profile-tbl show profile-id
<profile-id>
```

To delete a queue shaper profile, enter the following command in root view:

```
root> ethernet qos queue-shaper-profile-tbl delete profile-id
<profile-id>
```

You cannot delete a queue shaper profile if it is attached to a queue. You must first remove the profile from the queue. You can then delete the profile.

Table 215: Queue Shaper Profiles CLI Parameters

Parameter	Inpu	Permitted	Description
profile-id	Nu mbe	1 - 32	A unique ID that identifies the profile.
cir	Nu mbe r	16000 – 131008000	The Committed Information Rate (CIR) assigned to
shaper-	Text	Up to 20	A description of the

The following command creates Queue Shaper 1, named “p1”, with a CIR value of

16000 bps:

```
root> ethernet qos queue-shaper-profile-tbl add profile-id 1
cir 16000 shaper-profile-name p1
```

The following command changes the CIR value of the profile created above from 16000 to 32000, and changes the profile name to p3:

```
root> ethernet qos queue-shaper-profile-tbl edit profile-id 1
cir 32000 shaper-profile-name p3 burst-type short
```

Attaching a Shaper Profile to a Queue for PTP 850S (CLI)

You can attach one of the configured queue shaper profiles to each priority queue. If no profile is attached to the queue, no egress shaping is performed on that queue. Shapers are attached to queues based on the logical interface and service bundle to which the queue belongs, and the queue's CoS value.

To attach a queue shaper profile to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> queue-shaper add capability service-bundle-
id <service-bundle-id> cos <cos> admin-state <admin-state>
profile-id <profile-id>
```

To change the queue shaper profile attached to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> queue-shaper edit service-bundle-id
<service-bundle-id> cos <cos> admin-state <admin-state>
profile-id <profile-id>
```

To display the queue shaper profile attached to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> queue-shaper show configuration service-
bundle-id <service-bundle-id> cos <cos>
```

To remove a queue shaper profile from a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> queue-shaper delete service-bundle-id
<service-bundle-id> cos <cos>
```

Table 216: Attaching Shaper Profile to Queue CLI Parameters

Paramet	Inp	Permitted	Description
service-bundle-id	Number	1 – 63 **Note:** In the current release, only Service	The service bundle to which you are attaching the queue shaper profile.
cos	Number	0 – 7	The CoS queue ID of the queue to which you want to assign the shaper. Queues are numbered

admin-state	Variable	enable	Select `enable` to enable egress queue shaping on the queue, or `disable` to disable egress queue shaping on the queue. If you set shaping to `disable`, the shaper profile remains attached
profile-id	Number	1 – 32	Enter the ID of one of the configured queue shaper

The following command adds Queue Shaper Profile 5 to queues with CoS 0, on Service Bundle 1, on GbE 1, and enables shaping on these queues:

```
eth type eth [1/1]> queue-shaper add capability service-bundle-id 1 cos 0 admin-state enable profile-id 5
```

The following command changes the Queue Shaper Profile assigned in the previous command to Queue Shaper Profile 2:

```
eth type eth [1/1]> queue-shaper edit service-bundle-id 1 cos 0 admin-state enable profile-id 2
```

Configuring Service Bundle Shapers for PTP 850S (CLI)

You can configure up to 256 dual leaky bucket service bundle shaper profiles. The profiles can be configured as follows:

Valid CIR values are:

0 – 32,000,000 bps, with granularity of 16,000 bps

32,000,000 – 1,000,000,000 bps, with granularity of 64,000 bps Valid PIR values are:

16,000 – 32,000,000 bps, with granularity of 16,000 bps

32,000,000 – 1,000,000,000 bps, with granularity of 64,000 bps

> You can enter any value within the permitted range. Based on the
>
> value you enter, the software automatically rounds off the setting according to the granularity. If you enter a value below the lowest granular value (except 0), the software adjusts the setting to the minimum

You can attach one of the configured service bundle shaper profiles to each service bundle. If no profile is attached to the service bundle, no egress shaping is performed on that service bundle.

This section includes:

Configuring Service Bundle Shaper Profiles for PTP 850S (CLI)

Attaching a Shaper Profile to a Service Bundle for PTP 850S (CLI)

Configuring Service Bundle Shaper Profiles for PTP 850S (CLI)

To configure a service bundle shaper profile, enter the following command in root view:

```
root> ethernet qos service-bundle-shaper-profile-tbl add
profile-id <profile-id> cir <cir> pir <pir> shaper-profile-name
<shaper-profile-name>
```

To edit the parameters of an existing service bundle shaper profile, enter the following command in root view:

```
root> ethernet qos service-bundle-shaper-profile-tbl edit
profile-id <profile-id> cir <cir> pir <pir> shaper-profile-name
<shaper-profile-name>
```

To display the parameters of a service bundle shaper profile, enter the following command in root view:

```
root> ethernet qos service-bundle-shaper-profile-tbl show
profile-id <profile-id>
```

To display the parameters of all configured service bundle shaper profiles, enter the following command in root view:

```
root> ethernet qos service-bundle-shaper-profile-tbl show
profile-id all
```

To delete a service bundle shaper profile, enter the following command in root view:

```
root> ethernet qos service-bundle-shaper-profile-tbl delete
profile-id <profile-id>
```

You cannot delete a service bundle shaper profile if it is attached to a service bundle. You must first remove the profile from the service bundle. You can then delete the profile.

Table 217: Service Bundle Shaper Profiles CLI Parameters

Parameter	Inpu	Permitted	Description
profile-id	Nu	1 - 256	A unique ID that identifies the
cir	Nu mbe	1 - 10000000	The Committed Information Rate (CIR) assigned to the
pir	Nu mbe	16000 - 10000000	The Peak Information Rate (PIR) assigned to
shaper-profile-name	Text Strin	U p	A description of the profile.

The following command creates Service Bundle Shaper 1, named “p1”, with a CIR

value of 100000000 bps and a PIR value of 200000000 bps:

```
root> ethernet qos service-bundle-shaper-profile-tbl add
profile-id 1 cir 100000000 pir 200000000 shaper-profile-name p1
```

The following command changes the CIR value in the Service Bundle Shaper created above from 100000000 bps to 110000000 bps:

```
root> ethernet qos service-bundle-shaper-profile-tbl edit
profile-id 1 cir 110000000 pir 200000000 shaper-profile-name p1
```

Attaching a Shaper Profile to a Service Bundle for PTP 850S (CLI)

You can attach one of the configured service bundle shaper profiles to each service bundle. If no profile is attached to the service bundle, no egress shaping is performed on that service bundle.

To attach a service bundle shaper profile to a service bundle, go to interface view for the service bundle and enter the following command:

```
eth type eth [x/x]> service-bundle-shaper add capability
service-bundle-id <service-bundle-id> admin-state <admin-state>
profile-id <profile-id>
```

To change the service bundle shaper profile attached to a service bundle, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> service-bundle-shaper edit service-bundle-
id <service-bundle-id> admin-state <admin-state> profile-id
<profile-id>
```

To display the service bundle shaper profile attached to a service bundle, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> service-bundle-shaper show configuration
service-bundle-id <service-bundle-id>
```

To remove a service bundle shaper profile from a service bundle, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> service-bundle-shaper delete service-
bundle-id <service-bundle-id>
```

Table 218: Attaching Shaper Profile to Service Bundle CLI Parameters

Paramet	Inp	Permitted	Description
service-bundle-id	Number	1 – 63 **Note:** In the current release, only Service	The service bundle to which you are attaching the queue shaper profile.
admin-state	Variable	e n a b	Select enable to `enable` egress shaping on the service bundle, or `disable` to disable egress shaping on the service bundle.
profile-id	Number	1 – 256	Enter the ID of one of the configured service bundle

The following command adds Service Bundle Shaper Profile 5 to Service Bundle 1, on GbE 1, and enables shaping on this service bundle:

```
eth type eth [1/1]> service-bundle-shaper add capability
service-bundle-id 1 admin-state enable profile-id 5
```

The following command changes the Service Bundle Shaper Profile assigned in the previous command to Service Bundle 1, from 5 to 4:

```
eth type eth [1/1]> service-bundle-shaper edit service-bundle-
id 1 admin-state enable profile-id 4
```

Configuring Egress Line Compensation for Shaping for PTP 850S (CLI)

You can configure a line compensation value for all the shapers under a specific logical interface. This value is used to compensate for Layer 1 non-effective traffic bytes on egress.

To set the egress line compensation value, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>shaping-compensation-value set <value>
```

To display the egress line compensation value, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>shaping-compensation-value get
```

Table 219: Egress Line Compensation for Shaping CLI Parameters

Para	Input	Permitted	Description
valu e	Num ber	0 – 26 (even numbers	Shapers attached to the interface use this value to compensate for Layer 1

The following command sets the egress line compensation value to 0 on GbE 1:

```
eth type eth [1/1]>shaping-compensation-value set 0
```

22.6 Configuring Scheduling (CLI)

This section includes:

- Overview of Egress Scheduling (CLI)
- Configuring Queue Priority (CLI)
- Configuring Interface Priority Profiles (CLI)
- Attaching a Priority Profile to an Interface (CLI)
- Configuring Weighted Fair Queuing (WFQ) (CLI)
- Configuring Service Bundle Weighted Fair Queueing (WFQ) (CLI)

22.6.1 Overview of Egress Scheduling (CLI)

Egress scheduling is responsible for transmission from the priority queues. PTP 850 uses a unique algorithm with a hierarchical scheduling model over the three levels of the egress path that enables compliance with SLA requirements.

The scheduler scans all the queues over all the service bundles, per interface, and determines which queue is ready to transmit. If more than one queue is ready to transmit, the scheduler determines which queue transmits first based on:

Queue Priority – A queue with higher priority is served before lower-priority queues.

Weighted Fair Queuing (WFQ) – If two or more queues have the same priority and are ready to transmit, the scheduler transmits frames from the queues based on a WFQ algorithm that determines the ratio of frames per queue based on a predefined weight assigned to each queue.

22.6.2 Configuring Queue Priority (CLI)

A priority profile defines the exact order for serving the eight priority queues in a single service bundle. When you attach a priority profile to an interface, all the service bundles under the interface inherit the profile.

The priority mechanism distinguishes between two states of the service bundle:

Green State – Committed state

Yellow state – Best effort state

Green State refers to any time when the service bundle rate is below the user-defined CIR. Yellow State refers to any time when the service bundle is above the user-defined CIR but below the PIR.

You can define up to four Green priority profiles, from 4 (highest) to 1 (lowest). An additional four Yellow priority profiles are defined automatically and cannot be changed or edited.

The following table provides a sample of an interface priority profile. This profile is also used as the default interface priority profile.

Table 208 Interface Priority Profile Example

Profile ID (1-9)			
CoS	**Green Priority (user defined)**	**Yellow Priority (read only)**	**Description**
0	1	1	Best Effort
1	2	2	Data Service 4
2	2	2	Data Srvice 3
3	2	2	Data Service 2
4	2	2	Data Service 1
5	3	3	Real Time 2 (Video with large buffer)
6	3	3	Real Time 1 (Video with small buffer)
7	4	4	Management (Sync, PDUs, etc.)

When the service bundle state is Green (committed state), the service bundle priorities are as defined in the Green Priority column. When the service bundle state is Yellow (best effort state), the service bundle priorities are system-defined priorities shown in the Yellow Priority column.



Note

CoS 7 is always marked with the highest priority and cannot be changed or edited, no matter what the service bundle state is, since it is assumed that only high priority traffic will be tunneled via CoS 7.

The system supports up to nine interface priority profiles. Profiles 1 to 8 are defined by the user, while profile 9 is the pre-defined read-only default interface priority profile.

22.6.3 Configuring Interface Priority Profiles (CLI)

To define an interface priority profile, enter the following command in root view:

```
root> ethernet qos port-priority-profile-tbl add profile-id <profile-id> cos0-
priority <cos0-priority> description <description> cos1-priority <cos1-
priority> description <description> cos2-priority <cos2-priority> description
<description> cos3-priority <cos3-priority> description <description> cos4-
priority <cos4-priority> description <description> cos5-priority <cos5-
priority> description <description> cos6-priority <cos6-priority> description
<description> cos7-priority <cos7-priority> description <description>
```

To edit an existing interface priority profile, enter the following command in root view:

```
root> ethernet qos port-priority-profile-tbl edit profile-id <profile-id>
cos0-priority <cos0-priority> description <description> cos1-priority <cos1-
priority> description <description> cos2-priority <cos2-priority> description
<description> cos3-priority <cos3-priority> description <description> cos4-
priority <cos4-priority> description <description> cos5-priority <cos5-
priority> description <description> cos6-priority <cos6-priority> description
<description> cos7-priority <cos7-priority> description <description>
```

To display the parameters of an interface priority profile, enter the following command in root view:

```
root> ethernet qos port-priority-profile-tbl show profile-id <profile-id>
```

To delete an interface priority profile, enter the following command in root view:

```
root> ethernet qos port-priority-profile-tbl delete profile-id <profile-id>
```

You can only delete an interface priority profile if the profile is not attached to any interface.

Table 209 Interface Priority Profile CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 – 8	A unique ID to identify the profile.
cos0-priority	Number	1 – 4	The Green priority for the CoS 0 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 0 egressing the service bundle to which the profile is assigned.
description	Text String	Up to 20 characters.	A description of the priority level.
cos1-priority	Number	1 – 4	The Green priority for the CoS 1 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 1 egressing the service bundle to which the profile is assigned.

Parameter	Input Type	Permitted Values	Description
cos2-priority	Number	1 – 4	The Green priority for the CoS 2 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 2 egressing the service bundle to which the profile is assigned.
cos3-priority	Number	1 – 4	The Green priority for the CoS 3 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 3 egressing the service bundle to which the profile is assigned.
cos4-priority	Number	1 –4	The Green priority for the CoS 4 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 4 egressing the service bundle to which the profile is assigned.
cos5-priority	Number	1 – 4	The Green priority for the CoS 5 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 5 egressing the service bundle to which the profile is assigned.
cos6-priority	Number	1 – 4	The Green priority for the CoS 6 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 6 egressing the service bundle to which the profile is assigned.
cos7-priority	Number	1 – 4	The Green priority for the CoS 7 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 7 egressing the service bundle to which the profile is assigned.

Example

The following command configures a priority profile with Profile ID 1.

```
root> ethernet qos port-priority-profile-tbl add profile-id 1 cos0-priority 1
description c0_p1 cos1-priority 1 description c1_p1 cos2-priority 1
description c2_p1 cos3-priority 2 description c3_p2 cos4-priority 2
description c4_p2 cos5-priority 3 description c5_p3 cos6-priority 4
description c6_p4 cos7-priority 4 description c7_p4
```

This profile has the parameters listed in the following table.

Table 210 Interface Priority Sample Profile Parameters

CoS	Green Priority (user defined)	Yellow Priority (read only)	Description
0	1	1	c0_p1
1	1	1	c1_p1

CoS	Green Priority (user defined)	Yellow Priority (read only)	Description
2	1	1	c2_p1
3	2	1	c3_p2
4	2	1	c4_p2
5	3	1	c5_p3
6	4	1	c6_p4
7	4	4	c7_p4

The following command edits the profile you created in the previous command so that CoS 6 queues have a Green priority of 3 instead of 4, and a description of “c6_p3”.

```
root> ethernet qos port-priority-profile-tbl edit profile-id 1 cos0-priority 1
description c0_p1 cos1-priority 1 description c1_p1 cos2-priority 1
description c2_p1 cos3-priority 2 description c3_p2 cos4-priority 2
description c4_p2 cos5-priority 3 description c5_p3 cos6-priority 3
description c6_p3 cos7-priority 4 description c7_p4
```

22.6.4 Attaching a Priority Profile to an Interface (CLI)

To attach a priority profile to an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> priority set profile-id <profile-id>
```

To display which priority profile is attached to an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> port-priority show profile-id
```

Table 211 Attaching Priority Profile to Interface CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 – 9	Enter the ID of one of the configured logical interface priority profiles.

Examples

The following command attaches Interface Priority Profile 3 to GbE 1:

```
eth type eth [1/1]> priority set profile-id 3
```

The following is a sample output from the `port-priority show profile-id` command:

```
eth type eth [1/1]>port-priority show profile-id
Profile ID: 9
```

```
CoS   Priority              Priority               Description
     (When queue is green)  (When queue is yellow)

0     1                     1                      best effort
1     2                     1                      data service
2     2                     1                      data service
3     2                     1                      data service
4     2                     1                      data service
5     3                     1                      real time
6     3                     1                      real time
7     4                     4                      management
eth type eth [1/1]>
```

22.6.5 Configuring Weighted Fair Queuing (WFQ) (CLI)

This section includes:

- Overview of WFQ for PTP 850C and PTP 850E (CLI)
- Configuring a WFQ Profile for PTP 850S (CLI)
- Attaching a WFQ Profile to an Interface (CLI)

Overview of WFQ for PTP 850C and PTP 850E (CLI)

The scheduler serves the queues based on their priority, but when two or more queues have data to transmit and their priority is the same, the scheduler uses Weighted Fair Queuing (WFQ) to determine the priorities within each priority. WFQ defines the transmission ratio, in bytes, between the queues. All the service bundles under the interface inherit the WFQ profile attached to the interface.

> For each WFQ profile, you can determine the relative weights for both CIR and EIR traffic.

The system supports up to six WFQ interface profiles. Profile ID 1 is a pre-defined read-only profile, and is used as the default profile. Profiles 2 to 6 are user-defined profiles.

The following table provides an example of a WFQ profile.

Table 212 WFQ Profile Example

	Profile ID (1-7)	
CoS	**Queue Weight (Green)**	**Queue Weight (Yellow – not visible to users, and cannot be edited)**
0	15	20
1	15	20
2	15	20
3	15	20
4	15	20

	Profile ID (1-7)	
CoS	**Queue Weight (Green)**	**Queue Weight (Yellow – not visible to users, and cannot be edited)**
5	15	20
6	15	20
7	20	20

You can attach one of the configured interface WFQ profiles to each interface. By default, the interface is assigned Profile ID 1, the pre-defined system profile.

Configuring a WFQ Profile for PTP 850C and PTP 850E (CLI)

To define a WFQ profile, enter the following command in root view:

```
root> ethernet qos wfq-weight-profile-tbl add profile-
id <2-7>  cos0-weight <1-20> cos1-weight <1-20> cos2-
weight <1-20> cos3-
weight <1-20> cos4-weight <1-20> cos5-weight <1-20>
cos6-weight
<1-20> cos7-weight <1-20> cos0-eir-weight <1-20> cos1-
eir-
```

To edit an existing WFQ profile, enter the following command in root view:

```
root> ethernet qos wfq-weight-profile-tbl edit profile-
id <2-7>  cos0-weight <1-20> cos1-weight <1-20> cos2-
weight <1-20> cos3-
weight <1-20> cos4-weight <1-20> cos5-weight <1-20>
cos6-weight
<1-20> cos7-weight <1-20> cos0-eir-weight <1-20> cos1-
eir-
weight <1-20> cos2-eir-weight <1-20> cos3-eir-weight <1-
```

To display the parameters of a WFQ profile, enter the following command in root view:

```
root> ethernet qos wfq-weight-profile-tbl show profile-id
<profile-id>
```

To delete a WFQ profile, enter the following command in root view:

```
root> ethernet qos wfq-weight-profile-tbl delete profile-id
<profile-id>
```

You can only delete a WFQ profile if the profile is not attached to any interface.

The following command configures a WFQ profile with Profile ID 2:

```
root>ethernet qos wfq-weight-profile-tbl add profile-id 2 cos0-
weight 15 cos1-weight 15 cos2-weight 15 cos3-weight 15 cos4-
weight 15 cos5-weight 15 cos6-weight 15 cos7-weight 20 cos0-
eir-weight 20 cos1-eir-weight 20 cos2-eir-weight 20 cos3-eir-
weight 20 cos4-eir-weight 20 cos5-eir-weight 20 cos6-eir-weight
```

This profile has the parameters listed in the following table.

Table 225: WFQ Sample Profile Parameters

C	Queue Weight	Queue Weight (Yellow)
0	15	20
1	15	20
2	15	20
3	15	20
4	15	20
5	15	20
6	15	20
7	20	20

The following command edits the profile you created in the previous command so that CoS 6 queues have a CIR weight of 20 instead of 15:

```
root>ethernet qos wfq-weight-profile-tbl add profile-id 2 cos0-
weight 15 cos1-weight 15 cos2-weight 15 cos3-weight 15 cos4-
weight 15 cos5-weight 15 cos6-weight 20 cos7-weight 20 cos0-
eir-weight 20 cos1-eir-weight 20 cos2-eir-weight 20 cos3-eir-
weight 20 cos4-eir-weight 20 cos5-eir-weight 20 cos6-eir-weight
```

Attaching a WFQ Profile to an Interface for PTP 850C and PTP 850E (CLI)

To attach a WFQ profile to an interface, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]> port-wfq set profile-id <profile-id>
```

To display which WFQ profile is attached to an interface, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]> port-wfq show profile-id
```

Table 226: Attaching WFQ Profile to Interface CLI Parameters

Pa	Inp	Permitted	Description
pr ofi le-	Nu mb er	1 – 6	Enter the ID of one of the configured WFQ profiles.

The following command assigns WFQ Profile 3 to Eth 7:

```
eth type eth [1/7]> port-wfq set profile-id 3
```

The following is a sample display for the `port-wfq show profile-id` command:

```
eth type eth [1/7]>port-wfq show
profile-id

     Queue Weight
       (Green)

        20
        20
        20
        20
        20
        20
        --

eth type
```

Configuring a WFQ Profile for PTP 850S (CLI)

To define a WFQ profile, enter the following command in root view:

```
root> ethernet qos wfq-weight-profile-tbl add profile-id <2-7>
cos0-weight <1-20> cos1-weight <1-20> cos2-weight <1-20> cos3-
weight <1-20> cos4-weight <1-20> cos5-weight <1-20> cos6-weight
<1-20> cos7-weight <1-20> cos0-eir-weight <1-20> cos1-eir-
weight <1-20> cos2-eir-weight <1-20> cos3-eir-weight <1-20>
cos4-eir-weight <1-20> cos5-eir-weight <1-20> cos6-eir-weight
```

To edit an existing WFQ profile, enter the following command in root view:

```
root> ethernet qos wfq-weight-profile-tbl edit profile-id <profile.id> cos0-
weight <cos0-weight> cos1-weight <cos1-weight> cos2-weight <cos2-weight>
cos3-weight <cos3-weight> cos4-weight <cos4-weight> cos5-weight <cos5-
weight> cos6-weight <cos6-weight> cos7-weight <cos7-weight>
```

To display the parameters of a WFQ profile, enter the following command in root view:

```
root> ethernet qos wfq-weight-profile-tbl show profile-id
<profile-id>
```

To delete a WFQ profile, enter the following command in root view:

```
root> ethernet qos wfq-weight-profile-tbl delete profile-id
<profile-id>
```

You can only delete WFQ profile if the profile is not attached to any interface.

Table 213 WFQ Profile CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	2 – 6	A unique ID to identify the profile.
cos0-weight	Number	1 - 20	The relative weight for the CoS 0 queue.
cos1- weight	Number	1 - 20	The relative weight for the CoS 1 queue.
cos2- weight	Number	1 - 20	The relative weight for the CoS 2 queue.
cos3- weight	Number	1 - 20	The relative weight for the CoS 3 queue.
cos4- weight	Number	1 - 20	The relative weight for the CoS 4 queue.
cos5- weight	Number	1 - 20	The relative weight for the CoS 5 queue.
cos6- weight	Number	1 - 20	The relative weight for the CoS 6 queue.
cos7- weight	Number	1 - 20	The relative weight for the CoS 7 queue.

Examples

The following command configures a WFQ profile with Profile ID 2.

```
root> ethernet qos wfq-weight-profile-tbl add profile-id 2
cos0-weight 15 cos1-weight 15 cos2-weight 15 cos3-weight 15
cos4-weight 15 cos5-weight 15 cos6-weight 15 cos7-weight 20
```

This profile has the parameters listed in the following table. Note that the yellow queue weight is constant and cannot be changed. This means that all best effort traffic (yellow) will always have the same weight, regardless of CoS.

Table 214 WFQ Sample Profile Parameters

CoS	Queue Weight (Green)	Queue Weight (Yellow – not visible to users, and cannot be edited)
0	15	20
1	15	20
2	15	20
3	15	20
4	15	20
5	15	20
6	15	20

CoS	Queue Weight (Green)	Queue Weight (Yellow – not visible to users, and cannot be edited)
7	20	20

The following command edits the profile you created in the previous command so that CoS 6 queues have a weight of 20 instead of 15:

```
root> ethernet qos wfq-weight-profile-tbl edit profile-id 2 cos0-weight 15
cos1-weight 15 cos2-weight 15 cos3-weight 15 cos4-weight 15 cos5-weight 15
cos6-weight 20 cos7-weight 20
```

Attaching a WFQ Profile to an Interface (CLI)

To attach a WFQ profile to an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> port-wfq set profile-id <profile-id>
```

To display which WFQ profile is attached to an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> port-wfq show profile-id
```

Table 215 Attaching WFQ Profile to Interface CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 – 6	Enter the ID of one of the configured WFQ profiles.

Examples

The following command assigns WFQ Profile 3 to GbE 1:

```
eth type eth [1/1]> port-wfq set profile-id 3
```

The following is a sample display for the `port-wfq show profile-id` command:

```
eth type eth [1/1]>port-wfq show profile-id

Profile ID: 1

CoS          Queue Weight
               (Green)

0               20
1               20
2               20
3               20
4               20
5               20
6               20
7               20

eth type eth [1/1]>
```

22.7 Displaying Ingress Statistics (CLI)

You can display the following statistics counters for ingress frames and bytes per interface and per service point:

- Green Frames
- Green Bytes
- Yellow Frames
- Yellow Bytes
- Red Frames
- Red Bytes

Note: Ingress statistics are displayed in granularity of 64 bits.

Service point statistics can be displayed for the service point in general or for specific CoS queues on the service point.

22.7.1 Displaying Ingress Statistics per Interface (CLI)

To display ingress statistics per interface, enter the following command in interface view:

```
eth type eth [x/x]>logical-port statistics show clear-in-read
<yes|no>
```

The following commands display statistics for Ethernet interface Eth 7. These commands clear the counters after displaying them.

```
root>ethernet interfaces eth slot 1 port 7
eth type eth [1/7]>logical-port statistics show clear-on-read
yes

_____________________________________________

| Green Packets          |                  0|
| Green Bytes            |                  0|
| Yellow Packets         |                  0|
| Yellow Bytes           |                  0|
| Red Packets            |                  0|
| Red Bytes              |                  0|
eth type eth [1/7]>
```

22.7.2 Displaying Ingress Statistics per Service Point (CLI)

To enable the collection of ingress statistics for a service point, enter the following command in service view:

```
service[x]>sp statistics set spid <1-32> admin-state
<enable|disable>
```

To display ingress statistics for a service point, enter the following command in service view:

```
service[x]>sp statistics show spid <1-30> clear-on-read
<yes|no> layer-1 <yes|no>
```

To enable the collection of ingress statistics for a specific CoS queue on a service point, enter the following command in service view:

```
service[x]>sp statistics set spid <1-32> cos <0-6> admin-state
<enable|disable>
```

To view ingress statistics for a specific CoS queue on a service point, enter the following command in service view:

```
service[x]>sp statistics show spid <1-30> cos <0-6> clear-on-
read <yes|no> layer-1 <yes|no>
```

Note: You cannot enable ingress statistics for both a service point and a CoS queue on the service point at the same time. You can, however, enable ingress statistics on multiple CoS queues at the same time.

The following commands enable and display statistics for service point 30 on service 10. These commands clear the counters after displaying them.

```
root>ethernet service sid 10
service[10]>sp statistics set spid 30 admin-state enable
service[10]>sp statistics show spid 30 clear-on-read yes layer-
1 no

_____________________________________________

| Green Packets          |                   0|
| Green Bytes            |                   0|
| Yellow Packets         |                   0|
| Yellow Bytes           |                   0|
| Red Packets            |                   0|
| Red Bytes              |                   0|
|________________________|____________________|

service[10]>
```

The following commands enable and display statistics for CoS 1 of service point 1 on service 10. These commands clear the counters after displaying them.

```
root>ethernet service sid 10
service[10]>sp statistics set spid 1 cos 1 admin-state enable
service[10]>sp statistics show spid 1 cos 1 clear-on-read yes
layer-1 no
_____________________________________________

| Green Packets          |                   0|
| Green Bytes            |                   0|
| Yellow Packets         |                   0|
| Yellow Bytes           |                   0|
| Red Packets            |                   0|
| Red Bytes              |                   0|
|________________________|____________________|

service[10]>
```

22.8 Displaying Egress PMs and Statistics (CLI)

PTP 850 collects egress PMs and statistics at the queue level and the service bundle level.

22.8.1 Displaying Queue-Level Statistics (CLI)

PTP 850 supports the following counters per queue at the queue level:

- Transmitted Green Packets (64 bits counter)
- Transmitted Green Bytes (64 bits counter)
- Transmitted Green Bits per Second (32 bits counter)
- Dropped Green Packets (64 bits counter)
- Dropped Green Bytes (64 bits counter)
- Transmitted Yellow Packets (64 bits counter)
- Transmitted Yellow Bytes (64 bits counter)
- Transmitted Yellow Bits per Second (32 bits counter)
- Dropped Yellow Packets (64 bits counter)
- Dropped Yellow Bytes (64 bits counter)

To display queue-level PMs, enter interface view for the interface and enter the following command:

```
eth type eth [x/x]> tm-queue show statistics service-bundle-id <service-bundle-id> cos <cos> clear-on-read <clear-on-read> layer-1 <layer-1>
```

To clear queue-level PMs for a specific service bundle, enter interface view for the interface and enter the following command:

```
eth type eth [x/x]> tm-queue clear statistics service-bundle-id <service-bundle-id>
```

Table 216 Egress Queue Level PMs CLI Parameters

Parameter	Input Type	Values	Description
service-bundle-id	Number	1 – 63 **Note**: In the current release, only Service Bundle 1 is supported.	The service bundle for which you want to display PMs.
cos	Number	0 - 7	The queue for which you want to display PMs.
clear-on-read	Boolean	yes no	If you enter yes, the statistics are cleared once you display them.
layer-1	Boolean	yes no	`yes` – Statistics are represented as Layer 1 statistics, including preamble and IFG. `no` – Statistics are represented as Layer 2 statistics.

The following command displays PMs for the CoS 0 queue in Service Bundle 1, on GbE 2. The PMs are cleared after they are displayed.

```
eth type eth [1/2]> tm-queue show statistics service-bundle-id
1 cos 0 clear-on-read yes layer-1 yes
```

The following command clears PMs for all queues in Service Bundle 1, on GbE 2.

```
eth type eth [1/2]> tm-queue clear statistics service-bundle-id
1
```

22.8.2 Configuring and Displaying Queue-Level PMs (CLI)

PTP 850E devices support advanced traffic PMs per CoS queue and service bundle. For each logical interface, you can configure thresholds for Green and Yellow traffic per queue. You can then display the following PMs for 15-minute and 24-hour intervals, per queue and color:

- Maximum bytes passed per second
- Minimum bytes passed per second
- Average bytes passed per second
- Maximum bytes dropped per second
- Minimum bytes dropped per second
- Average bytes dropped per second
- Maximum packets passed per second
- Minimum packets passed per second
- Average packets passed per second
- Maximum packets dropped per second
- Minimum packets dropped per second
- Average packets dropped per second
- Seconds bytes per second were over the configured threshold per interval

These PMs are available for any type of logical interface, including groups. To activate collection of these PMs, the user must add a PM collection rule on a logical interface and service bundle and set the relevant thresholds per CoS and Color. When the PM is configured on a group, queue traffic PMs are recorded for the group and not for the individual interfaces that belong to the group.

One collection rule is available per interface.

PMs for queue traffic are saved for 30 days, after which they are removed from the database. It is important to note that they are not persistent, which means they are not saved in the event of unit reset.

To configure and display queue-level PMs, you must first enter interface view. See Entering Interface View (CLI).

To display whether any service bundles are configured on an interface, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show configuration all
```

If no service bundles have been configured, the following output is displayed:

```
eth type eth [1/x]>pm tm-queue show configuration all
Num entries: 0
```

If a service bundle has been configured and enabled, the following output is displayed:

```
eth type eth [1/x]>pm tm-queue show configuration all
Service bundle: 1   Admin: enable
Num entries: 1
```

If a service bundle has been configured but it's Admin status is disabled, the following output is displayed:

```
eth type eth [1/x]>pm tm-queue show configuration all
Service bundle: 1   Admin: disable
Num entries: 1
```

To configure a service bundle, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue create service-bundle-id <1-6>
admin-state <enable|disable>
```

To change the Admin state of a service bundle, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue set service-bundle-id <1-6> admin-
state <enable|disable>
```

To remove a service bundle, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue remove service-bundle-id <1-6>
```

For example:

```
eth type eth [1/7]>pm tm-queue remove service-bundle-id 1
WARNING: All PM history for that service bundle will be deleted.
Are you sure? (yes/no):yes
eth type eth [1/7]>
```

To display the threshold settings for a service bundle, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show configuration service-bundle-id <1-
6>
```

For example:

```
eth type eth [1/7]>pm tm-queue show configuration service-
bundle-id 1
Admin: enable
cos0 green  bytes passed threshold:     675000 bytes
cos1 green  bytes passed threshold:     675000 bytes
cos2 green  bytes passed threshold:     675000 bytes
cos3 green  bytes passed threshold:     675000 bytes
cos4 green  bytes passed threshold:     675000 bytes
cos5 green  bytes passed threshold:     675000 bytes
cos6 green  bytes passed threshold:     675000 bytes
cos7 green  bytes passed threshold:     675000 bytes
cos0 yellow bytes passed threshold:     675000 bytes
cos1 yellow bytes passed threshold:     675000 bytes
cos2 yellow bytes passed threshold:     100000 bytes
cos3 yellow bytes passed threshold:     675000 bytes
cos4 yellow bytes passed threshold:     675000 bytes
cos5 yellow bytes passed threshold:     675000 bytes
cos6 yellow bytes passed threshold:     675000 bytes
cos7 yellow bytes passed threshold:     675000 bytes
```

To set thresholds for green bytes, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue set service-bundle-id <1-6> cos <0-7>
green-bytes-passed-threshold <0-4294967295>
```

To set thresholds for yellow bytes, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue set service-bundle-id <1-6> cos <0-7>
yellow-bytes-passed-threshold <0-4294967295>
```

To display PMs for green bytes passed, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show counter green_bytes_passed service-
bundle-id 1 cos <0-7> interval <15min|24hr>
```

To display PMs for green packets passed, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show counter green_packets_passed
service-bundle-id 1 cos <0-7> interval <15min|24hr>
```

To display PMs for green bytes dropped, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show counter green_bytes_dropped
service-bundle-id 1 cos <0-7> interval <15min|24hr>
```

To display PMs for green packets dropped, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show counter green_packets_dropped
service-bundle-id 1 cos <0-7> interval <15min|24hr>
```

To display PMs for yellow bytes passed, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show counter yellow_bytes_passed
service-bundle-id 1 cos <0-7> interval <15min|24hr>
```

To display PMs for yellow packets passed, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show counter yellow_packets_passed
service-bundle-id 1 cos <0-7> interval <15min|24hr>
```

To display PMs for yellow bytes dropped, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show counter yellow_bytes_dropped
service-bundle-id 1 cos <0-7> interval <15min|24hr>
```

To display PMs for yellow packets dropped, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show counter yellow_packets_dropped
service-bundle-id 1 cos <0-7> interval <15min|24hr>
```

The integrity column indicates whether the PM is valid:

- 0 indicates a valid entry.
- 1 indicates an invalid entry. This can occur for a number of reasons, including but not limited to a disconnected cable, a missing SFP transceivers, muting of a radio interface, and an operational status of Down.

22.8.3 Displaying Service Bundle-Level Statistics (CLI)

PTP 850 supports the following counters per service bundle at the service bundle level:

- Transmitted Green Packets (64 bits counter)
- Transmitted Green Bytes (64 bits counter)

- Transmitted Green Bits per Second (32 bits counter)
- Dropped Green Packets (64 bits counter)
- Dropped Green Bytes (64 bits counter)
- Transmitted Yellow Packets (64 bits counter)
- Transmitted Yellow Bytes (64 bits counter)
- Transmitted Yellow Bits per Second (32 bits counter)
- Dropped Yellow Packets (64 bits counter)
- Dropped Yellow Bytes (64 bits counter)

To display service bundle-level PMs, enter interface view for the interface and enter the following command:

```
eth type eth [x/x]> tm-service-bundle show statistics service-bundle-id <service-bundle-id> clear-on-read <clear-on-read> layer-1 <layer-1>
```

To clear service bundle-level PMs for all service bundles on an interface, enter interface view for the interface and enter the following command:

```
eth type eth [x/x]> tm-service-bundle clear statistics
```

Table 217 Egress Service Bundle Level PMs CLI Parameters

Parameter	Input Type	Permitted Values	Description
service-bundle-id	Number	1 – 63 **Note:** In the current release, only Service Bundle 1 is supported.	The service bundle for which you want to display PMs.
clearon-read	Boolean	yes no	If you enter yes, the statistics are cleared once you display them.
layer-1	Boolean	yes no	• `yes` – Statistics are represented as Layer 1 statistics, including preamble and IFG. • `no` – Statistics are represented as Layer 2 statistics.

Examples

The following command displays service bundle PMs for Service Bundle 1, on GbE 1. The PMs are cleared after they are displayed.

```
eth type eth [1/1]> tm-service-bundle show statistics service-bundle-id 1 clear-on-read yes layer-1 yes
```

23. Ethernet Protocols (CLI)

This section includes:

- Configuring G.8032 (CLI)
- Configuring MSTP (CLI)
- Configuring Ethernet Bandwidth Notification (ETH-BN) (CLI)
- Configuring LLDP (CLI)

Related Topics:

- Configuring Service OAM (SOAM) Fault Management (FM) (CLI)

23.1 Configuring G.8032 (CLI)

This section includes:

- Configuring the Destination MAC Address (CLI)
- Configuring ERPIs (CLI)
- Configuring the RPL Owner (CLI)
- Configuring Timers (CLI)
- Initiating a Manual or Forced Switch and Clearing the Switch or Initiating Reversion (CLI)
- Blocking or Unblocking R-APS Messages on a Service Point (CLI)
- Displaying the ERPI Attributes (CLI)

P2P services are not affected by G.8032, and continue to traverse

ports that are blocked by G.8032

G.8032 cannot be configured on management ports, including

Configuring the Destination MAC Address (CLI)

To set the destination MAC address for PDUs generated by the node, enter the following command in root view:

```
root> ethernet generalcfg g8032-dest-mac-address set MAC <MAC address>
```

To display the destination MAC address, enter the following command in root view:

```
root> ethernet generalcfg g8032-dest-mac-address show
```

To display the destination MAC address and the node ID, enter the following command in root view:

```
root> ethernet g8032 show-node-attributes
```

The node ID is the base MAC address for the node.

Table 233: G.8032 Destination MAC Address CLI Parameters

Pa	Input Type	Permitted Values	Description
M AC ad dr	Six groups of two hexade	01:19:a7:00:00:x where x can be any number between 0 and 16.	The destination MAC address for PDUs generated by the node.

The following command sets the destination MAC address as 01:19:a7:00:00:02:

```
root> ethernet generalcfg g8032-dest-mac-address set MAC
01:19:a7:00:00:02
```

Configuring ERPIs (CLI)

You can configure up to 16 Ethernet Ring Protection instances (ERPIs). Each ERPI is associated with an Ethernet service defined in the system. An ERPI can be:

- **Ring**: A Ring is an Ethernet ring that is connected on two ports (East and West service points) to an interconnection node.
- **Sub-Ring**: A Sub-Ring is an Ethernet ring which is connected to another ring or network through the use of interconnection nodes (East and West service points). On their own, the Rub-Ring links do not form a closed physical loop. A closed loop may be formed by the sub-ring links and the link between interconnection nodes that is controlled by other ring or network.
- **Ring with Sub-Ring**: The ERPI includes both a ring, with East and West service points, and a connection to a sub-ring using a Sub-Ring service point.

Service points on the PTP 820 side of the link must have a single, determinate VLAN. This means the service point type must be dot1q, s-tag, or QinQ. On the customer side, any service point

To add a Ring ERPI, enter the following command in root view:

```
root> ethernet g8032 create-erpi erp-type ring erpi-id <erpi-
id> erpi-service-id <erpi-service-id> west-sp <west-sp> east-sp
```

To add a Sub-Ring ERPI, enter the following command in root view:

```
root> ethernet g8032 create-erpi erp-type sub-ring erpi-id
<erpi-id> erpi-service-id <erpi-service-id> west-sp <west-sp>
```

To add a Ring with Sub-Ring ERPI, enter the following command in root view:

```
root> ethernet g8032 create-erpi erp-type ring-with-sub-ring
erpi-id <erpi-id> erpi-service-id <erpi-service-id> west-sp
<west-sp> east-sp <east-sp> sub-ring-sp <sub-ring-sp> level
```

To assign a name to an ERPI, enter the following command in root view:

```
root> ethernet g8032 set-erpi-name erpi-id <erpi-id> erpi-name
<erpi-name>
```

To delete an ERPI, enter the following command in root view:

```
root> ethernet g8032 delete-erpi erpi-id 1
```

Table 234: G.8032 ERPI Configuration CLI Parameters

Para	In	Permitted	Description
er	Nu	1-64	A unique ID that identifies the ERPI.
er	Numb	1-4095	The ID of the Ethernet service to which the ERPI belongs.
wes	Numb	1-32	The first endpoint for the ERPI. This can be any service point that has been configured
east-	Numb	1-32	The second endpoint for the ERPI. This can be any service point that has been configured for
sub-rin	Number	1-32	The service point that connects the Ring with the Sub- Ring. This can be any service point that has been configured for the
leve	Numb	0-7	Optional. The Maintenance Entity Group (MEG) level used for R-APS messages sent in the ERPI.
versi	Numb	1-2	Optional. The ERPI (G.8032) protocol version currently being used in the unit.
er	Text		A descriptive name for the ERPI.

The following commands create a Ring ERPI with ID 1, and name the ERPI "service_x". This ERPI is associated with Ethernet Service 1. The end points of the ERPI are Service Point 1 and Service Point 2. The ERPI is configured with MEG level 2:

```
root> ethernet g8032 create-erpi erp-type ring erpi-id 1 erpi-
service-id 1 west-sp 1 east-sp 2 level 2

root> ethernet g8032 set-erpi-name erpi-id 1 erpi-name
```

The following commands create a Sub-Ring ERPI with ID 10, and name the ERPI "Sub_ring". This ERPI is associated with Ethernet Service 20. The end points of the ERPI are Service Point 1 and Service Point 2. The ERPI is configured with MEG level 4:

```
root> ethernet g8032 create-erpi erp-type sub-ring erpi-id 10
erpi-service-id 20 west-sp 1 east-sp 2 level 4
```

The following commands create a Ring with Sub-Ring ERPI with ID 20, and name the ERPI "RSRi". This ERPI is associated with Ethernet Service 30. The end points of the ERPI are Service Point 1 and Service Point 2, and the point of connection between the Ring and the Sub-Ring is Service Point 3. The ERPI is configured with MEG level 5:

```
root> ethernet g8032 create-erpi erp-type ring-with-sub-ring
erpi-id 20 erpi-service-id 30 west-sp 1 east-sp 2 sub-ring-sp 3
level 5
```

The following command deletes ERPI 1:

```
root> ethernet g8032 delete-erpi erpi-id 1
```

Configuring the RPL Owner (CLI)

The RPL Owner Node is a node in the ERPI that is responsible for blocking traffic at one end of the ERPI. You can select one RPL per ERPI.

To set the RPL Owner Node, enter the following command in root view:

```
root> ethernet g8032 set-rpl-owner erpi-id <erpi-id> SP <SP>
```

To remove the RPL Owner Node, enter the following command in root view:

```
root> ethernet g8032 remove-rpl-owner erpi-id <erpi-id>
```

Table 235: G.8032 RPL Owner CLI Parameters

Par	Input Type	Permitted Values	Description
erpi	Number	1-64	The ID of the ERPI for which you want to set or delete the RPL
SP	Num	east	Specifies the service point you want to designate as the RPL owner.

The following command sets the East service point as the RPL owner for ERPI 1:

```
root> ethernet g8032 set-rpl-owner erpi-id 1 SP east
```

The following command sets the Sub-Ring service point as the RPL owner for ERPI 20:

```
root> ethernet g8032 set-rpl-owner erpi-id 20 SP sub-ring
```

The following command removes the RPL owner for ERPI 1

Configuring Timers (CLI)

You can configure timers per ERPI to control the ERPI's switching and convergence parameters. The following timers are available:

- **Wait to Restore (WTR) Timer** – Defines a minimum time the system waits after signal failure is recovered before reverting to idle state, when the RPL can again be blocked.
- **Guard Time** – The guard time is the minimum time the system waits after recovery from a signal failure before accepting new R-APS messages. The Guard Time should be greater than the maximum expected forwarding delay for which one R-APS message circles around the ring.

The Guard Time is used to prevent Ethernet ring nodes from acting upon outdated R-APS messages and prevents the possibility of

- **Hold-Off Time** – Determines the time period from failure detection to response. It is used to coordinate between recovery mechanisms (which mechanism takes place first).

To configure the WTR timer, enter the following command in root view:

```
root> ethernet g8032 set-wtr erpi-id <erpi-id> wtr <wtr>
```

To configure the guard time, enter the following command in root view:

```
root> ethernet g8032 set-guard-time erpi-id <erpi-id> guard-
time <guard-time>
```

To configure the hold-off, enter the following command in root view:

```
root> ethernet g8032 set-holdoff-time erpi-id <erpi-id>
holdoff-time <holdoff-time>
```

Table 236: G.8032 Timer Configuration CLI Parameters

Parameter	In	Per	Description
erpi-	Nu	1-64	The ID of the ERPI for which you want to
wtr	Number	1-12	The minimum time (in minutes) the system waits after signal failure is recovered before reverting to idle
gua	Number	10-2000, in multiples	The minimum time (in msec) the system waits after recovery from a signal failure before accepting new R-APS
hold	Number	0-10000, in multiples of 100	The minimum time (in msec) the system waits before reacting to a signal failure.

The following command sets the WTR timer for ERPI 1 to 2 minutes:

```
root> ethernet g8032 set-wtr erpi-id 1 wtr 2
```

The following command sets the guard time for ERPI 1 to 20 msecs:

```
root> ethernet g8032 set-guard-time erpi-id 1 guard-time 20
```

The following command sets the hold-off time for ERPI 1 to 1000 msecs:

```
root> ethernet g8032 set-holdoff-time erpi-id 1 holdoff-time
1000
```

Initiating a Manual or Forced Switch and Clearing the Switch or Initiating Reversion (CLI)

To initiate a forced switch, enter the following command in root view:

```
root> ethernet g8032 fs-erpi erpi-id <erpi-id> SP <SP>
```

To initiate a manual switch, enter the following command in root view:

```
root> ethernet g8032 ms-erpi erpi-id <erpi-id> SP <SP>
```

You can use a "clear" command to clear a forced or manual switch. You can also use a "clear" command to trigger convergence prior to the expiration of the relevant timer. To issue a "clear" command, enter the following command in root view:

```
root> ethernet g8032 clear-erpi erpi-id <erpi-id> SP <SP>
```

Table 237: G.8032 Switching and Reversion CLI Parameters

Par	Input Type	Permit	Description
erpi-	Number	1-64	The ID of the ERPI on which you want to perform or clear the switch or initiate convergence.
SP	Num	east	Specifies the service point on which to clear the manual or forced switch or to implement convergence.

The following command initiates a forced switch in the East service point of ERPI 1:

```
root> ethernet g8032 fs-erpi erpi-id 1 SP east
```

The following command initiates a manual switch in the Sub-Ring service point of ERPI 20:

```
root> ethernet g8032 ms-erpi erpi-id 20 SP sub-ring
```

The following command initiates convergence in the East service point of ERPI 1:

```
root> ethernet g8032 clear-erpi erpi-id 1 SP east
```

Blocking or Unblocking R-APS Messages on a Service Point (CLI)

To enable or disable transmission of R-APS messages on a service point, enter the following command in root view:

```
root> ethernet g8032 set-erpi-sp-tx-raps-cntrl erpi-id <erpi-
```

Table 238: G.8032 Switching and Reversion CLI Parameters

Par	Input Type	Permit	Description
erpi-	Number	1-64	The ID of the ERPI on which you want to perform or clear the switch or initiate convergence.
SP	Variable	east	Specifies the service point on which to clear the manual or forced switch or to implement convergence.
txraps	Variable	true	`true` – R-APS message transmission is enabled on the service point. `false` – R-APS message transmission is blocked on the service point.

Displaying the ERPI Attributes (CLI)

To display a list of all ERPIs configured on the unit, enter the following command in root view:

```
root> ethernet g8032 show-all-erpi
```

The following is an example of this command's output.

```
root> ethernet g8032 show-all-erpi
=============================================================================================
|ERPI id  |ERPI name       |Service |User      |Ring state  |West SP |East SP |Sub-ring SP |
|         |                |        |instance  |            |        |        |            |
=============================================================================================
|1        |                |1       |1         |protecting  |3       |2       |1           |
+---------+----------------+--------+----------+------------+--------+--------+------------+
|2        |                |2       |2         |protecting  |3       |2       |N/A         |
+---------+----------------+--------+----------+------------+--------+--------+------------+
|3        |                |5       |5         |protecting  |3       |2       |N/A         |
+---------+----------------+--------+----------+------------+--------+--------+------------+
|4        |                |6       |6         |protecting  |3       |2       |N/A         |
+---------+----------------+--------+----------+------------+--------+--------+------------+
|5        |                |7       |7         |protecting  |3       |2       |N/A         |
+---------+----------------+--------+----------+------------+--------+--------+------------+
|6        |                |8       |8         |protecting  |3       |2       |N/A         |
+---------+----------------+--------+----------+------------+--------+--------+------------+
|8        |                |3       |15        |protecting  |2       |1       |N/A         |
+---------+----------------+--------+----------+------------+--------+--------+------------+
|16       |                |4       |16        |protecting  |2       |1       |N/A         |
+---------+----------------+--------+----------+------------+--------+--------+------------+
root>
```

To display all ERPIs that include a service point on a specific port, enter the following command in root view:

```
root> ethernet g8032 show-all-port-erpi interface <interface>
slot <slot> port <port>
```

To display all ERPIs that include a service point on a specific group, enter the following command in root view:

```
root> ethernet g8032 show-all-port-erpi group <group>
```

The following command displays all ERPIs with a service point on LAG group 1:

```
root> ethernet g8032 show-all-port-erpi group lag1
```

The following command displays all ERPIs with a service point on HSB protection group 2:

```
root> ethernet g8032 show-all-port-erpi group rp2
```

The following command displays all ERPIs with a service point on Multi-Carrier ABC group 1:

```
root> ethernet g8032 show-all-port-erpi group mc-abc1
```

The following is an example of this command's output.

```
root> ethernet g8032 show-all-port-erpi interface radio slot 5 port 1
=============================================================================================
|ERPI id  |ERPI name        |Service |User      |Ring state  |West SP |East SP |Sub-ring SP |
|         |                 |        |instance  |            |        |        |            |
=============================================================================================
|1        |                 |1       |1         |protecting  |3       |2       |1           |
+---------+-----------------+--------+----------+------------+--------+--------+------------+
|2        |                 |2       |2         |protecting  |3       |2       |N/A         |
+---------+-----------------+--------+----------+------------+--------+--------+------------+
|3        |                 |5       |5         |protecting  |3       |2       |N/A         |
+---------+-----------------+--------+----------+------------+--------+--------+------------+
|4        |                 |6       |6         |protecting  |3       |2       |N/A         |
+---------+-----------------+--------+----------+------------+--------+--------+------------+
|5        |                 |7       |7         |protecting  |3       |2       |N/A         |
+---------+-----------------+--------+----------+------------+--------+--------+------------+
|6        |                 |8       |8         |protecting  |3       |2       |N/A         |
+---------+-----------------+--------+----------+------------+--------+--------+------------+
|8        |                 |3       |15        |protecting  |2       |1       |N/A         |
+---------+-----------------+--------+----------+------------+--------+--------+------------+
|16       |                 |4       |16        |protecting  |2       |1       |N/A         |
+---------+-----------------+--------+----------+------------+--------+--------+------------+
root>
```

To display detailed information about a specific ERPI, enter the following command in root view:

```
root> ethernet g8032 show-erpi-config erpi-id <erpi-id>
```

The following command displays detailed output for ERPI 1:

```
root> ethernet g8032 show-erpi-config erpi-id 1
```

The following is an example `of this command's output.

```
root> ethernet g8032 show-erpi-config erpi-id 1
=============================================================================================================================================
|ERPI id  |ERPI name        |Service |User      |West SP |East SP |Sub-ring SP |ERPI type          |MEG level |Version |Virtual |RPL owner |
|         |                 |        |instance  |        |        |            |                   |          |        |channel |          |
=============================================================================================================================================
|1        |                 |1       |1         |3       |2       |1           |ring               |1         |2       |0       |none      |
=============================================================================================
|Revertive |WTR    |Guard time |Hold-off |SD handling |West SP SD          |East SP SD          |Sub-ring SP SD     |
|          |       |time       |time     |            |capacity threshold  |capacity threshold  |capacity threshold|
=============================================================================================
|true      |5      |500        |0        |2           |50                  |50                  |50                 |
+----------+-------+-----------+---------+------------+--------------------+--------------------+-------------------+

root>
```

To display state information about a specific ERPI, enter the following command in root view:

```
root> ethernet g8032 show-erpi-dynamic erpi-id <erpi-id>
```

The following command displays detailed output for ERPI 1:

```
root> ethernet g8032 show-erpi-dynamic erpi-id 1
```

The following is an example of this command's output.

```
root> ethernet g8032 show-erpi-dynamic erpi-id 1
================================================================================
|ERPI id  |Ring state  |Local state |Remote state |Last HP request |Last change time |
================================================================================
|1        |protecting  |clear-sf    |raps-sf      |nr              |0                |
+---------+------------+------------+-------------+----------------+-----------------+
root> 
```

Table 239: G.8032 ERPI Display Command Input Parameters

Par	Ir	Permitted Values	Description
interfa	Variabl	eth r	Enter the type of interface: eth – Ethernet radio – Radio
slot	Numbe	Ether n	
port	Numbe	• Ethernet interface on PTP 850C: 1-4 • Ethernet interface on PTP 850E: 1-7 • Ethernet interface on PTP 850S: 1-3 • Radio interface on an PTP 850C: 1-2 Radio interface on an PTP 850E or	The port number of the interface.
group	Variable	lag1 lag2	To enter interface view for a LAG group, enter the group (lag1 - lag4). To enter interface view for a Multi- Carrier ABC group, enter the group (mc-abc1 – mc-abc4) (PTP 850C only).
erpi-id	Numb	1-64	The ID of the ERPI for which you want to perform or clear the switch, initiate

Table 240: G.8032 ERPI Display Command Output Parameters

Parameter	Description
ERPI ID	A unique ID that identifies the ERPI.
ERPI Name	A descriptive name for the ERPI.
Service	The ID of the Ethernet service to which the ERPI belongs.
User Instance	The MSTI to which the Ethernet service is mapped.

Parameter	Description
Ring State	Indicates the current ERPI state. Possible values are: Initializing I d l e P
West SP	The interface to which the west ERPI service point belongs.
East SP	The interface to which the east ERPI service point belongs.
Sub-Ring SP	The interface to which the ERPI service point that connects the Ring to the Sub-Ring belongs.
ERPI Type	The ERPI type (Ring, Sub-Ring, or Ring with Sub-Ring).
MEG Level	The Maintenance Entity Group (MEG) level used for R-APS messages sent in the ERPI.
Version	The ERPI (G.8032) protocol version currently being used in the unit.
Virtual Channel	Reserved for future use.
RPL Owner	Indicates whether the ERPI is currently an RPL owner, and if it is, which ERPI port is the owner.
Revertive	Indicates whether the ERPI is currently in revertive mode.
WTR	The Wait to Restore (WTR) timer. This timer sets the minimum time (in minutes) the system waits after signal failure before entering revertive mode.
Guard Time	The minimum time (in msec) the system waits after recovery from a signal failure before accepting new R-APS messages. The purpose of this timer is to prevent unnecessary state changes that might be caused by outdated messages.
Hold-Off Time	The minimum time (in msec) the system waits before reacting to a signal failure.
SD Handling	Reserved for future use.
West SP SD Capacity	Reserved for future use.
East SP SD Capacity	Reserved for future use.
Sub-Ring SP SD Capacity	Reserved for future use.
Local State	The current local state input to the ERPI state machine.
Remote State	The last event received from the other end of the link.
Last HP Request	The last high priority request.
Last Change Time	The time of the last ring state transition.

To display the state of a specific service point, enter the following command in root view:

```
root> ethernet g8032 show-erpi-sp-state erpi-id <erpi-id> SP
<SP>
```

The following command displays the current state of the East service point for ERPI 1:

```
root> ethernet g8032 show-erpi-sp-state erpi-id 1 SP east
```

The following is an example of this command's output.

```
root> ethernet g8032 show-erpi-sp-state erpi-id 1 SP east
+-------+--------+-----+------------+-----------------+-----------------+-------------+----------+---------+---------+---------+---------+
|ERPI id|SP index|SP ID|Active state|R-APS channel    |Data             |RPL link     |Defect    |Tx R-APS |Tx R-APS |Tx R-APS |Tx R-APS |
|       |        |     |            |forwarding state |forwarding state |blocked state|state     |frames   |SF       |NR       |RB       |
+-------+--------+-----+------------+-----------------+-----------------+-------------+----------+---------+---------+---------+---------+
|1      |east    |2    |true        |true             |true             |false        |no-defect|3        |0        |3        |0        |
+-------+--------+-----+------------+-----------------+-----------------+-------------+----------+---------+---------+---------+---------+

+---------+---------+---------+---------+-------------+---------+---------+---------+---------+---------+---------+
|Tx R-APS |Tx R-APS |Tx R-APS |Rx R-APS |Rx invalid   |Rx R-APS |Rx R-APS |Rx R-APS |Rx R-APS |Rx R-APS |Rx R-APS |
|FS       |MS       |event    |frames   |R-APS frames |SF       |NR       |RB       |SD       |FS       |MS       |event    |
+---------+---------+---------+---------+-------------+---------+---------+---------+---------+---------+---------+---------+
|0        |0        |0        |1762     |0            |1756     |6        |0        |0        |0        |0        |0        |
+---------+---------+---------+---------+-------------+---------+---------+---------+---------+---------+---------+---------+
root>
```

Table 241: G.8032 Service Point Display Command Output Parameters

Parameter	Description
ERPI ID	A unique ID that identifies the ERPI.
SP Index	Identifies the service point in the ERPI.
SP ID	The Service Point ID.
Active State	Indicates whether or not the service point is active for traffic forwarding.
R-APS Channel Forwarding State	Indicates whether the service point is forwarding R-APS messages.
Data Forwarding State	Indicates whether the service point is in unblocked (forwarding) state.
RPL Link Blocked State	Only relevant if the ERPI to which the service point belongs is the RPL owner. Indicates whether the service
Defect State	Indicates whether the service point is in Signal Fail (SF) or Signal Defect (SD) state. **Note:** Support for Signal Defect state is planned for future release.
TX R-APS Frames	The number of R-APS frames that have been transmitted via the service point.
TX R-APS SF	The number of R-APS Signal Fail (SF) frames that have been transmitted via the service point.
TX R-APS NR	The number of R-APS No Request (NR) frames that have been transmitted via the service point.
TX R-APS RB	The number of R-APS RPL Blocked (RB) frames that have been transmitted via the service point.
TX R-APS SD	The number of R-APS Signal Degrade (SD) frames that have been transmitted via the service point.

Parameter	Description
TX R-APS FS	The number of R-APS Forced Switch (FS) frames that have been transmitted via the service point.
TX R-APS MS	The number of R-APS Manual Switch (MS) frames that have been transmitted via the service point.
TX R-APS Event	Reserved for future use.
RX R-APS Frames	The number of R-APS frames that have been received by the service point.
RX Invalid R-APS Frames	The number of R-APS frames with an invalid format that have been received by the service point.
RX R-APS SF	The number of R-APS Signal Fail (SF) frames that have been received by the service point.
RX R-APS NR	The number of R-APS No Request (NR) frames that have been received by the service point.
TX R-APS RB	The number of R-APS RPL Blocked (RB) frames that have been transmitted by the service point.
TX R-APS SD	The number of R-APS Signal Degrade (SD) frames that have been transmitted by the service point.
TX R-APS FS	The number of R-APS Forced Switch (FS) frames that have been transmitted by the service point.
TX R-APS MS	The number of R-APS Manual Switch (MS) frames that have been transmitted by the service point.
TX R-APS Event	Reserved for future use.

23.2 Configuring MSTP (CLI)

This section includes:

- *Configuring the MSTP Bridge Parameters (CLI)*
- *Configuring the MSTP Port Parameters (CLI)*

P2P services are not affected by MSTP, and continue to traverse ports

MSTP cannot be configured on management ports, including

Configuring the MSTP Bridge Parameters (CLI)

This section includes:

- Enabling and Disabling MSTP (CLI)
- Defining the Number of MSTIs (CLI)
- Setting the BPDU Destination MAC Address (CLI)
- Freezing MSTP (CLI)
- Resetting the MSTP Stack (CLI)
- Handling Signal Degrade (SD) Failures (CLI)
- Setting the Configuration ID (CLI)
- Mapping Services to MSTIs (CLI)
- Setting the Bridge Level Spanning Tree Parameters (CLI)
- Setting and Viewing the Bridge Level MSTI Parameters (CLI)
- Viewing the MSTP Parameters (CLI)

Enabling and Disabling MSTP (CLI)

Enabling MSTP starts the protocol and sets all port states in all MSTP instances to Blocking. Convergence upon enabling the protocol generally takes less than two seconds.

All mapping of Ethernet services to MSTP instances (MSTIs) should be

performed *before* enabling MSTP, For instructions, see *Mapping Services to MSTIs (CLI)*

To enable MSTP on the unit, enter the following command in root view:

```
root> ethernet mstp mstp-enable
```

Disabling MSTP stops the MSTP protocol from running and sets all ports in all MSTP instances to Forwarding state.

To disable MSTP on the unit, enter the following command in root view:

```
root> ethernet mstp mstp-disable
```

To display whether MSTP is currently enabled or disabled on the unit, enter the following command in root view:

```
root> ethernet mstp show-mstp-enabled
```

Defining the Number of MSTIs (CLI)

PTP 820C and PTP 820V can support from 1 to 16 Multiple Spanning Tree Instances (MSTIs) on a single unit. This does not include the Common and Internal Spanning Tree (CIST).

To specify the number of MSTIs, enter the following command in root view:

```
root> ethernet mstp set number-of-instances <MSTI>
```

To display the number of MSTIs on the unit, enter the following command in root view:

```
root> ethernet mstp show-number-of-instances
```

Table 242: Defining Number of MSTIs CLI Parameters

P	In	Permitted	Description
MSTI	Number	2-16	The number of MSTIs on the unit. This number does not include the Common and Internal Spanning Tree

The following command sets the number of MSTIs to 14:

```
root> ethernet mstp set number-of-instances 14
```

Setting the BPDU Destination MAC Address (CLI)

To specify the destination MAC address for BPDUs generated in the unit, enter the following command in root view:

```
root> ethernet mstp set bpdu-destination-mac <bpdu-destination-
```

Table 243: BPDU Destination MAC Address CLI Parameters

Parameter	In	Permitted Values	Description
bpdu-destination-mac	Variable	customer	`customer` – The destination MAC address of BPDUs is 0x0180-C200-0000. Provider BPDUs are either tunneled or discarded. `provider` – The destination MAC address of BPDUs is

Freezing MSTP (CLI)

You can freeze MSTP in the unit. When MSTP is frozen, BPDUs are neither transmitted nor processed, and all port states are maintained as they were before MSTP was frozen.

To freeze MSTP, enter the following command in root view:

```
root> ethernet mstp mstp-freeze
```

To unfreeze MSTP, enter the following command in root view:

```
root> ethernet mstp mstp-defreeze
```

To display whether MSTP is or is not currently frozen in the unit, enter the following command in root view:

```
root> ethernet mstp show-mstp-frozen
```

Resetting the MSTP Stack (CLI)

To reset MSTP on the unit, enter the following command in root view:

```
root> ethernet mstp mstp-reset
```

Handling Signal Degrade (SD) Failures (CLI)

Signal Degrade failures (SD) can either be ignored or treated the same as SF, which means an SD failure triggers a topology change.

To determine how SD failures are treated, enter the following command in root view:

```
root> ethernet mstp set sd-handling <sd-handling>
```

Table 244: MSTP Signal Degrade Failure CLI Parameters

Par	Ir	Pe	Description
sd-han	Variab	ignored sam	ignored – Signal Degrade (SD) failures are ignored in MSTP. same-as-SF – MSTP handles SD failures the same as Signal Failure, i.e., an SD failure triggers a topology change.

Setting the Configuration ID (CLI)

The configuration ID attributes include the Configuration Name and the Revision Level. These attributes are part of the Bridge Configuration Identifier.

To set the configuration ID attributes, enter the following command in root view:

```
root> ethernet mstp set configuration-name <configuration-name>
revision-level <revision-level>
```

To display the configuration ID attributes, enter the following command in root view:

```
root> ethernet mstp show-config-id
```

Table 245: MSTP Configuration ID CLI Parameters

Parameter	In	Pe	Description
configuratio	Tex		The IEEE 802.1Q Configuration Name. The Configuration Name is part of the bridge configuration
revision-level	Num	0-65535	The IEEE 802.1Q Revision Level. The Revision Level is part of the bridge configuration Identifier.

Mapping Services to MSTIs (CLI)

By default, all Ethernet services are assigned to MSTI 0 (CIST). You can map Ethernet services to other MSTIs.

All mapping of Ethernet services to MSTP instances (MSTIs) should be

To assign a service to another MSTI, enter the following command in root view:

```
root> ethernet generalcfg instance-to-service-mapping set
```

To assign a range of services to another MSTI, enter the following command in root view:

```
root> ethernet generalcfg instance-to-service-mapping set
```

To display the service to MSTI mapping for a specific service, enter the following command in root view:

```
root> ethernet generalcfg instance-to-service-mapping show
```

To display the service to MSTI mapping for a range of services, enter the following command in root view:

```
root> ethernet generalcfg instance-to-service-mapping show
```

Table 246: MSTP Service to MSTI Mapping CLI Parameters

P	Input	Permitted Values	Description
sid	Num	Any Ethernet service or range of services configured in the	The service ID.

i n	Num ber	1-16, 4095	The MSTI to which you want to map the

The following command assigns Service 1 to MSTI 2:

```
root> ethernet generalcfg instance-to-service-mapping set
service sid 1 instance id 2
```

The following command assigns Services 1 through 10 to MSTI 2:

```
root> ethernet generalcfg instance-to-service-mapping set
service sid 1 to 10 instance id 2
```

The following command displays the service to MSTI mapping for services 1 through 1000:

```
root> ethernet generalcfg instance-to-service-mapping show
service sid 1 to 1000
```

Setting the Bridge Level Spanning Tree Parameters (CLI)

The bridge level spanning tree parameters determine most of the bridge MSTP parameters, including parameters that are applied to all bridges when this bridge is acting as the root.

To set the CIST bridge priority, enter the following command in root view:

```
root> ethernet mstp set cist-bridge-priority <cist-bridge-
priority>
```

To set the CIST hold time, enter the following command in root view:

```
root> ethernet mstp set cist-bridge-hold-time <cist-bridge-
hold-time>
```

To set the CIST maximum age, enter the following command in root view:

```
root> ethernet mstp set cist-bridge-max-age <cist-bridge-max-
age>
```

To set the CIST forward delay, enter the following command in root view:

```
root> ethernet mstp set cist-bridge-forward-delay <cist-bridge-
forward-delay>
```

To set the CIST Hello Time, enter the following command in root view:

```
root> ethernet mstp set cist-bridge-hello-time <cist-bridge-
hello-time>
```

To set the CIST maximum number of hops, enter the following command in root view:

```
root> ethernet mstp set cist-bridge-max-hops <cist-bridge-max-
hops>
```

Table 247: MSTP Bridge Level Spanning Tree CLI Parameters

Parameter	In	Permitted Values	Description
cist-bridge-priority	Num	0-61440, in steps of 4096.	Enter a value as the writeable portion of the Bridge ID. This value constitutes the first two
cist-bridge-hold-time	Numb	10-100	Enter a value (in cs) as the interval length during which no more than two configuration bridge PDUs
cist-bridge-max-age	Numb	600-4000	Enter a value (in cs) that all bridges will use, when this bridge is the root, as the maximum age of MSTP
cist-bridge-forwar	Numb	400-3000	Enter a value (in cs) that all bridges will use, when this bridge is the root, as the speed at which ports change
cist-bridge-hello-time	Numb	100-1000	Enter the value (in cs) that all bridges will use, when this bridge is the root, as the Hello Time. The Hello Time
cist-bridge-max-hops	Numb	6-40	Enter the value that all bridges will use, when this bridge is the root, as the maximum number of hops

Setting and Viewing the Bridge Level MSTI Parameters (CLI)

To set the bridge priority for an MSTI, enter the following command in root view:

```
root> ethernet mstp set instance <msti-id> msti-bridge-priority
<msti-bridge-priority>
```

To display the bridge parameters of an MSTI, enter the following command in root view:

```
root> ethernet mstp show-msti-attributes instance <msti-id>
```

Table 248: Bridge Level MSTI CLI Parameters

Par	In	Permitted Values	Description
inst	Nu	1-16	Enter the MSTI ID of the MSTI you want to configure.

Par	Ir	Permitted Values	Description
mst	N ur	0-61440, in steps of 4096.	The MSTI writeable portion of the Bridge ID.
interfac	V ar ia	e t h r a	Enter the type of interface: `eth` – Ethern
slot	N ur be	Et h er n	
port	N ur be r	• Ethernet interface on PTP 850C: 1-4 • Ethernet interface on PTP 850E: 1-7 • Ethernet interface on PTP 850S: 1-3 • Radio interface on an PTP 850C: 1-2 • Radio interface on an PTP 850E or PTP 850S: 1	The port number of the interface.
group	Variable	lag1 lag2 lag3 lag4 mc-abc1 mc-abc2 mc-abc3 mc-abc4	To enter interface view for a LAG group, enter the group (lag1 - lag4). To enter interface

The following command sets the bridge priority for MSTI 15 to 28672:

```
root> ethernet mstp set instance 15 msti-bridge-priority 28672
```

The following command displays the bridge parameters of MSTI 10:

```
root> ethernet mstp show-msti-attributes instance 10
```

Viewing the MSTP Parameters (CLI)

To display the general MSTP parameters, enter the following command in root view:

```
root> ethernet mstp show-gen-attributes
```

Configuring the MSTP Port Parameters (CLI)

This section includes:

- Configuring and Viewing the CIST Port Parameters (CLI)
- Configuring and Viewing the MSTI Port Parameters (CLI)

- Viewing and Resetting Port BPDU Counters (CLI)

Configuring and Viewing the CIST Port Parameters (CLI)

To set the CIST port priority of a port, enter the following command in root view:

```
root> ethernet mstp set interface <interface> slot <slot> port
<port> cist-port-priority <cist-port-priority>
```

To set the CIST port priority of an interface group, enter the following command in root view:

```
root> ethernet mstp set group <group> cist-port-priority <cist-
port-priority>
```

To set the CIST path cost of a port, enter the following command in root view:

```
root> ethernet mstp set interface <interface> slot <slot> port
<port> cist-port-path-cost <cist-port-path-cost>
```

To set the CIST path cost of an interface group, enter the following command in root view:

```
root> ethernet mstp set group <group> cist-port-path-cost
<cist-port-path-cost>
```

To set a port's administrative edge port parameter for the CIST, enter the following command in root view:

```
root> ethernet mstp set interface <interface> slot <slot> port
<port> cist-port-edge-port <cist-port-edge-port>
```

To set an interface group's administrative edge port parameter for the CIST, enter the following command in root view:

```
root> ethernet mstp set group <group> cist-port-edge-port
<cist-port-edge-port>
```

To set a port's MAC Enabled parameter for the CIST, enter the following command in root view:

```
root> ethernet mstp set interface <interface> slot <slot> port
<port> cist-port-mac-enabled <cist-port-mac-enabled>
```

To set an interface group's MAC Enabled parameter for the CIST, enter the following command in root view:

```
root> ethernet mstp set group <group> cist-port-mac-enabled
<cist-port-mac-enabled
```

To display a port's CIST parameters, enter the following command in root view:

```
root> ethernet mstp show-cist-port-attributes interface
<interface> slot <slot> port <port>
```

To display an interface group's CIST parameters, enter the following command in root view:

```
root> ethernet mstp show-cist-port-attributes group <group>
```

Table 249: CIST Port CLI Parameters

P	In	Permitted Values	Description
interfa	Variable	eth r	Enter the type of interface: `eth` – Ethernet
slot	Number	Ethernet: 1 Radi	
port	Number	• Ethernet interface on PTP 850C: 1-4 • Ethernet interface on PTP 850E: 1-7 • Ethernet interface on PTP 850S: 1-3 • Radio interface on an PTP 850C: 1-2 • Radio interface on an PTP 850E or PTP	The port number of the interface.
group	Variable	lag1 lag2	To enter interface view for a LAG group, enter the group (lag1 - lag4). To enter interface view for a Multi-Carrier
cist	Numbe	0-240, in multiples of 16.	The priority contained in the first octet of the two-
cist-port-p	Number	1-200000000.	The configurable assigned value for the contribution of this port to the path cost of paths towards the spanning tree root. **Note:**
cist-po	Variable	truefal	`true` – The port is considered an edge port in the CIST. `false` – The port is

P	In	Permitted Values	Description
cist-port-mac-e	Variable	forceTrue forceFalse auto	forceTrue – The MAC is treated as if it is connected to a point-to- point LAN, regardless of any indications to the contrary that are generated by the MAC entity. forceFalse –The MAC is treated as if it is connected to a non-point- to-point LAN, regardless of any indications to the contrary that are generated by the MAC entity. auto – The MAC Enabled parameter is set to True if the MAC is connected to a point-to- point or full-duplex LAN. The MAC Enabled parameter is set to

The following command sets the CIST port priority for Ethernet port 3 to 192:

```
root> ethernet mstp set interface eth slot 1 port 3 cist-port-
priority 192
```

The following command sets the CIST port priority for HSB protection group 1 to 192:

```
root> ethernet mstp set group rp1 cist-port-priority 192
```

The following command sets the CIST path cost for Ethernet port 3 to 20,000:

```
root> ethernet mstp set interface eth slot 1 port 3 cist-path-
cost 20000
```

The following command sets the CIST path cost for LAG 1 to 20,000:

```
root> ethernet mstp set group lag1 cist-path-cost 20000
```

The following command sets radio interface 1 on an PTP 850C to be an Edge port in the CIST:

```
root> ethernet mstp set interface radio slot 1 port 1 cist-
port-admin-edge true
```

The following command displays the CIST parameters of LAG 1:

```
root> ethernet mstp show-cist-port-attributes group lag1
```

Configuring and Viewing the MSTI Port Parameters (CLI)

To set the port priority for an MSTI and port, enter the following command in root view:

```
root> ethernet mstp set instance <instance> interface
<interface> slot <slot> port <port> msti-port-priority <msti-
```

To set the port priority for an MSTI and an interface group, enter the following command in root view:

```
root> ethernet mstp set instance <instance> group <group> msti-
```

To set the path cost for a port in a specific MSTI, enter the following command in root view:

```
root> ethernet mstp set instance <instance> interface
<interface> slot <slot> port <port> msti-port-path-cost <msti-
```

To set the path cost for an interface group in a specific MSTI, enter the following command in root view:

```
root> ethernet mstp set instance <instance> group <group> msti-
```

To display the MSTI parameters for a specific MSTI and port, enter the following command in root view:

```
root> ethernet mstp show-msti-port-attributes instance
<instance> interface <interface> slot <slot> port <port>
```

To display the MSTI parameters for a specific MSTI and interface group, enter the following command in root view:

```
root> ethernet mstp show-msti-port-attributes instance
<instance> group <group>
```

Table 250: MSTI Port CLI Parameters

Par	Ir	Permitted Values	Description
inst	N u	1-16	Enter the MSTI ID of the MSTI you want to configure.
interfa	V a r i	e t h r	Enter the type of interface: `eth` – Ethernet `radio` – Radio

slot	Number	Ethernet	

Par	Ir	Permitted Values	Description
port	Number	• Ethernet interface on PTP 850C: 1-4 • Ethernet interface on PTP 850E: 1-7 • Ethernet interface on PTP 850S: 1-3 • Radio interface on an PTP 850C: 1-2 • Radio interface on an PTP 850E or PTP 850S: 1	The port number of the interface.
group	Variable	lag1 lag2	To enter interface view for a LAG group, enter the group (lag1 - lag4). To enter interface view for a Multi-Carrier ABC group, enter the group (mc-abc1 – mc-abc4) (PTP 850C only).
ms	Nu	0-240, in multiples of 16.	The priority contained in the first octet of the
msti-por	Number	1-200000000.	The port's Path Cost parameter for the MSTI. **Note:** Changing the value of this parameter may cause re- initialization of the MSTI for which the parameter is changed. No other MSTI

The following command sets the MSTI port priority for MSTI 14 on Ethernet port 2 to 192:

```
root> ethernet mstp set instance 14 interface eth slot 1 port 2
msti-port-priority 192
```

The following command sets the MSTI port priority for MSTI 14 on LAG 1 to 192:

```
root> ethernet mstp set instance 14 group lag1 msti-port-
priority 192
```

The following command sets the MSTI path cost for MSTI 12 on Ethernet port 3 to 20000:

```
root> ethernet mstp set instance 12 interface eth slot 1 port 3
msti-port-path-cost 20000
```

The following command sets the MSTI path cost for MSTI 12 on HSB protection group 1 to 20000:

```
root> ethernet mstp set instance 12 group rp1 msti-port-path-
cost 20000
```

The following command displays the MSTI parameters for MSTI 10 and radio interface 1:

```
root> ethernet mstp show-msti-port-attributes instance 10
interface radio slot 2 port 1
```

The following command displays the MSTI parameters for MSTI 10 and LAG 1:

```
root> ethernet mstp show-msti-port-attributes instance 10 group
lag1
```

Viewing and Resetting Port BPDU Counters (CLI)

To view the BPDU counters for a port, enter the following command in root view:

```
root> ethernet mstp show-port-counters interface <interface>
slot <slot> port <port>
```

To view the BPDU counters for an interface group, enter the following command in root view:

```
root> ethernet mstp show-port-counters group <group>
```

To reset the BPDU counters, enter the following command in root view:

```
root> ethernet mstp reset-counters
```

Table 251: Port BPDU Counters CLI Parameters

Par	Ir	Permitted Values	Description
interfa	Variri	eth r	Enter the type of interface: `eth` – Ethernet
slot	Numbe	Ether n	
port	Numbe r	• Ethernet interface on PTP 850C: 1-4 • Ethernet interface on PTP 850E: 1-7 • Ethernet interface on PTP 850S: 1-3 • Radio interface on an PTP 850C: 1-2 • Radio interface on an PTP 850E or PTP 850S:1	The port number of the interface.

group	Variable	lag1 lag2 lag3	To enter interface view for a LAG group, enter the group (lag1 - lag4). To enter interface view for a Multi-Carrier ABC group, enter the group (mc-abc1 – mc-abc4) (PTP 850C only).

23.3 Configuring Ethernet Bandwidth Notification (ETH-BN) (CLI)



Note

For an overview of ETH-BN, see ETH-BN Overview.

You must first create an ETH-BN entity consisting of the Monitored Interface on the one hand, and the Control Interface on the other. You must then use separate commands to enable or disable bandwidth monitoring of the monitored interface and transmission of messages. You can also set various parameters related to the bandwidth sampling and the transmitted bandwidth messages.

To create an ETH-BN entity, enter the following command in root view:

```
root> ethernet ebn ebn-entity-create ebn-name <eb-name> monitored-interface <monitored-interface> monitored-slot <monitored-slot> monitored-port <monitored-port> control-interface <control-interface> control-slot <control-slot> vlan <vlan>
```

To change the name of an ETH-BN entity, enter the following command in root view:

```
root> ethernet ebn ebn-name-set ebn-name <ebn-name> new-ebn-name <ebn-name>
```

To set the Admin status of an ETH-BN entity, enter the following command in root view:

```
root> ethernet ebn ebn-admin-set ebn-name <ebn-name> admin <admin-state>
```

To set the Maintenance Level of messages sent by the ETH-BN entity, enter the following command in root view:

```
root> ethernet ebn ebn-mel-set ebn-name <ebn-name> mel <mel>
```



Note

If CFM MEPs are being used, the MEL must be set to a value greater than the MEG level of the MEP. Otherwise, the BNM frames will be dropped.

If CFM MEPs are not being used, the MEL for ETH-BN must be set to a value greater than 0. Otherwise, the BNM frames will be dropped.

To set the VLAN with which messages sent by the ETH-BN entity are transmitted, enter the following command in root view:

```
root> ethernet ebn ebn-vlan-set ebn-name <ebn-name> vlan <vlan>
```

To determine whether periodic BNM frames should be sent even when there is no bandwidth degradation in the monitored interface, enter the following command in root view:

```
root> ethernet ebn ebn-is-always-send ebn-name <string> is-always-send <is-always-send>
```

To delete an ETH-BN entity, enter the following command in root view:

```
root> ethernet ebn ebn-entity-delete ebn-name <ebn-name>
```

To show a summary of all ETH-BN entities defined, enter the following command in root view:

```
root> ethernet ebn ebn-entities-summary-show
```

To show a summary of the configuration and status of a specific ABN entity, enter the following command in root view:

```
root> ethernet ebn ebn-entity-show ebn-name <ebn-name>
```

To set how often messages are transmitted when bandwidth is below the nominal value, enter the following command in root view:

```
root> ethernet ebn ebn-period-set ebn-name <ebn-name> period <period>
```

To set the holdoff time, enter the following command in root view. Holdoff time is the amount of time the system waits when bandwidth degradation occurs, before transmitting a message. If the bandwidth is below the nominal value when the holdoff period ends, the system starts transmitting messages:

```
root> ethernet ebn ebn-holdoff-set ebn-name <ebn-name> holdoff <holdoff-time>
```

To clear the messages counter, enter the following command in root view:

```
root> ethernet ebn ebn-entity-counter-reset ebn-name <ebn-name>
```

Table 218 ETH-BN Entity CLI Parameters

Parameter	Input Type	Permitted Values	Description
ebn-name	Text String		The name of the ABN entity.
monitored-interface	Variable	radio	This parameter is always set to radio.
monitored-slot	Number	1	
monitored-port	Number	1	
control-interface	Variable	eth	This parameter is always set to eth.
control-slot	Number	1	This parameter is always set to 1.
control-port	Number	1-7	The specific Ethernet interface to which messages are transmitted when bandwidth in the monitored interface degrades below the nominal value.
mel	Number	0-7	The CFM Maintenance Level of messages sent by an ETH-BN entity.
vlan	Variable	untag 1 - 4094, except 4092 (reserved for the default management service)	The VLAN on which messages are transmitted (optional). The CoS of the VLAN is automatically set to 7.
is-always-send	Variable	true false	Specifies whether periodic BNM frames are sent even when there is no bandwidth degradation in the monitored interface:

Parameter	Input Type	Permitted Values	Description
			• **true** – BNM frames are always sent, even when the bandwidth is at its nominal value. **false** – BNM frames are only sent when the current bandwidth is lower than the nominal bandwidth (default value).
admin-state	Variable	up down	Enter up to enable ETH-BN monitoring on the interface, or down to disable EBN monitoring on the interface.
period	Variable	4-one-second 5-ten-seconds 6-sixty-seconds	How often messages are transmitted when **is-always-send** is set to **true** or, if not, when bandwidth is below the nominal value: **4-one-second** – Message is sent every one second. **5-ten-seconds** – Message is sent every ten seconds. **6-sixty-seconds** – Message is sent every minute. The default value is ten seconds.

Parameter	Input Type	Permitted Values	Description
holdoff-time	Number	0-10	The amount of time (in seconds) the system waits when bandwidth degradation occurs, before transmitting a message. The default value is 0 seconds.

The following command creates an EBN entity with the following attributes:

- The name of the EBN entity is Test.
- The monitored radio interface is interface 1
- The Ethernet control interface is Ethernet port 1
- The MEL is set to 7.
- BNM frames are only sent when the current bandwidth is lower than the nominal bandwidth.
- When the current bandwidth is below the nominal value, BNM frames are sent every 60 seconds, after a holdoff time of 10 seconds.
- BNM frames are untagged

```
root>ethernet ebn ebn-entity-create ebn-name Test monitored-
interface radio monitored-slot 1 monitored-port 1 control-
interface eth control-slot 1 control-port 7 vlan untag

root>ethernet ebn ebn-admin-set ebn-name Test admin up

root>ethernet ebn ebn-mel-set ebn-name Test mel 7

root>ethernet ebn ebn-is-always-send ebn-name Test is-always-send
false

root>ethernet ebn ebn-period-set ebn-name Test period 6-sixty-
seconds

root>ethernet ebn ebn-holdoff-set ebn-name Test holdoff 10

root>
```

23.4 Configuring LLDP (CLI)

Link Layer Discovery Protocol (LLDP) is a vendor-neutral layer 2 protocol that can be used by a network element attached to a specific LAN segment to advertise its identity and capabilities and to receive identity and capacity information from physically adjacent layer 2 peers. LLDP is a part of the IEEE 802.1AB – 2005 standard that enables automatic network connectivity discovery by means of a port identity information exchange between each port and its peer. Each port periodically sends and also expects to receive frames called Link Layer Discovery Protocol Data Units (LLDPDU). LLDPDUs contain information in TLV format about port identity, such as MAC address and IP address.

LLDP is used to send notifications to the NMS, based on data of the local unit and data gathered from peer systems. These notifications enable the NMS to build an accurate network topology.

This section includes:

- Configuring the General LLDP Parameters (CLI)
- Displaying the General LLDP Parameters (CLI)
- Configuring LLDP Port Parameters (CLI)
- Displaying LLDP Port Parameters (CLI)
- Displaying LLDP Local System Parameters (CLI)
- Displaying the LLDP Remote System Parameters (CLI)
- Displaying LLDP Statistics (CLI)

Configuring the General LLDP Parameters (CLI)

This section explains how to define the general LLDP parameters for the unit. For instructions on defining port-specific parameters, see Configuring LLDP Port Parameters (CLI).

To define the Transmit Interval, which is the interval at which LLDP frames are transmitted, enter the following command in root view:

```
root> ethernet lldp tx-interval-set tx-interval <tx-interval>
```

The time-to-live (TTL) determines the length of time LLDP frames are retained by the receiving device. The TTL is determined by multiplying the Transmit Interval by the TTL Multiplier.

To define the TTL Multiplier, enter the following command in root view:

```
root> ethernet lldp tx-hold-multiplier-set hold-multiplier
<hold-multiplier>
```

To define the interval between transmission of LLDP notifications during normal transmission periods, enter the following command in root view:

```
root> ethernet lldp notif-interval-set notif-interval <notif-
interval>
```

Table 253: General LLDP CLI Parameters

P	Inp	Permitted	Description
tx-in	Number	5-3600	The interval, in seconds, at which LLDP frames are transmitted. The default value is 30.
hold	Number	2-10	The TTL Multiplier, which is multiplied by the Transmit Interval to determine the TTL, in seconds, of LLDP frames. The default value is 4.
noti	Number	5-3600	The interval, in seconds, between transmission of LLDP notifications during normal transmission periods. The

The following commands set the Transmit Interval to 50 seconds with a TTL Multiplier of 5. This produces a TTL of 4 minutes and 10 seconds.

```
root> ethernet lldp tx-interval-set tx-interval 50
root> ethernet lldp tx-hold-multiplier-set hold-multiplier 50
```

The following command sets a Notification Interval of 20 seconds:

```
root> ethernet lldp notif-interval-set notif-interval 20
```

Displaying the General LLDP Parameters (CLI)

To display the general LLDP parameters, enter the following command in root view:

```
root> ethernet lldp configuration-scalers-show
```

The following information is displayed:

Message Tx Interval - The interval, in seconds, at which LLDP frames are transmitted, as defined by the `ethernet lldp tx-interval-set tx-interval` command. The default value is 30.

Message Tx Hold Multiplier - The TTL Multiplier, as defined by the `ethernet lldp tx-hold-multiplier-set hold-multiplier` command. The TTL Multiplier is multiplied by the Transmit Interval to determine the TTL, in seconds, of LLDP frames. The default value is 4.

Reinit Delay - The minimum time, in seconds, the system waits after the LLDP Admin status becomes Disabled until it will process a request to reinitialize LLDP. In this release, this parameter is set at 2.

Notification Interval - The interval, in seconds, between transmission of LLDP notifications during normal transmission periods, as defined by the `ethernet lldp notif-interval-set notif-interval` command. The default value is 30.

Tx Credit Max - The maximum number of consecutive LLDPDUs that can be transmitted at any one time. In this release, the Tx Credit Max is set at 5.

Message Fast Tx - The interval, in seconds, at which LLDP frames are transmitted during fast transmission periods, such as when the unit detects a new neighbor. In this release, this parameter is set at 1.

Message Fast Init - The initial value used to initialize the variable which determines the number of transmissions that are made during fast transmission periods. In this release, this parameter is set at 4.

Configuring LLDP Port Parameters (CLI)

This section explains how to enable LLDP per port, and determine how LLDP operates and which TLVs are sent for each port:

To define how the LLDP agent operates on a specific port, enter the following command in root view:

```
root> ethernet lldp agent-admin-set interface eth slot <slot>
port <port> agent-admin <agent-admin>
```

To enable or disable LLDP notifications to the NMS on a specific port, enter the following command in root view:

```
root> ethernet lldp agent-notif-enable interface eth slot
<slot> port <port> agent-notif-enable <agent-notif-enable>
```

Table 254: LLDP Port CLI Parameters

Para	Input	Permitted	Description
slot	Num	1	The slot in which the card resides.
port	Number	• IP—50C: 1-4 • PTP 850E: 1-7 • PTP 850S: 1-	The port for which you want to configure LLDP.
agent-admin	Variable	txOnly rxOnly txAndRx disabled	Defines how the LLDP protocol operates for this port: • txOnly - The LLDP agent transmits LLDP frames on this port but does not update information about its peer. • rxOnly - The LLDP agent receives but does not transmit LLDP frames on this port. • txAndRx - The LLDP agent transmits and receives LLDP frames on this port (default value). • disabled - The LLDP agent does not transmit or receive LLDP frames on this port.

agent-n	Variable	true false	• `true` - The agent sends a Topology Change trap to the NMS whenever the system information received from its peer changes. • `false` - Notifications to the NMS are disabled (default value).

The following commands configure Ethernet port 3 to transmit and receive LLDP frames and to send a Topology Change trap to the NMS whenever the system information of its peer changes:

```
root> ethernet lldp agent-admin-set interface eth slot 1 port 3
agent-admin txAndRx

root> ethernet lldp agent-notif-enable interface eth slot 1
port 3 agent-notif-enable true
```

Displaying LLDP Port Parameters (CLI)

To display the LLDP agent configuration on all ports, enter the following command in root view:

```
root> ethernet lldp agent-configuration-show
```

The following is a sample output of the command:

```
root> ethernet lldp agent-configuration-show
=============================================================================|
 Interface              |  Mac DA    |  Admin   |  Notification  | TLV TX    |
 type        |slot|port | Identifier |  Status  |  Enable        |           |
=============================================================================|
 ethernet    | 1  | 1   | 1          | txAndRx  | false          | None      |
-----------------------------------------------------------------------------
 ethernet    | 1  | 2   | 1          | txAndRx  | false          | None      |
-----------------------------------------------------------------------------
 ethernet    | 1  | 3   | 1          | disabled | false          | None      |
-----------------------------------------------------------------------------
root>
```

Displaying LLDP Local System Parameters (CLI)

This section includes:

- Displaying Local Unit Parameters (CLI)
- Displaying Local Port Parameters (CLI)
- Displaying Local Unit Management Information (CLI)
- Displaying Local Unit Management Information per Port (CLI)
- Displaying Unit's Destination MAC Addresses (CLI)

Displaying Local Unit Parameters (CLI)

To display the local unit's unit parameters, as transmitted by the LLDP agents, enter the following command in root view:

```
root> ethernet lldp local-system-scalars-show
```

The following information is displayed:

- **local Chassis Id Subtype** - The type of encoding used to identify the local unit. In this release, this parameter is always set to 4 (MAC Address).
    - **local Chassis Id** - The MAC Address of the local unit.
    - **local System Name** - The system name included in TLVs transmitted by the LLDP agent. To define the system name, see *Configuring Unit Parameters (CLI)*.
    - **local System Description** - The system description included in TLVs transmitted by the LLDP agent.
- **local System Cap Supported** - A bitmap value used to identify which system capabilities are supported on the local system, as included in TLVs transmitted by the LLDP agent. The bitmap is defined by the following parameters:
    - 0 - other
    - 1 - repeater
    - 2 - bridge
    - 3 - wlanAccessPoint
    - 4 - router
    - 5 - telephone
    - 6 - docsisCableDevice
    - 7 - stationOnly
    - 8 - cVLANComponent
    - 9 - sVLANComponent
    - 10 - twoPortMACRelay
- **local System Cap Enabled** - A bitmap value used to identify which system capabilities are enabled on the local system, as included in TLVs transmitted by the LLDP agent. The bitmap is defined by the following parameters:
    - 0 - other
    - 1 - repeater
    - 2 - bridge
    - 3 - wlanAccessPoint
    - 4 - router
    - 5 - telephone
    - 6 - docsisCableDevice
    - 7 - stationOnly
    - 8 - cVLANComponent
    - 9 - sVLANComponent

- 10 - twoPortMACRelay

Displaying Local Port Parameters (CLI)

To display local port parameters, as transmitted by the LLDP agent, enter the following command in root view:

```
root> ethernet lldp local-port-show
```

The following information is displayed:

- **Interface type/slot/port** - The port type, slot number, and port number.
- **Port ID Subtype** - The type of encoding used to identify the port in LLDP transmissions. In this release, this parameter is always set to MAC Address.
  - **Port ID** - The port's MAC address.
- **Description** - A text string that describes the port. In this release, this parameter is always set to ethPort.

Displaying Local Unit Management Information (CLI)

To display the local unit's management information, enter the following command in root view:

```
root> ethernet lldp local-mng-show
```

The following information is displayed:

- **Mng Addr SubType** - The format of the local unit's IP Address. In this release, only IPV4 is supported.
  - **Management Address** - The local unit's IP address.
  - **Mng Addr Length** - Reserved for future use.
  - **Mng Addr IF SubType** - Reserved for future use.
  - **Mng Addr IF** - Reserved for future use.
  - **Mng Addr OID** - Reserved for future use.

Displaying Local Unit Management Information per Port (CLI)

To display the local unit's management information per port, enter the following command in root view:

```
root> ethernet lldp mng-addr-table-show
```

The following information is displayed:

- **Interface type/slot/port** - The port type, slot number, and port number.
- **Dest Mac Address** - Defines the MAC address associated with the port for purposes of LLDP transmissions.
- **Mng Address subType** - Defines the type of the management address identifier encoding used for the Management Address. In this release, only IpV4 is supported.
  - **Management Address** - The unit's IP address.

- **Mng Address Tx Enable** - Indicates whether the unit's Management Address is transmitted with LLDPDUs. In this release, the Management Address is always sent.

Displaying Unit's Destination MAC Addresses (CLI)

To display the destination MAC address or range of MAC addresses associated with the unit, and their internal index, enter the following command in root view:

```
root> ethernet lldp mac-da-table-show
```

The following information is displayed:

- **LLDP DA Index** - The internal index associated with the unit's destination LLDP MAC address.
- **LLDP DA** - The unit's destination LLDP MAC address.

Displaying the LLDP Remote System Parameters (CLI)

This section includes:

- Displaying the LLDP Remote Unit Parameters (CLI)
- Displaying the LLDP Remote Management Data per Port (CLI)

Remote information is not displayed for ports that belong to a LAG

group

Displaying the LLDP Remote Unit Parameters (CLI)

To display the peer's LLDP unit parameter information, starting from a specific time, enter the following command in root view. If no time is specified, all data is displayed.

```
root> ethernet lldp agent-remote-table-show agent-start-time
<agent-start-time> interface eth slot <slot> port <port>
```

Table 255: LLDP Remote Unit CLI Parameters

Par	Input	Permitted Values	Description
slot	Num	1	The slot in which the card
port	Number	• PTP 850S: 1-3 • PTP 850E: 1-7	The port for which you want to configure
agen	Date	Use the format: dd-mm-yyyy,hh:mm:ss	The sys-up-time of the entry creation.

The following information is displayed:

- **Time Mark** – The time the entry was created.
- **Interface Type/Slot/Port** – The port for which you are displaying data

about the peer.
    - **Rem Dest Mac Address** – The peer LLDP agent's destination MAC Address.
- **Remote Index** – An arbitrary local integer value used by this agent to identify a particular connection instance, unique only for the indicated peer.
    - **Remote Chassis ID subType** – The type of encoding used to identify the peer hardware unit.
    - **Remote Chassis ID** – An octet string used to identify the peer hardware unit.
    - **Rem Port ID subType** – The type of port identifier encoding used in the peer's Port ID.
- **Rem Port ID** – An octet string used to identify the port component associated with the peer.
    - **Rem Port Description** – A description of the peer's port.
    - **Rem System Name** – The peer's system name.
    - **Rem System Description** – The peer's system description.
- **Rem System Cap Supported** - The bitmap value used to identify which system capabilities are supported on the peer. The bitmap is defined by the following parameters:
    - 0 - other
    - 1 - repeater
    - 2 - bridge
    - 3 - wlanAccessPoint
    - 4 - router
    - 5 - telephone
    - 6 - docsisCableDevice
    - 7 - stationOnly
    - 8 - cVLANComponent
    - 9 - sVLANComponent
    - 10 - twoPortMACRelay
- **Rem System Cap Enabled** - The bitmap value used to identify which system capabilities are enabled on the peer. The bitmap is defined by the following parameters:
    - 0 - other
    - 1 - repeater
    - 2 - bridge
    - 3 - wlanAccessPoint
    - 4 - router
    - 5 - telephone

- 6 - docsisCableDevice
- 7 - stationOnly
- 8 - cVLANComponent
- 9 - sVLANComponent
- 10 - twoPortMACRelay
  - **Remote Changes** - Indicates whether there are changes in the peer's MIB, as determined by the variable **remoteChanges**. Possible values are:
- **True** - Changes have taken place in the peer's MIB since the defined agent- start-time.
- **False** - No changes have taken place in the peer's MIB since the defined agent-*start-time*.

Displaying the LLDP Remote Management Data per Port (CLI)

To display remote LLDP management data from a specific port, starting from a specific time, enter the following command in root view. If no time is specified, all data is displayed.

```
root> ethernet lldp agent-remote-mng-show agent-start-time
<agent-start-time> interface eth slot <slot> port <port>
```

Table 256: LLDP Remote Management Data Per Port CLI Parameters

Paramete	Inpu	Permitted Values	Description
slot	Num	1	
port	Num ber	• PTP 850S: 1-3 • PTP 850E: 1-7	The port for which you want to configure LLDP.
agent-start-time	Date	Use the format: dd-mm-yyyy,hh:mm:ss	The sys-up-time of the entry creation.

The following information is displayed:

- **Time Mark** - The time the entry was created.
- **Interface Type/Slot/Port** - The port for which you are displaying data about the peer.
- **Rem Dest Mac Address** - The peer LLDP agent's destination MAC Address.
- **Remote Index** - An arbitrary local integer value used by this agent to identify a particular connection instance, unique only for the indicated peer.
- **Remote Mng Addr subType** - The type of management address identifier encoding used in the associated LLDP Agent Remote Management Address.
- **Remote Mng Address** - The octet string used to identify the management address component associated with the remote system. The purpose of this address is to contact the management entity.

- **Remote Mng IF subType** - The enumeration value that identifies the interface numbering method used for defining the interface number, associated with the remote system. Possible values are:
  - unknown(1)
  - ifIndex(2)
  - systemPortNumber(3)
- **Agent Rem OID** - The OID value used to identify the type of hardware component or protocol entity associated with the management address advertised by the remote system agent.

Displaying LLDP Statistics (CLI)

This section includes:

- Displaying Statistics Regarding Changes in Peer Unit (CLI)
- Displaying LLDP Transmission Statistics (CLI)
- Displaying LLDP Received Frames Statistics (CLI)

Displaying Statistics Regarding Changes in Peer Unit (CLI)

To display statistics about changes reported via LLDP by the remote unit, enter the following command in root view:

```
root> ethernet lldp statistics-scalars-show
```

The following information is displayed:

- **stats Rem Tables Last Change Time** - The time of the most recent change in the remote unit, as reported via LLDP.
- **stats Rem Tables Inserts** - The number of times the information from the remote system has changed.
- **stats Rem Tables Deletes** - The number of times the information from the remote system has been deleted.
- **stats Rem Tables Drops** - Reserved for future use.
- **stats Rem Tables Ageouts** - The number of times the information from the remote system has been deleted from the local unit's database because the information's TTL has expired. The `RX Ageouts` counter is similar to this counter, but is for specific ports rather than the entire unit.

Displaying LLDP Transmission Statistics (CLI)

To display statistics about LLDP transmissions and transmission errors, enter the following command in root view:

```
root> ethernet lldp statistics-port-tx-show
```

The following information is displayed:

- **LLDP TX Statistics Ifindex** - The index value used to identify the port in LLDP transmissions.
- **LLDP TX Statistics DA ID** - The LLDP MAC address associated with this entry.

- **LLDP TX Statistics Total Frames** - The number of LLDP frames transmitted by the LLDP agent on this port to the destination MAC address.

- **LLDP TX Statistics No. of Length Error** - The number of LLDPDU Length Errors recorded for this port and destination MAC address. If the set of TLVs that is selected in the LLDP local system MIB by network management would result in an LLDPDU that violates LLDPDU length restrictions, then the No. of Length Error statistic is incremented by 1, and an LLDPDU is sent containing the mandatory TLVs plus as many of the optional TLVs in the set as will fit in the remaining LLDPDU length.

Displaying LLDP Received Frames Statistics (CLI)

To display statistics about LLDP frames received by the unit, enter the following command in root view:

```
root> ethernet lldp statistics-port-rx-show
```

The following information is displayed:

- **RX Destination Port** - The index value used to identify the port in LLDP transmissions.

- **RX DA Index** - The index value used to identify the destination MAC address associated with this entry.
- **RX Total Discarded** - The number of LLDP frames received by the LLDP agent on this port, and then discarded for any reason. This counter can provide an indication that LLDP header formatting problems may exist with the local LLDP agent in the sending system or that LLDPDU validation problems may exist with the local LLDP agent in the receiving system.
- **RX Invalid Frames** - The number of invalid LLDP frames received by the LLDP agent on this port while the agent is enabled.
- **RX Valid Frames** - The number of valid LLDP frames received by the LLDP agent on this port.
- **RX Discarded TLVs** - The number of LLDP TLVs discarded for any reason by the LLDP agent on this port.
- **RX Unrecognized TLVs** - The number of LLDP TLVs received on the given port that are not recognized by LLDP agent.
- **RX Ageouts** - The number of age-outs that occurred on the port. An age-out is the number of times the complete set of information advertised by the remote system has been deleted from the unit's database because the information timeliness interval has expired. This counter is similar to the `LLDP No. of Ageouts` counter, except that it is per port rather than for the entire unit. This counter is set to zero during agent initialization. This counter is incremented only once when the complete set of information is invalidated (aged out) from all related tables on a particular port. Partial ageing is not allowed.

24. Synchronization (CLI)

This section includes:

- Changing the ETSI/ANSI Mode (CLI)
- Configuring the Sync Source (CLI)
- Configuring the Outgoing Clock (CLI)
- Changing the Default Quality (CLI)
- Configuring the Revertive Timer (CLI)
- Configuring SSM Messages (CLI)
- Displaying Synchronization Status and Parameters (CLI)
- Configuring 1588 Transparent Clock (CLI)

24.1 Changing the ETSI/ANSI Mode (CLI)

By default, PTP 850 units are set to ETSI mode. No mode change is necessary to configure an MRMC script, even if an FCC (ANSI) script is used. However, to configure a sync source on which the sync source Quality parameter must be set according to ANSI specifications. You must change the ETSI/ANSI mode to ANSI before configuring the sync source.

To change the ETSI/ANSI mode, enter the following command in root view:

```
root> platform management set interfaces-standard <ansi|etsi>
```

The following command changes the ETSI/ANSI mode from the default value of ETSI to ANSI mode:

```
root> platform management set interfaces-standard ansi
```

To display the current ETSI/ANSI mode, enter the following command in root view:

```
root> platform management show interfaces-standard
```

Changing the ETSI/ANSI mode does *not* require unit reset.

24.2 Configuring the Sync Source (CLI)



Note

To configure a sync source on which the sync source Quality parameter must be set according to ANSI specifications, change the ETSI/ANSI mode to ANSI before configuring the sync source. See Changing the ETSI/ANSI Mode (CLI).

Frequency signals can be taken by the system from Ethernet and radio interfaces. The reference frequency may also be conveyed to external equipment through different interfaces.

Frequency is distributed by configuring the following parameters in each node:

System Synchronization Sources – These are the interfaces from which the frequency is taken and distributed to other interfaces. Up to 16 sources can be configured in each node. A revertive timer can be configured. For each interface, you must configure:

Priority (1-16) – No two synchronization sources can have the same priority.

Quality – The quality level applied to the selected synchronization source. This enables the system to select the source with the highest quality as the current synchronization source.

Each unit determines the current active clock reference source interface:

The interface with the highest available quality is selected.

From among interfaces with identical quality, the interface with the highest priority is selected.

When configuring the Sync source, the Sync mode must be set to its default setting of automatic. To display the current Sync mode, enter the following CLI command in root view:

```
root> platform sync mode show
```

If the Sync mode is set to pipe, you must set it to automatic by entering the following CLI command in root view:

```
root> platform sync mode set automatic
```

When configuring an Ethernet interface as a Sync source, the Media Type of the interface must be rj45 or sfp, *not* auto-type. To view and configure the Media Type of an Ethernet interface, see Configuring an Interface's Media Type (CLI).

This section includes:

Configuring an Ethernet Interface as a Synchronization Source (CLI)

Configuring a Radio Interface as a Synchronization Source (CLI)

24.2.1 Configuring an Ethernet Interface as a Synchronization Source (CLI)



Note

In order to select an Ethernet interface, you must first specify the media type for this interface. See Configuring Ethernet Services (CLI).

To configure an Ethernet interface as a synchronization source, enter the following command in root view:

```
root> platform sync source add eth-interface slot <slot> port
<port> priority <priority> quality <quality>
```

To edit the parameters of an existing Ethernet interface synchronization source, enter the following command in root view:

```
root> platform sync source edit eth-interface slot <slot> port
<port> priority <priority> quality <quality>
```

To remove an Ethernet interface as a synchronization source, enter the following command in root view:

```
root> platform sync source remove eth-interface slot <slot> port
<port>
```

Table 219 Sync Source Ethernet CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	1	
port	Number	1-7	The interface to be configured as a synchronization source.
priority	Number	1 – 16	The priority of this synchronization source relative to other synchronization sources configured in the unit.

quality	Variable	For ETSI systems: automatic prc ssu-a ssu-b g813.8262 For ANSI (FCC) systems: automatic prs stratum-2 transit-node	The quality level applied to the selected synchronization source. This enables the system to select the source with the highest quality as the current synchronization source. If the quality is set to automatic, then the quality is determined by the received SSMs. If no valid SSM messages are received or in case of interface failure (such as LOS, LOC, LOF), the quality becomes "failure." SSM must be enabled on the remote interface in order for the interface to receive SSM messages. If the quality is configured to a fixed value, then the quality status becomes “failure” upon interface failure (such as LOS, LOC, LOF).

Parameter	Input Type	Permitted Values	Description
		stratum-3e stratum-3 smc unknown	

The following command configures Ethernet port 2 as a synchronization source with priority = 8, and quality = automatic:

```
root> platform sync source add eth-interface slot 1 port 2
priority 8 quality automatic
```

The following command changes the priority of this synchronization source to 6:

```
root> platform sync source edit eth-interface slot 1 port 2
priority 6
```

The following command removes this synchronization source:

```
root> platform sync source remove eth-interface slot 1 port 2
```

24.2.2 Configuring a Radio Interface as a Synchronization Source (CLI)

To configure a radio interface as a synchronization source, enter the following command in root view:

```
root> platform sync source add radio-interface slot <slot> port
<port> radio-channel <radio-channel> priority <priority> quality
<quality>
```

To edit the parameters of an existing radio interface synchronization source, enter the following command in root view:

```
root> platform sync source edit radio-interface slot <slot> port
<port> radio-channel <radio-channel> priority <priority> quality
<quality>
```

To remove a radio interface as a synchronization source, enter the following command in root view:

```
root> platform sync source remove radio-interface slot <slot> port
<port> radio-channel <radio-channel>
```

Table 220 Sync Source Radio CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	1	
port	Number	1	
radio-channel	Number	0	

Parameter	Input Type	Permitted Values	Description
priority	Number	1 – 16	The priority of this synchronization source relative to other synchronization sources configured in the unit.

quality	Variable	For ETSI systems: automatic prc ssu-a ssu-b g813.8262 For ANSI (FCC) systems: automatic prs stratum-2 transit-node	The quality level applied to the selected synchronization source. This enables the system to select the source with the highest quality as the current synchronization source. If the quality is set to automatic, then the quality is determined by the received SSMs. If no valid SSM messages are received or in case of interface failure (such as LOS, LOC, LOF), the quality becomes "failure." SSM must be enabled on the remote interface in order for the interface to receive SSM messages.

Parameter	Input Type	Permitted Values	Description
		stratum-3e stratum-3 smc unknown	

The following command configures the radio interface as a synchronization source with priority = 16, and quality = automatic:

```
root> platform sync source add radio-interface slot 2 port 1
radio-channel 0 priority 16 quality automatic
```

The following command changes the priority of this synchronization source to 14:

```
root> platform sync source edit radio-interface slot 2 port 1
radio-channel 0 priority 14
```

The following command removes this synchronization source:

```
root> platform sync source remove radio-interface slot 2 port 1
radio-channel 0
```

24.3 Configuring the Outgoing Clock (CLI)

For each interface, you can choose between using the system clock or the interface's internal clock as its synchronization source. By default, interfaces use the system clock.

When configuring the outgoing clock, the Sync mode must be set to its default setting of automatic. To display the current Sync mode, enter the following command in root view:

```
root> platform sync mode show
```

If the Sync mode is set to pipe, you must set it to automatic by entering the following command in root view:

```
root> platform sync mode set automatic
```

;

To set the interface clock for a radio interface, enter the following command in root view:

```
root> platform sync interface-clock set radio-interface slot 1
port 1 radio-channel <radio-channel> source <source>
```

To set the interface clock for an Ethernet interface, enter the following command in root view:

```
root> platform sync interface-clock set eth-interface slot <slot>
port <port> source <source>
```

Note

To configure the interface clock on an Ethernet interface, the Media Type of the interface must be rj45 or sfp, *not* auto-type. To view and configure the Media Type of an Ethernet interface, see Configuring Ethenet Interfaces (CLI).

Table 221 Outgoing Clock CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	1	
port	Number	ethernet: 1-7 radio: 1	The port number of the interface.
radio-channel	Number	0 – 84	The radio-channel configured for the synchronization source.
source	Variable	system-clock local-clock	system-clock – The interface uses the system clock as its synchronization source. local-clock – The interface uses its internal clock as its synchronization source.

The following command sets the clock source for the radio interface to its internal clock:

```
root> platform sync interface-clock set radio-interface slot 1
port 1 radio-channel 0 source local-clock
```

The following command sets the clock source for Eth7 to the system clock:

```
root> platform sync interface-clock set eth-interface slot 1 port
7 source system-clock
```

24.4 Changing the Default Quality (CLI)

Under certain circumstances in which an adequate clock signal is unavailable, an interface may go from locked state to holdover state. Normally, when an interface is in holdover state, it uses stored data to determine its outgoing clock. However, you can set the unit to apply a default quality of DNU (Do Not Use) to any interface in holdover state. To set the default quality to DNU, enter the following CLI command in root view:

```
root> platform sync default-quality set quality DNU
```

To set the default quality back to its default value, enter the following CLI command in root view:

```
root> platform sync default-quality set quality Default
```

To display the default quality, enter the following CLI command in root view:

```
root> platform sync default-quality show
```

24.5 Configuring the Revertive Timer (CLI)

You can configure a revertive timer for the unit. When the revertive timer is configured, the unit will not switch to another synchronization source unless that source has been stable for at least the number of seconds defined in the revertive timer. This helps to prevent a situation in which numerous switchovers occur when a synchronization source reports a higher quality for a brief time interval, followed by a degradation of the source's quality. By default, the revertive timer is set to 0, which means that it is disabled.

To configure the revertive timer, enter the following command in root view:

```
root> platform sync revertive-timer set rev_time <rev_time>
```

Table 222: Synchronization Revertive Timer CLI Parameters

Parameter	Input Type	Permitted Values	Description
rev_time	Number	1-1800	The revertive timer, in seconds.

The following command sets the revertive timer as 7 seconds:

```
root> platform sync revertive-timer set rev_time 7
```

To display the revertive timer, enter the following command in root view:

```
root> platform sync revertive-timer show
```

24.6 Configuring SSM Messages (CLI)

In order to provide topological resiliency for synchronization transfer, PTP 850E implements the passing of SSM messages over the Ethernet and radio interfaces. SSM timing in PTP 850E complies with ITU-T G.781.

In addition, the SSM mechanism provides reference source resiliency, since a network may have more than one source clock.

The following are the principles of operation:

At all times, each source interface has a “quality status” which is determined as follows:

If quality is configured as fixed, then the quality status becomes “failure” upon interface failure (such as LOS, LOC, LOF).

If quality is automatic, then the quality is determined by the received SSMs. If no valid SSM messages are received or in case of interface failure (such as LOS, LOC, LOF), the quality becomes "failure."

Each unit holds a parameter which indicates the quality of its reference clock. This is the quality of the current synchronization source interface.

The reference source quality is transmitted through SSM messages to all relevant radio interfaces.

In order to prevent loops, an SSM with quality “Do Not Use” is sent from the active source interface (both radio and Ethernet).

In order for an interface to transmit SSM messages, SSM must be enabled on the interface. By default, SSM is disabled on all interfaces.

When configuring SSM, the Sync mode must be set to its default setting of automatic. To display the current Sync mode, enter the following command in root view:

```
root> platform sync mode show
```

If the Sync mode is set to pipe, you must set it to automatic by entering the following command in root view:

```
root> platform sync mode set automatic
```

To enable SSM on a radio interface, enter the following command in root view:

```
root> platform sync ssm admin radio-interface slot <slot> port
<port> admin on
```

To disable SSM on a radio interface, enter the following command in root view:

```
root> platform sync ssm admin radio-interface slot <slot> port
<port> admin off
```

To enable SSM on an Ethernet interface, enter the following command in root view:

```
root> platform sync ssm admin eth-interface slot <slot> port
<port> admin on
```

To disable SSM on an Ethernet interface, enter the following command in root view:

```
root> platform sync ssm admin eth-interface slot <slot> port
<port> admin off
```

The following command enables SSM on radio interface 2:

```
root> platform sync ssm admin radio-interface slot 2 port 2 admin
on
```

The following command enables SSM on Ethernet port 1:

```
root> platform sync ssm admin eth-interface slot 1 port 1 admin on
```

24.7 Displaying Synchronization Status and Parameters (CLI)

To display the synchronization sources configured in the system, enter the following command in root view:

```
root> platform sync source config show
```

The following is a sample synchronization source display output:

```
number of configured sources = 4
|=============================================================|
| Slot | Port | Type | Instance | Priority | Quality |
|=============================================================|
| 1 | 7 | Ethernet | | 11 | automatic |
|-------------------------------------------------------------|
| 1 | 1 |  Radio   | | 6 | automatic |
|-------------------------------------------------------------|
```

To display the synchronization source status, enter the following command in root view:

```
root> platform sync source status show
```

The following is a sample synchronization source status display output:

```
root>platform sync source config show
number of configured sources = 1
|=============================================================================|
|  Slot  |  Port  |      Type      | Instance |  Priority  |      Quality      |
|=============================================================================|
| 1      | 7      | ethernet       |          | 1          | automatic         |
|-----------------------------------------------------------------------------|
root>
```

To display the current system reference clock quality, enter the following command in root view:

```
root> platform sync source show-reference-clock-quality
```

To display the current synchronization configuration of the unit's interfaces, enter the following command in root view:

```
root> platform sync interface config show
```

The following is a sample interface synchronization configuration display output:

```
root>platform sync interface config show
number of configured clock-interfaces = 8
|=============================================================================|
| Slot   | Port   | Type       | Trail Radio Ch. | Source-Type  | SSM-Admin   |
|=============================================================================|
| 1      | 1      | ethernet   |                 | system-clock | Off         |
|-----------------------------------------------------------------------------|
| 1      | 2      | ethernet   |                 | system-clock | Off         |
|-----------------------------------------------------------------------------|
| 1      | 3      | ethernet   |                 | system-clock | Off         |
|-----------------------------------------------------------------------------|
| 1      | 4      | ethernet   |                 | system-clock | Off         |
|-----------------------------------------------------------------------------|
| 1      | 5      | ethernet   |                 | system-clock | Off         |
|-----------------------------------------------------------------------------|
| 1      | 6      | ethernet   |                 | system-clock | Off         |
|-----------------------------------------------------------------------------|
| 1      | 7      | ethernet   |                 | system-clock | On          |
|-----------------------------------------------------------------------------|
| 1      | 1      | radio      |                 | system-clock | Off         |
|-----------------------------------------------------------------------------|
root>
```

To display the current system clock status, enter the following command in root view:

```
root> platform sync clu-state show
```

The following is a sample system clock status display output:

```
CLU is in Free-running mode
```

24.8 Configuring 1588 Transparent Clock (CLI)

PTP 850E uses 1588v2-compliant Transparent Clock to counter the effects of delay variation. Transparent Clock measures and adjusts for delay variation, enabling the PTP 850 to guarantee ultra-low PDV.

A Transparent Clock node resides between a master and a slave node, and updates the timestamps of PTP packets passing from the master to the slave to compensate for delay, enabling the terminating clock in the slave node to remove the delay accrued in the Transparent Clock node. The Transparent Clock node is itself neither a master nor a slave node, but rather, serves as a bridge between master and slave nodes.

Note the following:

- 1588 TC is not supported when Master-Slave communication is using the IPv6 transport layer.
- 1588 TC cannot be used in Multiband configurations.



Note

It is recommended to ensure that the PTP service uses the same type of equipment and physical connection (SFP or RJ-45) on both sides of the radio link. This makes Transparent Clock timestamping more accurate.

Make sure to enable Transparent Clock on the remote side of the link before enabling it on the local side.

To configure Transparent Clock:

1. Add the port receiving synchronization from the customer side as a Sync source, with Sync Interface Priority 1. See Configuring an Ethernet Interface as a Synchronization Source (CLI).
2. Add a radio interface as a Sync source, with lower priority than the port receiving synchronization from the customer side. See Configuring a Radio Interface as a Synchronization Source (CLI).
3. On the remote side of the radio link, add the radio interface facing the local device as a Sync source, with Sync Interface Priority 1. See Configuring a Radio Interface as a Synchronization Source (CLI).
4. Add the port receiving synchronization from the customer side as a Sync source, with Sync Interface Priority 1. See Configuring an Ethernet Interface as a Synchronization Source (CLI).
5. Verify that the Sync Interface Quality Status of the first Sync source is not Failure.
6. Enter the following command in root view to enable Transparent Clock:

```
root> platform sync ptp set admin enable
```



Note

To disable Transparent Clock, enter the following command in root view:

```
root> platform sync ptp set admin disable
```



Note

Disabling 1588 PTP can drastically affect time synchronization performance in the entire network.

7. Enter the following command in root view to assign the radio that will carry the PTP packets and determine the direction of the PTP packet flow.

```
root> platform sync ptp-tc set radio slot <slot> port <port>
direction <upstream|downstream>
```

The direction parameter must be set to different values on the two sides of the link, so that if you set the local side to `upstream`, you must set the remote side to `downstream`, and vice versa. Otherwise than that, it does not matter how you set this parameter.

To display the Transparent Clock settings, enter the following command in root view:

```
root> platform sync ptp-tc show status
```

The following commands enable Transparent Clock and configure the radio to send PTP packets upstream:

```
root> platform sync ptp-tc set admin enable
root> platform sync ptp-tc set radio slot 1 port 1 direction
upstream
```

8 1588 packets should be mapped to CoS 7. By default, 1588 packets are *not* mapped to any CoS. To map 1588 packets to CoS 7, you must *disable* CoS preservation for 1588 packets. This must be performed via CLI, using the following command:

```
root> ethernet generalcfg ptp-tc cos-preserve set admin disable
```

9 To map 1588 packets to CoS 7, enter the following command:

```
root> ethernet generalcfg ptp-tc cos-preserve cos value 7
```

After you enter these commands, 1588 packets will automatically be mapped to CoS 7.



Note

If necessary, you can use the ethernet generalcfg ptp-tc cos-preserve cos value command to map a different CoS value (0-7) to 1588 packets, but it is recommended to map 1588 packets to CoS 7.

24.9 Configuring 1588 Boundary Clock (CLI)

Boundary Clock complies with ITU-T Telecom Profile G.8275.1. This enables PTP 850E, with Boundary Clock, to meet the rigorous synchronization requirements of 5G networks.

The Boundary Clock in PTP 850E supports up to 16 1588 slave clock devices.

The Boundary Clock terminates the PTP flow it receives on the slave port, recovers the time and phase, and regenerates the PTP flow on the master ports.

The Boundary Clock node selects the best synchronization source available in the domain and regenerates PTP towards the slave clocks. This reduces the processing load from grandmaster clocks and increases the scalability of the synchronization network, while rigorously maintaining timing accuracy.

The PTP 850E Boundary Clock mechanism requires the use of untagged Ethernet multicast PTP packets as specified in G.8275.1.



Note

Boundary Clock and Transparent Clock can be used together in the same PTP 850E node

Note that in release 11.1:

- 1588 BC can only be used in a chain or star topology. It cannot be used in a ring topology.
- 1588 BC is not supported when Master-Slave communication is using the IPv6 transport layer.

Enabling Boundary Clock (CLI)



Note

Before configuring Boundary Clock, you must configure Transparent

Clock. See Configuring 1588 Transparent Clock (CLI).

To enable Boundary Clock, enter the following command in root view to enable:

```
root> platform sync ptp set admin enable
```

You can configure up to 16 interfaces per unit to be part of the Boundary Clock node. These interfaces can be radio and Ethernet interfaces, but not TDM interfaces or groups (e.g., LAG or Multi-Carrier ABC groups).

For each interface, use the following commands to enable and define Boundary Clock.

To enable Boundary Clock on a port, enter the following command in root view:

```
root> platform sync ptp-bc interfaces set interface-type
<interface-type> slot 1 port <port> admin enable
```

To set the port's role in the Boundary Clock node, enter the following command in root view:

```
root> platform sync ptp-bc interfaces set interface-type
<interface-type> slot <slot> port <port> master-only <master-  only>
```

To enable Boundary Clock on a Multi-Carrier ABC group (PTP 850C only), enter the following command in root view:

```
root> platform sync ptp-bc groups-on-slot set interface-type
enhanced-abc slot 1 port 1 admin enable
```

To set the group's role in the Boundary Clock node, enter the following command in root view:

```
root> platform sync ptp-bc groups-on-slot set interface-type
enhanced-abc slot 1 port 1 master-only <master-only>
```

Optionally, use the following command to set the Local Priority. The Local Priority value is taken into account when two identical announce messages are received by at least two different ports. In such a case, the Boundary Clock mechanism selects the slave port based on the best (lowest) Local Priority. The default value is 128.

```
root> platform sync ptp-bc interfaces set interface-type
<interface-type> slot <slot> port <port> local-priority <local-
priority>
```

Use the following command to set a MAC address for multicast re-transmission of PTP packets:

```
root> platform sync ptp-bc interfaces set interface-type
<interface-type> slot <slot> port <port> dest-mac <dest-mac>
```

Table 223 Boundary Clock Configuration CLI Parameters

Parameter	Input Type	Permitted Values	Description
interface-type	Variable	ethernet radio	
port	Number	ethernet: 1-7 radio: 1	The port number.
admin	Variab	enabled	Enables or disables Boundar

	le	isable	y Clock on the port.
master-only	Variable	yes no	yes – The port can only be used as the master port, which means the port acts as a PTP synchronization source for other nodes. no – The port can be used as either a master port or the slave port. The slave port receives PTP synchronization input from an external grandmaster cloc

			k. The Best Master Clock Algorithm (BMCA) determines the port's role, based on its determination of which is the best available grandmaster clock. Only one slave port can exist in a single PTP 850 E node at any one time.

local-priority	Number	1-255	
dest-mac	Variable	01-1B-19-00-00-00 01-80-C2-00-00-0E	01-1B-19-00-00-00 – General group address. An 802.1Q VLAN Bridge would forward the frame unchanged. 01-80-C2-00-00-0E – Individual LAN Scope group address. An 802.1Q VLAN Bridge would drop the

			fram e.

The following commands set up a Boundary Clock node that includes Ethernet interfaces Eth3 and Eth7 and the radio carrier. The Ethernet interfaces can serve as master or slave; the slave role is allocated dynamically according to the interface receiving the best grandmaster announce message according to the BMCA. The radio interfaces can only serve in the master role, i.e., they distribute PTP synchronization but do not receive PTP synchronization from an external grandmaster.

```
root> platform sync ptp set admin enable

root> platform sync ptp-bc interfaces set interface-type
ethernet slot 1 port 3 admin enable

root> platform sync ptp-bc interfaces set interface-type
ethernet slot 1 port 3 master-only no

root> platform sync ptp-bc interfaces set interface-type
ethernet slot 1 port 7 admin enable

root> platform sync ptp-bc interfaces set interface-type
ethernet slot 1 port 7 master-only no

root> platform sync ptp-bc interfaces set interface-type radio
slot 1 port 1 admin enable
```

In addition, you must perform the following steps to properly configure the Boundary Clock node:

1. To map PTP packets into the Boundary Clock node, a service point must be created on each interface in the Boundary Clock node. This service point must be defined to gather untagged packets. See *Adding a Service Point (CLI)*.
2. Add a port receiving synchronization from the customer side as a Sync source, with Sync Interface Priority 1. See Configuring the Sync Source (CLI).
3. Add a radio interface as a Sync source, with lower priority than the port receiving synchronization from the customer side. See Configuring the Sync Source (CLI).
4. On the remote side of the radio link, add the radio interface facing the local device as a Sync source, with Sync Interface Priority 1. See Configuring the Sync Source (CLI).
5. On the remote side of the radio link, if there is an Ethernet port conveying synchronization, add this port as a Sync source, with lower priority than the radio interface. See Configuring the Sync Source (CLI).
6. Verify that the Sync Interface Quality Status of the first Sync source is not Failure. See Displaying Synchronization Status and Parameters (CLI).

Use the following command to display the current Boundary Clock configuration:

```
root> platform sync ptp-bc interfaces show config
```

Figure 546 1588 Boundary Clock – Current Configuration Sample Display (CLI)

```
root>platform sync ptp-bc interfaces show config

1588 BC ports config table:
===========================

Interface location                Master Only     Local Priority  Admin           Destination
                                                                                  Mac Address
=================================================================================================
Ethernet: Slot 1, Port 1          yes             128             disable         1:1b:19:0:0:0
Ethernet: Slot 1, Port 2          yes             128             disable         1:1b:19:0:0:0
Ethernet: Slot 1, Port 3          yes             128             disable         1:1b:19:0:0:0
Ethernet: Slot 1, Port 4          yes             128             disable         1:1b:19:0:0:0
Ethernet: Slot 1, Port 5          yes             128             disable         1:1b:19:0:0:0
Ethernet: Slot 1, Port 6          yes             128             disable         1:1b:19:0:0:0
Ethernet: Slot 1, Port 7          yes             128             enable          1:1b:19:0:0:0
Radio: Slot 1, Port 1             yes             128             disable         1:1b:19:0:0:0
root>
```

Displaying and Setting the Boundary Clock Default Parameters (CLI)

The following commands set the Boundary Clock default parameters.

The Priority 2 value is one of the factors used by the BMCA to determine the grandmaster. The PTP 850E's Boundary Clock node advertises this value when it is not locked on an external grandmaster. The default value is 128. The following command can be used to change the Boundary Clock node's Priority 2 value.

```
root> platform sync ptp-bc clock set priority2 <priority2>
```

The following command sets the Boundary Clock node's Domain Number. The default value is 24. The following command can be used to change the Boundary Clock node's Domain Number.

```
root> platform sync ptp-bc clock set domain-number <domain-
number>
```

The Local Priority value is taken into account when two identical announce messages are received by at least two different ports. In such a case, the Boundary Clock mechanism selects the slave port based on the best (lowest) Local Priority. The default value is 128. The following command can be used to change the Boundary Clock node's default Local Priority.

```
root> platform sync ptp-bc clock set local-priority <local-
priority>
```

You can select the maximum number of PTP clocks traversed from the grandmaster to the slave clock in the local PTP 850E Boundary Clock node. If the defined number is exceeded, packets from this grandmaster candidate are discarded and the grandmaster will not be eligible for use by the Boundary Clock node. The default value is 255. The following command can be used to change the Boundary Clock node's maximum number of PTP clocks traversed.

```
root> platform sync ptp-bc clock set max-steps-removed <max-
steps-removed>
```

Table 224 Boundary Clock Default Settings – CLI Parameters

Parameter	Input Type	Permitted Values
priority2	Number	0-255
domain-number	Number	24-43
local-priority	Number	1-255
max-steps-removed	Number	1-255

Use the following command to display the Boundary Clock node's default parameters.

```
root> platform sync ptp-bc clock show default
```

Figure 547 1588 Boundary Clock – Default Parameters Sample Display (CLI)

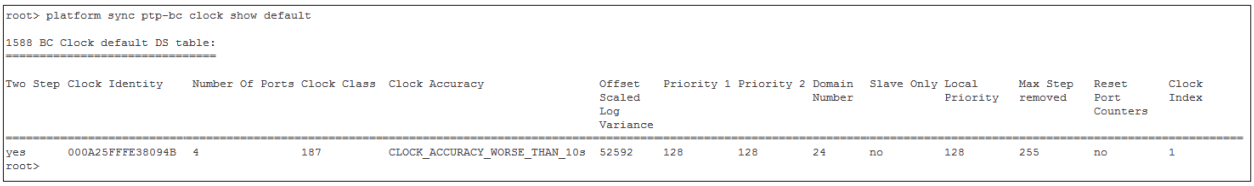


Table 225 Boundary Clock Default Parameters

Parameter	Definition
Two Step (read only)	Indicates whether the Boundary Clock node is operating in two-step mode. In PTP 850E, this is always set to Yes.
Clock Identity (read only)	Identifies the system clock.
Number of Ports (read only)	Displays the number of ports on the unit on which Boundary Clock is enabled. The maximum is 16 per PTP 850E unit.
Clock Class (read only)	One of the elements of the clock quality, as defined in IEEE-1588.
Clock Accuracy (read only)	One of the elements of the clock quality, as defined in IEEE-1588.
Offset Scaled Log Variance (read only)	One of the elements of the clock quality, as defined in IEEE-1588.
Priority 1 (read only)	Always displays 128.
Priority 2	One of the factors used by the BMCA to determine the grandmaster. The PTP 850E's Boundary Clock node advertises this value when it is not locked on an external grandmaster. The default value is 128 (user- configurable).

Domain Number	The default value is 24 (user-configurable).
Slave Only (read only)	Indicates whether the Boundary Clock node is operating in slave mode only. In PTP 850E, this is always set to no.
Max Step Removed	The maximum number of PTP clocks traversed from the grandmaster to the slave clock in the local PTP 850E Boundary Clock node. If the defined number is exceeded, packets from this grandmaster candidate are discarded and the grandmaster will not be eligible for use by the Boundary Clock node. The default value is 255 (user- configurable).
Reset Port Counters	In PTP 850E, this is always set to no.
Clock Index	In PTP 850E, this is always set to 1.

Displaying the Boundary Clock Advanced Parameters (CLI)

Use the following command to display the Boundary Clock node's general sadvanced parameters.

```
root> platform sync ptp-bc clock show current
```

Figure 548 1588 Boundary Clock – Advanced (General) Parameters Sample Display (CLI)

```
root> platform sync ptp-bc clock show current

1588 BC Clock current DS table:
===============================

Steps Removed   Offset From     Mean Path Delay Clock Index     Lock Status     Free Running
                Master
=============================================================================================================
0               ==============  scale           1               Unknown         yes
                ==============
                ==============
                ==============
                ==============
                ==============
                ==========
root>
```

Use the following command to display information about the Boundary Clock node's current time parameters.

```
root> platform sync ptp-bc clock show time
```

Figure 549 1588 Boundary Clock – Time Parameters Sample Display (CLI)

```
root> platform sync ptp-bc clock show time

1588 BC Clock time DS table:
============================

Current     Current  Leap 59  Leap 61  Time        Frequency  PTP         Time        Clock
UTC         UTC                        Traceable   Traceable  Timescale   Source      Index
Offset      Offset
(Seconds)   Valid
=============================================================================================
36          no       no       no       no          no         yes         INTERNAL_   1
                                                                          OSCILLATOR
root>
```

All of the advanced Boundary Clock parameters are read-only. Below table lists and describes the Boundary Clock advanced parameters.

Table 226 Boundary Clock Advanced Parameters (CLI)

Parameter	Definition
Steps Removed	The number of PTP clocks traversed from the grandmaster to the slave clock in the local PTP 850E Boundary Clock node. You can define a maximum number of steps in the Clock Default Parameters page.
Offset from Master (Nanoseconds)	The time difference between the master clock and the local slave clock (in ns).
Mean Path Delay (Nanoseconds)	The mean propagation time for the link between the master and the local slave (in ns).
Lock Status	Provides 1588 Boundary Clock stack lock status information.
Free Running	APR stack manual freerun state.
Master Clock Identity	The clock identity of the current master clock.
Master Port Number	The clock identity of the current master port.
Grandmaster Identity	The clock identity of the current grandmaster.
Grandmaster Clock Class	The clock class of the current grandmaster. The clock class is one of the elements of the clock quality, as defined in IEEE-1588.
Grandmaster Clock Accuracy	The clock accuracy of the current grandmaster. The clock accuracy is one of the elements of the clock quality, as defined in IEEE-1588.
Grandmaster Offset Scaled Log Variance	The offset scaled log variance of the current grandmaster. The offset scaled log variance is one of the elements of the clock quality, as defined in IEEE-1588.
Grandmaster Priority 1	The Priority 1 value of the current grandmaster.

Grandmaster Priority 2	The Priority 2 value of the current grandmaster.
Current UTC Offset (Seconds)	The current UTC offset value (in seconds).
Current UTC Offset Valid	Indicates whether the current UTC offset value is valid.
Leap 59	Indicates that the last minute of the current UTC day contains 59 seconds.
Leap 61	Indicates that the last minute of the current UTC day contains 61 seconds.
Time Traceable	Traceability to the primary time reference.
Frequency Traceable	Traceability to the primary frequency reference.
PTP Timescale	Indicates whether the clock time scale of the grandmaster clock is PTP.
Time Source	The source of the time used by the grandmaster clock.

Displaying the Boundary Clock Port Parameters (CLI)

Use the following command to display the Boundary Clock port parameters.

```
root> root> platform sync ptp-bc interfaces show status
```

Figure 550 1588 Boundary Clock Port Parameters (CLI)

```
root>platform sync ptp-bc interfaces show status

1588 BC ports status table:
===========================

Interface location         Clock Identity      Port    Port State                Log Min Delay   Log Sync     Log Announce    Announce        Version    Delay
                                               Number                            Req Interval    Interval     Interval        Receipt Timeout Number     Mechanism
=============================================================================================================================================================
Ethernet: Slot 1, Port 1   0000000000000000    1       PORT_STATE_INITIALIZING                                                4294967293      2          1
Ethernet: Slot 1, Port 2   0000000000000000    1       PORT_STATE_INITIALIZING                                                4294967293      2          1
Ethernet: Slot 1, Port 3   0000000000000000    1       PORT_STATE_INITIALIZING                                                4294967293      2          1
Ethernet: Slot 1, Port 4   0000000000000000    1       PORT_STATE_INITIALIZING                                                4294967293      2          1
Ethernet: Slot 1, Port 5   0000000000000000    1       PORT_STATE_INITIALIZING                                                4294967293      2          1
Ethernet: Slot 1, Port 6   0000000000000000    1       PORT_STATE_INITIALIZING                                                4294967293      2          1
Ethernet: Slot 1, Port 7   000A25FFFE000000    1       PORT_STATE_MASTER         -4 (16 pps)     -4 (16 pps)  -3 (8 pps)      3               2          1
Radio: Slot 1, Port 1      0000000000000000    1       PORT_STATE_INITIALIZING                                                4294967293      2          1
root>
```

Table 227 Boundary Clock Port Parameters (CLI)

Parameter	Definition

Clock Identity	The PTP 850E unit's clock identity. The same value is used for every port that belongs to the Boundary Clock node.
Port Number	Displays the number of the port according to the activation sequence of every port.
Port State	Indicates whether the port is currently acting as Master (distributing PTP to other nodes) or Slave (receiving PTP from a grandmaster).
Log Min Delay Req Interval	The minimum allowed interval between Delay Request messages.
Log Sync Interval	Interval between sync messages.
Log Announce Interval	The interval between Announce messages.
Announce Receipt Timeout	The maximum allowed number of intervals without receiving any Announce messages.
Version Number	Always displays 2.
Delay Mechanism	Always displays 1.

Displaying the Boundary Clock Port Statistics (CLI)

Use the following command to display the Boundary Clock statistics.

```
root> platform sync ptp-bc interfaces show statistics
interface-type <interface-type> slot 1 port <port> clear-on-
read <yes|no>
```

Table 228 Boundary Clock Configuration CLI Parameters

Parameter	Input Type	Permitted Values	Description
in te	V a	e t	

rface-type	riable	hernetradio	
port	Number	ethernet:1-7 radio:1	The port number.
clear-on-read	Boolean	yesno	If yes is selected, the interface statistics are cleared af

			te r th e co m m an d is ex ec ut e d.

The following command displays statistics for Eth3, and clears the statistics after displaying them.

```
root> platform sync ptp-bc interfaces show statistics
interface-type ethernet slot 2 port 1 clear-on-read yes
```

Figure 551 1588 Boundary Clock Statistics (CLI)

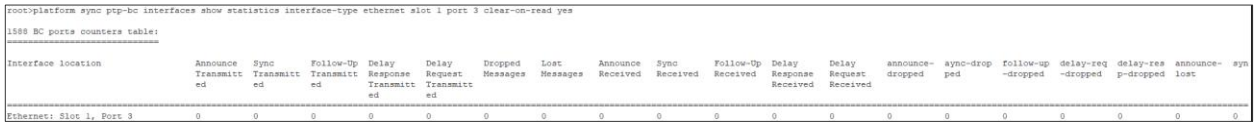


Table 229 Boundary Clock Port Statistics (CLI)

Parameter	Definition
Announce Transmitted	The number of Announce messages that have been transmitted from the port.
Sync Transmitted	The number of Sync messages that have been transmitted from the port.
Follow-Up Transmitted	The number of Follow-Up messages that have been transmitted from the port.
Delay Response	The number of Delay Response messages that have been transmitted from the port.
Delay Request	The number of Delay Request messages that have been transmitted from the port.
Dropped Messages	The number of dropped messages.
Lost Messages	The number of lost messages.

Parameter	Definition
Announce Received	The number of Announce messages that have been received by the port.
Sync Received	The number of Sync messages that have been received by the port.
Follow-Up Received	The number of Follow-Up messages that have been received by the port.
Delay Response	The number of Delay Response messages that have been received by the port.
Delay Request	The number of Delay Request messages that have been received by the port.

Disabling 1588 PTP Clock (CLI)

Use the following command to disable each Boundary Clock interface in the node. It is important to disable Boundary Clock on the interfaces *before* disabling

1588 PTP.

```
root> platform sync ptp-bc interfaces set interface-type
<interface-type> slot 1 port <port> admin disable
```

After disabling the Boundary Clock interfaces, enter the following command in root view:

```
root> platform sync ptp set admin disable
```



Note

Disabling 1588 PTP disables both Transparent Clock and Boundary Clock, and can drastically affect time synchronization performance in the entire network.

You can disable 1588 PTP synchronization on a specific interface or Multi-Carrier ABC group without disabling it on the device. You can do this by disabling Transparent Clock on the interface, as follows.

- To disable Clock on a specific radio interface, enter the following command in root view:

  ```
  root> platform sync ptp-tc set radio slot 1 port <1-2> admin
  disable
  ```

- To disable Transparent Clock on a Multi-Carrier ABC group, enter the following command in root view:

  ```
  root> platform sync ptp-tc set group-on-slot type enhanced-abc
  slot 1 group-number <1-16> admin enable
  ```

25. Access Management and Security (CLI)

This section includes:

- Configuring the General Access Control Parameters (CLI)
- Configuring the Password Security Parameters (CLI)
- Configuring Users (CLI)
- Configuring RADIUS (CLI)
- Configuring TACACS+ (CLI)
- Displaying Remote Access Users
- Configuring X.509 CSR Certificates (CLI)
- Enabling HTTPS (CLI)
- Downloading and Installing an RSA Key (CLI)
- Blocking Telnet Access (CLI)
- Configuring Access Control Lists (CLI)
- Uploading the Security Log (CLI)
- Uploading the Configuration Log (CLI)
- ***Error! Reference source not found.***
- Enabling NETCONF (CLI)
- Terminating all Active Sessions (CLI)

Related Topics:

25.1 Blocking Telnet Access (CLI)

- Operating in FIPS Mode (CLI)
- Configuring AES-256 Payload Encryption (CLI)

25.2 Configuring the General Access Control Parameters (CLI)

To avoid unauthorized login to the system, the following parameters should be set:

- Inactivity Timeout
- Blocking access due to login failures
- Blocking unused accounts

This section includes:

- Configuring the Inactivity Timeout Period (CLI)

- Configuring Blocking Upon Login Failure (CLI)
- Configuring Blocking of Unused Accounts (CLI)

25.2.1 Configuring the Inactivity Timeout Period (CLI)

A system management session automatically times out after a defined period (in minutes) with no user activity. To configure the session timeout period, enter the following command in root view:

```
root> platform security protocols-control session inactivity-timeout set <inactivity-timeout>
```

To display the currently configured session timeout period, enter the following command in root view:

```
root> platform security protocols-control session inactivity-timeout show
```

Table 230 Inactivity Timeout Period CLI Parameters

Parameter	Input Type	Permitted Values	Description
inactivity-timeout	Number	1 - 60	The session inactivity timeout period (in minutes).

The following command sets the session inactivity timeout period to 30 minutes:

```
root> platform security protocols-control session inactivity-timeout set 30
```

25.2.2 Configuring Blocking Upon Login Failure (CLI)

Upon a configurable number of failed login attempts, the system blocks the user from logging in for a configurable number of minutes.

To configure the number of failed login attempts that will temporarily block the user from logging into the system, enter the following command in root view:

```
root> platform security access-control block-failure-login attempt set <attempt>
```

To define the period (in minutes) for which a user is blocked after the configured number of failed login attempts, enter the following command in root view:

```
root> platform security access-control block-failure-login period set <period>
```

To display the current failed login attempt blocking parameters, enter the following command in root view:

```
root> platform security access-control block-failure-login show
```

Table 231 Blocking Upon Login Failure CLI Parameters

Parameter	Input Type	Permitted Values	Description
attempt	Number	1 - 10	If a user attempts to login to the system with incorrect credentials this number of times consecutively, the user will temporarily be prevented from logging into the system for the time period defined by the platform security access-control block-failure-login period set command.
period	Number	1 - 60	The duration of time, in minutes, that a user is prevented from logging into the system after the defined number of failed login attempts.

The following commands configure a blocking period of 45 minutes for users that perform 5 consecutive failed login attempts:

```
root> platform security access-control block-failure-login attempt
set 5

root> platform security access-control block-failure-login period
set 45
```

25.2.3 Configuring Blocking of Unused Accounts (CLI)

You can configure a number of days after which a user is prevented from logging into the system if the user has not logged in for the configured number of days. You can also manually block a specific user.

To configure the blocking of unused accounts period, enter the following command in root view:

```
root> platform security access-control block-unused-account period
set <period>
```

Once the user is blocked, you can use the following command to unblock the user:

```
root> platform security access-control user-account block user-
name <user-name> block no
```

To manually block a specific user, enter the following command in root view:

```
root> platform security access-control user-account block user-
name <user-name> block yes
```

To display the currently configured blocking of unused account period, enter the following command in root view:

```
root> platform security access-control block-unused-account show
```

Table 232 Blocking Unused Accounts CLI Parameters

Parameter	InputType	Permitted Values	Description
period	Number	0, 30 - 90	The number of days after which a user is prevented from logging into the system if the user has not logged in for the configured number of days. If you enter 0, this feature is disabled.
user-name	Text String	Any valid user name.	The name of the user being blocked or unblocked.

The following command configures the system to block any user that does not log into the system for 50 days:

```
root> platform security access-control block-unused-account period
set 50
```

The following commands block, then unblock, a user with the user name John_Smith:

```
root> platform security access-control user-account block user-
name John_Smith block yes

root> platform security access-control user-account block user-
name John_Smith block no
```

25.3 Configuring the Password Security Parameters (CLI)

You can configure enhanced security requirements for user passwords.

This section includes:

- Configuring Password Aging (CLI)
- Configuring Password Strength Enforcement (CLI)
- Forcing Password Change Upon First Login (CLI)
- Displaying the System Password Settings (CLI)

25.3.1 Configuring Password Aging (CLI)

Passwords remain valid from the first time the user logs into the system for the number of days (20-90) set by this command. If you set this parameter to 0, password aging is disabled, and passwords remain valid indefinitely.

To configure password aging, enter the following command in root view:

```
root> platform security access-control password aging set
<password aging>
```

Table 233 Password Aging CLI Parameters

Parameter	Input Type	Permitted Values	Description
password aging	Number	0, 20 - 90	The number of days that user passwords will remain valid from the first time the user logs into the system.

Example

The following command sets the password aging time to 60 days:

```
root> platform security access-control password aging set 60
```

25.3.2 Configuring Password Strength Enforcement (CLI)

To set password strength enforcement, enter the following command in root view:

```
root> platform security access-control password enforce-strength
set <enforce-strength>
```

Table 234 Password Strength Enforcement CLI Parameters

Parameter	Input Type	Permitted Values	Description
password aging	Number	0, 20 - 90	The number of days that user passwords will remain valid from the first time the user logs into the system.
enforce-strength	Boolean	Yes no	When yes is selected: Password length must be at least eight characters. Password must include characters of at least three of the following character types: lower case letters, upper case letters, digits, and special characters. For purposes of meeting this requirement, upper case letters at the beginning of the password and digits at the end of the password are not counted. The last five password you used cannot be reused.

Example

The following command enables password strength enforcement:

```
root> platform security access-control password enforce-strength
set yes
```

25.3.3 Forcing Password Change Upon First Login (CLI)

To determine whether the system requires users to change their password the first time they log into the system, enter the following command in root view.

```
root> platform security access-control password first-login set
<first-login>
```

To require users to change their password the first time they log in, enter the following command in root view:

```
root> platform security access-control password first-login set
yes
```

Table 235 Force Password Change on First Time Login CLI Parameters

Parameter	Input Type	Permitted Values	Description
first-login	Boolean	Yes no	When yes is selected, the system requires users to change their password the first time they log in.

25.3.4 Displaying the System Password Settings (CLI)

Use the following command to display the system password settings:

```
root> platform security access-control password show-all
```

25.4 Configuring Users (CLI)

This section includes:

- User Configuration Overview (CLI)
- Configuring User Profiles (CLI)
- Configuring User Accounts (CLI)

Related topics:

- Logging On (CLI)

25.4.1 User Configuration Overview (CLI)

User configuration is based on the Role-Based Access Control (RBAC) model. According to the RBAC model, permissions to perform certain operations are assigned to specific roles. Users are assigned to particular roles, and through those role assignments acquire the permissions to perform particular system functions.

In the PTP 850 GUI, these roles are called user profiles. Up to 50 user profiles can be configured. Each profile contains a set of privilege levels per functionality group, and defines the management protocols (access channels) that can be used to access the system by users to whom the user profile is assigned.

The system parameters are divided into the following functional groups:

- Security
- Management
- Radio
- TDM
- Ethernet
- Synchronization

A user profile defines the permitted access level per functionality group. For each functionality group, the access level is defined separately for read and write operations. The following access levels can be assigned:

None – No access to this functional group.

Normal – The user has access to parameters that require basic knowledge about the functional group.

Advanced – The user has access to parameters that require advanced knowledge about the functional group, as well as parameters that have a significant impact on the system as a whole, such as restoring the configuration to factory default settings.

25.4.2 Configuring User Profiles (CLI)

User profiles enable you to define system access levels. Each user must be assigned a user profile. Each user profile contains a detailed set of read and write permission levels per functionality group.

The system includes a number of pre-defined user profiles. You can edit these profiles, and add user profiles. Together, the system supports up to 50 user profiles.

For devices with Unit Redundancy, user profiles are copied dynamically to the standby unit, without the need to perform a Copy-to-Mate operation. This includes both new user profiles and changes to existing user profiles.

Note that it may take up to a minute for new user profile and changes to existing user profiles to be copied to the Standby unit. Therefore, if an unexpected switchover takes place less than one minute after adding or modifying a user profile:

Check that the user profile is configured in the new Active unit. If it is not, reconfigure the user profile and make sure at least one minute passes before another switchover occurs.

If the user profile is configured in the new Active unit, check that you can successfully log into the unit with that user. If you cannot, delete the user profile and re-configure it in the new Active unit.

To create a new user profile with default settings, enter the following command:

```
root> platform security access-control profile add name <profile-name>
```

To edit the settings of a user profile, enter the following command:

```
root> platform security access-control profile edit group name <profile-name> group <group> write-lvl <write-lvl> read-lvl <read-lvl>
```

Table 236 User Profile CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile--name	Text String	Up to 49 characters	The name of the user profile.

Parameter	Input Type	Permitted Values	Description
group	Variable	security management radio ethernet sync	The functionality group for which you are defining access levels.
write-lvl	Variable	none normal advanced	The read level for the functionality group.
read-lvl	Variable	none normal advanced	The read level for the functionality group.

Example

The following commands create a user profile called “operator” and give users to whom this profile is assigned normal write privileges for all system functionality and advanced read privileges for all functionality except security features.

```
root> platform security access-control profile add name operator

root> platform security access-control profile edit group name
operator group security write-lvl normal read-lvl normal group
management write-lvl normal read-lvl advanced group radio write-
lvl normal read-lvl advanced group ethernet write-lvl normal read-
lvl advanced group sync write-lvl normal read-lvl advanced
```

Limiting Access Protocols for a User Profile (CLI)

The user profile can limit the access channels that users with the user profile can use to access the system. By default, a user profile includes all access channels.

Use the following command to limit the protocols users with this user profile can use to access the system.

```
root> platform security access-control profile edit mng-channel
name <profile-name> channel-type <channel-type> allowed <allowed>
```

Table 237 User Profile Access Protocols CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile--name	Text String	Up to 49 characters	The name of the user profile.

Parameter	Input Type	Permitted Values	Description
profile-name	Text String	Up to 49 characters	The name of the user profile.
channel-type	Variable	Serial Web NMS Telnet SSH	The access channel type allowed or disallowed by the command for users with this user profile.
allowed	Boolean	yes no	yes – Users with this user profile can access the access channel type defined in the preceding parameter. no - Users with this user profile cannot access the access channel type defined in the preceding parameter.

Example

The following command prevents users with the user profile “operator” from accessing the system via NMS:

```
root> platform security access-control profile edit mng-channel
name operator channel-type NMS allowed no
```

25.4.3 Configuring User Accounts (CLI)

You can configure up to 2,000 users. Each user has a user name, password, and user profile. The user profile defines a set of read and write permission levels per functionality group (see Configuring User Profiles (CLI)).

To create a new user account, enter the following command:

```
root> platform security access-control user-account add user-name
<user-name> profile-name <profile-name> expired-date <expired-
date>
```

When you create a new user account, the system will prompt you to enter a default password. If Enforce Password Strength is activated (refer to Configuring Password Strength Enforcement (CLI)), the password must meet the following criteria:

Password length must be at least eight characters.

Password must include characters of at least three of the following character types: lower case letters, upper case letters, digits, and special characters. For purposes of meeting this requirement, upper case letters at the beginning of the password and digits at the end of the password are not counted.

The last five password you used cannot be reused.

To block or unblock a user account, enter the following command:

```
root> platform security access-control user-account block user-
name <user-name> block <block>
```

To change a user account's expiration date, enter the following command:

```
root> platform security access-control user-account edit expired-
date user-name <user-name> expired-date <expired-date>
```

To change a user account's profile, enter the following command:

```
root> platform security access-control user-account edit profile-
name user-name <user-name> profile-name <profile name>
```

To delete a user account, enter the following command:

```
root> platform security access-control user-account delete user-
name <user-name>
```

To display all user accounts configured on the unit and their settings, including whether the user is currently logged in and the time of the user's last logout, enter the following command:

```
root> platform security access-control user-account show
```

To display the settings of a specific user account, enter the following command:

```
root> platform security access-control user-account show user-name
<user-name>
```

Table 238 User Accounts CLI Parameters

Parameter	Input Type	Permitted Values	Description
user-name	Text String	Up to 32 characters	The name of the user profile.
profile name	Text String	Up to 49 characters	The name of the User Profile you want to assign to the user. The User Profile defines the user's access permissions per functionality group.
expired-date	Date	Use the format: YYYY-MM-DD	Optional. The date on which the user account will expire. On this date, the user automatically becomes inactive.
block	Variable	yes no	yes - blocks the account. no - unblocks the account.

Example

The following command creates a user account named Tom_Jones, with user profile "operator". This user's account expires on February 1, 2014.

```
root> platform security access-control user-account add user-name
Tom_Jones profile-name operator expired-date 2014-02-01
```

25.5 Configuring RADIUS (CLI)

This section includes:

- RADIUS Overview (CLI)
- Activating RADIUS Authentication (CLI)
- Configuring the RADIUS Server Attributes (CLI)



Note

For instructions on configuring a RADIUS server, see Configuring a RADIUS Server.

RADIUS Overview (CLI)

The RADIUS protocol provides centralized user management services. PTP 850E supports RADIUS server and provides a RADIUS client for authentication and authorization. When RADIUS is enabled, a user attempting to log into the system from any access channels (CLI, WEB, NMS) is not authenticated locally. Instead, the user's credentials are sent to a centralized standard RADIUS server which indicates to the PTP 850E whether the user is known, and which privilege is to be given to the user.

You can define up to two Radius servers. If you define two, one serves as the primary server and the other as the secondary server.

Activating RADIUS Authentication (CLI)

To enable or disable Radius access control, enter the following command:

```
root> platform security radius-admin set <admin>
```

Table 239 Activate RADIUS CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin	Variable	enable disable	Enables or disables Radius access control.

Configuring the RADIUS Server Attributes (CLI)

To configure Radius server attributes, enter the following command:

```
root> platform security radius-server-communication-ipv4 set
server-id <server-id> ip-address <ip-address> port <radius-
port> retries <retries> timeout <timeout> secret <shared-
secret>
```

Table 240 Configure RADIUS Server CLI Parameters

Parameter	Input Type	Permitted Values	Description

server-id	Number	1 2	1 - The primary Radius server 2 - The secondary Radius server.
ip-address	Dotted decimal format	Any valid IP address	The IP address of the Radius server.
radius-port	Number	0-65535	The port ID of the RADIUS server.
retries	Number	3-30	The number of times the device will try to communicate with the RADIUS server before declaring the server to be unreachable.
timeout	Number	1-10	The timeout (in seconds) that the agent will wait in each communication with the selected RADIUS server before retrying if no response is received.
shared-secret	String	Between 22- 128 characters	The shared secret of the RADIUS server.

The following command configures Radius server attributes for the primary Radius server:

```
root> platform security radius-server-communication-ipv4 set
server-id 1 ip-address 192.168.1.99 port 1812 retries 5 timeout

10 secret U8glp3KJ6FKGksdgase4IQ9FMm
```

25.6 Displaying Remote Access Users

You can view remote access user connectivity and permissions information for all RADIUS or users currently connected. To do so, enter the following command in root view:

```
root> platform security remote-access show
```

The following user information is displayed, for each currently connected remote access user:

- **User Name** – The user name
- **Access Channels** – The permitted access channels.
- **Number of Active Sessions** – The number of currently open sessions.
- **Security Func Group Read level** – The Read access level in the Security functional group: None, Regular or Advanced.

- **Security Func Group Write level** – The Write access level in the Security functional group: None, Regular or Advanced.
- **Management Func Group Read level** – The Read access level in the Management functional group: None, Regular or Advanced.
- **Management Func Group Write level** – The Write access level in the Management functional group: None, Regular or Advanced.
- **Radio Func Group Read level** – The Read access level in the Radio functional group: None, Regular or Advanced.
- **Radio Func Group Write level** – The Write access level in the Radio functional group: None, Regular or Advanced.
- **TDM Func Group Read level** – The Read access level in the TDM functional group: None, Regular or Advanced.
- **TDM Func Group Write level** – The Write access level in the TDM functional group: None, Regular or Advanced.
- **Eth Func Group Read level** – The Read access level in the Eth functional group: None, Regular or Advanced.
- **Eth Func Group Write level** – The Write access level in the Eth functional group: None, Regular or Advanced.
- **Sync Func Group Read level** – The Read access level in the Sync functional group: None, Regular or Advanced.
- **Sync Func Group Write level** – The Write access level in the Sync functional group: None, Regular or Advanced.

25.7 Configuring X.509 CSR Certificates (CLI)

The web interface protocol for accessing PTP 850 can be configured to HTTP (default) or HTTPS. It cannot be set to both at the same time.

Before setting the protocol to HTTPS, you must:

1 Create and upload a CSR file. See Generating a Certificate Signing Request (CSR) File (CLI).

2 Download the certificate to the PTP 850 and install the certificate. See Downloading a Certificate (CLI).

3 Enable HTTPS. See Enabling HTTPS (CLI).

When uploading a CSR and downloading a certificate, the PTP 850 functions as an SFTP client. You must install SFTP server software on the PC or laptop you are using to perform the upload or download. For details, see Installing and Configuring an FTP or SFTP Server.



Note

For these operations, SFTP must be used.

This section includes:

Generating a Certificate Signing Request (CSR) File (CLI)

Downloading a Certificate (CLI)

Enabling HTTPS (CLI)

Generating a Certificate Signing Request (CSR) File (CLI)

25.7.1 Generating a Certificate Signing Request (CSR) File (CLI)

To set the CSR parameters, enter the following command in root view:

```
root> platform security csr-set-parameters common-name <common-
name> country <country> state <state> locality <locality>
organization <organization> org-unit <org-unit> email <email>
file-format <file-format>
```

To display the currently-configured CSR parameters, enter the following command in root view:

```
root> platform security csr-show-parameters
```

If the IP address family is configured to be IPv4, enter the following command in root view to configure the SFTP server parameters for the CSR file upload:

```
root> platform security csr-set-server-parameters server-ipv4
<server-ipv4> server-path <server-path> filename <filename>
server-username <username> server-password <password>
```

If the IP address family is configured to be IPv6, enter the following command in root view to configure the SFTP server parameters for the CSR file upload:

```
root> platform security csr-set-server-parameters server-ipv6
<server-ipv6> server-path <server-path> filename <filename>
server-username <username> server-password <password>
```

To display the currently-configured SFTP parameters for CSR upload, enter the following command in root view:

```
root> platform security csr-show-server-parameters
```

To generate and upload a CSR, enter the following command in root view:

```
root> platform security csr-generate-and-upload
```

To display the status of a pending CSR generation and upload operation, enter the following command in root view:

```
root> platform security csr-generate-and-upload-show-status
```

Table 241 CSR Generation and Upload CLI Parameters

Parameter	Input Type	Permitted Values	Description
common name	String		The fully–qualified domain name for your web server. You must enter the exact domain name.
country	String		The two-letter ISO abbreviation for your country (e.g., US)

Parameter	Input Type	Permitted Values	Description
state	String		The state, province, or region in which the organization is located. Do not abbreviate.
locality	String		The city in which the organization is legally located.
organization	String		The exact legal name of your organization. Do not abbreviate.
org-unit	String		The division of the organization that handles the certificate.
email	String		An e-mail address that can be used to contact your organization.
file-format	Variable	PEM DER	The file format of the CSR. In this version, only PEM is supported.
server-ipv4	Dotted decimal format.	Any valid IPv4 IP address.	The IPv4 address of the PC or laptop you are using as the SFTP server.
server-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The IPv6 address of the PC or laptop you are using as the SFTP server.
server-path	Text String		The directory path to which you are uploading the CSR. Enter the path relative to the SFTP user's home directory, not the absolute path.If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
filename	Text String		The name you want to give the CSR.
username	Text String		The user name for the SFTP session.

Parameter	Input Type	Permitted Values	Description
password	Text String		The password for the SFTP session. To configure the SFTP settings without a password, simply omit this parameter.

25.7.2 Downloading a Certificate (CLI)

If the IP address family is configured to be IPv4, enter the following command in root view to configure the SFTP server parameters for downloading a certificate:

```
root> platform security certificate-set-download-parameters
server-ipv4 <server-ipv4> server-path <server-path> filename
<filename> server-username <username> server-password <password>
```

If the IP address family is configured to be IPv6, enter the following command in root view to configure the SFTP server parameters for downloading a certificate:

```
root> platform security certificate-set-download-parameters
server-ipv6 < server-ipv6> server-path <server-path> filename
<filename> server-username <username> server-password <password>
```

To display the currently-configured SFTP parameters for downloading a certificate, enter the following command in root view:

```
root> platform security certificate-show-download-parameters
```

To download a certificate, enter the following command in root view:

```
root> platform security certificate-download
```

To display the status of a pending certificate download, enter the following command in root view:

```
root> platform security certificate-download-show-status
```

To install a certificate, enter the following command in root view:

```
root> platform security certificate-install
```

Table 242 Certificate Download and Install CLI Parameters

Parameter	Input Type	Permitted Values	Description
server-ipv4	Dotted decimal format.	Any valid IPv4 IP address.	The IPv4 address of the PC or laptop you are using as the SFTP server.
server-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The IPv6 address of the PC or laptop you are using as the SFTP server.

Parameter	Input Type	Permitted Values	Description
server-path	Text String		The directory path from which you are downloading the certificate. Enter the path relative to the SFTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
filename	Text String		The certificate's file name in the SFTP server.
username	Text String		The user name for the SFTP session.
password	Text String		The password for the SFTP session. To configure the SFTP settings without a password, simply omit this parameter.

25.7.3 Enabling HTTPS (CLI)

By default, HTTP is used by PTP 850 as its web interface protocol.

To change the protocol to HTTPS, enter the following command in root view:

```
root> platform security url-protocol-set url-protocol https
```



Note

Make sure you have installed a valid certificate in the PTP 850 before changing the web interface protocol to HTTPS. Failure to do this may prevent users from accessing the Web EMS.

To change the protocol back to HTTP, enter the following command in root view:

```
root> platform security url-protocol-set url-protocol httpTo
display which protocol is currently enabled, enter the following
command in root view:

root> platform security url-protocol-show
```

25.8 Configuring HTTPS Cipher Hardening (CLI)

You can configure the PTP 850E to operate in HTTPS strong mode. In HTTPS strong mode, SSLv3, TLSv1.0, and TLSv1.1 are disabled completely and only certain ciphers are supported in TLSv1.2.

For a list of supported HTTPS ciphers, including an indication of which ciphers are supported in HTTPS strong mode, refer to Annex B – Supported Ciphers for Secured Communication Protocols in the Release Notes for the System release version you are using.

To set HTTPS strong mode, enter the following command:

```
root> platform security https-ciphers-hardening-level-set level
strong
```

To set HTTPS normal mode, enter the following command:

```
root> platform security https-ciphers-hardening-level-set level
normal
```

Note: The default HTTP cipher mode is normal.

To display the current HTTPS cipher mode, enter the following command:

```
root> platform security https-ciphers-hardening-level-show
```

25.9 Downloading and Installing an RSA Key (CLI)

PTP 850 devices support RSA keys for communication using HTTPS and SSH protocol. The PTP 850 device comes with randomly generated default private and public RSA keys. However, you can replace the private key with a customer-defined private key. The corresponding RSA public key will be generated based on this private key. The file must be in PEM format. Supported RSA private key sizes are 2048, 4096, and 8192.

The following is an example of a valid RSA private key file:

-----BEGIN PRIVATE KEY-----

MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC+7jRmt27yF4xD
h
5Pc8w4ikvXUu32BI0eOyELmeUBnEeIHbCOXD3upi8+ZnH51Q+8hzgoSqXgEYFgZM
o
F/sXCrO2yf62UJ5ohj3zadhx/7585zoGwHtYz1S62hsa4+cdAl/i1Vbc6CoUBh5642XYj
e+Q+q1XJtObed884eaQcXUFLIBipYKvVx2kuelymansE91WJU+UjFlc3aiQG8qsSgW5
Ar6wet0pXkP2Vdemo//QAXXjcTqqMBuizrlhIcvi+OKYFI9kSh21ZqSgjvK3cfAssCJBIY
5
d6t6bVkX9p2gjo/IPnErjAv7W6IZoemotb5KAeSHeR1sYTw17/xIpM7AgMBAAECggE
AAwIiLKQMOq4kh/UXD/OPAIPDXyp1jjaTw8dBm811OG5wttzXGrxJ+OIFX5Rn79Db
HnbayCiJL8tMe2dx5yhY+hA247roX3ua0w57cuPxnp21izc+S0fC7H/TTM1jpRCbATp
aruTRMlitinZshJGA73Lsod3v36GEXxm/6dHnz/drCs2F4NdHWpjMAAG/1CiBwut8jN
kJUwa78lvk3JF+XRoZ0txN2mlybQxxzjuNXqZbNO6H3Ua2u1iYyD+McfgOWCCUfSns
tGRhFg0OsQuqj6d74qKVQWaukEH91SVZHEoqX6DgpKy4INZBxORZmlTNmadwNh
w5O7rvFxZ205u4gQKBgQDT5bXvc0Ok+Ypm2xnIbu2GFjxNYwYhR3TvHPy14NIO5
Q

9l/uDqwrSL1igzaIr6EbZyLu8cDXa4aybrzCyBfPeG89Qq+a6J3JR/RwJndLyjV4h5CT8Z
y4O/wjgTrP3Rhq7LAbWgLjSarafLgruHTcnOifhkK7MK7Fr+xi2IJfOKQQKBgQDmq1eY
NzIMPIATESIsfbkcL49jSsu70kYg0g5Iol6+bVPo9K7mopICtWC/fwdNIUAfO+vr/231Y
UfSo7YNEDNNRoT/NwvqqtAYxZaIUdIQxhMywF9jjYBBuq6+f/7+dwDfNBtMb2q7hc
eTdk6yZ8/MehCkvSwOBmP+lq0FwTmmewKBgQClxmj31G1ve+rTXUZmkKly7OJwiL
AbCRRqnXr3r9Om43151i2QfJNTc1AwKVzTI1ftLNrUT5Q541qnzyxigaoFYmzy0jPCl1
d128/9sE6EW87hImLDg3ynYQMOIaDRc1T8bXHyxzNQb9t+U+DykeD4POifNbD1Ms
Rd3h1xDn/iAQKBgHmKpukJkCNgYgjp7g3AYR084izLaHZa4aDBjc0v4QQtzxzccJwN
5
SmQMJ42bL6wecz7YeBEAshcrd+La42Oj7mUAtgHRTwtLOEgm6TQmANGmy8OtjRa
hs4bc5/ICZNDWS5C4m9v9aIBYFuO5wCSOqffWY20L9Zj/6RR+HEj0yCpAoGAHwrb
R
qPVZtZptFuNsCq130dtmql7HFQAlqrc5DwP7YSsznE6biHfLUw891xu0vmevALrCaoe
OMaidugohgiorSJO4qk7l3XN3pUJhPYqbhtdCVnBI2Fm9pr3V/SHGvrl1NW92cXObe
Q2UEBiKPOyQKfOBIbac707u0HqaTu+/ts=

-----END PRIVATE KEY-----

You can download and install a private RSA key via HTTP, HTTPS, or SFTP. It is strongly recommended not to use HTTP to download RSA key files.



Note

To download an RSA key file using HTTP or HTTPS, you must use the Web EMS. See Downloading an RSA Key via HTTP or HTTPS.

To display the current RSA public key, enter the following command in root view:

```
root> platform security rsa-show-installed-public-key
```

If the IP address family is configured to be IPv4, enter the following command in root view to configure the SFTP server parameters for downloading the RSA key:

```
root> platform security rsa-set-download-parameters server-ipv4

<server-ipv4> server-path <server-path> filename <filename>
server-username <username> server-password <password>
```

If the IP address family is configured to be IPv6, enter the following command in root view to configure the SFTP server parameters for downloading the RSA key:

```
root> platform security rsa-set-download-parameters server-ipv6

<server-ipv6> server-path <server-path> filename <filename>
server-username <username> server-password <password>
```

To download an RSA key, enter the following command in root view:

```
root> platform security rsa-download
```

To install the RSA key, enter the following command in root view:

```
root> platform security rsa-install
```

Table 243 RSA Key Download and Install CLI Parameters

Parameter	Input Type	Permitted Values	Description
server-ipv4	Dotted decimal format.	Any valid IPv4 IP address.	The IPv4 address of the PC or laptop you are using as the SFTP server.
server-ipv6	Eight groups of four hexadecimal di	Any valid IPv6 addr	The IPv6 address of the PC or laptop you are using as the SFTP server.

	gits separated by colons.	ess.	
server-path	Text String		The directory path from which you are downloading the RSA key. Enter the path relative to the SFTP user's home directory, not the absolute path. If the location is the home directory, it should be populated with "". If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be populated with "".
filename	Text String		The RSA key file's name in the SFTP server.
username	Text String		The user name for the SFTP session.

password	Text String		The password for the SFTP session. To configure the SFTP settings without a password, populate this parameter with “”..

25.10 Blocking Telnet Access (CLI)

You can block telnet access to the unit. By default, telnet access is not blocked.

To block telnet access, enter the following command:

```
root> platform security protocols-control telnet admin set disable
```

To unblock telnet access, enter the following command:

```
root> platform security protocols-control telnet admin set enable
```

To display whether telnet is currently allowed (enable) or blocked (disable), enter the following command:

```
root> platform security protocols-control telnet show
```



Note

When you block telnet, any current telnet sessions are immediately disconnected.

25.11 Configuring Access Control Lists (CLI)

Note: For any overview of access controls lists, see Configuring Access Control Lists.

To add an access control rule, enter one of the following commands in root view.

- To add an access control rule for an IPv4 IP address, enter the following command:

```
root> platform security acl add ipv4 priority <1-4000> source-
address <x.x.x.x> prefix <0-32> protocol <any|tcp|udp|icmp]
destination-port <0-65535> action <accept|drop>
```

- To add an access control rule for an IPv6 IP address, enter the following command:

```
root> platform security acl add ipv6 priority <1-4000> source-
address <y:y:y:y:y:y:y:y> prefix <0-128> protocol
<any|tcp|udp|icmpv6> destination-port <0-65535> action
<accept|drop>
```

- To edit an access control rule for an IPv4 IP address, enter the following command using the priority to identify the rule:

```
root> platform security acl edit ipv4 priority <1-4000> source-
address <x.x.x.x> prefix <0-32> protocol <any|tcp|udp|icmp]
destination-port <0-65535> action <accept|drop>
```

- To edit an access control rule for an IPv6 IP address, enter the following command using the priority to identify the rule:

```
root> platform security acl edit ipv6 priority <1-4000> source-
address <y:y:y:y:y:y:y:y> prefix <0-128> protocol
<any|tcp|udp|icmpv6> destination-port <0-65535> action
<accept|drop>
```

Note the following:

- For the *priority* parameter, the lower the number, the higher the priority will be for the rule. For example, a rule with *priority* = 1 has the highest priority. Every rule must have a unique *priority* value. If you attempt to create a rule with an existing *priority* value, the command will return an error. The default value is 10.

Note: It is recommended to assign priorities in multiples of 10 (e.g., 10, 20, 30).

- If the ***source address*** is set to 0.0.0.0 (IPv4) or 0::0 (IPv6), the rule will be applied to all addresses, and the ***prefix*** parameter will have no meaning.
- The *prefix* parameter determines the network subnet prefix to be validated by the rule. If you enter 0 for the *prefix* parameter, the rule will apply to any subnet.
- For the *protocol* parameter, enter *any* to apply the rule to all protocol types.
- For the *destination port* parameter, enter 0 to apply the rule to all destination ports.

When you submit the command, the rule is applied immediately, but is only saved temporarily, and a five-minute failsafe timer begins. In order to confirm the rule, you must enter the following command. This command will confirm all the rules you have configured in the previous five minutes.

```
root> platform security acl confirm-config-set
```

If, before confirming them, you want to discard the rules you have configured without waiting for the five-minute timer to expire, enter the following command:

```
root> platform security acl revert-config
```

Note that rules that have not yet been confirmed are not included in backup configuration files, and are not copied to mate if you perform a copy-to-mate operation before confirming the rule.

Note: The purpose of the failsafe timer is to ensure that if you accidently enter a rule that causes management connectivity to be lost, the rule will be discarded and management restored in five minutes, with no user intervention required. A single timer runs for both IPv4 and IPv6, starting with the first rule configured for either IPv4 or IPv6.

To display all rules for either IPv4 or IPv6 source addresses, enter one of the following commands in root view:

```
root> platform security acl show ipv4

root> platform security acl show ipv6
```

For example:

```
root> platform security acl show ipv4

Priority  Source Address  Prefix  Protocol  Destination Port Action Packet counter
================================================================================
2         0.0.0.0         any     tcp       80               drop          65
4         0.0.0.0         any     any       0                drop          32
```

The *Packet counter* column displays the number of matching packets that have been received by the management interface, per rule. To clear the counters for all rules for a specific IP address type (IPv4 or IPv6), enter one of the following commands in root view:

```
root> platform security acl ipv4 clear-counters

root> platform security acl ipv6 clear-counters
```

To delete a rule, enter one of the following commands in root view:

```
root> platform security acl delete ipv4 priority <1-4000>

root> platform security acl delete ipv6 priority <1-4000>
```

To delete all rules for either IPv4 or IPv6 source addresses, enter one of the following commands in root view:

```
root> platform security acl ipv4 clear-table

root> platform security acl ipv6 clear-table
```

The following example allows all connections from the entire subnet 192.168.1/24. Note that you must add two rules, the first (with higher priority) to accept the subnet and the second (with lower priority) to drop all other traffic.

```
root> platform security acl add ipv4 priority 3 source-address
192.168.1.0 prefix 24 protocol any destination-port 0 action
accept

root> platform security acl add ipv4 priority 4 source-address
0.0.0.0 prefix 0 protocol any destination-port 0 action drop
```

The following example blocks all TCP packets for port 80:

```
root> platform security acl add ipv4 priority 2 source-address
0.0.0.0 prefix 0 protocol tcp destination-port 80 action drop
```

The following example blocks all traffic from subnet 10.12.20.1 - 10.12.20.254 (subnet 24):

root> platform security acl add ipv4 priority 1 source-address 10.12.20.0 subnet 24 protocol any destination-port 0 action dropUploading

25.12 Uploading the Security Log (CLI)

The security log is an internal system file which records all changes performed to any security feature, as well as all security related events.

In order to read the security log, you must upload the log to an FTP or SFTP server. PTP 850 works with any standard FTP or SFTP server. For details, see Installing and Configuring an FTP or SFTP Server.

Before uploading the security log, you must install and configure the FTP server on the laptop or PC from which you are performing the download. See Installing and Configuring an FTP or SFTP Server.

To set the FTP parameters for security log upload, enter the following command in root view:

```
root> platform security file-transfer set server-path <server-
path> file-name <file-name> ip-address <ip-address> protocol
<protocol> username <username> password <password>
```

To display the FTP channel parameters for uploading the security log, enter the following command in root view:

```
root> platform security file-transfer show configuration
```

To upload the security log to your FTP server, enter the following command in root view:

```
root> platform security file-transfer operation set upload-
security-log
```

To display the progress of a current security log upload operation, enter the following command in root view:

```
root> platform security file-transfer show operation
```

To display the result of the most recent current security log upload operation, enter the following command in root view:

```
root> platform security file-transfer show status
```

Table 244 Security Log CLI Parameters

Parameter	Input Type	Permitted Values	Description
server-path	Text String		The directory path to which you are uploading the security log. Enter the path relative to the FTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
file-name	Text String		The name you want to give the file you are uploading. Since the file is a text file, make sure to add the file extension *.txt*. For example: *[site name]_security_log.txt*.
ip-address	Dotted decimal format.	Any valid IP address.	The IP address of the FTP server.

Parameter	Input Type	Permitted Values	Description
protocol	Variable	ftp sftp	
username	Text String		The user name for the FTP or SFTP session.
password	Text String		The password for the FTP or SFTP session. To configure the FTP settings without a password, simply omit this parameter.

Example

The following commands configure an FTP channel for security log upload to IP address 192.168.1.80, in the directory “current”, with file name “security_log_Oct8.zip”, user name “anonymous”, and password “12345”, and initiate the upload:

```
root> platform security file-transfer set server-path \current
file-name security_log_Oct8.zip ip-address 192.168.1.80 protocol
ftp username anonymous password 12345

root> platform security file-transfer operation set upload-
security-log
```

25.13 Uploading the Configuration Log (CLI)

The configuration log lists actions performed by users to configure the system. This file is mostly used for security, to identify suspicious user actions. It can also be used for troubleshooting.

In order to upload the configuration log, you must install an FTP or SFTP server on the laptop or PC from which you are performing the upload. PTP 850 works with any standard FTP or SFTP server. For details, see Installing and Configuring an FTP or SFTP Server.

To set the FTP or SFTP parameters for configuration log export, enter the following command in root view:

```
root> platform security configuration-log-upload-params set path
<path> file-name <file-name> ip-address <ip-address> protocol
<protocol> username <username> password <password>
```

To display the FTP or SFTP parameters for configuration log export, enter the following command in root view:

```
root> platform security configuration-log-upload-params show
```

To export the configuration log, enter the following command in root view:

```
root> platform security configuration-log upload
```

To display the status of a configuration log export operation, enter the following command in root view

```
root> platform security configuration-log-upload-status show
```

Table 245 Configuration Log CLI Parameters

Parameter	Input Type	Permitted Values	Description
path	Text String		The directory path to which you are exporting the configuration log. Enter the path relative to the FTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
file-name	Text String		The name you want to give the file you are exporting. Since the file is a text file, make sure to add the file extension *.txt*. For example: *[site name]_configuration_log.txt*. If the Unit Information file is exported several times consecutively, the file itself will not be replaced. Instead, the filename will be updated by time stamp. For example: UnitInfo.zip.11-05-14 03-31-04
ip-address	Dotted decimal format.	Any valid IP address.	The IP address of the PC or laptop you are using as the FTP or SFTP server.
protocol	Variable	ftpsftp	The file transfer protocol.
username	Text String		The user name for the FTP or SFTP session.
password	Text String		The password for the FTP or SFTP session. To configure the FTP or SFTP settings without a password, simply omit this parameter.

Note

The path and fie name, together, cannot be more than:

If the IP address family is configured to be IPv4: 236 characters
If the IP address family is configured to be IPv6: 220 characters

Examples

The following commands configure an FTP channel for configuration log export to IP address 192.168.1.99, in the directory “current”, with file name “cfg_log”, user name “anonymous”, and password “12345.”

```
root> platform security configuration-log-upload-params set path
\file-name cfg_log ip-address 192.168.1.99 protocol ftp username
anonymous password 12345

root> platform unit-info channel set protocol frp
```

The following command exports the configuration log to the external server location:

```
root> platform security configuration-log upload
```

25.14 Enabling NETCONF (CLI)

PTP 850E devices support SDN, with NETCONF/YANG capabilities. This enables PTP 850E devices to be managed via SDN using Cambium’s SDN controller, SDN Master.

In order for the device to be managed via SDN, you must enable NETCONF on the device. By default, NETCONF is disabled.

To enable NETCONF, enter the following command in root view:

```
root>platform security protocols-control netconf admin set enable
```

To disable NETCONF, enter the following command in root view:

```
root>platform security protocols-control netconf admin set disable
```

To display the current NETCONF configuration on the device, enter the following command in root view:

```
root>platform security protocols-control netconf show-all
```

25.15 Terminating all Active Sessions (CLI)

You can terminate all active sessions of all users by entering the following command in root view:

```
root> platform security access-control disconnect all
```

This command terminates sessions using any channel type:

- Serial
- Web
- NMS
- Telnet
- SSH

26. Alarm Management and Troubleshooting (CLI)

This section includes:

- Viewing Current Alarms (CLI)
- Viewing the Event Log (CLI)
- Editing Alarm Text and Severity (CLI)
- Configuring a Timeout for Trap Generation (CLI)
- Disabling Alarms and Events (CLI)
- Configuring Voltage Alarm Thresholds and Displaying Voltage PMs (CLI)
- Uploading Unit Info (CLI)
- Activating the Radio Logger (CLI)
- Configuring Port Mirroring (CLI)
- Configuring Syslog (CLI)
- Performing Diagnostics (CLI)
- Working in CW Mode (Single or Dual Tone) (CLI)

26.1 Viewing Current Alarms (CLI)

To display all alarms currently raised on the unit, enter the following command in root view:

```
root> platform status current-alarm show module unit
```

To display the most severe alarm currently raised in the unit, enter the following command in root view:

```
root> platform status current-alarm show most-severe-alarm module
unit
```

26.2 Viewing the Event Log (CLI)

The Event Log displays a list of current and historical events and information about each event.

To display the event log, enter the following command in root view:

```
root> platform status event-log show module unit
```

To clear the event log, enter the following command in root view:

```
root> platform status event-log clear module unit
```

26.3 Editing Alarm Text and Severity (CLI)

You can view a list of alarm types, edit the severity level assigned to individual alarm types, and add additional descriptive text to individual alarm types.

This section includes:

- Displaying Alarm Information (CLI)
- Editing an Alarm Type (CLI)
- Setting Alarms to their Default Values (CLI)

26.3.1 Displaying Alarm Information (CLI)

To display a list of all alarm types and their severity levels and descriptions, enter the following command in root view:

```
root> platform status alarm-management show alarm-id all
```

26.3.2 Editing an Alarm Type (CLI)

To edit an alarm type's severity level, enter the following command in root view:

```
root> platform status alarm-management set alarm-id <alarm-id>
severity-level <severity-level>
```

To add descriptive information to an alarm type, enter the following command in root view:

```
root> platform status alarm-management set alarm-id <alarm-id>
additional-text <additional-text>
```

Table 246 Editing Alarm Text and Severity CLI Parameters

Parameter	Input Type	Permitted Values	Description
alarm-id	Number	All valid alarm type IDs, depending on system configuration	Enter the unique Alarm ID that identifies the alarm type.
severity-level	Variable	indeterminate critical major minor warning	The severity of the alarm, as displayed to users.
additional-text	Text String	255 characters	An additional text description of the alarm type.

Example

The following command changes the severity level of alarm type 401 (Ethernet Loss of Carrier) to minor:

```
root> platform status alarm-management set alarm-id 401 severity-
level minor
```

26.3.3 Setting Alarms to their Default Values (CLI)

To restore an alarm type's severity level and description to their default values, enter the following command in root view:

```
root> platform status alarm-management set alarm-id <alarm-id>
restore default
```

To restore the severity levels and descriptions of all alarm types to their default values, enter the following command in root view:

```
root> platform status alarm-management set all default
```

Table 247 Restoring Alarms to Default CLI Parameters

Parameter	Input Type	Permitted Values	Description
alarm-id	Number	All valid alarm type IDs, depending on system configuration	Enter the unique Alarm ID that identifies the alarm type.

Example

The following command restores alarm type 401 (Ethernet Loss of Carrier) to its default severity level:

```
root> platform status alarm-management set alarm-id 401 restore
default
```

26.4 Configuring a Timeout for Trap Generation (CLI)

You can configure a wait time of up to 120 seconds after an alarm is cleared in the system before the alarm is actually reported as being cleared. This prevents traps flooding the NMS in the event that some external condition causes the alarm to be raised and cleared continuously.

This means that when the alarm is cleared, the alarm continues to be displayed and no clear alarm trap is sent until the timeout period is finished.

The timeout for trap generation can be configured via CLI. By default, the timeout is 10 seconds.



Note

If the unit is upgraded from an earlier version to System Release 10.0 or higher, the timeout retains its previous value until it is changed. That means if it was never configured, it retains its previous default value of 0. If the unit is set to its factory default configuration, the timeout is set to 10 seconds.

To configure the timeout (in seconds) for trap generation, enter the following command in root view:

```
root> platform status alarm-management alarm-stabilization-set time <0-120>
```

To disable the timeout for trap generation, enter the following command in root view:

```
root> platform status alarm-management alarm-stabilization-set time 0
```

To display the current trap generation timeout, enter the following command in root view:

```
root> platform status alarm-management alarm-stabilization-show
```

The following command sets a trap generation timeout of 60 seconds:

```
root> platform status alarm-management alarm-stabilization-set
time 60
```

26.5 Disabling Alarms and Events (CLI)

You can choose to disable selected alarms and events. Any alarm or event can be disabled, so that no indication of the alarm is displayed, and no traps are sent for the alarm.

If you disable an alarm that is currently raised, the alarm is treated as if it has been cleared. If an alarm that has been disabled is enabled while it is in a raised state, the alarm is treated as if it has just been raised when it is enabled.

If a timeout for trap generation is configured, and a disabled alarm is enabled while the alarm is raised, the timeout count begins to run when the alarm is enabled. If an alarm is disabled while raised, the timeout count begins to run upon disabling the alarm, and an alarm cleared trap is sent when the timeout expires.

To disable an alarm or event, enter the following command in root view:

```
root> platform status alarm-management set alarm-id <alarm ID> admin
disable
```

To enable an alarm or event, enter the following command in root view:

```
root> platform status alarm-management set alarm-id <alarm ID> admin enable
```

To display a list of all disabled alarms and events, and their attributes, enter the following command in root view:

```
root> platform status alarm-management show all admin disable attributes
```

To display a list of all enabled alarms and events and their attributes, enter the following command in root view:

```
root> platform status alarm-management show all admin enable attributes
```

To enable all alarms and events, enter the following command in root view:

```
root> platform status alarm-management set all admin default
```

The alarm status commands `platform status alarm-management show alarm-id all` and `platform status alarm-management show alarm-id <alarm-id> attributes` display alarms, even if they are disabled. The Alarm Admin column in the output displays whether the alarm or event is enabled or disabled.

26.6 Configuring Voltage Alarm Thresholds and Displaying Voltage PMs (CLI)

You can configure undervoltage and overvoltage alarm thresholds.

The default thresholds for PTP 850E are:

Undervoltage Raise Threshold: 36V

Undervoltage Clear Threshold: 38V

Overvoltage Raise Threshold: 60V

Overvoltage Clear Threshold: 58V

These thresholds determine when the following alarms are raised and cleared:

Alarm #32000: Under voltage

Alarm #32001: Over voltage

To display the current thresholds, enter the following command in root view.

```
root> platform management voltage thresholds show
```

To change the threshold for raising an undervoltage alarm, enter the following command in root view:

```
root> platform management undervoltage set raise-threshold <0-100>
```

To change the threshold for clearing an undervoltage alarm, enter the following command in root view:

```
root> platform management undervoltage set clear-threshold <0-100>
```

To change the threshold for raising an overvoltage alarm, enter the following command in root view:

```
root> platform management overvoltage set raise-threshold <0-100>
```

To change the threshold for clearing an overvoltage alarm, enter the following command in root view:

```
root> platform management overvoltage set clear-threshold <0-100>
```

You can display voltage PMs that indicate, per 15-minute and 24-hour periods:

The number of seconds the unit was in an undervoltage state during the measured period.

The number of seconds the unit was in an overvoltage state during the measured period.

The lowest voltage during the measured period.

The highest voltage during the measured period.

To display voltage PMs, enter the following command in root view:

```
root> platform management voltage pm show pm-interval-type
<all|15min|24hr>
```

For example:

```
root>platform management voltage pm show pm-interval-type 24hr

Voltage PM table:
=================

Interface       PM Type    Time Interval Integrity   Interval time   Minimum      Maximum      Undervoltage  Overvoltage
Location                                             stamp           Voltage (V)  Voltage (V)  Seconds       Seconds
=============================================================================================================================
PDC #1          24hr       0             1           14-05-2000,     48           48           0             0
                                                     03:00:00
PDC #1          24hr       1             1           14-05-2000,     48           48           0             0
                                                     00:00:00
PDC #1          24hr       6             1           09-05-2000,     48           48           0             0
                                                     23:00:00
PDC #1          24hr       16            1           30-04-2000,     48           48           0             0
                                                     03:15:00
root>
```

The Integrity column indicates whether the PM is valid:

0 indicates a valid entry.

1 indicates an invalid entry. This can be caused by a power surge or power failure that occurred during the interval.

26.7 Uploading Unit Info (CLI)

You can generate a unit information file, which includes technical data about the unit. This file can be forwarded to customer support, at their request, to help in analyzing issues that may occur.



Note

For troubleshooting, it is important that an updated configuration file be included in Unit Info files that are sent to customer support. To ensure that an up-to-date configuration file is included, it is recommended to back up the unit's configuration before generating the Unit Info file.

In order to export a unit information file, you must install an FTP or SFTP server on the laptop or PC from which you are performing the upload. PTP 850 works with any standard FTP or SFTP server. For details, see Installing and Configuring an FTP or SFTP Server.

To set the FTP or SFTP parameters for unit information file export, enter one of the following commands in root view. If the IP protocol selected in platform management ip set ip-address-family is IPv4, enter the destination IPv4 address. If the selected IP protocol is IPv6, enter the destination IPv6 address.

```
root> platform unit-info channel server set ip-address <server-
ipv4> directory <directory> filename <filename> username
<username> password <password>
```

```
root> platform unit-info channel server-ipv6 set ip-address
<server-ipv6> directory <directory> filename <filename> username
<username> password <password>
```

To set the protocol for unit information file export, enter the following command in root view.

```
root> platform unit-info channel set protocol <protocol>
```

To display the FTP or SFTP parameters for unit information file export, enter one of the following commands in root view:

```
root> platform unit-info-file channel show

root> platform unit-info-file channel-ipv6 show
```

To create a unit information file based on the current state of the system, enter the following command in root view:

```
root> platform unit-info-file create
```

To export the unit information file you just created, enter the following command in root view:

```
root> platform unit-info-file export
```

To display the status of a unit information file export operation, enter the following command in root view

```
root> platform unit-info-file status show
```

Table 248 Uploading Unit Info CLI Parameters

Parameter	Input Type	Permitted Values	Description
server-ipv4	Dotted decimal format.	Any valid IPv4 address.	The IPv4 address of the PC or laptop you are using as the FTP or SFTP server.
server-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The IPv6 address of the PC or laptop you are using as the FTP or SFTP server.
directory	Text String		The directory path to which you are exporting the unit information file. Enter the path relative to the FTP or SFTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".

Parameter	Input Type	Permitted Values	Description
filename	Text String		The name you want to give the file you are exporting. **Note:** You must add the suffix .zip to the file name. Otherwise, the file import may fail. You can export the file using any name, then add the suffix .zip manually.
username	Text String		The user name for the FTP or SFTP session.
password	Text String		The password for the FTP or SFTP session. To configure the FTP or SFTP settings without a password, simply omit this parameter.
protocol	Variable	ftp sftp	The file transfer protocol.

The following commands configure an FTP or SFTP channel for configuration log export to IP address 192.168.1.99, in the directory “current”, with file name “cfg_log”, user name “anonymous”, and password “12345.”

```
root> platform security configuration-log-upload-params set path
\\ file-name cfg_log ip-address 192.168.1.99 protocol ftp username
anonymous password 12345
root> platform unit-info channel set protocol ftp
```

The following commands create a unit information file and export the file to the external server location:

```
root> platform unit-info-file create
root> platform unit-info-file export
```

Example

The following commands configures an FTP channel for unit information file export to IP address 192.168.1.99, in the directory “current”, with file name “version_8_backup.zip”, user name “anonymous”, and password “12345.”

```
root> platform unit-info channel server set ip-address
192.168.1.99 directory \current filename version_8_backup.zip
username anonymous password 12345

root> platform unit-info channel set protocol ftp
```

The following commands create a unit information file and export the file to the external server location:

```
root> platform unit-info-file create
```

```
root> platform unit-info-file export
```

26.8 Activating the Radio Logger (CLI)

The Radio Logger, when it is activated, gathers technical data about the radio and its operation. By default, the Radio Logger is inactive. It should only be activated by technical support personnel, or by the customer upon request of Customer Support team. Data gathered by the Radio Logger is added to the Unit Info file, which can be exported from the unit and sent to Customer Support upon their request.

Note: In order to conserve CPU resources, do not activate the Radio Logger unless it is necessary for unit diagnostic purposes, and do not leave it active longer than necessary.

To activate the Radio Logger, enter the following command in root view:

```
root> logger start logger-type radio logger-duration <1-1440>
slot1 1 port1 1 slot2 2 port2 2
```

The `logger-duration` parameter is set in minutes. The following command activates the logger for 40 minutes:

```
root> logger start logger-type radio logger-duration 40 slot1 2
port1 1
```

To display whether the Radio Logger is currently active, enter the following command in root view:

```
root> logger get status logger-type radio
```

For example, the following display indicates the Radio Logger has been set on both carriers for 20 minutes, and that the Logger is set to run for an additional 1191 seconds:

```
root> logger get status logger-type radio
Logger status:
Logger duration(in minutes): 20
Logger time left(in seconds): 1191
Active instances list:
Slot 1 Port 1
root>
```

To stop the Radio Logger manually, enter the following command in root view:

```
root> logger stop logger-type radio
```

To delete all data that has been saved by the Radio Logger, enter the following command in root view:

```
root> logger delete logger files<logger-type>.
```



Important Note: Whenever you activate the Radio Logger, any previous Radio Logger results are deleted.

26.9 Configuring Port Mirroring (CLI)

Port Mirroring can be used to send a copy of all traffic to and/or from a specified port to another port (the destination port). This can be a useful diagnostics tool for analyzing and debugging packets without affecting the traffic flow.

To enable Port Mirroring:

1 Go to interface view for the interface you want to mirror. See Entering Interface View (CLI).
2 In interface view, enter the following command:

```
eth type eth [x/x]>mirroring-enable mirroring-type <ingress-mirroring|egress-mirroring|ingress-and-egress-mirroring> destination-interface <eth|radio|mng|pwe> eth destination-slot <slot> destination-port <port>
```

3 Mirroring remains enabled until you manually disable it. To disable Port Mirroring, enter the following command in interface view:

```
eth type eth [x/x]>mirroring-disable
```

Note: As long as Port Mirroring is enabled, an alarm is raised (Alarm ID 103: Slot X port XX is mirrored to slot Y port YY).

To display the current Port Mirroring configuration, enter the following command in interface view for the source port:

```
eth type eth [x/x]> mirroring-show-configuration
```

26.10 Configuring Syslog (CLI)

Syslog can be used to send Security Log, Event Log, and Configuration Log messages to up to two external Syslog servers. This can simplify network monitoring and maintenance for operators by enabling them to centralize troubleshooting and monitoring information for multiple network elements in a single location.

For an overview of PTP 850's Syslog implementation.

26.10.1 Syslog Configuration (CLI)

You can configure up to two Syslog servers, using either IPv4 or IPv6 format. To set the message format, enter the following command in root view:

```
root> platform remote-syslog set-rfc-number <3163|5424>
```

- 3163: RFC-3163 (default, also known as BSD format)
- 5424: RFC-5424

To configure a Syslog server with IPv4 IP address, enter the following command:

```
root> platform remote-syslog set server-id <1-2> admin-mode <2-3|enable|disable> ipv4-address <x.x.x.x>
```

For example, to configure and enable the first Syslog server with IP address 192.168.1.18, enter the following command:

```
root> platform remote-syslog set server-id 1 admin-mode enable ipv4-address 192.168.1.18
```

To configure a Syslog server with IPv6 IP address, enter the following command:

```
root> platform remote-syslog set server-id <1-2> admin-mode <2-
3|enable|disable> ipv6-address <y:y:y:y:y:y:y:y>
```

For example, to configure and enable the second Syslog server with IP address 2003::1:18, enter the following command:

```
root> platform remote-syslog set server-id 2 admin-mode enable
ipv6-address 2003::1:18
```

Note: You can configure a Syslog server with Admin mode disable and enable it at a later time.

To enable or disable Secure Syslog, enter the following command in root view. By default, Secure Syslog is disabled. This parameter is set globally for all configured Syslog servers.

```
root> platform remote-syslog set-secure-syslog-admin <enable|
disable>
```

When Secure Syslog is enabled, you can enter the following command in root view to display the connection status. This command displays the connection status of all configured Syslog servers.

```
root> root>platform remote-syslog get-secure-syslog-admin
```

Possible values are:

- Status is empty – The **Admin Mode** for the server is set to **Disable**.
- **N/A –Secure Syslog Admin** is set to or **Disable**. Enabling Secure Syslog enables TLS-based Secure Syslog.
- **Unreachable** – The IP of the Syslog server is currently unreachable.
- **TLS Failure** – TLS handshake failed because of either TLS version mismatch or cipher suite mismatch during the TLS handshake.
- **Authentication Failure** – The server could not be authenticated.
- **Success** – TLS authentication was performed successfully and the device successfully connected to the Syslog server.

Note that events that exist as of when the Syslog server is enabled are *not* sent. Only events generated after the server is enabled are sent.

Once you have configured a Syslog server, you cannot change the IP address from IPv4 to IPv6 format or from IPv6 to IPv4 format. Instead you must delete the server configuration and re-configure it with the new IP address.

To delete a Syslog server, enter the following command in root view:

```
root> platform remote-syslog delete server-id <1|2>
```

To display the Syslog server configuration, enter the following command in root view:

```
root> platform remote-syslog show
```

The following is an example of the output of this command:

```
root>platform remote-syslog show
Remote syslog configuration table:
==================================
Server Id  IPV4 address        IPV6 address         Admin Mode
-----------------------------------------------------------------
1          192.168.1.18        ::                   enable
2          ::                  2003::1:18           disable
root>
```

26.11 Performing Diagnostics (CLI)

This section includes:

- Performing Radio Loopback (CLI)
- Performing Ethernet Loopback (CLI)

26.11.1 Performing Radio Loopback (CLI)

You can perform loopback on a radio.

To set the timeout for a radio loopback, enter the following command:

```
radio[x/x]> radio loopbacks-timeout set duration <duration>
```

To display the radio loopback timeout, enter the following command:

```
radio[x/x]>radio loopbacks-timeout show
```

To activate an RF loopback, enter the following command:

```
radio[x/x]>rf loopback-rf set admin <admin>
```

Table 249 Radio Loopback CLI Parameters

Parameter	Input Type	Permitted Values	Description
duration	Number	0 – 1440	The timeout, in minutes, for automatic termination of a loopback. A value of 0 indicates that there is no timeout.
admin	Variable	on off	Set on to initiate an RF loopback.

Examples

The following commands initiate an RF loopback on radio carrier 1 with a timeout of two minutes:

```
radio[2/1]> radio loopbacks-timeout set duration 2
radio[2/1]>rf loopback-rf set admin on
```

26.11.2 Performing Ethernet Loopback (CLI)

Ethernet loopbacks can be performed on any logical Ethernet interface except a LAG. When Ethernet loopback is enabled on an interface, the system loops back all packets ingressing the interface. This enables loopbacks to be performed over the link from other points in the network.

To configure loopback on an Ethernet interface, go to interface view for the interface and enter the following command:

```
eth type eth[x/x]> loopback admin <loopback-admin-state>
```

To configure the loopback duration time, go to interface view for the interface and enter the following command:

```
eth type eth[x/x]> loopback set duration <loopback-duration>
```

You can select whether to swap DA and SA MAC addresses during the loopback. Swapping addresses prevents Ethernet loops from occurring. It is recommended to enable MAC address swapping if LLDP is enabled.
To configure MAC address swapping, go to interface view for the interface and enter the following command:

```
eth type eth[x/x]> loopback swap-mac-address admin <MAC_swap-
admin-state>
```

To view loopback status, go to interface view for the interface and enter the following command:

```
eth type eth[x/x]> loopback status show
```

Table 250 Ethernet Loopback CLI Parameters

Parameter	Input Type	Permitted Values	Description
loopback-admin-state	Variable	enable disable	Enter **enable** to enable Ethernet loopback on the interface, or **disable** to disable Ethernet loopback on the interface.
loopback-duration	Number	1 - 900	The loopback duration time, in seconds.
MAC_swap-admin-state	Variable	enable disable	Enter **enable** to enable MAC address swapping, or **disable** to disable MAC address swapping.

Examples

The following command enables Ethernet loopback on Ethernet interface 2.

```
eth type eth [1/2]> loopback admin enable
```

The following command sets the loopback duration time to 900 seconds.

```
eth type eth [1/2]> loopback set duration 900
```

The following command enables MAC address swapping during the loopback.

```
eth type eth [1/2]> loopback swap-mac-address admin enable
```

The following command displays Ethernet port loopback status.

```
eth type eth [1/2]> loopback status show
```

26.11.3 Configuring Service OAM (SOAM) Fault Management (FM) (CLI)

This section includes:

- SOAM Overview (CLI)
- Configuring MDs (CLI)
- Configuring MA/MEGs (CLI)
- Configuring MEPs (CLI)
- Displaying MEP and Remote MEP Attributes (CLI)
- Displaying Detailed MEP Error Information (CLI)
- Performing Loopback (CLI)

26.11.4 SOAM Overview (CLI)

The Y.1731 standard and the MEF-30 specifications define Service OAM (SOAM). SOAM is concerned with detecting, isolating, and reporting connectivity faults spanning networks comprising multiple LANs, including LANs other than IEEE 802.3 media.

Y.1731 Ethernet FM (Fault Management) consists of three protocols that operate together to aid in fault management:

Continuity check

Link trace

Loopback



Note

Link trace is planned for future release.

PTP 850 utilizes these protocols to maintain smooth system operation and non-stop data flow.

The following are the basic building blocks of FM:

MD (Maintenance Domain) – An MD defines the management space on a network, typically owned and operated by a single entity, for which connectivity faults are managed via SOAM.

MA/MEG (Maintenance Association/Maintenance Entity Group) – An MA/MEG contains a set of MEPs or MIPs.

MEP (MEG End Points) – Each MEP is located on a service point of an Ethernet service at the boundary of the MEG. By exchanging CCMs (Continuity Check Messages), local and remote MEPs have the ability to detect the network status, discover the MAC address of the remote unit/port where the peer MEP is defined, and identify network failures.

MIP –(MEG Intermediate Points) – Similar to MEPs, but located inside the MEG and can only respond to, not initiate, CCM messages.

CCM (Continuity Check Message) – MEPs in the network exchange CCMs with their peers at defined intervals. This enables each MEP to detect loss of connectivity or failure in the remote MEP.

26.11.5 Configuring MDs (CLI)

In the current release, you can define one MD, with an **MD Format** of **None**.

To add an MD, enter the following command in root view:

```
root> ethernet soam md create md-id <md-id> md-format none md-name
<md-name> md-level <md-level>
```



Note

Support for MDs with the MD format Character String is planned for future release. In this release, the software enables you to configure such MDs, but they have no functionality.

The following command creates MD 5, named TR-988 with maintenance level 5.

```
root> ethernet soam md create md-id 5 md-format none md-name TR-
988 md-level 5
```

To delete an MD, enter the following command in root view. Before deleting an MD, you must delete any MA/MEG associated with the MD.

```
root> ethernet soam md delete md-id <md-id>
```

To display a list of MDs and their attributes, enter the following command in root view:

```
root> ethernet soam md show
```

Table 251 Maintenance Domain CLI Parameters

Parameter	Input Type	Permitted Values	Description
md-id	Number	1-4294967295	
md-name	String	Up to 43 alphanumeric characters.	An identifier for the MD. The MD Name should be unique over the domain.

Parameter	Input Type	Permitted Values	Description
md-level	Number	0-7	The maintenance level of the MD. The maintenance level ensures that the CFM frames for each domain do not interfere with each other. Where domains are nested, the encompassing domain must have a higher level than the domain it encloses. The maintenance level is carried in all CFM frames that relate to that domain. The maintenance level must be the same on both sides of the link. **Note:** In the current release, the maintenance level is not relevant to the SOAM functionality.

26.11.6 Configuring MA/MEGs (CLI)

You can configure up to 1280 MEGs per network element. MEGs are classified as Fast MEGs or Slow MEGs according to the CCM interval (see Table 252):

Fast MEGs have a CCM interval of 1 second.

Slow MEGs have a CCM interval of 10 seconds, 1 minute, or 10 minutes.

You can configure up to 64 MEP pairs per network element.

To add an MA/MEG, enter the following command in root view:

```
root> ethernet soam meg create meg-id <meg-id> meg-fmt charString
meg-name <meg-name> meg-level <meg-level> service-id <0-4095>
```



Note

In the current release, charString is the only available MEG name format.

The following command creates MEG ID 1, named FR-10, with MEG level 4, assigned to Ethernet service 20.

```
root> ethernet soam meg create meg-id 1 meg-fmt charString meg-
name FR-10 meg-level 4 service-id 20
```

To set the interval at which CCM messages are sent within the MEG, enter the following command in root view:

```
root> ethernet soam meg ccm-interval set meg-id <meg-id> ccm <ccm>
```

The following command sets an interval of one second between CCM messages for MEG 1.

```
root> ethernet soam meg ccm-interval set meg-id 1 ccm interval1s
```

To determine whether MIPs are created on the MEG, enter the following command in root view:

```
root> ethernet soam meg mip set meg-id <meg-id> mhf <1-
4|defMHFnone|defMHFdefault|defMHFexplicit|defMHFdefer>
```

The following command creates MIPs on any service point in the MEG:

```
root> ethernet soam meg mip set meg-id 1 mhf defMHFdefault
```

To delete a MEG, enter the following command in root view:

```
root> ethernet soam meg delete <meg-id> ccm <ccm>
```



Note

To can only delete a MEG if no MEPs or MIPs are attached to the MEP.

To display a list of all MEGs configured on the unit, enter the following command in root view:

```
root> ethernet soam meg show
```

To display MEG attributes, including the number of MEPS, local MEPS, and MIPs attached to the MEG, enter the following command in root view:

```
root> ethernet soam meg attributes show meg-id <meg-id>
```

Table 252 SOAM MEG CLI Configuration Parameters

Parameter	Input Type	Permitted Values	Description
meg-id	Number	1-4294967295	Enter an ID for the MEG.
meg-name	String	Up to 44 alphanumeric characters	A name to identify the MEG.

Parameter	Input Type	Permitted Values	Description
meg-level	Number	0-7	The MEG level must be the same for MEGs on both sides of the link. Higher levels take priority over lower levels. If MEGs are nested, the OAM flow of each MEG must be clearly identifiable and separable from the OAM flows of the other MEGs. In cases where the OAM flows are not distinguishable by the Ethernet layer encapsulation itself, the MEG level in the OAM frame distinguishes between the OAM flows of nested MEGs. Eight MEG levels are available to accommodate different network deployment scenarios. When customer, provider, and operator data path flows are not distinguishable based on means of the Ethernet layer encapsulations, the eight MEG levels can be shared among them to distinguish between OAM frames belonging to nested MEGs of customers, providers and operators. The default MEG level assignment among customer, provider, and operator roles is: The customer role is assigned MEG levels 6 and 7 The provider role is assigned MEG levels 3 through 5 The operator role is assigned MEG levels: 0 through 2 The default MEG level assignment can be changed via a mutual agreement among customer, provider, and/or operator roles. The number of MEG levels used depends on the number of nested MEs for which the OAM flows are not distinguishable based on the Ethernet layer encapsulation.
service-id	Number	0-4095	Assign the MEG to an Ethernet service. You must define the service before you configure the MEG.

Parameter	Input Type	Permitted Values	Description
ccm	Variable	interval1s interval10s interval1min interval10min	interval1s – One second (default) interval10s – 10 seconds interval1min – One minute interval10min – 10 minutes It takes a MEP 3.5 times the CCM interval to determine a change in the status of its peer MEP. For example, if the CCM interval is 1 second, a MEP will detect failure of the peer 3.5 seconds after it receives the first CCM failure message. If the CCM interval is 10 minutes, the MEP will detect failure of the peer 35 minutes after it receives the first CCM failure message.
mhf	Variable	defMHFnone defMHFdefault defMHFexplicit defMHFdefer	Determines whether MIPs are created on the MEG. Options are: defMHFnone – No MIPs are created. defMHFdefault – MIPs are created on any service point in the MEG. defMHFexplicit – MIPs are created on the service points of the MEG when a lower-level MEP exists on the service point. This option is usually used when the operator's domain is encompassed by another domain. defMHFdefer – No MIPs are created.

26.11.7 Configuring MEPs (CLI)

Each MEP is attached to a service point in an Ethernet service. The service and service point must be configured before you configure the MEP. See Configuring Ethernet Services (CLI).

Each MEP inherits the same VLAN, C-VLAN, or S-VLAN configuration as the service point on which it resides. See Configuring Service Points (CLI).

In order to set the VLAN used by CCM/LBM/LTM if the service point is defined ambiguously (for example PIPE, Bundle-C, Bundle-S, or All-to-One), the service point's C-VLAN/S-VLAN parameter should not be set to N.A.

To configure a MEP, you must:

1 Add MEPs to the relevant MA/MEG. In this stage, you add both local and remote MEPs. The only thing you define at this point is the MEP ID. See Adding Local and Remote MEPs (CLI).

2 Configure the local MEPs. At this point, you determine which MEPs are local MEPs. The system automatically defines the other MEPs you configured in the previous step as remote MEPs. See Configuring the Local MEPs (CLI).

3 Enable the Local MEPs. See Enabling Local MEPs (CLI).

26.11.7.1 Adding Local and Remote MEPs (CLI)

To add a MEP, enter the following command in root view:

```
root> ethernet soam meg mep add meg-id <meg-id> mep-id <mep-id>
```

The following command adds MEP 25 on MEG 2.

```
root> ethernet soam meg mep add meg-id 2 mep-id 25
```

To remove a MEP, enter the following command in root view:

```
root> ethernet soam meg mep remove meg-id <meg-id> mep-id <mep-id>
```

The following command removes MEP 25 from MEG 2.

```
root> ethernet soam meg mep remove meg-id 2 mep-id 25
```

To display a list of all MEPs that belong to a specific MEG, enter the following command in root view:

```
root> ethernet soam meg mep show meg-id <meg-id>
```

26.11.7.2 Configuring the Local MEPs (CLI)

Once you have added local and remote MEPs, you must configure the MEPs and determine which are the local MEPs.

To make a defined MEP a local MEP, you must assign the MEP to a service point on the Ethernet service on which the MEG resides.

To assign a MEP to a service point, enter the following command in root view:

```
root> ethernet soam mep create meg-id <meg-id> mep-id <mep-id> sp-
id <sp-id> mep-dir <mep-dir>
```

The following command assigns MEP 35 on MEG 2 to Service Point 3 on the service on which MEG 2 resides.

```
root> ethernet soam mep create meg-id 2 mep-id 35 sp-id 3 mep-dir
down
```

To change a MEP from a local to a remote MEP, enter the following command in root view:

```
root> ethernet soam mep delete meg-id <meg-id> mep-id <mep-id>
```

The following command changes MEP 35 from a local to a remote MEP.

```
root> ethernet soam mep delete meg-id 2 mep-id 35
```

To display a list of local MEPs for a specific MEG, enter the following command in root view:

```
root> ethernet soam meg local-mep show meg-id <meg-id>
```

For example:

```
root> ethernet soam meg local-mep show meg-id 2
MEG:
========
-------------------------------------------------------------------------------
|MA ID|Format       |Name                                          |Level |Service|
-------------------------------------------------------------------------------
|2    |charString   |TR-98                                         |0     |1      |
-------------------------------------------------------------------------------

MEP:
========
-------------------------------------------------------------
|MepId      |Interface  |Direction |Active          |SP ID |
-------------------------------------------------------------
|25         |eth   1/1  |down      |true            |1     |
-------------------------------------------------------------
|35         |eth   1/2  |down      |false           |3     |
-------------------------------------------------------------
root> _
```

26.11.7.3 Enabling Local MEPs (CLI)

Once you have added a MEP and defined it as a local MEP, you must enable the MEP by setting the MEP to Active, enabling CCM messages from the MEP, and assigning a CCM-LTM priority to the MEP.

To set a MEP to Active, enter the following command in root view:

```
root> ethernet soam mep active set meg-id <meg-id> mep-id <mep-id>
mep-active <mep-active>
```

The following command sets MEP 35 on MEG 2 to Active.

```
root> ethernet soam mep active set meg-id 2 mep-id 35 mep-active
true
```

To enable or disable the sending of CCM messages on a MEP, enter the following command in root view:

```
root> ethernet soam mep ccm-enable set meg-id <meg-id> mep-id
<mep-id> enabled <ccm-enabled>
```

The following command assigns enables CCM messages for MEP 35 on MEG 2.

```
root> ethernet soam mep ccm-enable set meg-id 2 mep-id 35 enabled true
```

To set a MEP's CCM-LTM priority, enter the following command in root view:

```
root> ethernet soam mep ccm-ltm-prio set meg-id <meg-id> mep-id
<mep-id> ccm-ltm-priority <ccm-ltm-priority>
```

The following command sets the CCM-LTM priority of MEP 35 in MEG 2 to 5.

```
root> ethernet soam mep ccm-ltm-prio set meg-id 2 mep-id 35 ccm-
ltm-priority 5
```

Table 253 MEP CLI Configuration Parameters

Parameter	Input Type	Permitted Values	Description
meg-id	Number	1-4294967295	Enter an ID for the MEG.
mep-id	Number	1-8191	A name to identify the MEG.

Parameter	Input Type	Permitted Values	Description
sp-id	Number	0-32	The Service Point ID of the service point to which you want to assign the MEP.
mep-dir	Variable	up down	The MEP direction.
ccm-enabled	Variable	true false	true – CCM messages are enabled on the MEP. false – CCM messages are disabled on the MEP.
ccm-ltm-priority	Number	0-7	The p-bit included in CCMs sent by this MEP.
mep-active	Variable	true false	true – The MEP is Active. false – The MEP is Inactive.

26.11.7.4 Displaying MEP and Remote MEP Attributes (CLI)

To display the attributes of a specific MEP, enter the following command in root view:

```
root> ethernet soam mep configuration general show meg-id <meg-id
<meg-id> mep-id <mep-id>
```

For example:

```
root> ethernet soam mep configuration general show meg-id 2 mep-id 25
MEG:
========
------------------------------------------------------------------------------
|MA ID|Format       |Name                                          |Level |Service|
------------------------------------------------------------------------------
|2    |charString   |TR-98                                         |0     |1      |
------------------------------------------------------------------------------

SOAM MEP Table:
===============
Interface  MEP        MEP Active MEP CCM    CCM and    MEP MAC           MEP Lowest      MEP Alarm  MEP Alarm
Location   Direction             TX Enable  LTM        Address           priority fault  on time    Clear Time
                                            Priority                     alarm
=============================================================================================================
eth   1/1 |down       |true      |true       |7         |0:a:25:38:9:4b    |allDef         |250       |1000
-------------------------------------------------------------------------------------------------------------
root>
```

To display a list of remote MEPs (RMEPs) and their parameters per MEG and local MEP, enter the following command in root view:

```
root> ethernet soam mep rmep list show meg-id <meg-id <meg-id>
mep-id <mep-id>
```

For example:

```
root> ethernet soam mep rmep list show meg-id 2 mepid 25
MD:
-------------------------------------------------------------------------------
|MD ID|MD Name                                    |MD Format        |MD Level|
-------------------------------------------------------------------------------
|1    |TR-995                                     |none             |5       |
-------------------------------------------------------------------------------

MEG:
-------------------------------------------------------------------------------------------------------------------------
|MA ID|Format       |Name              |Level |Service|CCM Interval    |Number of MEPs |Number of Local MEPs |Number of MIPs|
-------------------------------------------------------------------------------------------------------------------------
|2    |charString   |TR-98             |0     |1      |interval1s      |4              |2                    |0             |
-------------------------------------------------------------------------------------------------------------------------
SOAM MEP Table:
===============
MEP ID     Interface  MEP        MEP Active MEP CCM    CCM and
           Location   Direction             TX Enable  LTM Priority

=================================================================
25        |eth   1/1 |down      |true      |true      |7
-----------------------------------------------------------------
RMEPs:
========
-------------------------------------------
| RmepId | State    | MAC             | Rdi |
-------------------------------------------
|45      |rMepFailed|ff:ff:ff:ff:ff:ff|false|
-------------------------------------------
|55      |rMepFailed|ff:ff:ff:ff:ff:ff|false|
-------------------------------------------
```

To display a list of remote MEPs (RMEPs) and their parameters per MEG and local MEP, enter the following command in root view:

```
root> ethernet soam mep rmep show meg-id meg-id < meg-id <meg-id>
mep-id <mep-id> rmep-id <rmep-id>
```

For example:

```
root> ethernet soam mep rmep show meg-id 2 mep-id 35 rmep-id 45
MD:
-------------------------------------------------------------------------------
|MD ID|MD Name                                    |MD Format        |MD Level|
-------------------------------------------------------------------------------
|1    |TR-995                                     |none             |5       |
-------------------------------------------------------------------------------

MEG:
-------------------------------------------------------------------------------------------------------------------------
|MA ID|Format       |Name                                       |Level |Service|CCM Interval    |Number of MEPs |Number of Local MEPs |Number of MIPs|
-------------------------------------------------------------------------------------------------------------------------
|2    |charString   |TR-98                                      |0     |1      |interval1s      |4              |2                    |0             |
-------------------------------------------------------------------------------------------------------------------------

SOAM MEP Table:
===============
MEP ID     Interface  MEP        MEP Active MEP CCM TX Enable  CCM and    MEP MAC           MEP Lowest    MEP Alarm  MEP Alarm  Sequence   CCM
           Location   Direction                                LTM        Address           priority      on time    Clear Time Errors     Messages
                                                               Priority                     fault alarm                             CCM Frames TX
=============================================================================================================================================
35        |eth   2/4 |down      |true      |true               |5         |0:a:25:38:9:50   |allDef       |250       |1000      |0         |389
---------------------------------------------------------------------------------------------------------------------------------------------

RMEP:
=====
-------------------------------------------------------------------------------------------------------------------------------------------
|MepId|RmepId|operState |OKorFail Time| MAC             | Rdi | port Status     |interface Status   | ChassisID format | Chassis ID     | Mng Addr Domain |
-------------------------------------------------------------------------------------------------------------------------------------------
|35   |45    |rMepFailed|6874         |ff:ff:ff:ff:ff:ff|false|psNoPortStateTLV|isNoInterfaceStatus|None              |                |0                |
-------------------------------------------------------------------------------------------------------------------------------------------
root> _
```

Table 254 MEP and Remote MEP Status Parameters (CLI)

Parameter	Description
MD Parameters	
MD ID	The MD ID.
MD Name	The MD name (44 characters).
MD Format	The MD format (None).
MD Level	The maintenance level of the MD (0-7).

Parameter	Description
MEG Parameters	
MA ID	The MA/MEG ID.
Format	charString in the current release.
Name	The MA/MEG name (43 characters).
Level	The MEG Level (0-7).
Service	The Service ID of the Ethernet service to which the MEG belongs.
CCM Interval	The interval at which CCM messages are sent within the MEG.
Number of MEPs	The number of MEPs that belong to the MEG.
Number of Local MEPs	The number of local MEPs that belong to the MEG.
Number of MIPs	The number of MIPs that belong to the MEG.
SOAM MEP Table Parameters	
MEP ID	The MEP ID.
Interface Location	The interface on which the service point associated with the MEP is located.
MEP Direction	Up or Down.
MEP Active	Indicates whether the MEP is enabled (true) or disabled (false).
MEP CCM TX Enable	Indicates whether the MEP is configured to send CCMs (true or false).
CCM and LTM Priority	The p-bit included in CCMs sent by the MEP (0-7).
MEP MAC Address	The MAC address of the service point associated with the MEP.
MEP Lowest priority fault alarm	The lowest defect priority that can trigger alarm generation. Defects with a lower priority will not trigger alarms.
MEP Alarm on time	The amount of time that defects must be present before an alarm is generated, in msec intervals (250-1000).
MEP Alarm Clear Time	The amount of time that defects must be absent before an alarm is cleared, msec intervals (250-1000).

Parameter	Description
Sequence errors CCM Frames	The number of out-of-sequence CCM messages received.
CCM Messages TX	The number of transmitted CCM messages.
RMEP Parameters	
MepId	The MEP ID of the local MEP paired with the remote MEP.
Rmep Id	The remote MEP ID.
operState	The operational state of the remote MEP.
OKorFail Time	The timestamp marked by the remote MEP indicating the most recent CCM OK or failure it recorded. If none, this field indicates the amount of time, in msec intervals, since SOAM was activated.
MAC	The MAC Address of the interface on which the remote MEP is located.
Rdi	Displays the state of the RDI (Remote Defect Indicator) bit in the most recent CCM received by the remote MEP: **True** – RDI was received in the last CCM. **False** – No RDI was received in the last CCM.
Port Status	The Port Status TLV in the most recent CCM received from the remote MEP. Reserved for future use.
Interface Status	The Interface Status TLV in the most recent CCM received from the remote MEP. Indicates the operational status of the interface (Up or Down).
Chassis ID Format	Displays the address format of the remote chassis (in the current release, MAC Address).
Chassis ID	Displays the MAC Address of the remote chassis.
Mng Addr Domain	Displays the BASE MAC address of the remote unit (the unit on which the remote MEP resides).,

26.11.7.5 Displaying Detailed MEP Error Information (CLI)

To display the entire frame of the last CCM error message and the last CCM cross-connect error message received by a specific local MEP, along with other detailed information, enter the following command in root view:

```
root> ethernet soam mep status general show meg-id <meg-id> mep-id
<mep-id> detailed yes
```

For example:

```
root> ethernet soam mep status general show meg-id 2 mep-id 25 detailed yes
MEG:
========
--------------------------------------------------------------------------------
|MA ID|Format       |Name                                          |Level |Service|
--------------------------------------------------------------------------------
|2    |charString   |TR-98                                         |0     |1      |
--------------------------------------------------------------------------------


SOAM MEP Table:
===============

MEP Fault          MEP highest    MEP Defects     Sequence   CCM Messages TX
Notification State  priority                      Errors
                    fault alarm                   CCM Frames
================================================================================
fngDefectReported   defRemoteCCM   bDefRemoteCCM   0          10469

SOAM MEP Table:
===============

Last RX error CCM message         Last RX Xcon fault message
================================================================================
00000000000000000000000000000000  00000000000000000000000000000000
00000000000000000000000000000000  00000000000000000000000000000000
00000000000000000000000000000000  00000000000000000000000000000000
00000000000000000000000000000000  00000000000000000000000000000000
00000000000000000000000000000000  00000000000000000000000000000000
00000000000000000000000000000000  00000000000000000000000000000000
00000000000000000000000000000000  00000000000000000000000000000000
00000000000000000000000000000000  00000000000000000000000000000000

SOAM MEP MEF Status Table:
==========================

MEP Operational  Connectivity     Last Sent Port status TLV  Last Sent Interface        Last MEP        RDI TX
State            Status                                      status TLV                 Defects         indication
================================================================================================================
enabled          inactive         psNoPortStateTLV           isDown                     None            false
root> _
```

To display the same information without the last RX error CCM and fault messages, enter the following command in root view:

```
root> ethernet soam mep status general show meg-id <meg-id> mep-id
<mep-id> detailed no
```

The **Last RX error CCM message** field displays the frame of the last CCM that contains an error received by the MEP.

The **Last RX Xcon fault message** field displays the frame of the last CCM that contains a cross-connect error received by the MEP.



Note

A cross-connect error occurs when a CCM is received from a remote MEP that has not been defined locally.

26.11.7.6 Performing Loopback (CLI)

To set the interval between loopback message transmissions in a loopback session, enter the following command in root view:

```
root> ethernet soam loopback interval set meg-id <meg-id> mep-id
<mep-id> interval <0-60000>
```

For example, the following command sets the loopback interval for MEP 25 on MEG 1 to 5 seconds:

```
root> ethernet soam loopback interval set meg-id 1 mep-id 25
interval 5000
```

To set the loopback message frame size and data pattern, enter the following command in root view:

```
root> ethernet soam loopback data set meg-id <meg-id> mep-id <mep-
id> size <size> pattern <pattern>
```

For example, the following command sets the loopback frame size to 128 and the pattern to zero for MEP 25 on MEG 1 to 5 seconds:

```
root> ethernet soam loopback data set meg-id 1 mep-id 25 size 128
pattern zeroPattern
```

To set the loopback priority bit size and drop-enable parameters, enter the following command in root view:

```
root> ethernet soam loopback prio set meg-id <meg-id> mep-id <mep-
id> prio <priority> drop <drop>
```

For example, the following command sets a priority bit size of 5 and enables frame dropping for MEP 25 on MEG 1 to 5 seconds:

```
root> ethernet soam loopback prio set meg-id 1 mep-id 25 prio 5
drop true
```

To set the loopback destination by MAC address, set the number of loopback messages to transmit and the interval between messages, and initiate the loopback, enter the following command in root view:

```
root> ethernet soam loopback send meg-id <meg-id> mep-id <mep-id>
dest-mac-addr <dest-mac-addr> tx-num <tx-num> tx-interval
<interval>
```

For example, the following command initiates a loopback session with the interface having MAC address 00:0A:25:38:09:4B. The session is configured to send 100 loopback messages at six-second intervals.

```
root> ethernet soam loopback send meg-id 1 mep-id 25 dest-mac-addr
00:0A:25:38:09:4B tx-num 100 tx-interval 6000
```

To set the loopback destination by MEP ID, set the number of loopback messages to transmit and the interval between messages, and initiate the loopback, enter the following command in root view:

```
root> ethernet soam loopback send meg-id <meg-id> mep-id <mep-id>
dest-mep-id <dest-mac-addr> tx-num <tx-num> tx-interval <interval>
```

For example, the following command initiates a loopback session with the interface having MAC address 00:0A:25:38:09:4B. The session is configured to send 100 loopback messages at six-second intervals.

```
root> ethernet soam loopback send meg-id 1 mep-id 25 dest-mac-addr
00:0A:25:38:09:4B tx-num 100 tx-interval 6000
```



Note

If you initiate the loopback via MEP ID, the loopback will only be activated if CCMs have already been received from the MEP. For this reason, it is recommended to initiate loopback via MAC address.

To display the loopback attributes of a MEP, enter the following command in root view:

```
root> ethernet soam loopback config show meg-id <meg-id> mep-id
<mep-id>
```

For example:

```
root> ethernet soam loopback config show meg-id 1 mep-id 25

SOAM MEP LBM Attributes Table:
==============================

Loopback   Loopback     Loopback   Drop       Loopback   Loopback   Loopback   Loopback
messages   Messages     Messages   Enable     Messages   Messages   Messages   Replies
to be      Destination  Priority              Interval   Frame Size Data       Age-out
transmitt  MAC Address                                             Pattern    Time
ed                                                                 Type
================================================================================================
1          0:0:0:0:0:0  5          true       5000       128        zeroPatte  5
                                                                   rn

root> _
```

To stop a loopback that is already in progress, enter the following command in root view:

```
root> ethernet soam loopback stop meg-id <meg-id> mep-id <mep-id>
```

Table 255 Loopback CLI Parameters

Parameter	Input Type	Permitted Values	Description
meg-id	Number	1-4294967295	The MEG ID of the MEG on which the loopback is being configured or run.
mep-id	Number	1-8191	The MEP ID of the MEP on which the loopback is being configured or run.
interval	Number	0-60000	The interval (in ms) between each loopback message. Note that the granularity for this parameter is 100 ms. If you enter a number that is not in multiples of 100, the value will be rounded off to the next higher multiple of 100. Also, the lowest interval is 1000 ms (1 second). If you enter a smaller value, it will be rounded up to 1000 ms.
size	Number	64-1518	The frame size for the loopback messages. Note that for tagged frames, the frame size will be slightly larger than the selected frame size.
pattern	Variable	zeroPattern onesPattern	The type of data pattern to be sent in an OAM PDU Data TLV.

Parameter	Input Type	Permitted Values	Description
priority	Number	0-7	The priority bit for tagged frames.
drop	Boolean	true false	**true** – Frame dropping is enabled. **false** – Frame dropping is disabled.
dest-mac-addr	Six groups of two hexadecimal digits		The MAC address of the interface to which you want to send the loopback. If you are not sure what the interface's MAC address is, you can get it from the Interface Manager by entering the `platform if-manager show interfaces` command in root view.
dest-mep-id	Number	1-8191	The MEP ID of the interface to which you want to send the loopback.
tx-num	Number	0-1024	The number of loopback messages to transmit. If you enter 0, loopback will not be performed.

```
To display loopback results, enter the following command in root view:root> ethernet soam loopback status show meg-id <meg-id> mep-id <mep-id>
```

The following is a sample output for this command on MEG ID 127, MEP ID 1.

```
root> ethernet soam loopback status show meg-id 127 mep-id 1

SOAM MEP LBM Attributes Table:
==============================

Loopback   Loopback   Loopback   Transacti  Loopback   Next       Loopback   Loopback   Valid      Loopback   Valid      Bad MSDU   Loopback   Lo
messages   messages   replies    on ID of   session    transacti  messages   messages   in-order   replies    out-of-or  Loopback   messages   re
transmitt  left to    received   1st        state      on ID      transmitt  received   loopback   transmitt  der        Replies    recieved   re
ed in      transmit   in session loopback                         ed                    replies    ed         loopback                with bad   wi
session    in session            message                                               received              replies                 sender id  se
                                                                                                         received
==========================================================================================================================================
9          114        9          1          soamLbAct  10         9          0          9          0          0          0          0          0
                                             ive

root>
```

26.12 Working in CW Mode (Single or Dual Tone) (CLI)

CW mode enables you to transmit a single or dual frequency tones, for debugging purposes.

To work in CW mode, enter the following command:

```
radio[x/x] modem tx-source set admin enable
```

Once you are in CW mode, you can choose to transmit in a single tone or two tones.

To transmit in a single tone, enter the following command in radio view:

```
radio[x/x] modem tx-source set mode one-tone freq-shift <freq-
shift>
```

To transmit two tones, enter the following command in radio view:

```
radio[x/x] modem tx-source set mode two-tone freq-shift <freq-
shift> freq-shift2 <freq-shift>
```

To exit CW mode, enter the following command:

```
radio[x/x] modem tx-source set admin disable
```

Table 256 CW Mode CLI Parameters

Parameter	Input Type	Permitted Values	Description
freq-shift	Number	0-7000	Enter the frequency you want to transmit, in KHz.

The following commands set a single-tone transmit frequency of 5050 KHz on radio interface 1, then exit CW mode and return the interface to normal operation:

```
root> radio slot 2 port 1
radio[2/1] modem tx-source set admin enable
radio[2/1] radio[x/x] modem tx-source set mode one-tone freq-shift
5050
radio[2/1] modem tx-source set admin disable
```

27. Maintenance

This section includes:

- Troubleshooting Tips
- Temperature Ranges
- PTP 850C Interface Pin-outs and LEDS
- PTP 850E Interface Pin-outs and LEDS
- PTP 850S Interface Pin-outs and LEDS
- PoE Injector Pin-outs and LEDs – Standard PoE
- PoE Injector Pin-outs and LEDs – Passive PoE



Troubleshooting Tips

Platform

- If during or right after a software upgrade the message *Your session has expired, please login again* appears and you cannot log in, it is recommended to refresh the Web EMS page (F5) after completion of the upgrade. If pressing F5 does not help, clear the browser's cache by pressing Ctrl+Shift+Delete.

XPIC

- For XPIC links, if one of the polarizations has significantly reduced performance, check to make sure the antenna's rectangular interface was replaced with a circular adaptor.[17]
- For XPIC links, the RSL should be similar for both polarizations. The XPI value should be similar for both polarizations; the difference should not be more than 2 dB.[17]

[17] Only relevant for PTP 850C and PTP 850E.

Unit Protection

- When switchover takes place, a series of GARP packets are sent identifying the MAC address of the new management interface. This enables the management device to immediately re-establish the management connection. By default, three GARP packets are sent:
  - The first GARP packet is sent immediately upon switchover.
  - The second GARP packet is sent 500 ms after switchover.
  - The third GARP packet is sent one second after switchover.

The number of GARP packets is user-configurable. If you experience a delay in re-establishing management, you can increase the number of GARP packets that are sent upon switchover. The number of packets can be changed to any value from 0 (disabling the feature) to 10. Packets are sent at intervals of 500 ms.

Use the following CLI command to change the number of GARP packets to be sent upon switchover:

```
root>platform management protection debug set garp <0-10>
```

Use the following CLI command to show the current configuration of this parameter:

```
root>platform management protection debug show garp
```

27.2 Temperature Ranges

The following are the permissible unit temperature ranges for PTP 850E.

- **-33°C to 55°** – Temperature range for continuous operating temperature with high reliability.
- **-45°C to 60°C** – Temperature range for exceptional temperatures, tested successfully, with limited margins.

An extreme temperature alarm (32002) is raised if the unit's internal temperature goes above 90°C or below -40°C. The alarm is cleared when the temperature goes above 87°C or below -37°C.

To display the current unit temperature, see Configuring Unit Parameters.

The permissible IDU humidity range is 5%RH to 100%RH

27.2.1 Troubleshooting Tips

For XPIC links, if one of the polarizations has significantly reduced performance, check to make sure the antenna's rectangular interface was replaced with a circular adaptor.

For XPIC links, the RSL should be similar for both polarizations. The XPI value should be similar for both polarizations; the difference should not be more than 2 dB.

If during or right after a software upgrade the message *Your session has expired, please login again* appears and you cannot log in, it is recommended to refresh the Web EMS page (F5) after completion of the upgrade. If pressing F5 does not help, clear the browser's cache by pressing Ctrl+Shift+Delete.

27.3 PTP 850C Interface Pin-outs and LEDS

PTP 850C Interfaces

For traffic, the PTP 850C has an RJ-45 interface and two optical SFP/SFP+ cages. The PTP 850C also has an SFP cage for Dualband configurations.[18]

The PTP 850C also has an RJ-45 management port.

For power, the PTP 850C has a DC power interface (-48V) (P1). The PTP 850C can also be powered via PoE using the RJ-45 traffic port.

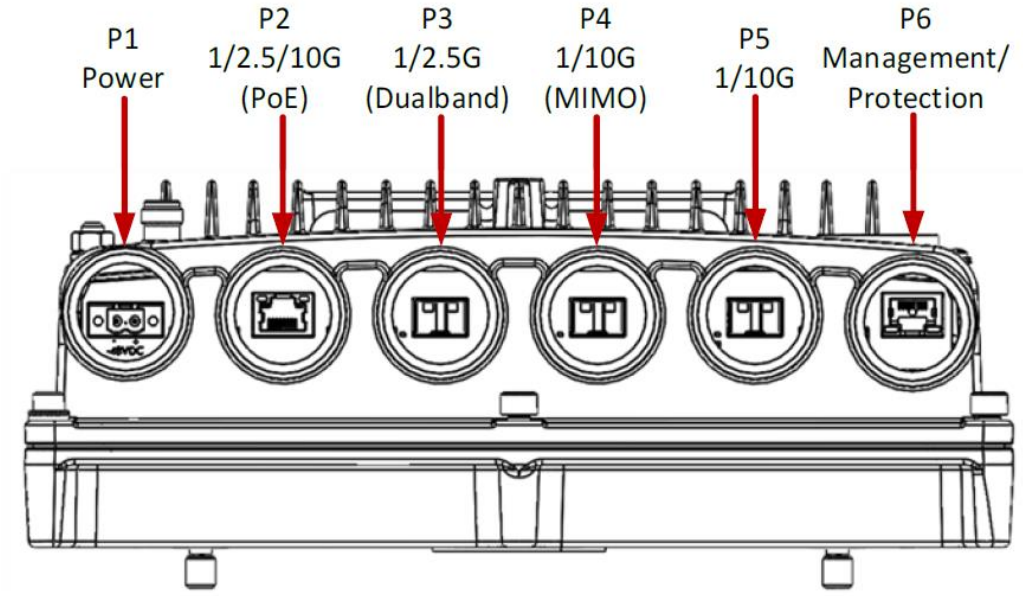


Figure 452: PTP 850C Interfaces

- Port 1 – Power Interface (-48V)
- Port 2 (Eth 1):

 RJ-45: 1000BASE-T, 2.5GBASE-T, 10GBASE-T

  PoE

- Port 3 (Eth 2):

 SFP cage which supports SFP standard Electric: 1000BASE-T, 2.5GBASE-T Optical: 1000BASE-X, 2.5GBASE-X

 Optical: 1/2.5GE Dualband

> Dualband is planned for future release.
>
> In System release 11.3, only 2.5G is supported for traffic.

[18] Dualband is planned for future release.

- Port 4 (Eth 3):
  - SFP cage which supports SFP+ standard
  - Electric: 1000BASE-T, 10GBASE-T
  - Optical: 1000BASE-X, 10GBASE-X
  - Optical: Cambium Networks proprietary MIMO interface, if this port serves as an extension port for data sharing. By default, the port is a traffic port unless a MIMO group has been created
- Port 5 (Eth 4):
  - SFP cage which supports SFP+ standard
  - Electric: 1000BASE-T, 10GBASE-T
  - Optical: 1000BASE-X, 10GBASE-X

Note: In System relase 11.3, only 10G is supported.

- Port 6:

- RJ-45: 100BASE-T
- Management and Protection port (no traffic)

- 2 RF Interfaces: Standard interface per frequency band
- RSL interface: BNC connector
- Source sharing: TNC connector
- Grounding screw

PTP 850C Interface Pin-outs

P2 (Eth 1) – PoE GbE Electrical Interface (RJ-45)

Table 295: PTP 850C P2 PoE Electric Interface - RJ-45/ Pinouts

Pin no.	Description
1	BI_DA+ (Bi-directional pair +A)
2	BI_DA- (Bi-directional pair -A)
3	BI_DB+ (Bi-directional pair +B)
4	BI_DC+ (Bi-directional pair +C)
5	BI_DC- (Bi-directional pair -C)
6	BI_DB- (Bi-directional pair -B)

7	BI_DD+ (Bi-directional pair +D)
8	BI_DD- (Bi-directional pair -D)

23.3.2.1 P3 (Eth 2) GbE Optical Interface (SFP)

P3 is an SFP cage that supports the SFP standard. This port is used exclusively for Dualband configurations.

P4 (Eth 3) 10G Optical Interface (SFP+)

P4 is an SFP cage that supports the SFP and SFP+ standards.

P5 (Eth 4) 10G Optical Interface (SFP+)

P5 is an SFP cage that supports the SFP and SFP+ standards.

P6 –Management Electrical Interface (RJ-45)

Table 296: PTP 850C MGT Interface - RJ-45/ Pinouts

Pin no.	Description
1	BI_DA+ (Bi-directional pair +A)
2	BI_DA- (Bi-directional pair -A)
3	BI_DB+ (Bi-directional pair +B)
4	BI_DC+ (Bi-directional pair +C)
5	BI_DC- (Bi-directional pair -C)
6	BI_DB- (Bi-directional pair -B)
7	BI_DD+ (Bi-directional pair +D)
8	BI_DD- (Bi-directional pair -D)

Table 297: GbE Port Pin-Outs

RSL Interface

PTP 850E uses a two-pin connection to measure the RSL level using standard voltmeter test leads:

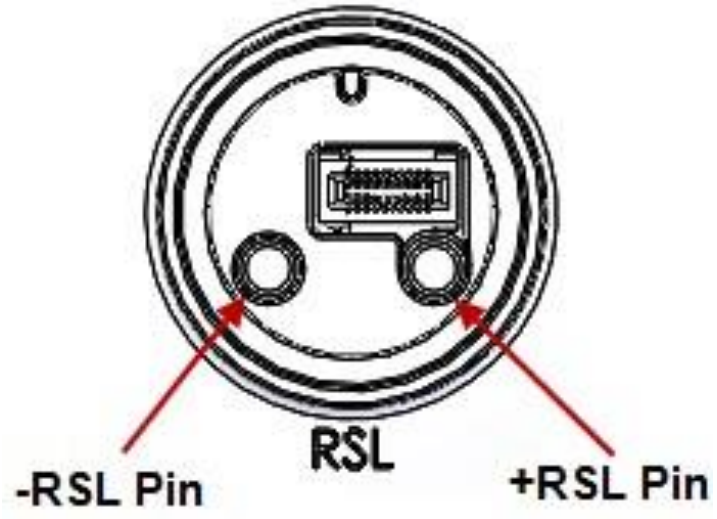


Figure 453: RSL sPins

PTP 850C LEDs

PTP 850C provides the following LEDs to indicate the status of the unit's interfaces, and the unit as a whole:

- P2 (Eth 1) – PoE GbE Electrical Interface (RJ-45) LEDs
- P3 (Eth 2) GbE Optical Interface (SFP) LEDs
- P4 (Eth 3) 10G Optical Interface (SFP+)
- P5 (Eth 4) 10G Optical Interface (SFP+)
- Status LED

P2 (Eth 1) – PoE GbE Electrical Interface (RJ-45) LEDs

Eth 1 is an RJ-45 traffic and PoE interface with two green LEDs, one on either side of the interface. Both LEDs indicate the interface's Admin and cable connection status:

> Only the right LED shows Blinking Green to indicate when there is
>
> traffic on the interface

The left LED indicates the link status In the current release, this LED is Green when Admin is Enabled.

The right LED indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

- **Off** – Admin is Disabled *or* no cable is connected to the interface.
- **Green** – Admin is Enabled and a cable is connected to the interface.
- **Blinking Green** – Admin is Enabled and a cable is connected to the interface,

and there is traffic on the interface.

P3 (Eth 2) GbE Optical Interface (SFP) LEDs

P3 is an SFP cage that supports the SFP standard. This port is used exclusively for Dualband configurations.

> **Note:** Dualband is planned for future release.

There is one Green LED to the left of the interface. The LED indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

- **Off** – Admin is Disabled *or* no cable is connected to the interface.
- **Green** – Admin is Enabled and a cable is connected to the interface.
- **Blinking Green** – Admin is Enabled and a cable is connected to the interface,

and there is traffic on the interface.

> The LED does not indicate traffic on the interface (Blinking Green) in
>
> 2.5G mode

P4 (Eth 3) 10G Optical Interface (SFP+)

P4 is an SFP cage that supports the SFP and SFP+ standards.

There is one Green LED to the left of the interface. The LED indicates the interface's Admin and cable connection status:

- **Off** – Admin is Disabled *or* no cable is connected to the interface.
- **Green** – Admin is Enabled and a cable is connected to the interface.

P5 (Eth 4) 10G Optical Interface (SFP+)

P5 is an SFP cage that supports the SFP and SFP+ standards.

There is one Green LED to the left of the interface. The LED indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

- **Off** – Admin is Disabled *or* no cable is connected to the interface.
- **Green** – Admin is Enabled and a cable is connected to the interface.
- **Blinking Green** – Admin is Enabled and a cable is connected to the interface,

and there is traffic on the interface.

Management/Protection GbE Electrical Interface (RJ-45) LEDs

P6 is an RJ-45 management interface. There are two LEDs next to the MGT interface, a Green LED to the left of the interface and an Orange LED to the right of the interface.

The Green LED indicates the interface's status as a management port:

- **Off** – Admin is Disabled.
    - **Green** – Admin is Enabled.
- **Blinking Green** – Admin is Enabled and management traffic is passing through the interface (TX, RX, or both).

If the port is being used for protection, the Orange LED indicates the status of the mate unit:

- **Off** – The interface is not operational (Down).
- **Green** – The interface is operational (Up).
- **Blinking Green** – The interface is operational, *and* there is traffic on the interface (TX, RX, or both).

> **Note:** Unit protection is planned for future release.

Status LED

The Status LED is located on the front of the PTP 850C unit, above the RSL interface. It indicates the overall status of the unit:

- **Off** – The power is off.
- **Red** – The unit is in init stage.
    - **Blinking Red** – The unit has a Major or Critical alarm.
- **Green** – The unit is Up, all enabled radios are Up, and there are no Major or Critical alarms. In unit protection configurations, Green indicates that the unit is the Active unit.

- **Blinking Green** – The unit is Up, all enabled radios are Up, and there are no Major or Critical alarms. In unit protection configurations, Blinking Green indicates that the unit is the Standby unit.

> **Note:** Unit protection for PTP 850C is planned for future release.

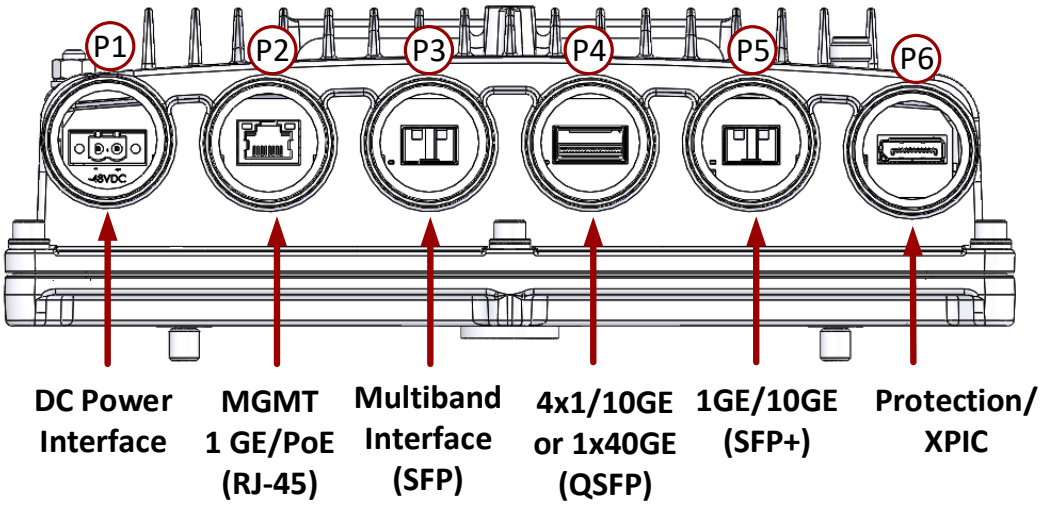
27.4 PTP 850E Connector Pin-outs

The PTP 850E has an optical SFP cage, an optical SFP/SFP+ cage, and a QSFP cage for traffic and one RJ-45 port for management and PoE.

For power, the PTP 850E has a DC power interface (-48V) (P1). Optionally, when used in all-outdoor configurations, the PTP 850E can also receive PoE power from a Cambium-approved PoE injector via P2, an RJ-45 port that is also used for management.

Power redundancy can be achieved by using both a DC power input and a passive PoE injector simultaneously. The PTP 850E monitors both power feeds and uses the best power source at any given moment.

Figure 552 PTP 850E Interfaces



Port 1 – Power Interface (-48V)

Port 2 (MNG 1/Eth 1):

Electric: 10/100/1000Base-T RJ-45

Management port (no traffic)

PoE

Port 3 (Eth 2):

SFP cage which supports SFP standard

1/2.5GE MultiBand port (user-configurable)

Port 4 (Eth 3, Eth 4, Eth 5, Eth 6):

QSFP cage which supports QSFP standard

4x1G/10G or 1x40GE Eth traffic (user configurable)

Option for SFP+ (1x10GE) with adaptor

Port 5 (Eth 7):

SFP cage which supports SFP+ standard

10GE Eth traffic

Port 6:

External Connection – Reserved for future use.

Antenna Port – Cambium proprietary flange (flange compliant with UG385/U)

RSL interface – DVM interface to enable voltage measurement for RSL indication. The RSL measurement is performed using standard DVM testing probes. To access the RSL interface, the user must remove the port's cover and insert the DVM plugs into the sockets, according to the polarization markings.

Grounding screw

27.4.1 P2 (Eth 1) – MGT/PoE GbE Electrical Interface (RJ-45)

Table 257: PTP 850E MGT Interface - RJ-45/ Pinouts

Pin no.	Description
1	BI_DA+ (Bi-directional pair +A)
2	BI_DA- (Bi-directional pair -A)
3	BI_DB+ (Bi-directional pair +B)
4	BI_DC+ (Bi-directional pair +C)
5	BI_DC- (Bi-directional pair -C)
6	BI_DB- (Bi-directional pair -B)
7	BI_DD+ (Bi-directional pair +D)
8	BI_DD- (Bi-directional pair -D)

27.4.2 P3 (Eth 2) GbE Optical Interface (SFP)

P3 is an SFP cage that supports the SFP standard. This port is used exclusively for Multiband configurations.

27.4.3 P4 (Eth 3, Eth 4, Eth 5, Eth 6) 40 GbE Optical Interface (QSFP)

P4 (QSFP) is a QSFP cage which supports the QSFP standard. With a QSFP to SFP adaptor, it also supports the SFP and SFP+ standards.

In release 11.1, Port 4 supports 4x1/10Gbps configurations. With a QSFP-to-SFP adaptor, Port 4 also supports 1x1/10Gbps configurations.

27.4.4 P5 (Eth 7) 10G Optical Interface (SFP+)

Eth1 is an SFP cage that supports the SFP+ standard. Eth 7 is supported for 10G Ethernet traffic only.

27.4.5 Protection/XPIC Port

This port is reserved for future use.

27.4.6 RSL Interface

PTP 850E uses a two-pin connection to measure the RSL level using standard voltmeter test leads:

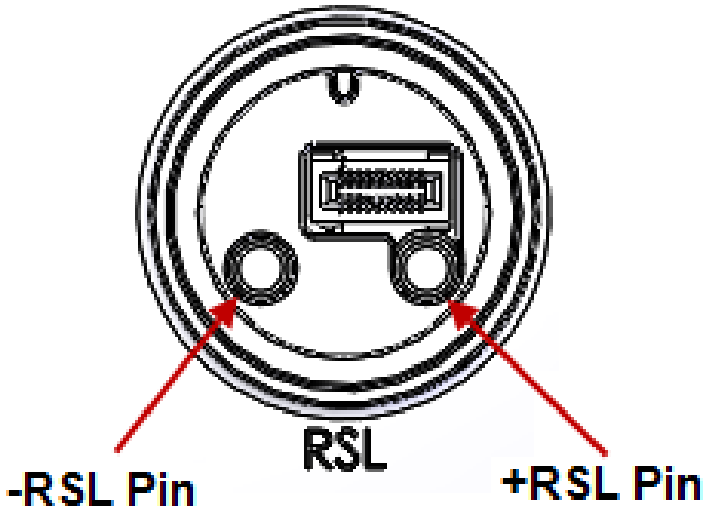


Figure 553: RSL Pins

27.5 PTP 850E LEDs

The PTP 850E provides the following LEDs to indicate the status of the unit's interfaces, and the unit as a whole:

- P2 MGT/PoE GbE Electrical Interface (RJ-45) LEDs
- P4/Eth3-6 40G Optical Interface (QSFP) LED
- P5/Eth7 1/10G Optical Interface (SFP+) LEDs
- Status LED
- Protection LED

27.5.1 P2 MGT/PoE GbE Electrical Interface (RJ-45) LEDs

There are two LEDs next to the MGT interface, a Green LED to the left of the interface and an Orange LED to the right of the interface.

The Orange LED indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

Off - Admin is Disabled *or* no cable is connected to the interface.

Green - Admin is Enabled and a cable is connected to the interface.

Blinking Green - Admin is Enabled and a cable is connected to the interface, *and* there is traffic on the interface.

The Green LED is not functional in this release.

27.5.2 P4/Eth3-6 40G Optical Interface (QSFP) LEDs

P4 (QSFP) is a QSFP cage which supports the QSFP standard. With a QSFP-to-SFP adaptor, it also supports the SFP and SFP+ standards.

In System release 11.1, Port 4 supports 4x1/10Gbps configurations. These are configured as Eth 3, Eth4, Eth5, and Eth6. With a QSFP-to-SFP adaptor, it also supports 1x1/10Gbps configurations (Eth3).

There is one Green LED to the left of the interface. This LED indicates the status of the interface:

- **Off** – Admin is Disabled for all of the interfaces connected to P4 (Eth3, Eth4, Eth5, and Eth6), or no cable is connected to the interface.
- **Green** – Admin is Enabled for at least one of the interfaces connected to P4 and a cable is connected to the interface.

27.5.3 P5/Eth7 1/10G Optical Interface (SFP+) LEDs

Eth1 is an SFP cage that supports regular SFP and SFP+.

There is one Green LED to the left of the interface. The LED is for Eth7 and indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

Off - Admin is Disabled *or* no cable is connected to the interface.

Green - Admin is Enabled and a cable is connected to the interface.

Blinking Green - Admin is Enabled and a cable is connected to the interface, *and* there is traffic on the interface.



Note

The LED does not indicate traffic on the interface (Blinking Green) in 10G mode.

27.5.4 Status LED

The Status LED indicates the status of the main board:

Off – The power is off.

Red – The unit is initializing.

Red Blinking - The power is on, and one or more major or critical alarms are raised.

Green - The power is on, the unit is up, the radio is up, and no major or critical alarms are raised.

27.5.5 Protection LED

Reserved for future use.

27.5.6 PTP 850S Interface Pin-outs

Port 1 – MGT/PoE GbE Electrical Interface (RJ-45)

Table 299: PTP 850S MGT Interface - RJ-45/ Pinouts

Pin no.	Description
1	BI_DA+ (Bi-directional pair +A)
2	BI_DA- (Bi-directional pair -A)
3	BI_DB+ (Bi-directional pair +B)
4	BI_DC+ (Bi-directional pair +C)
5	BI_DC- (Bi-directional pair -C)
6	BI_DB- (Bi-directional pair -B)
7	BI_DD+ (Bi-directional pair +D)
8	BI_DD- (Bi-directional pair -D)

Port 2 – Eth2/Eth3 GbE Optical Interface (SFP/CSFP)

Eth2/Eth3 is an SFP cage that supports regular and CSFP standards.

Port 3 – Eth1 10G Optical Interface (SFP+)

Eth1 is an SFP cage that supports the SFP+ standard. Eth1 can be configured by the user for 1G or 10G Ethernet traffic.

EXT – Extension Port

This port is reserved for future use.

Power Adaptor

For configurations in which power is not provided via PoE, a special adaptor (PTP 820_Mini_Power_Adaptor) is available that enables users to connect a two-wire power connector to the PoE port. This adaptor is located inside of the gland. In such configurations, only one electrical GbE interface is available (MGT).

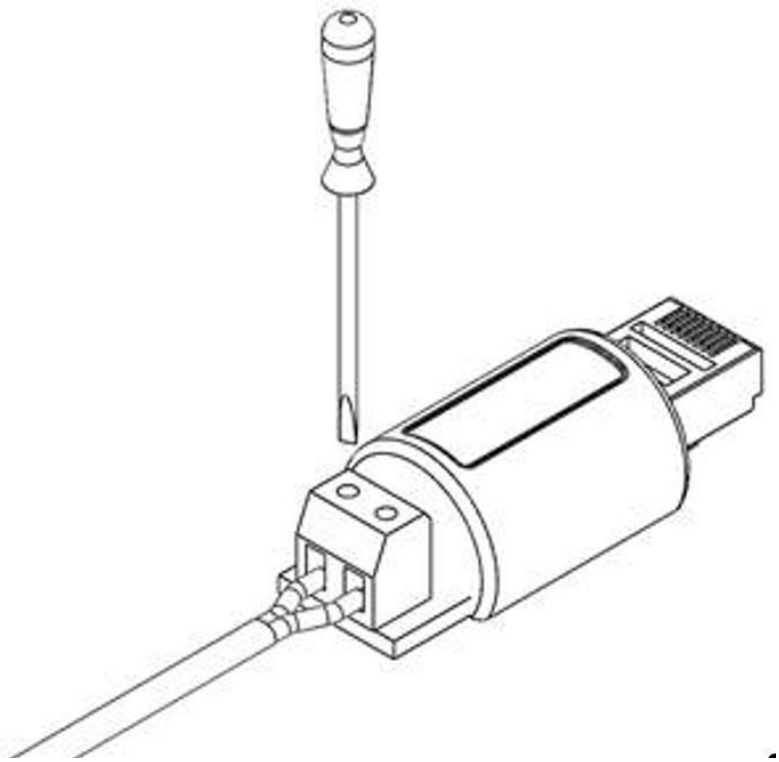


Figure 459: Two-Wire to PoE Port Power Adaptor

RSL Interface

PTP 850S uses a two-pin connection to measure the RSL level using standard voltmeter test leads:

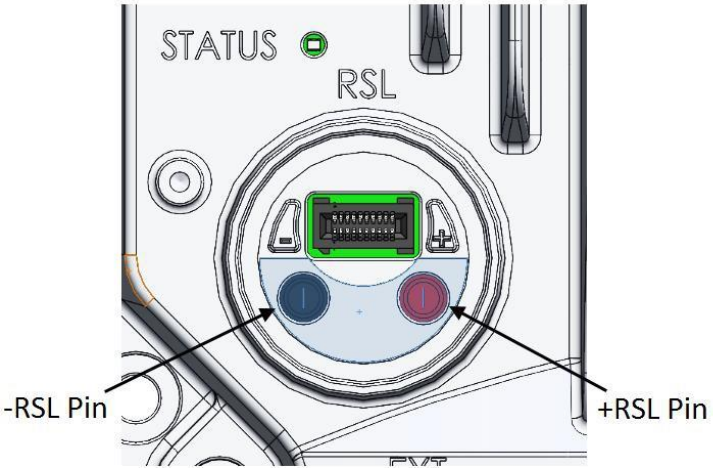


Figure 460: RSL Pins

PTP 850S LEDs

PTP 850S provides the following LEDs to indicate the status of the unit's interfaces, and the unit as a whole:

- Eth1 10G Optical Interface (SFP+) LEDs
- Eth2/Eth3 GbE Optical Interface (SFP/CSFP) LEDs
- MGT GbE Electrical Interface (RJ-45) LEDs
- Radio LED
- Status LED

Eth1 10G Optical Interface (SFP+) LEDs

Eth1 is an SFP cage that supports regular SFP and SFP+.

There is one Green LED to the left of the interface. The LED is for Eth1 and indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

- **Off** - Admin is Disabled *or* no cable is connected to the interface.
- **Green** - Admin is Enabled and a cable is connected to the interface.
- **Blinking Green** - Admin is Enabled and a cable is connected to the interface,

and there is traffic on the interface.

> The LED does not indicate traffic on the interface (Blinking Green) in
>
> 10G mode

Eth2/Eth3 GbE Optical Interface (SFP/CSFP) LEDs

Eth2/Eth3 is an SFP cage that supports regular and CSFP standards.

- When Eth2/Eth3 is used with a regular SFP, it provides Ethernet port 2.
- When Eth2/Eth3 is used with CSFP, it provides two Ethernet ports: Ethernet port 2 and Ethernet port 3.

> The Web EMS displays Ethernet port 3 even if a regular SFP is used,
>
> and there is no Ethernet port 3. You must avoid configuring Ethernet port 3 in this case.

There are two LEDS to the left of the interface. The LED to the left or the upper LED is for Eth2. When CSFP is used, the LED to the right or the lower LED is for Eth3; otherwise, it is inactive.

Each LED indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

- **Off** - Admin is Disabled *or* no cable is connected to the interface.
- **Green** - Admin is Enabled and a cable is connected to the interface.
- **Blinking Green** - Admin is Enabled and a cable is connected to the interface,

and there is traffic on the interface.

MGT GbE Electrical Interface (RJ-45) LEDs

There are two LEDs next to the MGT interface, a Green LED to the left of the interface and an Orange LED to the right of the interface.

The Orange LED indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

- **Off** - Admin is Disabled *or* no cable is connected to the interface.
- **Green** - Admin is Enabled and a cable is connected to the interface.
- **Blinking Green** - Admin is Enabled and a cable is connected to the interface,

and there is traffic on the interface.

The Green LED is not functional in this release.

Radio LED

The Radio LED indicates the status of the radio link:

- **Off** – The radio is off; the carrier is Admin = Disabled in the Interface Manager.
- **Green** - The power is on, and the carrier is operational (up).
- **Orange** – A signal degrade condition exists on the carrier.
- **Red** - A loss of frame (LOF) or excessive BER condition exists on the carrier.

Status LED

The Status LED indicates the status of the main board:

- **Off** – The power is off.
- **Green** - The power is on, and no alarms are raised on the motherboard.
- **Orange** - The power is on, and one or more minor alarms or warnings are raised on the motherboard.
- **Red** - The power is on, and one or more major or critical alarms are raised on the motherboard.

Protection LED

Reserved for future use.

27.6 PoE Injector Pin-outs and LEDs – Standard PoE

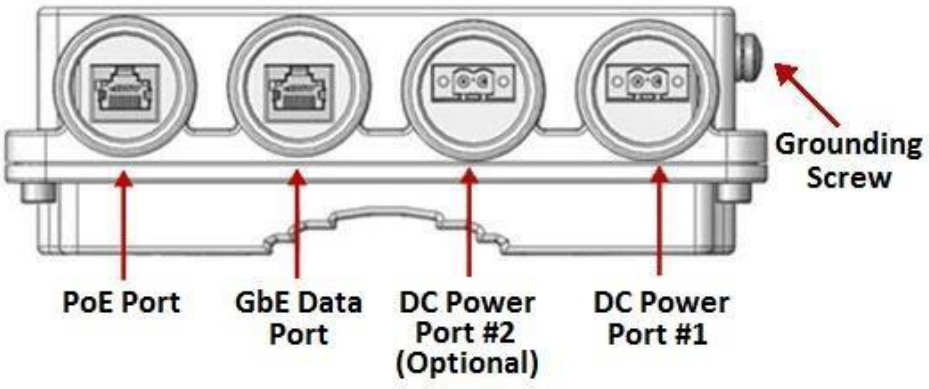


Figure 461: PoE Injector Connectors

27.7 PoE Injector Pin-outs and LEDs – Standard PoE

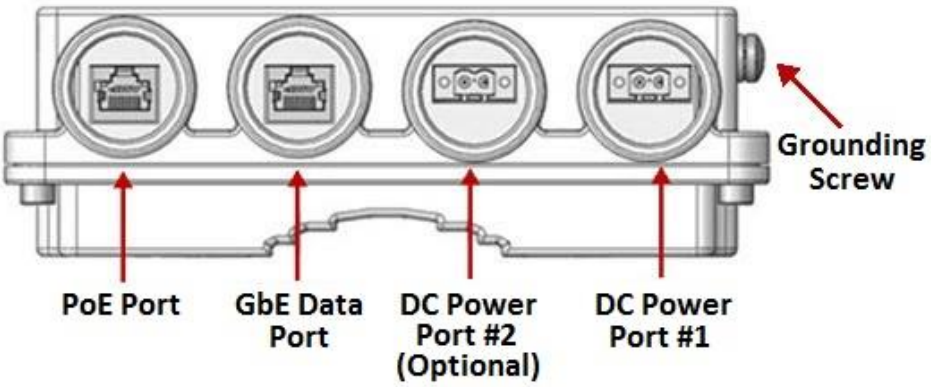


Figure 554: PoE Injector Connectors

27.7.1 PoE Injector Pin-outs and LEDs – Standard PoE

This section applies to the standard PoE Injector units with the following marketing models:

PoE_Inj_AO_2DC_24V_48V

PoE_Inj_AO

PoE Port

Table 258: PoE Injector PoE Port - RJ-45 Pinouts

Pin no.	Description
1	BI_DA+ (Bi-directional pair +A)
2	BI_DA- (Bi-directional pair -A)
3	BI_DB+ (Bi-directional pair +B)

Pin no.	Description
4	BI_DC+ (Bi-directional pair +C)
5	BI_DC- (Bi-directional pair -C)
6	BI_DB- (Bi-directional pair -B)
7	BI_DD+ (Bi-directional pair +D)
8	BI_DD- (Bi-directional pair -D)

Data Port

Table 259: PoE Injector RJ-45 Data Port Supporting 10/100/1000Base-T

Pin no.	Description
1	BI_DA+ (Bi-directional pair +A)
2	BI_DA- (Bi-directional pair -A)
3	BI_DB+ (Bi-directional pair +B)
4	BI_DC+ (Bi-directional pair +C)
5	BI_DC- (Bi-directional pair -C)
6	BI_DB- (Bi-directional pair -B)
7	BI_DD+ (Bi-directional pair +D)
8	BI_DD- (Bi-directional pair -D)

DC

One or two DC ports, depending on the PoE Injector model:

Two models of the PoE Injector are available:

PoE_Inj_AO_2DC_24V_48V – Includes two DC power ports with power input ranges of ±(18-60)V each.

PoE_Inj_AO – Includes one DC power port (DC Power Port #1), with a power input range of ±(40-60)V.

These ports are UL-60950 compliant, with a 2-pin connector.

27.7.2 PoE Injector LEDs – Standard PoE

PWR1 (Bi-color LED)

Green – Power available on PWR1 DC input

Off – No power is available on PWR1 DC input.

PWR2 (Bi-color LED)

Green – Power available on PWR2 DC input,

Off – No power is available on PWR2 DC input.

PoE (Tri -color LED)

Orange – No load is detected

Green – Providing in-line power

Blinking Red – Invalid/over-load

Off – no power to the injector unit.

Radio LED

The Radio LED indicates the status of the radio link:

Off – The radio is off.

Green - The power is on, and all carriers are operational (up).

Orange - A signal degrade condition exists in at least one carrier.

Red - A loss of frame (LOF) or excessive BER condition exists in at least one carrier.

27.8 PoE Injector Pin-outs and LEDs – Passive PoE

This section applies the passive PoE used with power redundancy. The marketing model of this PoE is: *AC_POE_STD_PWR_INDOOR*

27.8.1 PoE Injector Pin-outs and LEDs – Passive PoE

RJ-45 output pinout: 3,4,5,6 (+) and 1,2,7,8 (-)

AC Input Specifications

AC Input Voltage Rating:	100VAC to 240VAC
AC Input Voltage Range:	90VAC to 264VAC
AC Input Current:	2.5A (rms) Max 90 VAC at Full Load 1.2A (rms) Max 240VAC at Full Load
AC Input Frequency:	47Hz to 63Hz
ACInput Inrush Current:	50A Max @115VAC at Full Load 75A Max @230VAC at Full Load

DC Output Specifications

DC Output Voltage:	+57-54VDC (+56V Nominal)
Output Power:	90W Maximum

27.8.2 PoE Injector LEDs – Passive PoE

Blue Solid: Power Good/Power Out

28. Alarms List

The following table lists all alarms used in the PTP 850 products.

Table 302: Alarms

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
10	radio-digital-loopback	Alarm	Equipment	Framer digital loopback	Warning	User enabled framer digital loopback.	Disable framer digital loopback.
11	ntp-local	Alarm	Communications	NTP locked on local clock	Warning	The configured and enabled NTP servers are all unreachable or providing insufficient quality.	Configure or enable another NTP server, one that is reachable with sufficient quality.
15	ntp-locked	Event	Communications	NTP locked on server	Indeterminate		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
28	main-board-warm-reset	Event		Unit warm reset.	Indeterminate		
29	main-board-cold-reset	Event		Unit reset.	Warning		
30	main-board-poe-low-voltage-alarm	Alarm		POE input voltage is too low	Warning		
31		Event		Change Remote request was sent	Major		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
32		Event		Protection switchover due to remote request	Major		
33	protection-mimo-misconfiguration-alarm	Alarm			Major	Unit Redundancy and MIMO 4x4 cannot operate simultaneously.	
100	lag-degraded	Alarm	Equipment	LAG is not fully functional - LAG Degraded.	Major		
101	lag-down	Alarm	Equipment	LAG operational state is down	Critical		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
102	ethernet-loopback-active-alarm	Alarm	Equipment	Loopback is active	Major	Ethernet loopback is active.	Wait till loopback timeout expires or disable loopback.
103	port-mirroring-is-active	Alarm	Equipment	Slot X port XX is mirrored to slot Y port YY	Minor	Mirroring is enabled by user configuration.	Disable mirroring.
120	port-speed-mismatch-alarm	Alarm	Equipment	Port speed mismatch	Major	System reset is required after the port speed was changed.	Change the port speed to its previous value, OR Reset the system.
150	auto-state-propagation-interface-down-alarm	Alarm	Communications	Auto-state-propagation is triggered	Major	Failure of the radio interface which is monitored for automatic state propagation causes automatic shutdown of the controlled interface.	Check adjacent radio interface for failure conditions that caused automatic state propagation.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
200	protection-communication-down-alarm	Alarm	Equipment	Protection communication is down	Major	Mate unit is absent/failure. Protection cable is disconnected. Unit failure.	Check existence of mate unit. Check protection cable connection between units.Reset mate unit. Replace mate unit.
201	protection-lockout-alarm	Alarm	Equipment	Protection in Lockout State	Major		
202	protection-switch-command	Event	Equipment	Protection switchover due to local failure	Major		
203	protection-mate-not-present-alarm	Alarm	Equipment	Mate does not exist	Major	Mate does not exist or cable unplugged.	

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
204	protection-hsb-insufficient-alarm	Alarm	Equipment	HSB insufficient configuration	Critical	External Protection configured both with HSB.	Remove External Protection and HSB configuration.
205	protection-revertive-primary-insufficient-alarm	Alarm	Equipment	Protection revertive mode - insufficient configuration	warning	Identical configuration for the revertive-primary parameter.	Ensure one (and only one) unit is configured as the primary unit.
307	tdm-link-up	Event	Equipment	TDM interface is up	Warning		
308	tdm-link-down	Event	Equipment	TDM interface is down	Warning		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
401	TrafficPhyLocAlarm	Alarm	Equipment	Loss of Carrier	Major	Cable disconnected. Defective cable.	Check connection of cable Replace cable.
407	ethernet-link-up	Event	Equipment	Ethernet interface is up	Warning		
408	ethernet-link-down	Event	Equipment	Ethernet interface is down	Warning		
601	radio-excessive-ber	Alarm	Communications	Radio excessive BER	Major	Fade in the link. Defective IF cable. Fault in RFU. Fault in RMC (Radio Modem Card).	Check link performance. Check IF cable and replace if required. Replace RFU. Replace RMC (Radio Modem Card).

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
602	remote-link-id-mismatch	Alarm	Equipment	Link ID mismatch	Major	Link ID is not the same at both sides of link	Configure same Link ID for both sides of link
603	radio-lof	Alarm	Communications	Radio loss of frame	Critical	Fade in the link. Defective IF cable. Fault in RFU. Fault in RMC (Radio Modem Card). Different radio scripts at both ends of the link.	Check link performance. Check IF cable and replace if required. Replace RFU. Replace RMC (Radio Modem Card). Make sure same script is loaded at both ends of the link.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
604	radio-signal-degrade	Alarm	Communications	Radio signal degrade	Minor	Fade in the link. Defective IF cable. Fault in RFU. Fault in RMC (Radio Modem Card).	Check link performance. Check IF cable and replace if required. Replace RFU. Replace RMC (Radio Modem Card).
605	radio-link-up	Event	Equipment	Radio interface is up	Warning		
606	radio-link-down	Event	Equipment	Radio interface is down	Warning		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
607	rfu-frequency-scanner-in-process	Alarm	Equipment	Frequency scanner in progress	Warning	The frequency scanner activated.	Stop the frequency scanner process.
801	corrupted-file-card-failure	Alarm	Equipment	Corrupted inventory file	Major	The inventory file is corrupted	Reset the card. Reset the system. Replace the card.
802	file-not-found	Alarm	Equipment	Inventory file not found	Warning	The inventory file is missing	Reset the system. Reinstall the software.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
803	sfp-rx-power-level-low	Alarm	Equipment	SFP port RX power level is below the rx power level low threshold	Warning	Remote SFP port Tx laser power is too low. Fiber length is too long or fiber type doesn't fit the installed SFP.	Verify remote SFP Tx laser power is within range. Check fiber type and length fit the installed SFP. If not, replace it with an appropriate one.
804	sfp-rx-power-level-high	Alarm	Equipment	SFP port RX power level is above the rx power level high threshold	Warning	Remote SFP Tx power is too high.	Add attenuator on Rx side.
805	sfp-tx-power-level-low	Alarm	Equipment	SFP port TX power level is below the tx power level low threshold	Warning	SFP transmit laser power is too low	Check laser Bias current. If it is too low, replace SFP.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
806	sfp-tx-power-level-high	Alarm	Equipment	SFP port TX power level is above the tx power level high threshold	Warning	SFP laser Tx power is too high.	Check laser Bias current and laser temperature values. If either of them is too high, replace SFP.
807	recovered-inventory-on-boot-event	Event	Equipment	Default Activation Key activated due to failure	Critical	Corrupted Inventory	
808	recovered-inventory-on-running-event	Event	Equipment	Activation Key Configuration failed	Critical	Corrupted Inventory	
901	demo-license-alarm	Alarm	Equipment	Demo mode is active	Warning	Demo mode has been activated by the user	Disable demo mode

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
902	license-demo-expired	Event	Equipment	Demo mode is expired	Warning		
903	license-demo-start-by-user	Event	Processing	Demo mode is started	Warning		
904	license-demo-stop-by-user	Event	Processing	Demo mode is stopped	Warning		
905	license-load-fail	Event	Equipment	Activation key loading failure	Major		
906	license-load-successful	Event	Equipment	Activation key loaded successfully	Warning		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
907	license-violation-alarm	Alarm	Equipment	Activation key violation	Critical	The current configuration does not match the activation-key-enabled feature set. 48 hours after an "activation-key-violation" alarm is raised, sanction mode is activated in which all alarms except the activation key violation alarm are cleared and no new alarms are raised.	Get the list of features' configurations that are violated via the "activation key information report". Install a new activation key that allows the use of all required features.
908	demo-license-about-to-expire-alarm	Alarm	Equipment	Demo mode is about to expire	Major	Demo mode allowed period is about to end within 10 days	Disable demo mode and install a new valid activation key.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
910	license-signature-failed-alarm	Alarm	Equipment	Activation key signature failure	Major	Activation key validation has failed due to invalid product serial number	Replace the IDU
911	license-violation-runtime-counter-expired	Event	Equipment	Activation key violation sanction is enforced	Major		
913	license-bad-xml-file-alarm	Alarm	Equipment	Activation key components are missing or corrupted	Major	Essential internal activation key components are missing or corrupted.	Reinstall software

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1002	radio-protection-configuration-mismatch	Alarm	Equipment	Radio protection configuration mismatch	Major	The configuration between the radio protection members is not aligned	Apply a copy-to-mate command to copy the configuration from the required radio to the other one
1006	radio-protection-switchover-event	Event	Equipment	Radio protection switchover - reason	Warning	Protection decision machine initiated switchover due to local failure or user command	Check the system for local failures
1007	radio-protection-no-mate	Alarm	Equipment	Radio protection no mate	Major	Radio protection function is missing radio module, module defected or disabled	Add radio module. Replace a defective existing radio module. Make sure all radio interfaces are enabled.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1008	radio-protection-remote-switch-request	Event	Equipment	Remote switchover request was sent - reason	Warning		
1009	radio-protection-lockout	Alarm	Equipment	Radio protection lockout command is on	Major	The user has issued a lockout command	Clear the lockout command
1010	ethernet-protection-switchover	Event	Equipment	Ethernet Interface Group protection switchover	Warning	LOC event on an Ethernet interface. Protection group member was disabled or pulled out of the shelf.	Check the system for local failures. Check external equipment.
1011	interface-protection-lockout	Alarm	Equipment	Interface protection lockout is on	Major	The user has issued a lockout command	Clear the lockout command

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1012	interface-protection-no-mate	Alarm	Equipment	Interface protection no mate: mate interface is missing or disabled	Major	Interface protection function is missing interface module, module defected or disabled.	Add interface module. Replace a defective existing interface module. Make sure all interface interfaces are enabled.
1102	software-installation-status	Event	Processing	Software installation status:	Warning		
1105	software-new-version-installed	Event	Processing	New version installed	Warning	A software version has been installed but system has not been reset.	

AlarmID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1111	software-user-confirmation-for-version	Event	Processing	User approved download of software version file	Warning		
1112	software-download-status	Event	Processing	Software download status:	Warning		
1113	software-download-missing-components	Event	Processing	Missing SW components:	Warning		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1114	software-management-incomplete-bundle	Event	Processing	Incomplete file set; missing components	Warning	Software bundle is missing components.	Get a complete software bundle
1150	backup-started	Event	Processing	Configuration file backup generation started	Warning	User command	
1151	backup-succeeded	Event	Processing	Configuration file backup created	Warning	Backup file creation finished successfully	
1152	backup-failure	Event	Processing	Failure in configuration file backup generation	Warning	System failed in attempt to create backup configuration file	

AlarmID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1153	restore-succeeded	Event	Processing	Configuration successfully restored from file backup	Warning	Configuration restore finished successfully	
1154	restore-failure	Event	Processing	Failure in configuration restoring from backup file	Warning	System failed in attempt to restore configuration from backup file	Configuration file system type mismatch Invalid or corrupted configuration file
1155	restore-canceled	Event	Processing	Configuration restore operation cancelled	Warning	Restore operation cancelled because of user command or execution of another configuration management operation	Try again
1156	file-transfer-issued	Event	Processing	User issued command for transfer of configuration file	Warning	User command	

AlarmID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1157	file-transfer-succeeded	Event	Processing	Configuration file transfer successful	Warning	Configuration file transfer successful	
1158	file-transfer-failure	Event	Processing	Configuration file transfer failure	Warning	Communications failure. File not found in server	Mark sure protocol details are properly configured. Make sure file exists.
1159	file-transfer-in-progress	Event	Processing	Configuration file transfer in progress	Warning	File transfer started	
1163	cli-script-activation-started	Event	Processing	CLI configuration script activation started	Warning	User command	

AlarmID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1164	cli-script-activation-succeeded	Event	Processing	CLI Configuration script executed successfully	Warning		
1165	cli-script-activation-failure	Event	Processing	CLI Configuration script failed	Warning	Syntax Error. Error returned by system during runtime	Verify script in the relevant line, and run again. Note that script may assume pre-existing configuration.
1166	unit-info-file-transfer-status-changed	Event	Processing	Unit info file transfer status:	Warning		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1167	unit-info-file-creation-status-changed	Event	Processing	Unit info file creation status:	Warning		
1169	restore-started	Event	Processing	Configuration restore operation started	Warning	Restore operation started because of user command	
1201	file-missed	Alarm	Equipment	Modem firmware file not found	Critical	Modem file is missing	Download software package. Reset the system.
1202	load-failed	Alarm	Equipment	Modem firmware was not loaded successfully	Critical	Modem firmware file is corrupted. System failure.	Download software package. Reset the system.

AlarmID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1203	modem-wd-reset	Event	Equipment	Modem watch-dog reset event	Warning		
1301	fpga-file-currupt-alarm	Alarm	Equipment	Radio MRMC script LUT file is corrupted	Critical	Damaged radio MRMC script LUT file	Download the specific radio MRMC script LUT file
1302	fpga-file-not-found-alarm	Alarm	Equipment	Radio MRMC script LUT file is not found	Critical	Missing radio MRMC script LUT file	Download the specific radio MRMC script LUT file
1304	modem-script-file-corrupt-alarm	Alarm	Equipment	Radio MRMC script modem file is corrupted	Critical	Damaged radio MRMC script modem file	Download the specific radio MRMC script modem file

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1305	modem-script-file-not-found-alarm	Alarm	Equipment	Radio MRMC script modem file is not found	Critical	Missing radio MRMC script modem file	Download the specific radio MRMC script modem file
1308	rfu-file-corrupt-alarm	Alarm	Equipment	Radio MRMC file is corrupted	Critical	Damaged Radio MRMC script LUT file	Download the specific radio MRMC RFU file
1309	rfu-file-not-found-alarm	Alarm	Equipment	Radio MRMC RFU file is not found	Major	Missing radio MRMC RFU file	Download the specific radio MRMC RFU file
1312	script-loading-failed	Alarm	Equipment	Radio errrror! MRMC script loading failed	Major	Damaged hardware module	Replace the radio hardware module

AlarmID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1313	mrmc-profile-below-thresh1	Alarm	Equipment	MRMC RX profile below threshold 1	Major		
1314	mrmc-profile-below-thresh2	Alarm	Equipment	MRMC RX profile below threshold 2	Critical		
1401	incompatible-rfu-tx-calibration	Alarm	Equipment	Incompatible RFU TX calibration	Major	RFU calibration tables require SW upgrade	Upgrade IDU SW
1501	remote-communication-failure	Alarm	Equipment	Remote communication failure	Critical	Fade in the link	Check the link performance

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1601	if-loopback	Alarm	Equipment	IF loopback	Warning	User enabled IF loopback	Disable IF loopback
1602	lock-detect	Alarm	Equipment	IF synthesizer is unlocked.	Critical	Extreme temperature condition. HW failure.	Check installation. Reset the RMC (Radio Modem Card) module. Replace the RMC (Radio Modem Card).

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1610	rsl-degradation-threshold-out-of-range	Alarm	Equipment	Radio Receive Signal Level is below the configured threshold	Warning	RSL is very low due to: Weather conditions, obstruction in antenna line of sight, antennae alignment. Configured threshold needs to be adjusted.2.	Check for obstruction in link path. Check the antennae alignment and link planning. Recalculate the Path Loss and set the threshold accordingly. Check link settings - Tx Power and Tx Frequency. Hardware problem.

AlarmID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1651	atpc-override	Alarm	Communications	ATPC overridden: Tx level has been equal to the Max Tx level for a longer time than allowed	Warning	Actual transmitted signal level has been at its maximum value for longer than allowed. This is probably caused by a configuration error or link planning error.	Correct the transmission levels. The alarm will be cleared only upon manual clearing.
1697	radio-unit-extreme-temperature	Alarm	Equipment	Radio unit extreme temperature	Warning	Installation conditions. Defective RFU.	Check installation conditions. Verify operation as per product's specs. Replace RFU.
1698	radio-unit-low-voltage	Alarm	Equipment	Radio unit input voltage is too low	Warning	Power supply output too low. Power cable to RFU.	Check Power supply. Replace cable.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1699	radio-unit-high-voltage	Alarm	Equipment	Radio unit input voltage is too high	Warning	Power Supply output too high.	Check power supply.
1700	fw-download-failure	Alarm	Communications	Radio unit not aligned to IDU	Critical	FW alignment interrupted, power disruption, ODU cable malfunction. Damaged ODU.	Reinitiate FW download by disable/enable the corresponding port. Replace RFU.
1701	cable-open	Alarm	Equipment	Cable open	Major	Cable is not connected to the IDU's radio interface or the RFU.	Check IF cable and connectors. Verify that the N-Type connector inner pin is not spliced. Replace RMC (Radio Modem Card). Replace RFU.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1702	cable-short	Alarm	Equipment	Cable short	Major	Physical short at the IF cable	Check IF cable and connectors. Verify that the N-Type connector inner pin is not spliced. Replace RMC (Radio Modem Card). Replace RFU.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1703	communication-failure	Alarm	Equipment	RFU communication failure	Warning	Defective IF cable. IF cable not connected properly. Defective RMC (Radio Modem Card). Defective RFU. RFU software download in progress.	Check IF cable and connectors. Verify that N-Type connector inner pin is not spliced. Replace RMC (Radio Modem Card). Replace RFU. For a high power RF Unit: Check BMA connector on OCB Check BMA connector on RFU.
1704	delay-calibration-failure-1	Alarm	Equipment	RFU delay calibration failure 1	Warning	Defective RFU	Reset the RMC (Radio Modem Card) / RFU. Replace RFU.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1705	delay-calibration-failure-2	Alarm	Equipment	RFU delay calibration failure 2	Warning	Calibration cannot be completed due to notch detection	Enter delay calibration value manually.
1706	extreme-temp-cond	Alarm	Equipment	RFU extreme temperature	Warning	Installation conditions. Defective RFU.	Check installation conditions. Verify operation as per product's specs. Replace RFU.
1707	radio-unit-abc-incompatible-rfu	Alarm	Equipment	RFU is incompatible with ABC configuration	Warning	The RFU type does not support the type of Multi-Carrier ABC the user has configured.	Replace the RFU with an RFU type that supports the configured Multi-Carrier ABC type.
1708	freq-set-automatically	Event	Equipment	RFU frequency was set automatically	Warning	Defective RFU	Check if problem repeats and if errors/alarms reported. Replace RFU.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1709	hardware-failure-1	Alarm	Equipment	RFU hardware failure 1	Critical	Defective RFU.	Replace RFU.
1710	hardware-failure-2	Alarm	Equipment	RFU hardware failure 2	Critical	Defective RFU.	Replace RFU.
1711	low-if-signal-to-rfu	Alarm	Equipment	Low IF signal to RFU	Major	IF cable connection. Defective RFU. Defective RMC (Radio Modem Card).	Check IF cable connectors. Verify that N-Type connector inner pin is not spliced. Replace RMC (Radio Modem Card) Replace RFU.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1712	no-signal-from-rfu	Alarm	Equipment	Low IF signal from RFU	Warning	Low RX IF signal (140 MHz) from RFU.	Check IF cable and connectors. Verify that N-Type connector inner pin is not spliced. Replace RMC (Radio Modem Card). Replace RFU.
1713	pa-extreme-temp-cond	Alarm	Equipment	RFU PA extreme temperature	Warning	Installation conditions. Defective RFU.	Check installation conditions. Replace RFU.
1714	power-failure-12v	Alarm	Equipment	RFU power failure (12v)	Major	Defective IF cable/connector. Defective RFU. Defective IDU.	Replace IF cable/connector. Replace RFU. Replace IDU.

AlarmID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
17115	power-failure-1point5	Alarm	Equipment	RFU power failure (1.5v)	Major	Defective IF cable/connector. Defective RFU. Defective IDU.	Replace IF cable/connector. Replace RFU. Replace IDU.
17116	power-failure-24v	Alarm	Equipment	RFU power failure (24v)	Major	Defective IF cable/connector. Defective RFU. Defective IDU.	Replace IF cable/connector. Replace RFU. Replace IDU.
17117	power-failure-6v	Alarm	Equipment	RFU power failure (6v pro)	Major	Defective IF cable/connector. Defective RFU. Defective IDU.	Replace IF cable/connector. Replace FU. Replace IDU.
17118	power-failure-6v-sw	Alarm	Equipment	RFU power failure (6v SW)	Major	Defective IF cable/connector. Defective RFU. Defective IDU.	Replace IF cable/connector. Replace RFU. Replace IDU.

AlarmID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
17119	power-failure-minus-5v	Alarm	Equipment	RFU power failure (-5v)	Major	Defective IF cable/connector. Defective RFU. Defective IDU.	Replace IF cable/connector. Replace RFU. Replace IDU.
17120	power-failure-vd	Alarm	Equipment	RFU power failure (Vd)	Major	Defective IF cable/connector. Defective RFU. Defective IDU.	Replace IF cable/connector. Replace RFU. Replace IDU.
17121	reset-occurred	Event	Equipment	RFU reset	Major		
17122	rfu-loopback-active	Alarm	Equipment	RFU loopback is active	Major	User has activated RFU loopback.	Disable RFU loopback.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1723	rfu-mode-changed-to-combined	Event	Equipment	RFU mode changed to Combined	Indeterminate		
1724	rfu-mode-changed-to-diversity	Event	Equipment	RFU mode changed to Diversity	Indeterminate		
1725	rfu-mode-changed-to-main	Event	Equipment	RFU mode changed to Main	Indeterminate		
1726	rfu-power-supply-failure	Alarm	Equipment	RFU power supply failure	Major	At least one of the RFU's power supply voltages is too low.	Replace RFU.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1727	rx-level-out-of-range	Alarm	Equipment	RFU RX level out of range	Warning	RSL is very low, link is down.	Check antenna alignment & link planning. Check link settings (TX power, TX frequency). Check antenna connections. Replace local/remote RFU.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1728	rx-level-path1-out-of-range	Alarm	Equipment	RFU RX level path1 out of range	Warning	Improper installation. Fading event. Defective RFU.	Check that the fault is not due to rain/multi-path fading or lack of LOS. Check link settings (TX power, TX frequency). Check antenna alignment. Check antenna connections. Replace local/remote RFU.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1729	rx-level-path2-out-of-range	Alarm	Equipment	RFU RX level path2 out of range	Warning	Improper installation. Fading event. Defective RFU.	Check that the fault is not due to rain/multi-path fading or lack of LOS. Check link settings (TX power, TX frequency). Check antenna alignment. Check antenna connections. Replace local/remote RFU.

AlarmID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1730	radio-unit-communication-failure	Alarm	Equipment	Radio unit communication failure	Critical	Defective RFU cable. RFU cable not connected properly. Defective RIC (Radio Interface Card). Defective RFU. RFU initialization in progress. RFU powered off.	Check RFU power supply. Check RFU cable and connectors. Replace RIC (Radio Interface Card). Replace RFU.
1731	power-supply-radio-unit-cable-open	Alarm	Equipment	Power supply cable open	Major	Power is enabled but consumption is lower than threshold.	Check ETH cable and connectors. Verify RFU is connected. If RFU connected with optical cable, disable power interface.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1732	power-supply-radio-unit-cable-short	Alarm	Equipment	Power supply cable short	Major	Power is enabled but consumption reached the threshold. Physical short at the ETH cable.	Check ETH cable and connectors. Replace RIC (Radio Interface Card) Replace RFU. If RFU connected with optical cable, disable power interface.
1733	synthesizer-unlocked	Alarm	Equipment	RFU synthesizer unlocked	Major	At least one of the RFU synthesizers is unlocked	Replace RFU. In XPIC mode, replace mate RFU as well.
1734	tx-level-out-of-range	Alarm	Equipment	RFU TX level out of range	Minor	Defective RFU (the RFU cannot transmit the requested TX power)	Replace RFU. Intermediate solution - reduce TX power.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1735	tx-mute	Alarm	Equipment	RFU TX Mute	Warning	RFU Transmitter muted by user	Unmute the RFU transmitter
1736	unknown-rfu-type	Alarm	Equipment	IDU SW does not support this type of RFU	Major	IDC SW does not support the RFU	Upgrade IDC SW
1737	card-extracted-from-slot	Event	Equipment	Card was extracted from slot	Warning	Card was extracted from slot	NA
1738	card-failure	Alarm	Equipment	Card is in Failure state	Major	Card is down as a result of card failure	Reset Card. Check if slot was disabled.
1739	card-fpga-fw-not-found	Alarm	Equipment	FPGA Firmware file not found	Critical	There is no FPGA file found on the Main Board for the card on the slot	NA

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1740	card-fw-load-fail	Alarm	Equipment	Download card firmware has failed	Major	Firmware download was unsuccessful.	Reset Card. Download software package. Try to insert another Card.
1741	card-inserted-to-slot	Event	Equipment	Card was inserted to slot	Warning	Card was inserted to slot	NA
1742	card-intermediate-channel-failure	Alarm	Equipment	Card is in interconnection failure state	Major	Card is down as a result of card interconnection failure	Reset Card. Check if the slot was disabled.
1743	card-missing	Alarm	Equipment	Expected Card is missing in slot	Major	Card is missing. Expected Card Type configured on empty slot.	Insert Expected Card. Clear Expected Card Type.

AlarmID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1744	card-not-supported-for-slot	Alarm	Equipment	This Card type is not supported in this slot	Major	The card is not on the Allowed Card Types list for this slot.	Reset. Insert Card belongs to Allowed Card Types list.
1745	card-state-is-down	Event	Equipment	Card operational state is Down	Indeterminate	Card state was change to Down state	NA
1746	card-state-is-up	Event	Equipment	Card operational state is Up	Indeterminate	Card state was change to Up state	NA
1747	card-state-is-up-with-alarms	Event	Equipment	Card operational state is Up with Alarms	Indeterminate	Card state was change to Up state but with Alarms indication	NA

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1748	card-unexpected	Alarm	Equipment	Unexpected Card Type in slot	Minor	Expected card type is different than the actual card type	Insert Expected Card. Change Expected Card Type.
1749	slot-disabled	Event	Equipment	Slot was Disabled	Indeterminate	The user Disabled slot	NA
1750	slot-enabled	Event	Equipment	Slot was Enabled	Indeterminate	The user Enabled slot	NA
1751	slot-reseted	Ent	Equipment	Card on slot was Reset	Indeterminate	The user Reset slot	NA
1752	fan-card-extraction-event	Event	Equipment	FAN Card was extracted from slot	Warning	FAN Card was extracted from slot	

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1753	fan-card-failure-event	Event	Equipment	FAN failure	Major		
1754	fan-card-insertion-event	Event	Equipment	FAN Card was inserted to slot	Warning	FAN Card was inserted to slot	
1755	fan-card-missing	Alarm	Equipment	FAN Card is missing in slot	Critical	FAN Card is missing. Slot enabled when empty.	Insert FAN Card. Disable slot.
1757	fan-failure	Alarm	Equipment	FAN Card is in Failure state	Major	FAN Card is in Failure state	Change FAN Card
1758	pdc-card-extraction-event	Event	Equipment	Power Supply was extracted from slot	Warning	Power Supply was extracted from slot	

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1759	pdc-card-insertion-event	Event	Equipment	Power Supply was inserted to slot	Warning	Power Supply was inserted to slot.	
1760	pdc-card-missing	Alarm	Equipment	Power Supply is missing inslot	Major	Power Supply is missing. Slot enabled when empty.	Insert Power Supply. Disable slot.
1761	pdc-over-voltage	Alarm	Equipment	Over voltage	Major	System Power Voltage higher than allowed.	NA
1762	pdc-under-voltage	Alarm	Equipment	Under voltage	Major	System Power Voltage Lower than allowed.	NA
1763	TCC-fpga-fw-not-found	Alarm	Equipment	The Main board firmware is not found	Warning		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1764	TCC-fw-load-fail	Alarm	Equipment	Download Main Board firmware has failed	Major	Firmware download was unsuccessful.	Reset board. Download software package. Try to insert another board.
1765	tcc-powerup-reset-event	Event	Equipment	Main Board was reset	Warning		
1766	upload-software-failed	Event	Equipment	RFU installation failure	Warning	Unsupported RFU type. IDU-RFU communications problem. RFU failure.	Make sure RFU is supported by SW version. Check IDU-RFU cable. Replace RFU.
1767	upload-software-started	Event	Equipment	RFU installation in progress	Warning	User command	

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1768	upload-software-succeeded-event	Event	Equipment	RFU installation successfully completed	Warning	User command	
1770	cable-lof-rfu	Event	Equipment	Unit performing power-up.	Major		
1771	cable-error-rfu	Alarm	Equipment	RFU cable error.	Major	Errors in signal from IDU to XCVR.	Check the IF cable and connectors. Verify that the N-Type/TNC connector inner pin is not spliced. Replace RMC. Replace XCVR.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1772	xpic-data-los	Alarm	Equipment	Radio XPIC sync loss	Major	Signaling between RMCs (Radio Modem Cards) for XPIC functionality has failed	Check that the RMCs are in allowed slots. Populate the RMCs in different allowed location in the chassis. Replace RMC/s. Replace chassis.
1773	early-warning	Alarm	Communications	Radio early warning.	Warning	The estimated radio BER (Bit Error Rate) is above 10E-12.	Check link performance. Check IF cable, and replace if required. Replace XCVR. Replace RMC.
1774	sw-download-incompatible-rfu	Alarm	Equipment	RFU software download cannot be initiated.	Critical	The hardware of the XCVR is OK, but is it running with METRO radio application.	Upgrade the XCVR software application via XPAND-IP and then reinitiate software download..

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1775	hw-incompatible-rfu	Alarm	Equipment	RFU software download is not possible.	Critical	Wrong type of XCVR, the XCVR hardware is METRO.	Replace the XCVR
1776	pll-rmc	Alarm	Equipment	RMC hardware failure.	Major	RMC hardware failure of the clock distributor.	Replace the RMC.
1777	rfu-mute-with-timeout	Event	Equipment	RFU TX Mute with timeout	Warning	RFU Transmitter muted by user.	Unmute the RFU transmitter or wait for expiration of the timeout.
1778	rfu-power-decreased-due-to-pa-temp	Alarm	Equipment	RFU power decreased due to PA temperature	Major	Defective RFU (the RFU cannot transmit the requested TX power).	Replace RFU. Intermediate solution - reduce TX power.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1780	mrmc-running-script-deleted	Event	Equipment	MRMC running script is deleted	Warning	New installed software package does not include the running MRMC radio script	Make sure the required software package include the running MRMC radio script. Download and install the correct software package.
1781	mrmc-running-script-updated	Event	Equipment	MRMC running script is updated	Warning	New installed software package does has an updated version of the running MRMC radio script	Reset the radio carrier to reacquire the new updated MRMC radio script
1782	radio-2_5gbps-mismatch-configuration	Alarm	Equipment	2.5Gbps mismatch configuration	Warning	The card cannot function outside of an ABC group in 2.5Gbps mode.	Add the card to an ABC group, or change the Slot Section to 1Gbps.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1783	remote-fault-indication	Alarm	Communication	Radio remote fault indication (RFI)	Minor		
1790	np-hw-failure	Alarm	Equipment	Hardware failure	Critical	An internal hardware failure has been detected by the system.	Replace the card or unit reporting the hardware failure.
1794	interface-not-functional-until-reset	Alarm	equipment	Interface is not operational until chassis reset	Warning	Changes were made to platform due to user configuration	Reset chassis
1800	t3-loc-alarm	Alarm	Equipment	T3 sync interface Loss of Carrier	Major	Cable disconnected. Defective cable.	Check connection of the cable. Replace the cable.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1975	radio-fan-failure	Alarm	Equipment	RFU fan failure	Major	RFU fan is disconnected. RFU fan HW failure. RFU fan jammed.	Check fan cable connection to the RFU. Check/replace the fan. Clear/clean the fan.
2001	pwe3-pwc-s-card-reset	Alarm	Equipment	TDM-LIC has rebooted and is not in service now	Major	Recent TDM-LIC card reset; System malfunction.	Wait for card to reboot. Reset the TDM-LIC card.
2002	pwe3-pwc-s-config-mismatch	Alarm	Equipment	TDM-LIC configuration mismatch	Major	Recent warm reset of TDM-LIC; System malfunction.	Power cycle the TDM-LIC.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2003	pwe3-pwc-s-front-panel-clock-los	Alarm	Equipment	Loss of Signal (LOS) on TDM-LIC's front panel clock port	Major	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2004	pwe3-pwc-s-host-pw-lic-comm-disrupt	Alarm	Equipment	Communication with TDM-LIC is disrupted in Host-Card direction	Minor	System malfunction	Reset the TDM-LIC.
2005	pwe3-pwc-s-hw-failure	Alarm	Equipment	TDM-LIC hardware failure	Major	System malfunction	Reset the TDM-LIC.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2006	pwe3-pwc-s-pw-lic-host-comm-disrupt	Alarm	Equipment	No communication with TDM-LIC	Major	System malfunction	Reset the TDM-LIC.
2007	pwe3-pws-s-jitter-buffer-overrun	Alarm	Equipment	Jitter-buffer-overrun alarm on TDM service	Major	Something wrong on TDM service synchronization	Check TDM service configuration
2008	pwe3-pws-s-late-frame	Alarm	Equipment	Late-frame alarm on TDM service	Warning	Something wrong on TDM service	Check TDM service configuration
2009	pwe3-pws-s-loss-of-frames	Alarm	Equipment	Loss-of-frames alarm on TDM service	Major	Failure along the network path of TDM service	Check network or configuration for errors in the network transport side of the service

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2010	pwe3-pws-s-malformed-frames	Alarm	Equipment	Malformed-frames alarm on TDM service	Major	Payload size does not correspond to the defined value. Mismatch in PT value in RTP header (if used)	Check TDM service configuration
2011	pwe3-pws-s-misconnection	Alarm	Equipment	Misconnection alarm on TDM service	Major	Stray packets with wrong RTP configurations are received and dropped.	Check TDM service configuration
2012	pwe3-tdm-port-s-ais	Alarm	Equipment	Alarm Indication Signal (AIS) on TDM-LIC TDM port	Major	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment.
2013	pwe3-tdm-port-s-lof	Alarm	Equipment	Loss Of Frame (LOF) on TDM-LIC TDM port	Major	Line is not properly connected. External equipment is faulty.	

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2014	pwe3-tdm-port-s-lomf	Alarm	Equipment	Loss Of Multi-Frame (LOMF) on TDM-LIC TDM port	Major	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment.
2015	pwe3-tdm-port-s-loopback-alarm	Alarm	Equipment	Loopback on TDM-LIC TDM port	Warning	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment.
2016	pwe3-tdm-port-s-los	Alarm	Equipment	Loss Of Signal (LOS) on TDM-LIC TDM port	Major	Line is not properly connected. Cable is faulty. External equipment is faulty. Defective TDM-LIC.	Reconnect line. Check line cables. Check external equipment.
2017	pwe3-tdm-port-s-rai	Alarm	Equipment	Remote Alarm Indication (RAI) on TDM-LIC TDM port	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2018	pwe3-tdm-port-s-unexpected-signal-alarm	Alarm	Equipment	E1/DS1 Unexpected signal on TDM-LIC TDM port	Warning	Port is disabled. Line is connected to a disabled port.	Enable relevant port. Disconnect cable from relevant port.
2021	pwe3-pwc-s-ssm-rx-changed	Event	Equipment	SSM received pattern change was discovered	Warning		No action is required.
2022	pwe3-stm1oc3-s-excessive-ber-alarm	Alarm	Equipment	Excessive BER on TDM-LIC STM1/OC3 port	Major	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2023	pwe3-stm1oc3-s-lof-alarm	Alarm	Equipment	Loss Of Frame (LOF) on TDM-LIC STM1/OC3 port	Major	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2024	pwe3-stm1oc3-s-loopback-alarm	Alarm	Equipment	Loopback on TDM-LIC STM1/OC3 port	Warning	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2025	pwe3-stm1oc3-s-los-alarm	Alarm	Equipment	Loss Of Signal (LOS) on TDM-LIC STM1/OC3 port	Critical	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2026	pwe3-stm1oc3-s-mute-override-alarm	Alarm	Equipment	SFP is muted on TDM-LIC STM1/OC3 port	Warning		
2027	pwe3-stm1oc3-s-sfp-absent-alarm	Alarm	Equipment	SFP absent in TDM-LIC STM1/OC3 port	Critical	SFP is not properly installed. SFP is faulty.	Install SFP properly. Replace the card.
2028	pwe3-stm1oc3-s-sfp-failure-alarm	Alarm	Equipment	SFP failure on TDM-LIC STM1/OC3 port	Critical	SFP is not properly installed. SFP is faulty.	Install SFP properly. Replace the card.
2029	pwe3-stm1oc3-s-sfp-tx-fail-alarm	Alarm	Equipment	SFP transmit failure on TDM-LIC STM1/OC3 port	Critical	SFP is not properly installed. SFP is faulty.	Install SFP properly. Replace the card.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2030	pwe3-stm1oc3-s-signal-degrade-alarm	Alarm	Equipment	Signal Degrade on TDM-LIC STM1/OC3 port	Minor	Line is not properly connected. SFP is not properly installed. SFP is faulty. External equipment is faulty	Install SFP properly. Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2031	pwe3-stm1oc3-s-slm-alarm	Alarm	Equipment	J0 Trace Identifier Mismatch on TDM-LIC STM1/OC3 port	Minor	J0 misconfiguration. Line is not properly connected. SFP is not properly installed. External equipment is faulty.	Make sure expected and received J0 match. Install SFP properly. Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2032	pwe3-stm1oc3-s-ssm-rx-changed	Event	Equipment	SSM pattern received on TDM-LIC STM1/OC3 port changed	Warning		
2033	pwe3-vc12vt15-s-ais-alarm	Alarm	Equipment	Alarm Indication Signal (AIS) on TDM-LIC VC12/VT1.5	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment.Power cycle the TDM-LIC.
2034	pwe3-vc12vt15-s-excessive-ber-alarm	Alarm	Equipment	Excessive BER on TDM-LIC VC12/VT1.5	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2035	pwe3-vc12vt15-s-loopback-alarm	Alarm	Equipment	Loopback on TDM-LIC VC12/VT1.5	Warning	Line is not properly connected. External equipment is faulty.	Reconnect line.Check line cables. Check external equipment. Power cycle the TDM-LIC.
2036	pwe3-vc12vt15-s-rcv-plm-alarm	Alarm	Equipment	Payload Mismatch Path (PLM) received on TDM-LIC VC12/VT1.5	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2037	pwe3-vc12vt15-s-rcv-rdi-alarm	Alarm	Equipment	Remote Defect Indication (RDI) received on TDM-LIC VC12/VT1.5	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check lie cables. Check external equipment. Power cycle the TDM-LIC.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2038	pwe3-vc12vt15-s-rcv-slm-alarm	Alarm	Equipment	Signal Label Mismatch (SLM) received on TDM-LIC VC12/VT1.5	Minor	J2 misconfiguration. Line is not properly connected. External equipment is faulty.	Make sure expected and receive J2 match. Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2039	pwe3-vc12vt15-s-signal-degrade-alarm	Alarm	Equipment	Signal Degrade on TDM-LIC VC12/VT1.5	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2040	pwe3-vc12vt15-s-unequipped-alarm	Alarm	Equipment	Unequipped on TDM-LIC VC12/VT1.5	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2041	pwe3-card-group-s-config-mismatch	Alarm	Equipment	TDM-LIC card protection configuration mismatch	Major	The configuration between the TDM-LIC card protection members is not aligned	Apply a copy-to-mate command to copy the configuration from the required TDM-LIC to the other one
2042	pwe3-card-group-s-lockout	Alarm	Equipment	TDM-LIC card protection group lockout command is on	Minor	The user has issued a lockout command	Clear the lockout command

AlarmID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2043	pwe3-card-group-s-no-mate	Alarm	Equipment	A member of TDM-LIC card protection group is missing	Minor	TDM-LIC card is not installed in the shelf	Install the missing TDM-LIC card
2044	pwe3-card-group-s-protection-switch-evt	Event	Equipment	TDM-LIC card protection switch over, priority	Warning	LOS alarm on a STM1 interface of the TDM-LIC card protection group member; A TDM-LIC card protection group member was disabled or pulled out of the shelf	Check line cables. Check external equipment.
2045	pwe3-vc12vt15-s-lop-alarm	Alarm	Equipment	Loss Of Pointer (LOP) received on TDM-LIC VC12/VT1.5	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2046	pwe3-tunnel-groups-s-protection-switch	Event	Equipment	Path protection switch on TDM service	Minor	Failure along service primary path. User command.	Check errors along primary path Check local service configuration.
2047	pwe3-tunnel-groups-s-revertive-switch	Event	Equipment	Path protection revertive switch on TDM service	Minor	Primary path has been operational for the duration of the defined WTR time	-
2100	STM-1-OC-3-IN-LOS	Alarm	Equipment	Loss of Signal on Line Interface (LOS) on STM-1/OC-3 port.	Critical	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2101	STM-1-OC-3-IN-LOF	Alarm	Equipment	Loss of Frame on Line Interface (LOF) on STM-1/OC-3 port.	Major	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment.
2102	STM-1-OC-3-IN-MSAIS	Alarm	Equipment	Alarm Indication Signal on Line Interface (MS-AIS/AIS-L) received.	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment.
2103	STM-1-OC-3-IN-MSRDI	Alarm	Equipment	Remote Defect Indication on Line Interface (MS-RDI/RDI-L) received.	Minor	External equipment is faulty.	Check external equipment.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2104	STM-1-OC-3-RX-LOS	Alarm	Equipment	Loss of STM-1/OC-3 Frame on Radio Interface.	Major	All channels in Multi Carrier ABC group are down. Incorrect configuration on remote side.	Check link performance. Check radio alarms for channel. Check configuration.
2105	STM-1-OC-3-RX-MSAIS	Alarm	Equipment	MS-AIS/AIS-L on Radio Interface detected.	Minor	Remote STM-1/OC-3 signal is missing (LOS/LOF/MS-AIS/AIS-L on remote STM-1/OC-3 interface). STM-1/OC-3 Channel removed due to reduced radio capacity on remote side.	Check remote equipment.
2106	STM-1-OC-3-RX-RDI	Alarm	Equipment	MS-RDI/RDI-L on Radio Interface detected.	Minor	External equipment is faulty.	Check remote equipment.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2107	STM-1-OC-3-LOOPBACK	Alarm	Equipment	STM-1/OC-3 Loopback	Warning	Looping.	Remove looping.
2108	STM-1/OC-3-CHANNEL-1-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	Reduced capacity. Fading	Check link performance. Check radio alarms for channel.
2109	STM-1-OC-3-PBRS-INSERTION	Alarm	Equipment	PRBS insertion.	Warning	PRBS insertion on STM-1/OC-3 card.	Remove PRBS insertion.
2110	STM-1-OC-3-SFP-NOT-DETECTED	Alarm	Equipment	SFP absent in STM-1/OC-3 port.	Critical	SFP is not properly installed. SFP is faulty.	Install SFP properly. Replace the card.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2111	STM-1-OC-3-SFP-TX-FAILURE	Alarm	Equipment	SFP Transmit Failure on STM-1/OC-3 port.	Critical	SFP is faulty.	Replace SFP or insert SFP if it is not inserted correctly. Replace the card.
2112	STM-1-OC-3-SFP-TX-MUTED	Alarm	Equipment	SFP is muted on STM-1/OC-3 port.	Warning	SFP is muted by configuration.	Remove muting.
2113	STM-1/OC-3-CHANNEL-2-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	Reduced capacity. Fading.	Check link performance. Check radio alarms for channel.
2114	STM-1/OC-3-CHANNEL-3-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	Reduced capacity. Fading.	Check link performance. Check radio alarms for channel.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2115	STM-1/OC-3-CHANNEL-4-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	Reduced capacity. Fading.	Check link performance. Check radio alarms for channel.
2116	STM-1/OC-3-CHANNEL-5-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	Reduced capacity. Fading.	Check link performance. Check radio alarms for channel.
2117	STM-1/OC-3-CHANNEL-6-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	Reduced capacity. Fading.	Check link performance. Check radio alarms for channel.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2118	STM-1/OC-3-CHANNEL-7-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	Reduced capacity. Fading.	Check link performance. Check radio alarms for channel.
2119	STM-1/OC-3-CHANNEL-8-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	Reduced capacity. Fading.	Check link performance. Check radio alarms for channel.
2120	STM1-OC3-GROUP-ACTIVITY-CHANGED	Event	Equipment	STM-1/OC-3 Group protection switchover	Warning	LOS alarm on an STM-1/OC-3 interface. STM1-OC3 Group protection group member was disabled or pulled out of the shelf.	Check line cables. Check external equipment.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2200	MC-ABC-Local-LOF	Alarm	Communications	Multi Carrier ABC LOF.	Critical	All channels in Multi Carrier ABC group are down.	Check link performance on all radio channels in Multi Carrier ABC group. Check radio alarms for channels in Multi Carrier ABC group. Check configuration of Multi Carrier ABC group.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2201	MC-ABC-local-cap-below	Alarm		Multi Carrier ABC bandwidth is below the threshold	Major	One of the radio channels in the Multi Carrier ABC group has a lower capacity than expected Minimum bandwidth threshold configuration is wrong	Check link performance on all radio channels in Multi Carrier ABC group Check radio alarms for channels in Multi Carrier ABC group Check configuration of Multi Carrier ABC group Minimum bandwidth threshold
2203	MC-ABC-Lvds-Error-Sl2	Alarm	Equipment	LVDS RX Error Slot 1.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2204	MC-ABC-Lvds-Error-Sl3	Alarm	Equipment	LVDS RX Error Slot 3.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.
2205	MC-ABC-Lvds-Error-Sl4	Alarm	Equipment	LVDS RX Error Slot 4.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.
2206	MC-ABC-Lvds-Error-Sl5	Alarm	Equipment	LVDS RX Error Slot 5.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.
2207	MC-ABC-Lvds-Error-Sl6	Alarm	Equipment	LVDS RX Error Slot 6.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.
2208	MC-ABC-Lvds-Error-Sl7	Alarm	Equipment	LVDS RX Error Slot 7.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2209	MC-ABC-Lvds-Error-Sl8	Alarm	Equipment	LVDS RX Error Slot 8.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.
2210	MC-ABC-Lvds-Error-Sl9	Alarm	Equipment	LVDS RX Error Slot 9.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.
2211	MC-ABC-Lvds-Error-Sl10	Alarm	Equipment	LVDS RX Error Slot 10.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.
2212	MC-ABC-Lvds-Error-Sl12	Alarm	Equipment	LVDS RX Error Slot 12.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2213	MC-ABC-robustness-member-disabled	Alarm	Equipment	MC-ABC member has been disabled due to robustness reason	Major	The corresponding MC-ABC member has been temporarily disabled within the group. It was caused by consecutive RFU HW failures	Verify the proper functioning and connectivity of the cable and RF unit.
2219	MC-ABC-Ch-Id-Mismatch-Ch1	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch1.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.
2220	MC-ABC-Ch-Id-Mismatch-Ch2	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch2.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.
2221	MC-ABC-Ch-Id-Mismatch-Ch3	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch3.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2222	MC-ABC-Ch-Id-Mismatch-Ch4	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch4.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.
2223	MC-ABC-Ch-Id-Mismatch-Ch5	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch5.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.
2224	MC-ABC-Ch-Id-Mismatch-Ch6	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch6.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.
2225	MC-ABC-Ch-Id-Mismatch-Ch7	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch7.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.
2226	MC-ABC-Ch-Id-Mismatch-Ch8	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch8.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
235	MC-ABC-Ch-Id-Disabled-Ch1	Alarm	Equipment	Multi Carrier ABC Channel Id Manual Disabled Ch1.	Warning	Admin state for channel is down.	Enable admin state for channel.
236	MC-ABC-Ch-Id-Disabled-Ch2	Alarm	Equipment	Multi Carrier ABC Channel Id Manual Disabled Ch2.	Warning	Admin state for channel is down.	Enable admin state for channel.
237	MC-ABC-Ch-Id-Disabled-Ch3	Alarm	Equipment	Multi Carrier ABC Channel Id Manual Disabled Ch3.	Warning	Admin state for channel is down.	Enable admin state for channel.
238	MC-ABC-Ch-Id-Disabled-Ch4	Alarm	Equipment	Multi Carrier ABC Channel Id Manual Disabled Ch4.	Warning	Admin state for channel is down.	Enable admin state for channel.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2239	MC-ABC-Ch-Id-Disabled-Ch5	Alarm	Equipment	Multi Carrier ABC Channel Id Manual Disabled Ch5.	Warning	Admin state for channel is down.	Enable admin state for channel.
2240	MC-ABC-Ch-Id-Disabled-Ch6	Alarm	Equipment	Multi Carrier ABC Channel Id Manual Disabled Ch6.	Warning	Admin state for channel is down.	Enable admin state for channel.
2241	MC-ABC-Ch-Id-Disabled-Ch7	Alarm	Equipment	Multi Carrier ABC Channel Id Manual Disabled Ch7.	Warning	Admin state for channel is down.	Enable admin state for channel.
2242	MC-ABC-Ch-Id-Disabled-Ch8	Alarm	Equipment	Multi Carrier ABC Channel Id Manual Disabled Ch8.	Warning	Admin state for channel is down.	Enable admin state for channel.

AlarmID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2250	CRB-Group-Entity	Alarm	communications	Enhanced Multi Carrier ABC LOF	Critical	All channels in Enhanced Multi Carrier ABC group are down	Check link performance on all channels in Enhanced Multi Carrier ABC group. Check alarms for channels in Enhanced Multi Carrier ABC group. Check configuration of Enhanced Multi Carrier ABC group.
2300	protection-configuration-mismatc	Alarm	Equipment	Protection configuration mismatch!	Major	The configuration between the protected devices is not aligned.	Apply copy-to-mate command to copy the configuration from the required device to the other one.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2301	protection-copytomate-started	Event	Processing	Copy to mate started	Indeterminate	The copy-to-mate command has just begun!	This is a notification
2302	protection-copytomate-completed	Event	Processing	Copy to mate completed	Indeterminate	The copy-to-mate command was completed.	This is a notification
2400	cpri-optical-rx-los	Alarm	Equipment	Loss of CPRI optical signal - based on RX level lower than a predefined threshold	Critical	No SFP is connected. Issue with the Fiber link.	Check Fiber connection

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2401	cpri-los	Alarm	Equipment	CPRI LOS caused by at least 16 8B/10B violation events in a whole hyperframe	Major	Input signal is not in a CPRI format. CPRI format is different than the configured one. Errors in the CPRI link that feeds the system.	1. Check CPRI format. 2. Check CPRI link/cable.
2402	cpri-clock-unit-unlock	Alarm	Equipment	CPRI clock unit is not locked	Warning	The recovered clock of the CPRI module is not locked.	Check the clock source of the CPRI module.
3000	chassis-reset-event	Event	Equipment	Chassis was reset	Warning	User issued a command to reset the chassis.	Wait until the reset cycle is ended and the system is up and running.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
3001	10gbps-mode-front-panel-ports-unavailable	Alarm	Equipment	Reset chassis to activate front panel Ethernet ports	Warning	Front panel Ethernet ports cannot work when slot 12 is configured in 10Gbps mode.	Reset chassis.
3002	slot-mode-front-panel-ports-not-functional	Alarm	Equipment	Front panel Ethernet port cannot function in current configured capacity mode	Warning	Front panel Ethernet port cannot work in a mode other than 1Gbps.	Configure the relevant capacity mode to 1 Gbps mode.
3003	abc-mode-not-functional	Alarm	Equipment	Multi Carrier ABC group is not functional in current configured capacity mode	Warning	Multi Carrier ABC group does not support the configured capacity mode.	Configure the relevant capacity mode to 1 Gbps mode.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
3004	abc-mode-not-functional-until-reset	Alarm	Equipment	Multi Carrier ABC group is not functional in current configured capacity mode until chassis is reset	Warning	Multi Carrier ABC group capacity mode is different than the configured capacity mode.	Reset chassis.
4000	hw-failure	Alarm	Equipment	Card has one or more HW failures	Critical	One or more HW faults.	Replace card.
4001	slotsection-2_5gbps-compatibility	Alarm	Equipment	Card cannot function in 2.5Gbps mode.	Warning	The user set an expected card that does not support 2.5Gbps.	Change the Slot Section to 1Gbps.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
4002	slot-slotsection-10gbps-card-not-functional	Alarm	Equipment	Card is not functional until chassis is reset	Warning	Slot is not in 10Gbps mode.	Reset chassis.
5000	failure-login-event	Event	Equipment	User blocked due to consecutive failure login	Indeterminate	User blocked due to consecutive failure login	The user should wait few minutes until it account will be unblock
5001	g8032-protection-switching-alarm	Alarm	Processing	ERPI is either in protection state or forced protection state	Minor	Either link failure happened in the ring or force/manual command is active.	Fix the broken link in the ring or release the force/manual command.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5002	g8032-failure-of-protocol-pm-alarm	Alarm	Processing	More than a single RPL is configured in a ring	Warning	User configuration	Reconfigure the RPL
5003	lldp-topology-change	Event	Processing	LLDP topology change	Warning	New neighbor	None
5004	security-log-upload-started-event	Event	Equipment	Security log upload started	Indeterminate	Security log upload started	
5005	security-log-upload-failed-event	Event	Equipment	Security log upload failed	Indeterminate	Security log upload failed	

AlarmID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5006	security-log-upload-succeeded-event	Event	Equipment	Security log upload succeeded	Indeterminate	Security log upload succeeded	
5010	force-mode-alarm	Alarm	Equipment	System is in sync force mode state	Warning	User command	
5011	sync-quality-change-event	Event	Equipment	The sync-source quality level was changed	Major		
5012	system-clock-in-holdover-mode	Alarm	Equipment	System Synchronization Reference in Holdover Mode	Critical		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5013	sync-T0-quality-change-event	Event	Equipment	System sync reference T0 quality has changed	Major		
5014	sync-pipe-invalid-interface-clock-source	Alarm	Equipment	The pipe interface clock-source in signal-interface table is not system-clock	Major		
5015	sync-pipe-missing-edge	Alarm	Equipment	The pipe is missing an edge interface	Major	Regenerator contains less than 2 interfaces	Accomplish configuration by assigning second interface

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5016	sync-pipe-interface-op-state-down	Alarm	Equipment	Pipe interface operational state is down	Major	At least one of Regenerator Interfaces status is down	Checking regenerator Admin status
5017	sync-pipe-invalid-pipe	Alarm	Equipment	Pipe is invalid	Major	Interfaces has Configuration or Operation fails	Configuration not accomplished
5018	sync-1588-tc-not-operational	Alarm	Equipment	1588TC is not operational	Major	System Failure	Reboot the unit
5020	sync-T3-remote-loopback	Alarm	Equipment	T3 interface at loopback mode	Warning		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5021	sync-T4-analog-loopback	Alarm	Equipment	T4 interface at loopback mode	Warning		
5030	soam-connectivity-failure	Alarm	Processing	A connectivity failure in MA/MEG	Minor	Wrong link configurations.	Check the link in the traffic path
5031	soam-def-error-failure	Alarm	Processing	Error CCM received	Major	Invalid CCMs has been received	Check the link in the traffic path
5032	soam-def-mac-failure	Alarm	Processing	Remote mep MAC status not up	Minor	Remote MEP’s associated MAC is reporting an error status	Check remote MEP's MAC status
5033	soam-def-rdi-failure	Alarm	Processing	Mep Rdi received	Minor	Remote Defect indication has been received from remote MEP	Check the SOAM configurations

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5034	soam-remote-ccm-failure	Alarm	Processing	Remote mep CCMs are not received	Major	The MEP is not receiving CCMs from at least one of the remote MEPs	Check that all remote MEPs are configured or enabled
5035	soam-def-xcon-failure	Alarm	Processing	Cross Connect CCM received	Major	CCM from another MAID or lower MEG level have been received	Check MA/MEG and MEP configurations
5036	ptp-stream-state-change	Event	Processing	1588-BC port state changed	Warning		
5037	ptp-bmca-update	Event	Processing	1588-BC BMCA has been updated.	Warning		
5038	ptp-output-squelch	Event	Processing	1588-BC outputs are squelched.	Warning		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5039	ptp-parent-data-set-change	Event	Processing	1588-BC parent dataset has changed.	Warning		
5040	ptp-utc-offset-change	Event	Processing	1588-BC UTC offset value changed.	Warning		
5041	ptp-leap-seconds-flag-change	Event	Processing	1588-BC one of the leap seconds flags have changed.	Warning		
5042	ptp-message-interval-change	Event	Processing	1588-BC message interval change detected.	Warning		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5043	ptp-message-rate-announce	Alarm	Processing	1588-BC announce message rate is below expected.	Major	Misconfiguration of the peer system.	Check the configuration of the peer system.
5044	ptp-message-rate-sync	Alarm	Processing	1588-BC sync message rate is below expected.	Major	Misconfiguration of the peer system.	Check the configuration of the peer system.
5045	ptp-message-rate-delay-req	Alarm	Processing	1588-BC delay request message rate is below expected.	Major	Misconfiguration of the peer system.	Check the configuration of the peer system.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5046	ptp-no-syncE	Alarm	Processing	1588-BC performance is degraded due to loss of system clock reference.	Critical	Loss of system clock reference.	Restore the system clock synchronization to a PRC-traceable source.
5047	soam-csf-rdi-alarm	Alarm	Processing	Auto-state-propagation indication received	Major	Remote system triggered auto-state-propagation	Resolve the problem on the .remote system.
5048	lacp-port-out-of-sync-alarm	Alarm	processing	LACP port out of collecting-distributing	Major	LACP port was not selected by the aggregator or partner is out of sync	Resolve the problem on the remote system
5100	mkey-mismatch	Alarm	Equipment	Master key mismatch cross over the link	Critical	Master Key was not set correctly.	Verify the Master Key.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5101	mkey-no-exist	Alarm	Equipment	No Master Key set, default value used	Warning	Crypto module has been enabled, but no Master Key has been loaded.	Set the Master Key.
5102	general-encryption-failure	Alarm	Equipment	Payload Encryption failure	Critical	Radio LOF on Tx/Rx direction. The session key does not match across the link. The AES admin setting does not match across the link.	Validate the MSE on both sides of the link. Validate the session key on both sides of the link. Validate the AES admin setting on both sides of the link.
5104	kep-initiated	Event	Equipment	Key Exchange Protocol in progress, Traffic has been blocked	Indeterminate		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5105	kep-remote-initiated	Event	Equipment	Key Exchange Protocol initiated by remote side	Indeterminate		
5107	bypass-self-test-alarm	Alarm	Equipment	FIPS Bypass Self-Test failed	Critical	Disk failure	
5108	post-fail-alarm	Alarm	Equipment	Power On Self-Test Failed	Critical	System failure	Reboot the unit.
5109	main-board-non-fips-alarm	Alarm	Equipment	Main Board is not FIPS certified	Critical	Main Board used is not FIPS certified	Use a FIPS-certified TCC.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5110	radio-non-fips-alarm	Alarm	Equipment	Radio card is not FIPS certified	Major	Radio Card used is not FIPS certified	Use a FIPS-certified RMC.
5111	aes-self-test-fail-alarm	Alarm	Equipment	Radio crypto module fail	Critical	FIPS Radio Encryption Self-Test failed	Use different FIPS supported radio card
5112	hw-not-supported-alarm	Alarm	Equipment	Radio Encryption not supported	Major	No Payload Encryption Activation Key inserted	Insert suitable Activation Key and reboot the unit
5113	ipsec-pre-shared-key-alarm	Alarm	Equipment	IPSec Pre-Shared Key has the default value	Major	IPSec Pre-Shared Key was not configured	Configure the IPSec Pre-Shared Key to a different value than the default

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
300007	Clock-source-sharing-failure-event	Event	Equipment	Clock source sharing failure	Critical	Faulty coaxial cable between master and slave RFUs. Hardware failure in Master RFU. Hardware failure in Slave RFU.	Try re-initiation of MIMO. If still fails: Replace faulty coaxial cable and reset Master RFU. Replace faulty RFU.
310000	Insufficient-conditions-for-MIMO-alarm	Alarm	Equipment	Insufficient conditions for MIMO	Critical	Insufficient conditions for MIMO. Hardware failure.	Make sure all cables between master and slave are connected (MIMO 4x4 only). Replace faulty units and check that cables are plugged.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
31003	Unsuitable-hardware-for-MIMO-alarm	Alarm	Communications	Unsuitable hardware for MIMO	Critical	Unsuitable hardware for MIMO operation requirements. Dual carrier RFUs (MIMO 2x2 and 4x4). RFUs with MIMO bus interface (MIMO 4x4). Clock source sharing capability (MIMO 4x4).	Make sure both RFUs are compatible for MIMO operation.
31004	Unsuitable-software-configuration-for-MIMO-alarm	Alarm	Communications	Unsuitable software configuration for MIMO	Critical	Not all MIMO carriers are set to same radio script or script is not compatible for MIMO. Radio TX and RX frequency is not identical on all MIMO carriers. XPIC or Multi radio or ATPC features are enabled.	Load same MIMO compatible radio script to all MIMO carriers. Set same TX and RX frequency on all MIMO carriers. Disable XPIC, Multi radio and ATPC on all MIMO carriers.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
310005	Clock-source-sharing-failure-alarm	Alarm	Equipment	Clock source sharing cable unplugged	Critical	Faulty coaxial cable between master and slave RFUs Mate does not exist	Replace faulty coaxial cable and reset Master RFU. Replace faulty RFU.
311000	AMCC-Incompatible-radio-script-alarm	Alarm	Communications	Radio script is incompatible to AMCC	Critical	MRMC Script selected does not support AMCC Group type/subtype	Set AFR Script in both Agg1 & Agg2 carriers
311001	AMCC-Inconsistent-MRMC-Script-alarm	Alarm	Communications	Inconsistent MRMC script between members	Critical	All members of a group must be configured to the same MRMC Script	Set the members to the appropriate MRMC script
311002	AMCC-Inconsistent-radio-frequency-alarm	Alarm	Communications	Inconsistent radio frequency	Critical	Radio TX/RX frequency is not identical on all AMCC carriers	Set same radio TX/RX frequency on all AMCC carriers

AlarmID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
311103	AMCC-Failed-To-Load-Alarm	Alarm	Communications	Agg 1 failed Bring-up procedure	Critical	Agg1 did not complete Bring-up successfully	Drop both Agg1 & Agg2 into single carrier mode (Pre-Init)
311104	AMCC-Invalid-ACM-Configuration-alarm	Alarm	Communications	Invalid ACM configuration	Critical	AMCC member have been set to fixed profile	Set AMCC member to adaptive ACM profiles

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
311105	AMCC-Mimo-not-supported-alarm	Alarm	Equipment	MIMO insufficient condition – configuration is not supported	Critical	MIMO script is not enabled on any radio member. Different TX/RX frequency. ATPC enabled. XPIC enabled. ACM mode (adaptive/Fixed) is not the same. Unit Redundancy enabled. Platform not supported.	Align MIMO script on all radio members. Align same frequency on all radio members. Disable ATPC. Disable XPIC. Align ACM mode. Disable Unit Redundancy. Replace unit.
311106	AMCC-Master-failure-alarm	Alarm	Equipment	MIMO insufficient condition – Master unit failure.	Critical	Master unit failure.	Verify Master unit power. Replace hardware.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
311107	AMCC-Slave-failure-alarm	Alarm	Equipment	MIMO insufficient condition – Slave unit failure.	Critical	Slave unit failure.	Verify Slave unit power. Replace hardware.
311108	AMCC-Data-Sharing-cable-disconnected-alarm	Alarm	Equipment	MIMO insufficient condition – Data sharing cable failure.	Critical	Data sharing cable failure.	Verify Data sharing cable connected. Replace Data sharing cable.
311109	AMCC-Prot-port-cable-disconnected-alarm	Alarm	Equipment	MIMO insufficient condition – Mate communication cable failure.	Critical	Mate communication cable failure.	Verify Mate communication cable connected. Replace Mate communication cable.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
31110	AMCC-Source-Sharing-cable-disconnected-alarm	Alarm	Equipment	MIMO insufficient condition – Source sharing cable failure.	Critical	Source sharing cable failure.	Verify Source sharing cable connected. Replace Source sharing cable.
31111	AMCC-Master-Slave-config-mismatch-alarm	Alarm	Equipment	MIMO insufficient condition - Master/Slave configuration mismatch	Critical	Master/Slave configuration mismatch due to: Different TX/RX frequency. Different MIMO script ID. Different ACM mode (adaptive/Fixed).	Align Master/Slave configuration.
31112	AMCC-Remote-failure-alarm	Alarm	Equipment	MIMO insufficient condition – Remote failure	Critical	MIMO remote failure.	Handle MIMO remote failure.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
31115	AMCC-Data-Sharing-failure-alarm	alarm	Radio	AMCC insufficient condition - Units alignment failure.	Critical	Units alignment failure.	Verify Source sharing cable connected. Replace Source sharing cable. Verify Data sharing cable connected. Replace Data sharing cable. Verify using correct SFPs.
31118	AMCC-XPIC-not-supported-alarm	alarm	Radio	XPIC configuration is not supported	Critical	XPIC MRMC script is not configured Different TX/RX frequency. ACM mode (adaptive/fixed) is not configured the same.	Set XPIC MRMC script Align same frequency on all radio members. Align same ACM mode.

AlarmID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
311119	AMCC-XPIC-remote-failure-alarm	alarm	Radio	XPIC configuration failure in remote	Warning	XPIC remote failure	Handle XPIC remote failure
311120	AMCC-XPIC-mate-communication-failure-alarm	Alarm	Communications	XPIC communication with mate unit is interrupted	Warning	The mate unit is unreachable. In FIPS mode, possible mismatch between the IPSec pre-shared keys configured on the two units.	Check the cable between the two units. In FIPS mode, make sure that the same IPSec pre-shared key is configured on the two units.
311121	AMCC-Radio-unit-failure-alarm	Alarm	Communications	AMCC insufficient condition - Radio unit failure.	Critical	Radio Unit failure.	Verify radio unit power. Replace HW.
320000	unit-mgr-undervoltage-alarm	Alarm	Equipment	Under voltage	Major	System Power Voltage lower than allowed.	

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
32001	unit-mgr-overvoltage-alarm	Alarm	Equipment	Over voltage	Major	System Power Voltage higher than allowed.	
32003	unit-mgr-unit-reset-event	Event	Management	Unit was reset.	Warning	User issued a command to reset the unit	Wait until the reset cycle is ended and the system is up and running
32004	unit-mgr-power-up-event	Event	Equipment	Unit Performed Power up	Warning		
33001	anti-theft-enabled-event	Event	Management	Anti-Theft Procedures have been enabled	Indeterminate		

AlarmID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
33002	anti-theft-temporary-disabled-event	Event	Management	Anti-Theft Procedures have been temporary disabled	Indeterminate		
33003	anti-theft-sanction-timer-countdown-alarm	Alarm	Management	Anti-Theft Sanction Mode 24 hours window has been triggered	Critical	Watchdog timer countdown	Return the equipment to the network
33004	anti-theft-sanction-mode-entered-alarm	Alarm	Management	Anti-Theft Sanction Mode is Active	Critical	Equipment has been stolen	Return the equipment to the network

28.1.1 Glossary

Term	Definition
A	
ABC	Adaptive Bandwidth Control
ABN	Adaptive Bandwidth Notification
AC	Alternating Current
ACAP	Adjacent Channel Alternate Polarization
ACCP	Adjacent Channel Co-Polarization
ACM	Adaptive Coded Modulation
ACR	Adaptive Clock Recovery
AES	Advanced Encryption Standard
AFR	Advanced Frequency Reuse
AGC	Automatic Gain Control
AIS	Alarm Indicating Signal
ALC	Automatic Level Control
AMCC	Advanced Multi-Carrier Configuration
ANSI	American National Standards Institute
ASIC	Application Specified Integrated Circuit
ATPC	Automatic Transmit Power Control
AUX	Auxiliary Unit
B	
BB	Baseband
BBS	Baseband Switching
BER	Bit Error Rate

Term	Definition
BLSR	Bidirectional Line Switch Ring
BPDU	Bridge Protocol Data Units
BWA	Broadband Wireless Access
C	
CBS	Committed Burst Size
CCDP	Co-Channel Dual Polarization
CCITT	Comité Consultatif International de Télégraph et des Télécommunications (ITU)
CET	Carrier-Ethernet Transport
CFM	Connectivity Fault Management
CIR	Committed Information Rate
CLI	Command Line Interface
Clk	Clock
CODEC	Coder/Decoder
CoS	Class of Service
D	
DA	Destination Address
DC	Direct Current
DCB	Diversity Circulator Block
DCC	Data Communication Channel
DXC	Digital Cross Connect
DSCP	Differentiated Services Code Point
E	
EBS	Excess Burst Size
EIR	Excess Information Rate

Term	Definition
EMC	Electromagnetic Compatibility
EOW	Engineering Order Wire
EPROM	Erasable Programmable Read Only Memory
ESD	Electrostatic Discharge
ESE	Electrical SFP Electrical
ESP	Electrical SFP SFP+ 10G
ESS	Electrical SFP SFP
ETSI	European Telecommunications Standards Institute
F	
FCC	Federal Communications Commission
FCS	Frame Check Sequence
FTP	File Transfer Protocol
G	
GbE	Gigabit Ethernet
GFP	Generic Framing Procedure (Procedure for mapping of Ethernet traffic over a transport network)
GND	Ground
GRE	Generic Routing Encapsulation
GTP	GPRS Tunneling Protocol
H	
HBER	High Bit Error Rate
HDLC	High-level Data Link Control
HF	High Frequency (3-30 MHz)
HSB	Hot-Standby
HTTP	Hypertext Transfer Protocol

Term	Definition
HTTPS	Secured Hypertext Transfer Protocol
I	
IDC	Indoor Controller
IF	Intermediate Frequency
IFC	IF Combining
ISO	International Organization for Standardization
ITU	International Telecom. Union
ITU-R	International Telecom. Union (former CCIR)
ITU-T	International Telecom. Union (former CCITT)
IVM	Inventory Module
L	
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LAN	Local Area Network
LBER	Low Bit Error Rate
LCAS	Link Capacity Adjustment Scheme
LED	Light Emitting Diode
LIU	Line Interface Unit
LLDP	Link Layer Discovery Protocol
LLF	Link Loss Forwarding
LMS	License Management System
LO	Local Oscillator
LOC	Loss of Carrier
LOF	Loss of Frame

Term	Definition
LOS	Loss of Signal
LSI	Large Scale Integration
LTE	Long-Term Evolution
M	
MAID	Maintenance Association Identifier
MPLS	Multi Protocol Label Switching
MSP	Multiplex Section Protection
MUX	Multiplexer
N	
NE	Network Element
NMS	Network Management System
NTP	Network Time Protocol
O	
OAM	Operation Administration & Maintenance (Protocols)
OCB	Outdoor Circulator Box
OHC	OverHead Connections
OMT	Orthogonal Mode Transducer
OOF	Out of Frame
OPEX	Operational Expenditure
P	
PBB-TE	Provider Backbone Bridge Traffic Engineering
PBS	Peak Burst Rate
PC	Personal Computer
PCB	Printed Circuit Board

Term	Definition
PDV	Packed Delay Variation
PIR	Peak Information Rate
PLL	Phase Locked Loop
PM	Performance Monitoring
PN	Provider Network
PROM	Programmable Read Only Memory
PSN	Packet Switched Network
PTP	Precision Timing Protocol
PWR	Power
Q	
QoE	Quality of Experience
QoS	Quality of Service
R	
RBAC	Role Based Access Control
RCVR	Receiver
RDI	Reverse Defect Indication
RF	Radio Frequency
RIP	Routing Information Protocol
RMON	Ethernet Statistics
RPS	Radio Protection Switching
RSL	Received Signal Level
RSSI	Received Signal Strength Indicator
RSTP	Rapid Spanning Tree Protocol
S	

Term	Definition
SAP	Service Access Point
SDH	Synchronous Digital Hierarchy
SDWRR	Shaped Deficit Weighted Round Robin
SETS	Synchronous Equipment Timing Source
SFTP	Secure FTP
SLA	Service Level Agreements
SNCP	Simple Network Connection Protection
SNMP	Simple Network Management Protocol
SNP	Service Network Point
SNR	Signal to Noise Ratio
SNTP	Simple Network Time Protocol
SOH	Section OverHead (ETSI)
SONET	Synchronous Optical NETwork
SP	Service Point
SSH	Secured Shell (Protocol)
SSM	Synchronization Status Message
SSO	Single Sign-On
STP	Spanning Tree Protocol
SyncE	Synchronous Ethernet
SVCE	Service Channel Equipment
T	
TC	Traffic Class
TIM	Trace Identifier Mismatch
TOH	Transport OverHead (ANSI)

Term	Definition
TOS	Type Of Service
V	
VC	Virtual Container
VCO	Voltage Controlled Oscillator
VCXO	Voltage Controlled crystal Oscillator
VLSI	Very Large Scale of Integration
W	
WAN	Wide Area Network
Web EMS	Web-Based Element Management System
WFQ	Weighted Fair Queue
WG	Waveguide
WRED	Weighted Random Early Detection
WRR	Weighted Round Robin
X	
XCVR	Transceiver (Transmitter/Receiver)
XMTR	Transmitter
XO	Crystal Oscillator
XPD	Cross Polar Differentiation
XPI	Cross Polariztion Isolation
XPIC	Cross Polarization Interference Cancellation