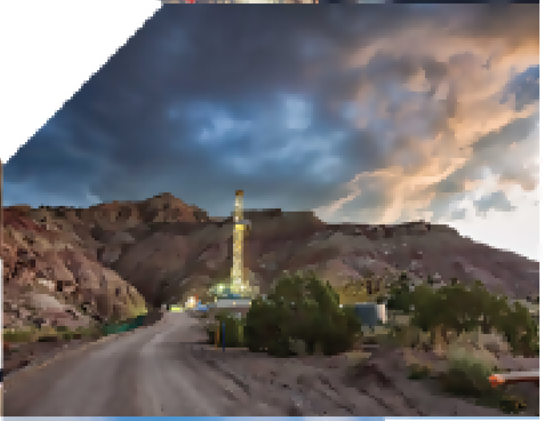
Cambium Networks™



User Guide

PTP 850EX

Release 12.7

Reservation of Rights

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 recommends reviewing the Cambium Networks website for the latest changes and updates to products. 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”).

This product is not restricted in the EU. 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.

Contents

Safety Precautions & Declared Material

General Equipment Precautions

⚠

Use of controls, adjustments, or performing procedures other than those specified herein, may result in hazardous radiation exposure.

When working with an PTP 850EX unit, note the following risk of electric shock and energy hazard: Disconnecting one power supply disconnects only one power supply module. To isolate the unit completely, disconnect all power sources.

Machine noise information order - 3. GPSGV, the highest sound pressure level amounts to 70 dB (A) or less, in accordance with ISO EN 7779.

Static electricity may cause body harm, as well as harm to electronic components inside the device.

To prevent damage, before touching components inside the device, all electrostatic charge must be discharged from both personnel and tools.

High Frequency Electromagnetic Fields!

⚠

Exposure to strong high frequency electromagnetic fields may cause thermal damage to personnel. The eye (cornea and lens) is easily exposed.

Any unnecessary exposure is undesirable and should be avoided.

In radio-relay communication installations, ordinary setup for normal operation, the general RF radiation level will be well below the safety limit.

In the antennas and directly in front of them the RF intensity normally will exceed the danger level, within limited portions of space.

Dangerous radiation may be found in the neighborhood of open waveguide flanges or horns where the power is radiated into space.

To avoid dangerous radiation, the following precautions must be taken:

- During work within and close to the front of the antenna; make sure that transmitters will remain turned off.
- Before opening coaxial - or waveguide connectors carrying RF power, turn off transmitters.
- Consider any incidentally open RF connector as carrying power, until otherwise proved. Do not look into coaxial connectors at closer than reading distance (30 cm). Do not look into an open waveguide unless you are absolutely sure that the power is turned off.

ESD

This equipment contains components which are sensitive to “ESD” (Electro Static Discharge). Therefore, ESD protection measures must be observed when touching the IDU.

Anyone responsible for the installation or maintenance of the PTP 850EX device must use an

ESD Wrist Strap.

Additional precautions include personnel grounding, grounding of work benches, grounding of tools and instruments, as well as transport and storage in special antistatic bags and boxes.

Laser

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.

CLASS 1 LASER PRODUCT
APPAREIL À LASER DE CLASSE 1
IEC60825-2:2000

The optical interface must only be serviced by qualified personnel, who are aware of the hazards involved to repair laser products.

When handling laser products, the following precautions must be taken:

- Never look directly into an open connector or optical cable.
- Before disconnecting an optical cable from the optical transmitter, the power should be switched off. If this is not possible, the cable must be disconnected from the transmitter before it is disconnected from the receiver.
- When the cable is reconnected it must be connected to the receiver before it is connected to the transmitter.

Special Requirements for North America

Grounding: This equipment is designed to permit connection between the earthed conductor of the DC supply circuit and the earthing conductor at the equipment.

Note

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Restricted Access Area: DC powered equipment should only be installed in a Restricted Access Area.

Installation Codes: The equipment must be installed according to country national electrical codes. For North America, equipment must be installed in accordance with the US National Electrical Code, Articles 110-16, 110-17 and 110-18, and the Canadian Electrical Code, Section 12.

Overcurrent Protection: A readily accessible listed branch circuit overcurrent protective device, rated 15 A, must be incorporated in the building wiring.

Grounded Supply System: The equipment shall be connected to a properly grounded supply system. All equipment in the immediate vicinity shall be grounded the same way, and shall not be grounded elsewhere.

Local Supply System: The DC supply system is to be local, i.e. within the same premises as the equipment.

Disconnect Device: A disconnect device is not allowed in the grounded circuit between the DC supply source and the frame/grounded circuit connection.

Special Requirements for Norway and Sweden

⚠ Equipment connected to the protective earthing of the building installation through the mains connection or through other equipment with a connection to protective earthing – and to a cable distribution system using coaxial cable, may in some circumstances create a fire hazard. Connection to a cable distribution system has therefore to be provided through a device providing electrical isolation below a certain frequency range (galvanic isolator, see EN 60728-11).

⚠ Utstyr som er koplet til beskyttelsesjord via nettplugg og/eller via annet jordtilkoplet utstyr – og er tilkoplet et kabel-TV nett, kan forårsake brannfare. For å unngå dette skal det ved tilkopling av utstyret til kabel-TV nettet installeres en galvanisk isolator mellom utstyret og kabel- TV nettet.

Utrustning som är kopplad till skyddsjord via jordat vägguttag och/eller via annan utrustning och samtidigt är kopplad till kabel-TV nät kan i vissa fall medfőra risk főr brand. Főr att undvika detta skall vid anslutning av utrustningen till kabel-TV nät galvanisk isolator finnas mellan utrustningen och kabel-TV nätet.

Précautions générales relatives à l'équipement

⚠ L’utilisation de commandes ou de réglages ou l'exécution de procédures autres que celles spécifiées dans les présentes peut engendrer une exposition dangereuse aux rayonnements.

L’usage de PTP 850EX’accompagne du risque suivant d'électrocution et de danger électrique : le débranchement d'une alimentation électrique ne déconnecte qu'un module d'alimentation électrique. Pour isoler complètement l'unité, il faut débrancher toutes les alimentations électriques.

Bruit de machine d’ordre - 3. GPSGV, le plus haut niveau de pression sonore s'élève à 70 dB (A) au maximum, dans le respect de la norme ISO EN 7779.

Allgemeine Vorsichtsmaßnahmen für die Anlage

⚠ Wenn andere Steuerelemente verwendet, Einstellungen vorgenommen oder Verfahren durchgeführt werden als die hier angegebenen, kann dies gefährliche Strahlung verursachen.

Beachten Sie beim Arbeiten mit PTP 850EX das folgende Stromschlag- und Gefahrenrisiko: Durch Abtrennen einer Stromquelle wird nur ein Stromversorgungsmodul abgetrennt. Um die Einheit vollständig zu isolieren, trennen Sie alle Stromversorgungen ab.

Maschinenlärminformations-Verordnung - 3. GPSGV, der höchste Schalldruckpegel beträgt 70 dB(A) oder weniger gemäß EN ISO 7779.

RoHS Compliance Declaration

Table 1 *Electronic Information Products Declaration of Hazardous/Toxic Substances20*

Component	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr VI)	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
PCB/Circuit Modules	Comply	Comply	Comply	Comply	Comply	Comply
Mechanical Parts	Comply	Comply	Comply	Comply	Comply	Comply
Cables	Comply	Comply	Comply	Comply	Comply	Comply

About This Guide

This document explains how to configure and operate PTP 850EX devices. This document applies to System Release versions 12.7 and 12.8. For a full description of feature limitations per release, refer to the Release Notes for the System Release version you are using.

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.

Note

PTP 850EX is not supported with System Release 12.8.

Target Audience

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

Related Documents

- Technical Description for PTP 850EX
- Installation Guide for PTP 850EX
- MIB Reference for PTP 850 Products
- Release Notes for System Release 12.7, PTP 850EX

Introduction

This section includes:

- PTP 850EX Overview
- Configuration Tips
- The Web-Based Element Management System
- Reference Guide to Web EMS Menu Structure (Advanced Mode)

This user guide provides instructions for configuring and operating an PTP 850EX.

PTP 850EX Overview

PTP 850EX is a compact, high-capacity, all-outdoor Ethernet backhaul system designed to operate in the E-Band frequency range. PTP 850EX provides up to 10 Gbps capacity in 1+0 configurations. PTP 850EX can operate over 250, 500, 1000, and 2000 MHz channels.

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

Note

Although System Release 12.7 supports PTP 850EX, the PTP 850EX hardware is not yet available as of the date of the System Release 12.7 GA release. For details about PTP 850EX availability, ask your Cambium representative.

Configuration Tips

This section describes common issues and how to avoid them.

- **Ethernet Port Configuration**

  The Ethernet ports of PTP 850 devices 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 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 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. See Configuring 1588 Transparent Clock.

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. See Configuring Ethernet Service(s).

For instructions on configuring in-band management, see Configuring In-Band Management.

- **Link Aggregation (LAG)**

  If you are configuring LAG with an external switch, the switch must support LAG. For instructions on configuring LAG, see Configuring Link Aggregation (LAG).

  When using IEEE 1588 PTP synchronization across a LAG link, follow the recommendations set forth in ITU-T standard G.8275.1, Annex 6 in order to prevent PTP packets from following different paths between the devices, which can lead to asymmetric delay. For instructions on configuring LAG, see Configuring Link Aggregation (LAG).

- **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 hardware type with the same part number as the unit from which they were originally saved.

The Web-Based Element Management System

This section includes:

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. Next is a page that summarizes the key security-related parameters of the unit.

A Web-Based EMS connection to the unit can be opened using a Web browser (Microsoft Edge, Mozilla Firefox, or Google Chrome). Only the latest three versions of each browser type are supported. 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

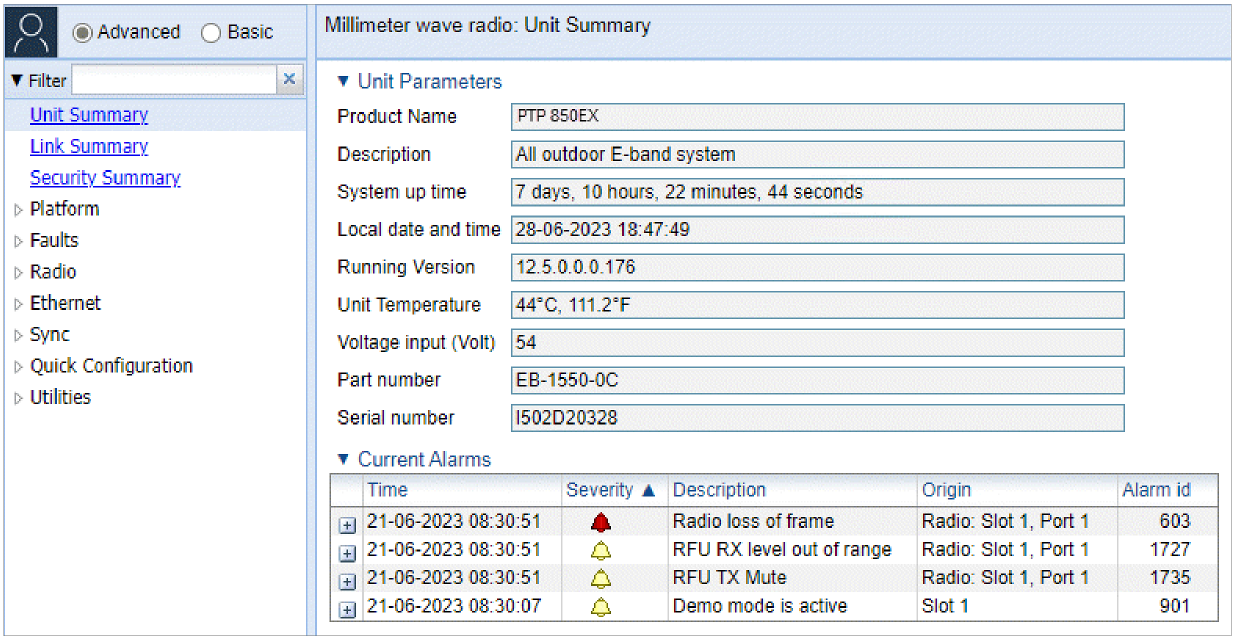
The alarms and system configuration details shown in this manual do not necessarily represent actual parameters and values on a fully operating device. Some of the pages and tasks described in this Manual may not be available to all users, based on the actual system configuration, activation key, and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

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 850EX*



Millimeter wave radio: Unit Summary

▼ Unit Parameters

Product Name	PTP 850EX
Description	All outdoor E-band system
System up time	7 days, 10 hours, 22 minutes, 44 seconds
Local date and time	28-06-2023 18:47:49
Running Version	12.5.0.0.0.176
Unit Temperature	44°C, 111.2°F
Voltage input (Volt)	54
Part number	EB-1550-0C
Serial number	I502D20328

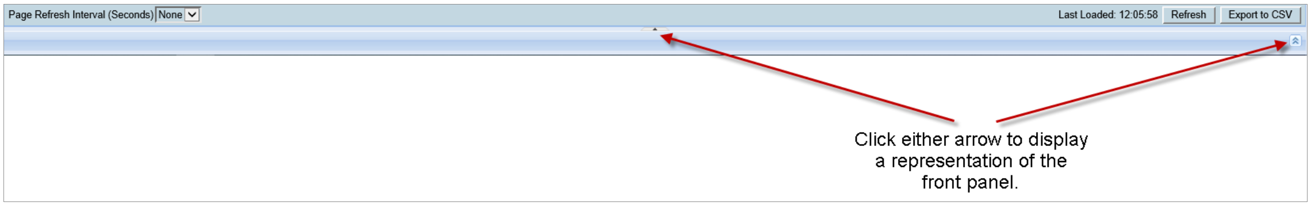
▼ Current Alarms

	Time	Severity ▲	Description	Origin	Alarm id
⊞	21-06-2023 08:30:51	🔔	Radio loss of frame	Radio: Slot 1, Port 1	603
⊞	21-06-2023 08:30:51	🔔	RFU RX level out of range	Radio: Slot 1, Port 1	1727
⊞	21-06-2023 08:30:51	🔔	RFU TX Mute	Radio: Slot 1, Port 1	1735
⊞	21-06-2023 08:30:07	🔔	Demo mode is active	Slot 1	901

Front Panel Representation

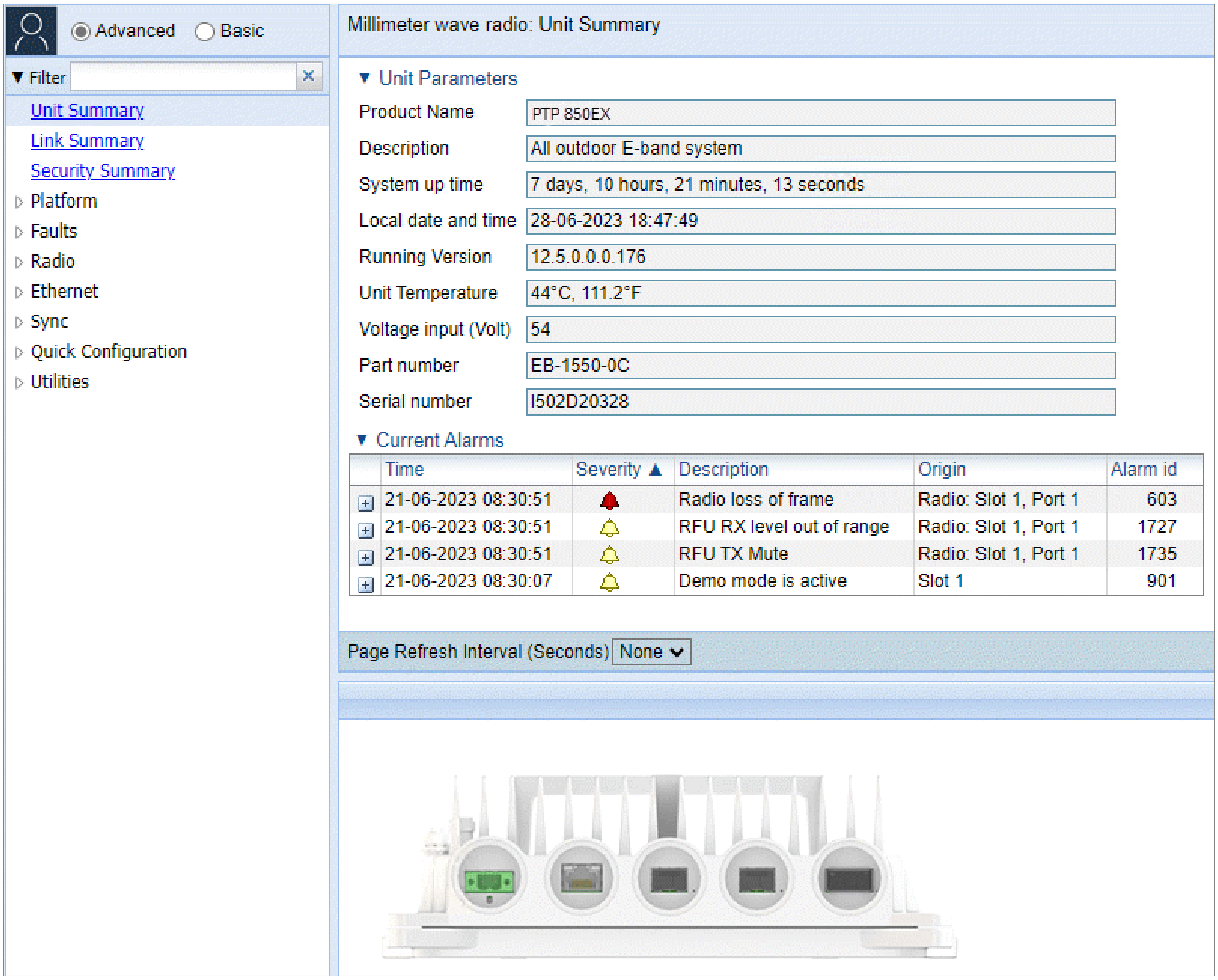
Optionally, you can display a representation of the device’s front panel by clicking either the arrow in the center or the arrow at the right of the bottom toolbar.

Figure 2 *Displaying a Representation of the Front Panel*



Click either arrow to display a representation of the front panel.

Figure 3 *Main Web EMS Page with Representation of Front Panel (PTP 850EX)*



Millimeter wave radio: Unit Summary

▼ Unit Parameters

Product Name	PTP 850EX
Description	All outdoor E-band system
System up time	7 days, 10 hours, 21 minutes, 13 seconds
Local date and time	28-06-2023 18:47:49
Running Version	12.5.0.0.176
Unit Temperature	44°C, 111.2°F
Voltage input (Volt)	54
Part number	EB-1550-0C
Serial number	I502D20328

▼ Current Alarms

	Time	Severity ▲	Description	Origin	Alarm id
⊞	21-06-2023 08:30:51	🔴	Radio loss of frame	Radio: Slot 1, Port 1	603
⊞	21-06-2023 08:30:51	🟡	RFU RX level out of range	Radio: Slot 1, Port 1	1727
⊞	21-06-2023 08:30:51	🟡	RFU TX Mute	Radio: Slot 1, Port 1	1735
⊞	21-06-2023 08:30:07	🟡	Demo mode is active	Slot 1	901

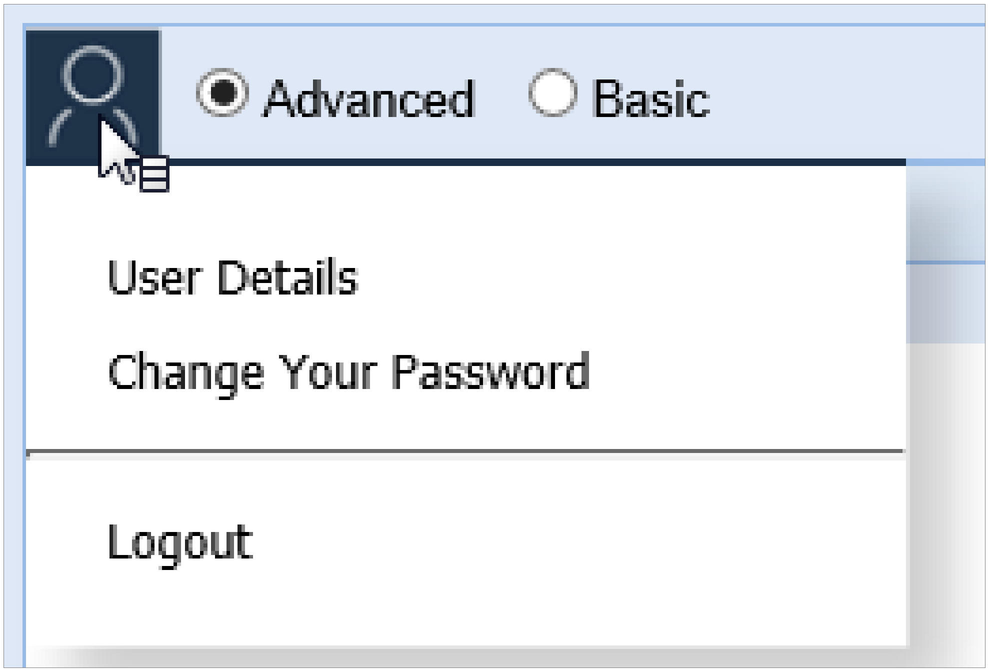
Page Refresh Interval (Seconds) None

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.

Note

For details about user and password configuration, see Access Management and Security .



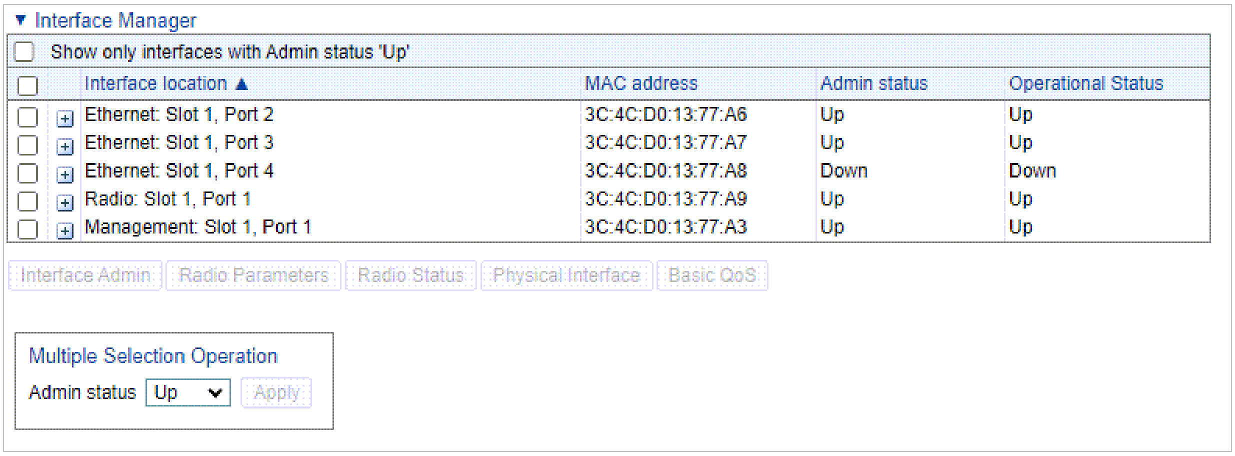
● Advanced ○ Basic

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, Interface Manager Page Showing All Interfaces (PTP 850EX) shows all interfaces and Interface Manager Page Showing Interfaces with Admin Status Up (PTP 850EX) displays only interfaces with Admin status Up after Show only interfaces with Admin status ‘Up’ has been selected.

Figure 4 *Interface Manager Page Showing All Interfaces (PTP 850EX)*



▾ Interface Manager

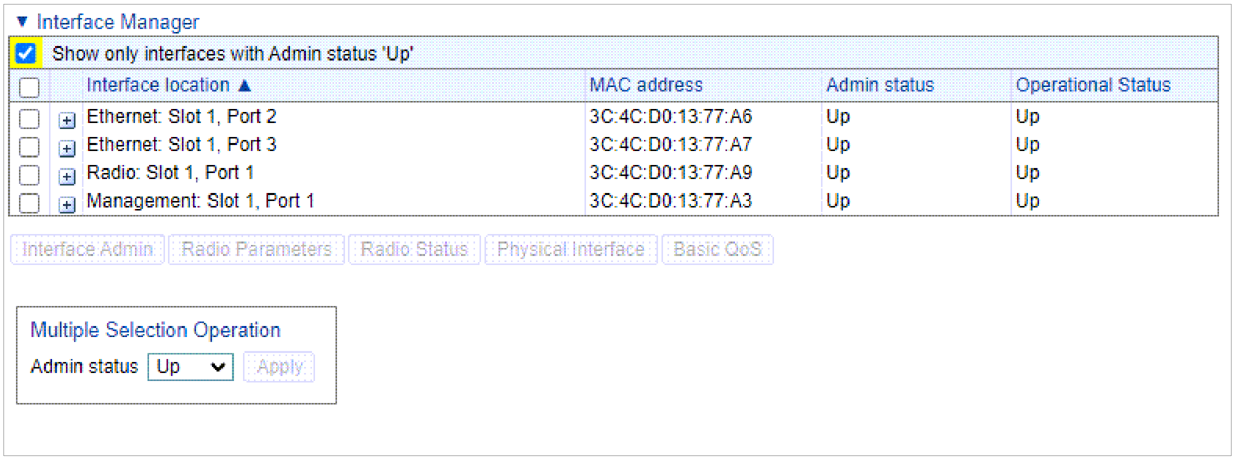
□ Show only interfaces with Admin status 'Up'

□	Interface location ▲	MAC address	Admin status	Operational Status
□	⊞ Ethernet: Slot 1, Port 2	3C:4C:D0:13:77:A6	Up	Up
□	⊞ Ethernet: Slot 1, Port 3	3C:4C:D0:13:77:A7	Up	Up
□	⊞ Ethernet: Slot 1, Port 4	3C:4C:D0:13:77:A8	Down	Down
□	⊞ Radio: Slot 1, Port 1	3C:4C:D0:13:77:A9	Up	Up
□	⊞ Management: Slot 1, Port 1	3C:4C:D0:13:77:A3	Up	Up

Multiple Selection Operation

Admin status: Up

Figure 5 *Interface Manager Page Showing Interfaces with Admin Status Up (PTP 850EX)*



▼ Interface Manager

☑ Show only interfaces with Admin status 'Up'

□	Interface location ▲	MAC address	Admin status	Operational Status
□	⊞ Ethernet: Slot 1, Port 2	3C:4C:D0:13:77:A6	Up	Up
□	⊞ Ethernet: Slot 1, Port 3	3C:4C:D0:13:77:A7	Up	Up
□	⊞ Radio: Slot 1, Port 1	3C:4C:D0:13:77:A9	Up	Up
□	⊞ Management: Slot 1, Port 1	3C:4C:D0:13:77:A3	Up	Up

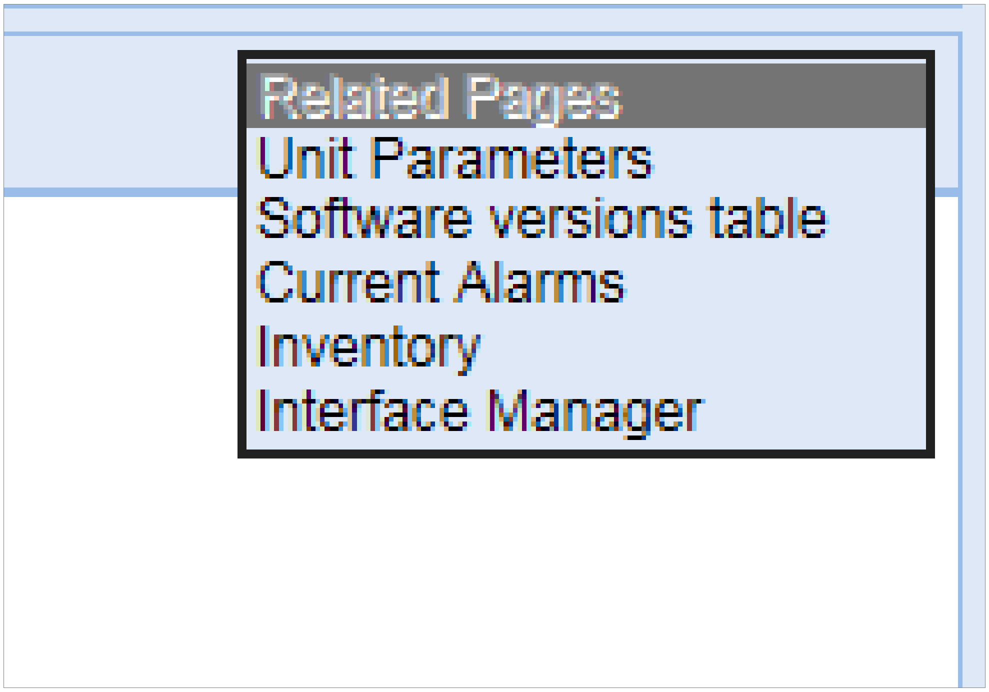
Multiple Selection Operation

Admin status: Up

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.

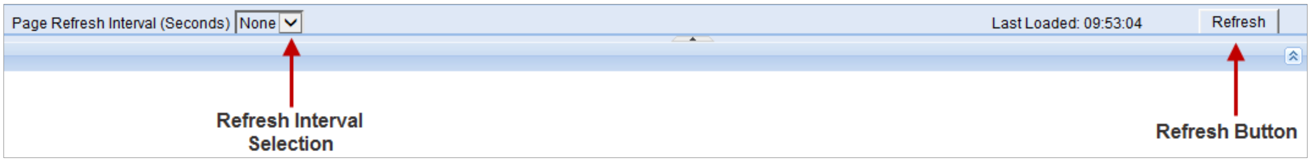
Figure 6 *Related Pages Drop-Down List*



Page Refresh and Refresh Interval

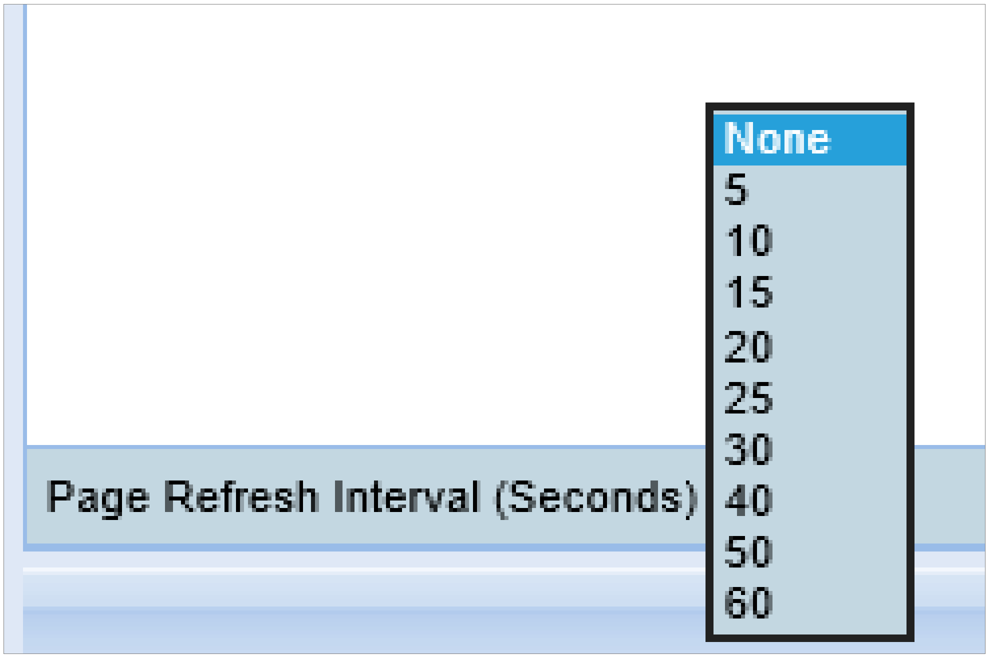
To refresh the current page in the Web EMS, click Refresh on the lower right of the page.

Figure 7 *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).

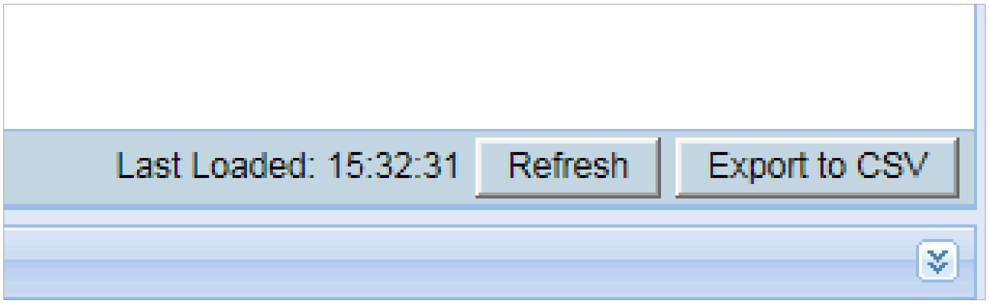
Figure 8 *Automatic Refresh Interval Drop-Down List*



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.

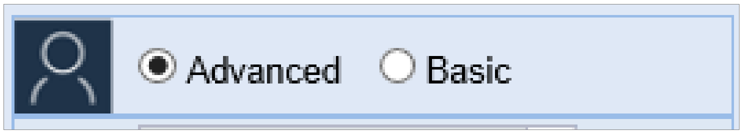
Figure 9 *Export to CSV Button*



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.

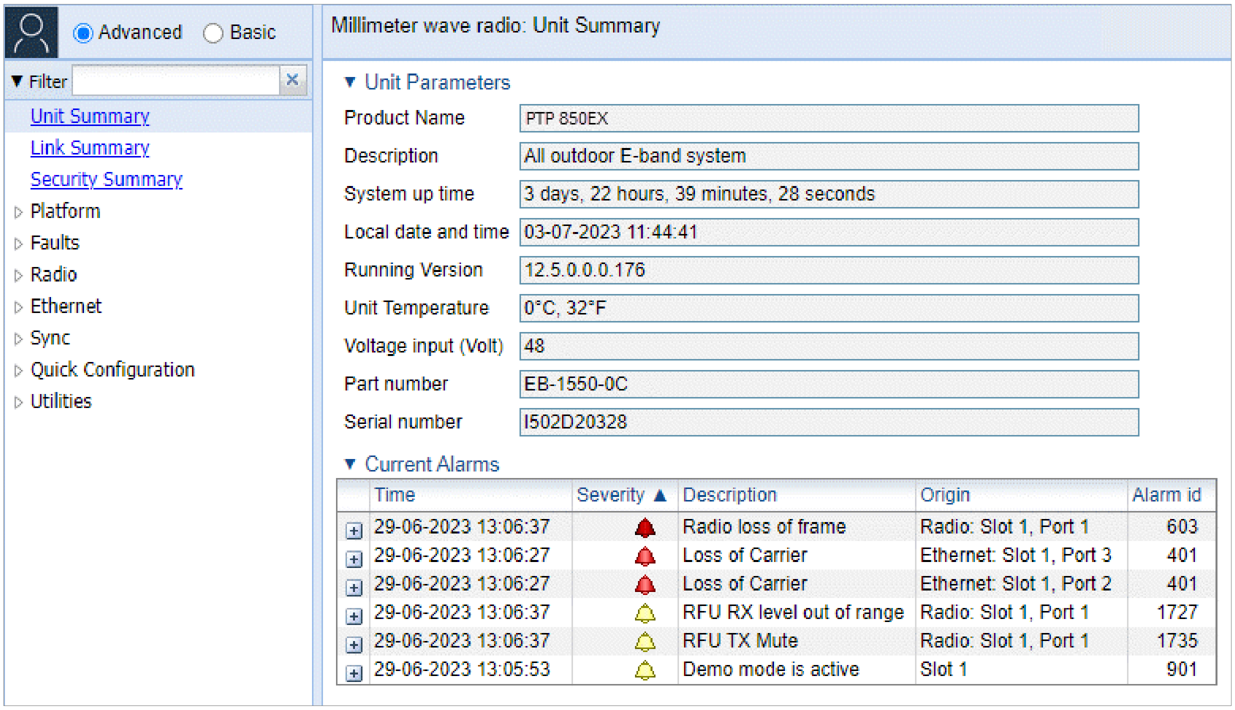
This manual includes a separate chapter to guide you through PTP 850 configuration using Basic mode, with cross-references to more detailed explanations of PTP 850 features found elsewhere in the manual. See Configuring an PTP 850 Unit Using Basic Mode.

Except in the Basic mode chapter, references to the Web EMS menu structure and screens refer to Advanced mode except when otherwise noted.

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 10 *Unit Summary Page*



Millimeter wave radio: Unit Summary

▼ Unit Parameters

Product Name	PTP 850EX
Description	All outdoor E-band system
System up time	3 days, 22 hours, 39 minutes, 28 seconds
Local date and time	03-07-2023 11:44:41
Running Version	12.5.0.0.0.176
Unit Temperature	0°C, 32°F
Voltage input (Volt)	48
Part number	EB-1550-0C
Serial number	I502D20328

▼ Current Alarms

	Time	Severity ▲	Description	Origin	Alarm id
⊞	29-06-2023 13:06:37	🔴	Radio loss of frame	Radio: Slot 1, Port 1	603
⊞	29-06-2023 13:06:27	🔴	Loss of Carrier	Ethernet: Slot 1, Port 3	401
⊞	29-06-2023 13:06:27	🔴	Loss of Carrier	Ethernet: Slot 1, Port 2	401
⊞	29-06-2023 13:06:37	🟡	RFU RX level out of range	Radio: Slot 1, Port 1	1727
⊞	29-06-2023 13:06:37	🟡	RFU TX Mute	Radio: Slot 1, Port 1	1735
⊞	29-06-2023 13:05:53	🟡	Demo mode is active	Slot 1	901

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.

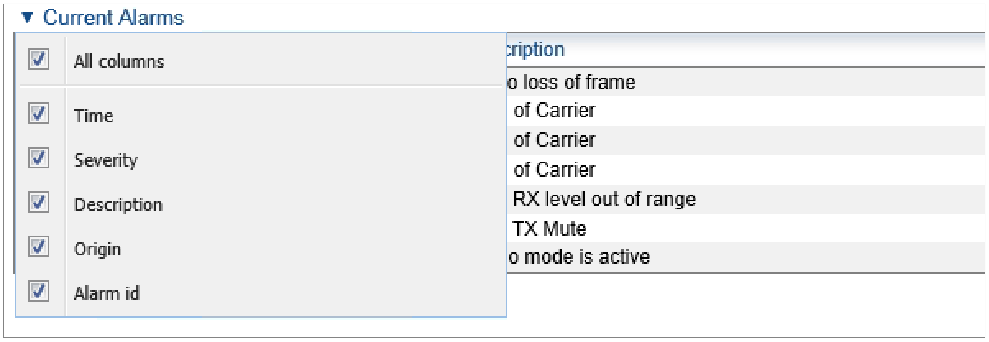
To hide a specific section of the Unit Summary page, click the section title. To display a section that has been hidden, click the section title again.

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 11 *Unit Summary Page – Customizing Columns*



▼ Current Alarms

☑ All columns

☑ Time

☑ Severity

☑ Description

☑ Origin

☑ Alarm id

cription

o loss of frame

of Carrier

of Carrier

of Carrier

RX level out of range

TX Mute

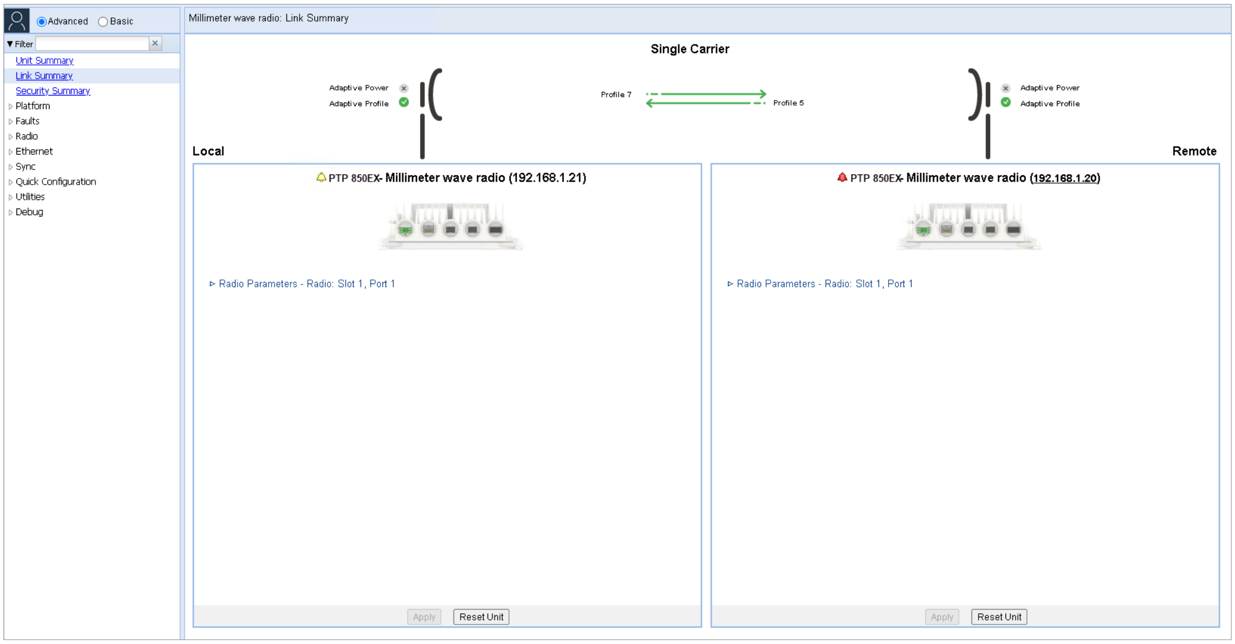
o mode is active

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 12 *Link Summary Page (PTP 850EX)*



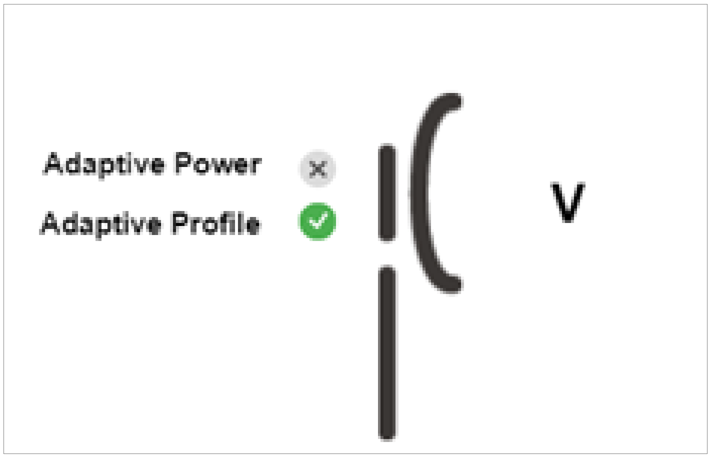
The Link Summary page includes the following information:

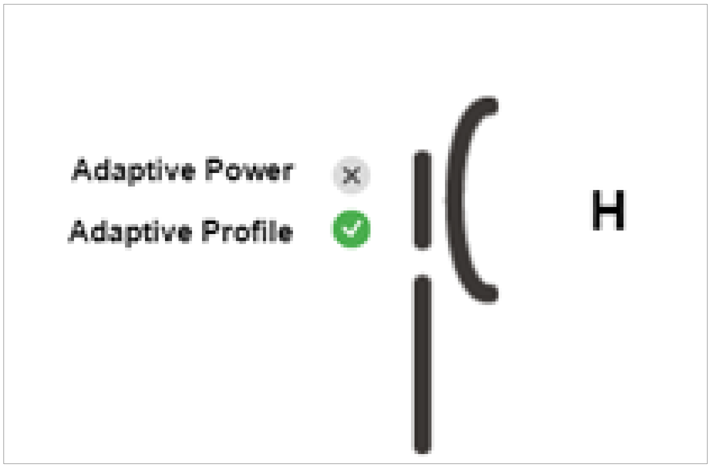
- **Type of Link** – The Link Summary page indicates at the top what kind of link is operating.
- **State of Link** – The color of the arrows indicates whether the link is Up or Down, as follows:
- ⇄ - Link is Up (green).
- ⇄ - Link is Down because the radio is not transmitting (mute) (grey).
- ⇄ - Link is Down because the radio is not receiving (red).
- **ACM Profile –** The Link Summary page displays the current operating ACM profile for each link direction. See Configuring the Radio (MRMC) Script(s).
- **Adaptive Power –** Indicates for each side of the link and each radio whether Adaptive TX Power is enabled (✓) or disabled (✗). See Configuring the Radio Parameters.
- **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 Configuring the Radio (MRMC) Script(s).
- **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:

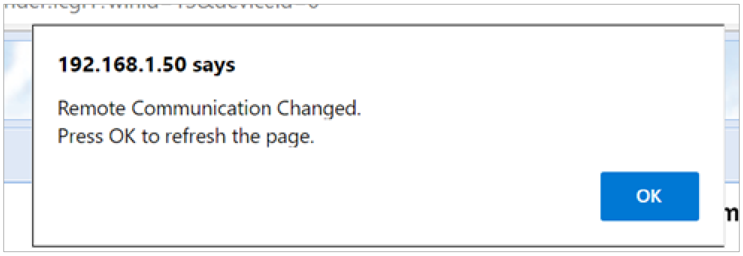
Note

For PTP 850EX, support for XPIC is planned for future release.





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



192.168.1.50 says

Remote Communication Changed.
Press OK 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

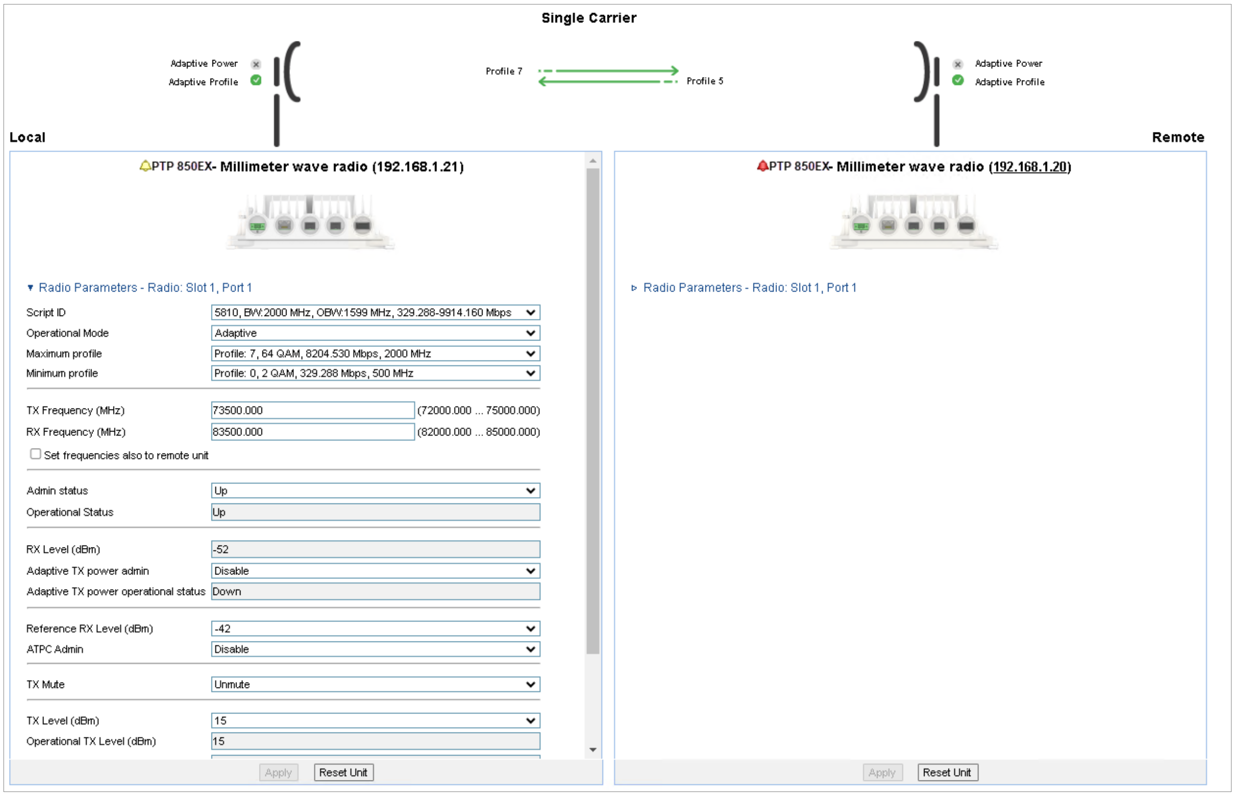
Radio Parameters. For links with two radio carriers, click Radio Parameters for the radio interface you want to display or configure.

The parameters available in the Link Summary page include:

- **MRMC script parameters** – See Configuring the Radio (MRMC) Script(s).
- **TX and RX Frequency** – See Configuring the Radio Parameters.
- **Admin and Operational Status** (Local only) – See Viewing the Radio Status and Settings.
- **RX Level and Adaptive TX Power** – See Configuring the Radio Parameters and Viewing the Radio Status and Settings.
- **ATPC** – See Configuring ATPC and ATPC Override Timer.
- **TX Mute** – See Configuring the Radio Parameters.
- **TX Level** – See Configuring the Radio Parameters.

> **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 13 *Link Summary Page – Radio Parameters (PTP 850EX)*



PTP 850EX- Millimeter wave radio (192.168.1.21)

▾ Radio Parameters - Radio: Slot 1, Port 1

Script ID	5810, BW:2000 MHz, OBW:1599 MHz, 329.288-9914.160 Mbps
Operational Mode	Adaptive
Maximum profile	Profile: 7, 64 QAM, 8204.530 Mbps, 2000 MHz
Minimum profile	Profile: 0, 2 QAM, 329.288 Mbps, 500 MHz
TX Frequency (MHz)	73500.000 (72000.000 ... 75000.000)
RX Frequency (MHz)	83500.000 (82000.000 ... 85000.000)
☐ Set frequencies also to remote unit	
Admin status	Up
Operational Status	Up
RX Level (dBm)	-52
Adaptive TX power admin	Disable
Adaptive TX power operational status	Down
Reference RX Level (dBm)	-42
ATPC Admin	Disable
TX Mute	Unmute
TX Level (dBm)	15
Operational TX Level (dBm)	15

PTP 850EX- Millimeter wave radio (192.168.1.20)

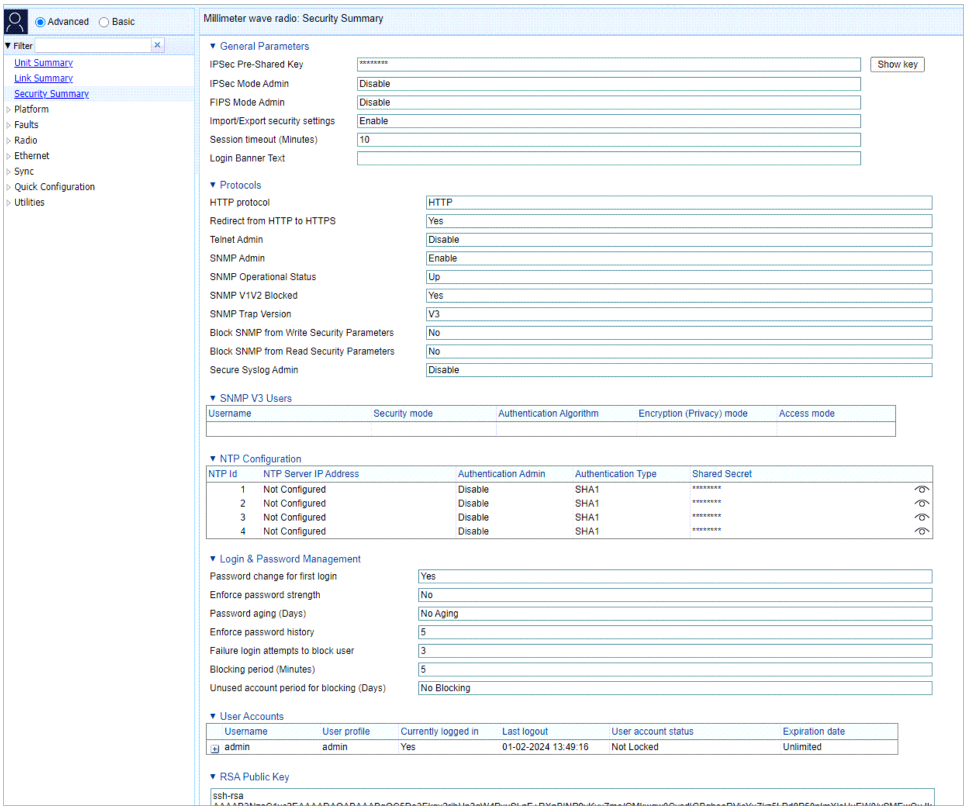
▹ Radio Parameters - Radio: Slot 1, Port 1

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 14 *Security Summary Page*



Millimeter wave radio: Security Summary

General Parameters

IPSec Pre-Shared Key	********
IPSec Mode Admin	Disable
FIPS Mode Admin	Disable
Import/Export security settings	Enable
Session timeout (Minutes)	10
Login Banner Text	

Protocols

HTTP protocol	HTTP
Redirect from HTTP to HTTPS	Yes
Telnet Admin	Disable
SNMP Admin	Enable
SNMP Operational Status	Up
SNMP V1V2 Blocked	Yes
SNMP Trap Version	V3
Block SNMP from Write Security Parameters	No
Block SNMP from Read Security Parameters	No
Secure Syslog Admin	Disable

SNMP V3 Users

Username	Security mode	Authentication Algorithm	Encryption (Privacy) mode	Access mode

NTP Configuration

NTP Id	NTP Server IP Address	Authentication Admin	Authentication Type	Shared Secret
1	Not Configured	Disable	SHA1	********
2	Not Configured	Disable	SHA1	********
3	Not Configured	Disable	SHA1	********
4	Not Configured	Disable	SHA1	********

Login & Password Management

Password change for first login	Yes
Enforce password strength	No
Password aging (Days)	No Aging
Enforce password history	5
Failure login attempts to block user	3
Blocking period (Minutes)	5
Unused account period for blocking (Days)	No Blocking

User Accounts

Username	User profile	Currently logged in	Last logout	User account status	Expiration date
admin	admin	Yes	01-02-2024 13:49:16	Not Locked	Unlimited

RSA Public Key

ssh-rsa

The Security Summary page includes:

- **General Parameters** – Includes the following fields:
  - IPSec Pre-Shared Key – Planned for future release.
  - IPSec Mode Admin – Planned for future release.
  - FIPS Mode Admin – Planned for future release.
  - Import/Export security settings – See Importing and Exporting 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 Enabling 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.
- **NTP Configuration** – Displays a list of NTP servers and their security configuration status. For additional information, see Configuring NTP.
- **Login & Password Management** – Displays login and password security parameters configured on the device. See Configuring the General Access Control Parameters.
- **User Accounts** – Displays a list of users configured for the device and their parameters. See Configuring Users.
- **RSA Public 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.

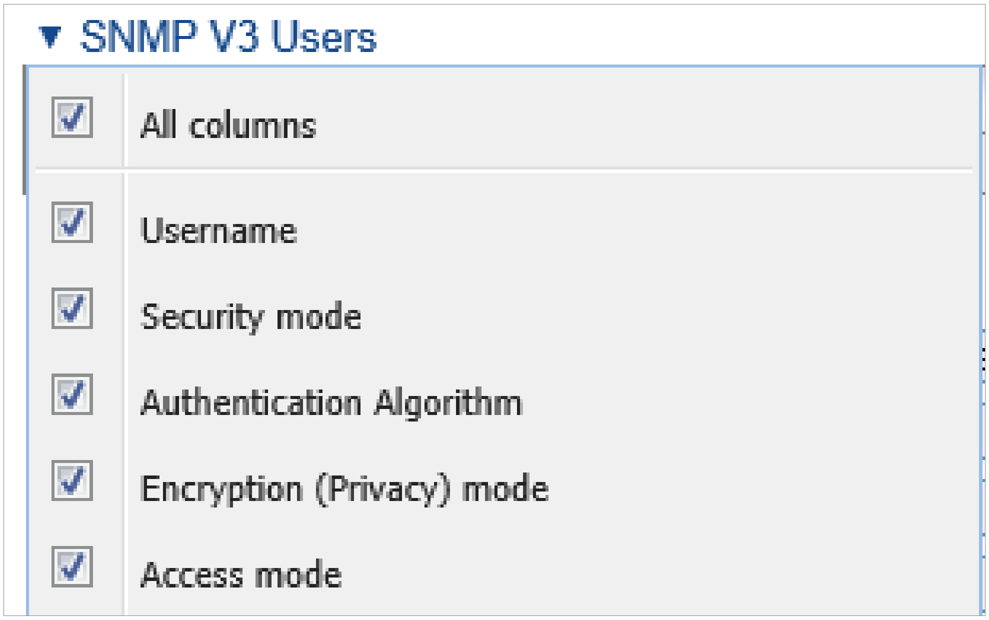
To hide a specific section of the Security Summary page, click the section title. To display a section that has been hidden, click the section title again.

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 15 *Security Summary Page – Customizing Columns*



▼ SNMP V3 Users

☑ All columns

☑ Username

☑ Security mode

☑ Authentication Algorithm

☑ Encryption (Privacy) mode

☑ Access mode

Reference Guide to Web EMS Menu Structure (Advanced Mode)

The following table shows the Web EMS menu hierarchy for Advanced mode, 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 2 *Web EMS Menu Hierarchy – Platform Menu*

Sub-Menus	For Further Information
Shelf Management > Chassis Configuration	Performing a Unit Reset
Shelf Management > Unit Redundancy	Planned for future release.
Interfaces > Interface Manager	Enabling the Interfaces (Interface Manager)
Interfaces > SFP	Planned for future release.
Interfaces > Traffic over Management	Planned for future release.
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 > Remote SysLog	Configuring Syslog
Management > Unit Info	Uploading Unit Info
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 Enabling Dynamic IPv6 Addresses Via DHCPv6 Configuring DSCP/TC for Management
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.

Sub-Menus	For Further Information
Configuration > Backup Files	Viewing Current Backup Files
Configuration > Configuration Management	Backing Up and Restoring Configurations
Activation Key & Usage > Activation Key Configuration	Configuring the Activation Key
Activation Key & Usage > Activation Key & Usage Table	Displaying a List of Activation-Key-Enabled Features
Activation Key & Usage > Usage Mode Overview	Only used with Smart Activation Key. For more information, refer to the Smart Activation Key User Guide.
Security > General > Configuration	Importing and Exporting Security Settings
Security > General > Security Log Upload	Uploading the Security Log
Security > General > Configuration Log Upload	Uploading the Configuration Log
Security > User Access Control > General	Configuring the General Access Control Parameters
Security > User Access Control > User Profiles	Configuring User Profiles
Security > User Access Control > User Accounts	Adding User Accounts
Security > User Access Control > Password Management	Configuring the Password Security Parameters
Security > User Access Control > Change Password	Changing Your Password
Security > User Access Control > Remote Access Control > Configuration	Configuring RADIUSTo check the logs each time a user connects to the server, enter:radius –X &
Security > User Access Control > Remote Access Control > Users	Viewing Remote Access User Connectivity and Permissions
Security > X.509 Certificate > CSR	Configuring X.509 CSR Certificates
Security > X.509 Certificate > Download & Install	Configuring X.509 CSR Certificates
Security > Access Control List	Configuring Access Control Lists
Security > RSA Key	Downloading and Installing an RSA Key
Security > Protocols Control	Configuring the Session Timeout Enabling HTTPS

Sub-Menus	For Further Information
	Enabling Telnet Access
PM & Statistics > SFP	Displaying SFP DDM and Inventory Information
PM & Statistics > Voltage	Configuring Voltage Alarm Thresholds and Displaying Voltage PMs

Table 3 *Web EMS Menu Hierarchy – Faults Menu*

Sub-Menus	For Further Information
Current Alarms	Viewing Current Alarms
Alarm Statistics	Viewing Alarm Statistics
Event Log	Viewing and Saving the Event Log
Alarm Configuration	Editing Alarm Text and Severity and Disabling Alarms and Events
Voltage Alarm Configuration	Configuring Voltage Alarm Thresholds and Displaying Voltage PMs

Table 4 *Web EMS Menu Hierarchy – Radio Menu*

Sub-Menus	For Further Information
Radio Parameters	Configuring the Radio Parameters
Frequency Scanner	Planned for future release (PTP 850EX only).
Remote Radio Parameters	Configuring the Remote Radio Parameters
Radio BER	Configuring BER Thresholds and Displaying Current BER
ATPC	Configuring ATPC and ATPC Override Timer
E-stabilizer	PTP 850EX only. Refer to the Installation and User Guide for E-Stabilizer
MRMC > Symmetrical Scripts > ETSI	Configuring the Radio (MRMC) Script(s)
MRMC > Symmetrical Scripts > FCC	Configuring the Radio (MRMC) Script(s)
MRMC > MRMC Status	Displaying MRMC Status
PM & Statistics > Counters	Displaying and Clearing Defective Block Counters
PM & Statistics > Signal Level	Displaying Signal Level PMs and Configuring Signal Level PM Thresholds
PM & Statistics > Aggregate	Displaying Modem BER (Aggregate) PMs
PM & Statistics > MSE	Displaying MSE PMs and Configuring MSE PM Thresholds
PM & Statistics > XPI	Displaying XPI PMs and Configuring XPI PM Thresholds
PM & Statistics > MRMC	Displaying MRMC PMs and Configuring ACM Profile

Sub-Menus	For Further Information
	Thresholds
PM & Statistics > Traffic > Capacity/Throughput	Displaying Capacity and Throughput PMs
PM & Statistics > Traffic > Utilization	Displaying Utilization PMs and Configuring Utilization Thresholds
PM & Statistics > Traffic > E-Stabilizer	PTP 850EX only. Refer to the Installation and User Guide for E-Stabilizer
Diagnostics > Loopback	Performing Radio Loopback
Groups > AMCC	Planned for future release.

Table 5 *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 Egress Byte Compensation Assigning WRED Profiles to Queues Assigning a Queue Shaper Profile to a Queue Assigning a Priority Profile to an Interface Assigning a Queue WFQ Profile to an Interface
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
QoS > Classification > 802.1Q	Modifying the C-VLAN 802.1Q UP and CFI Bit Classification Table

Sub-Menus	For Further Information
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 and 802.1AD	Modifying the Marking Table
QoS > WRED > WRED Profile	Configuring WRED
QoS > Shaper > Queue Profiles	Configuring Queue Shaper Profiles
QoS > Shaper > Service Bundle Profiles	Configuring Service Bundle Shaper Profiles
QoS > Scheduler > Priority Profiles	Configuring Priority Profiles
QoS > Scheduler > WFQ Profiles	Configuring Queue WFQ Profiles
Protocols > Bandwidth Notification	Configuring Ethernet Bandwidth Notification (ETH-BN)
Protocols > G.8032 > General Attribute	Configuring the Destination MAC Address
Protocols > G.8032 > ERPI Attribute	Adding ERPIs through Viewing ERPI Statistics
Protocols > MSTP > Bridge > General Attributes	Enabling MSTP and Configuring the MSTP Bridge General Attributes
Protocols > MSTP > Bridge > Configuration ID	Viewing and Configuring the MSTP Bridge Configuration ID
Protocols > MSTP > Bridge > Spanning Tree	Viewing and Configuring the MSTP Bridge Spanning Tree
Protocols > MSTP > Bridge > CIST	Viewing and Configuring the MSTP Bridge CIST Parameters
Protocols > MSTP > Bridge > MSTI	Viewing and Configuring the MSTP Bridge MSTI Parameters
Protocols > MSTP > Bridge > VLAN	Viewing the MSTP VLAN Parameters
Protocols > MSTP > Port > Spanning Tree	Viewing and Configuring the MSTP Port Spanning Tree
Protocols > MSTP > Port > CIST	Viewing and Configuring the MSTP Port CIST Parameters
Protocols > MSTP > Port > MSTI	Viewing and Configuring the MSTP Port MSTI Parameters

Sub-Menus	For Further Information
Protocols > MSTP > Port > BPDU Counters	Viewing and Resetting the BPDU Counters
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.
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	Configuring Link Aggregation (LAG)
Protocols > LACP > Port > Status	Configuring Link Aggregation (LAG)
Protocols > LACP > Port > Statistics	Configuring Link Aggregation (LAG)
Protocols > LACP > Port > Debug	Configuring Link Aggregation (LAG)

Sub-Menus	For Further Information
Groups > LAG	Configuring Link Aggregation (LAG)

Table 6 *Web EMS Menu Hierarchy – Sync Menu*

Sub-Menus	For Further Information
Sync Source	Configuring the Sync Source
Outgoing Clock	Configuring the Outgoing Clock and SSM Messages
1588 > General Configuration	Configuring 1588 Transparent Clock Configuring 1588 Boundary Clock
1588 > Transparent Clock	Configuring 1588 Transparent Clock
1588 > Boundary Clock > Clock Parameters > Default	Configuring 1588 Boundary Clock
1588 > Boundary Clock > Clock Parameters > Advanced	Configuring 1588 Boundary Clock
1588 > Boundary Clock > Port Parameters	Configuring 1588 Boundary Clock
1588 > Boundary Clock > Port Statistics	Configuring 1588 Boundary Clock

Table 7 *Web EMS Menu Hierarchy – Quick Configuration Menu*

Sub-Menus	For Further Information
From NMS	Applying a Pre-Defined Configuration File
Platform Setup	Performing Quick Platform Setup
Security > General Parameters	Quick Security Configuration – General Parameters Page
Security > Protocols	Quick Security Configuration – Protocols Page
Security > User Access Control	Quick Security Configuration – Access Control Page
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 > Multi Carrier ABC > 2 + 0	Configuring a 2+0 Multi-Carrier ABC Link Using the Quick Configuration Wizard
PIPE > Link Bonding > Configure as Attached	Configuring PTP 850EX as an Attached Unit in a Layer 1 Link Bonding Group

Table 8 *Web EMS Menu Hierarchy – Utilities Menu*

Sub-Menus	For Further Information
Restart HTTP	Restarting the HTTP Server

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

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:

- 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)
- Configuring the Radio Parameters
- Creating Service(s) for Traffic

Assigning IP Addresses in the Network

Before a remote connection is established, it is of high importance that you assign the PTP 850 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 850 unit has the following IP settings:

- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0

⚠ **Warning**

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

Establishing a Connection

Connect the device to a PC by means of a TP 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.

PC Setup

To obtain contact between the PC and the PTP 850 device, it is necessary to configure an IP address on the PC within the same subnet as the PTP 850 device. 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.

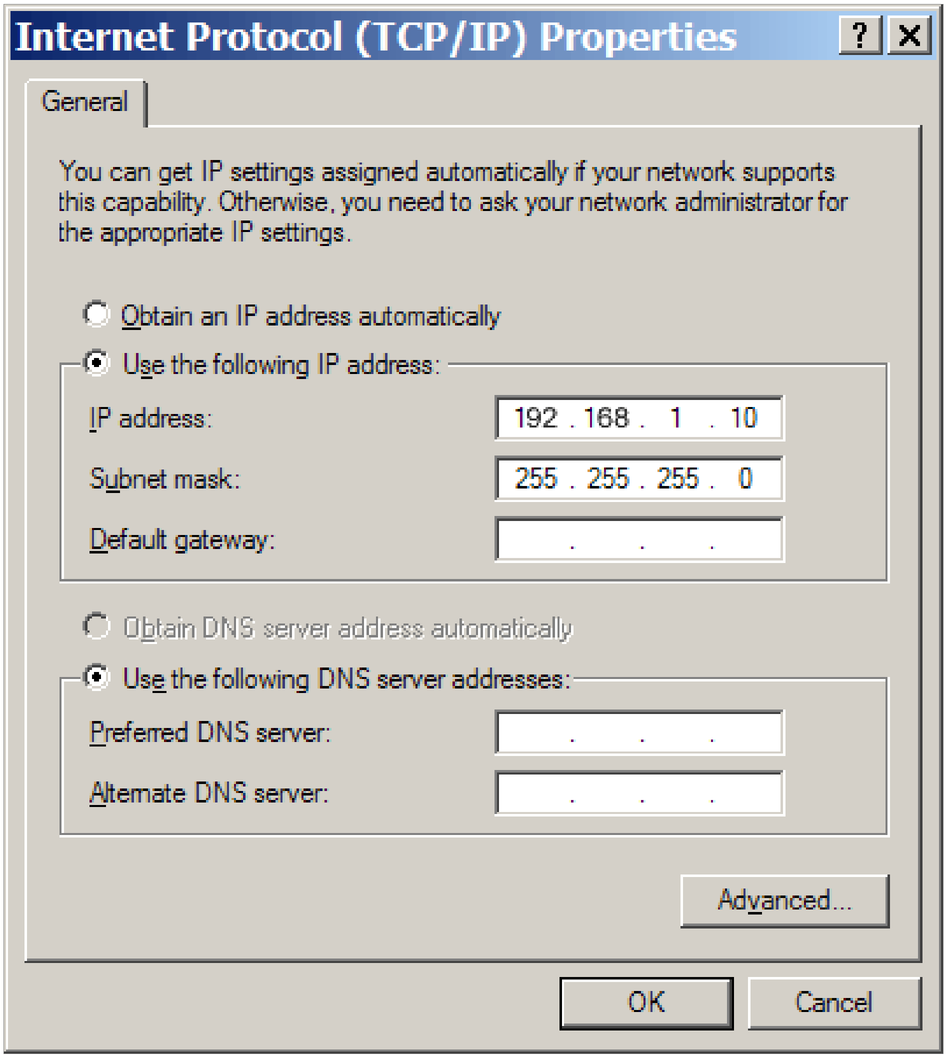
Note

The PTP 850 IP address, as well as the password, should be changed before operating the device. See Changing the Management IP Address and Changing Your Password. In Basic mode, select Platform > IP Configuration to change the device’s IP address. To change your password, click 👤 on the upper left of any Web EMS screen and select Change 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 16 *Internet Protocol Properties Window*



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

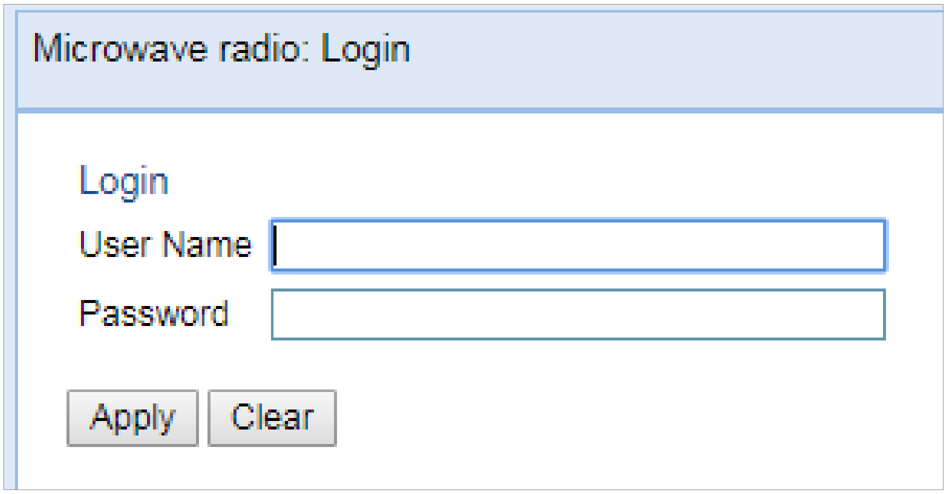
Preferred DNS server: . . .

Alternate DNS server: . . .

Logging on

1. Open an Internet browser (Microsoft Edge, Mozilla Firefox, or Google Chrome).
2. Enter the default IP address “**192.168.1.1**” in the Address Bar. The Login page opens.

Figure 17 *Login Page*



Microwave radio: Login

Login

User Name

Password

3. In the Login window, enter the following:
    - User Name: **admin**
    - Password: **admin**
4. Click **Apply**.

Note

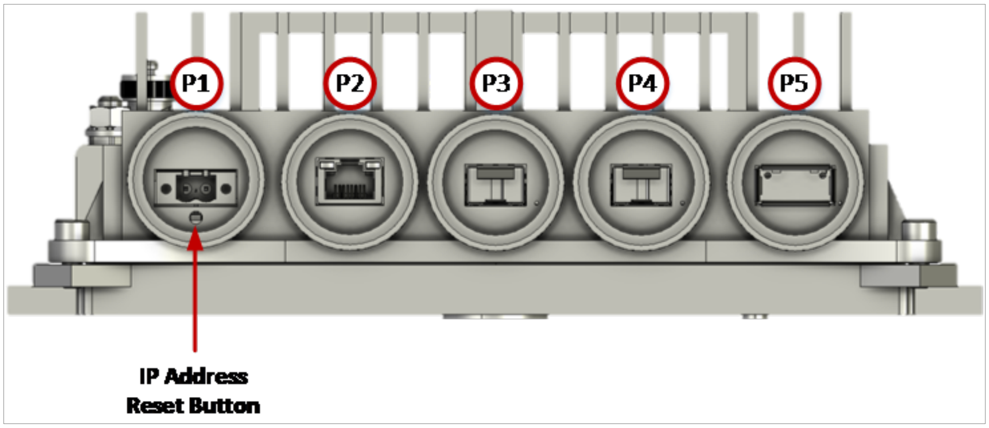
If the IP address is forgotten, you can access the device in the following ways:

- For PTP 850EX, there is a button that resets the IP address. See Resetting the IP Address (PTP 850EX Only).

For additional security, you can disable the Management and Protection ports. This eliminates the possibility of logging in directly to the CPU. See Disabling the Management and Protection/XPIC Interfaces.

Resetting the IP Address (PTP 850EX Only)

If the unit's IP address on an PTP 850EX has been changed from its default of 192.168.1.1, and you do not know the new IP address, you can reset the IP address by pressing a reset button underneath the DC Power Interface (P1). You must press the button for at least ten seconds.



Disabling the Management and Protection/XPIC Interfaces

If you want to prevent local access to the device, you must disable both the Management interface and the Protection/XPIC interface on an PTP 850EX . If the Management and Protection/XPIC interfaces are both disabled (PTP 850EX), , it will not be possible to access the device except through in-band management. Therefore, before disabling the Management and Protection/XPIC interfaces, you must make sure that in-band management of the device is properly configured and available.

Warning

Disabling the Management and Protection/XPIC interfaces without ensuring proper in-band management configuration will require RMA at the customer's expense.

To disable the Management interface on an PTP 850EX set the port to Admin = Disable in the Interface Manager. See Enabling the Interfaces (Interface Manager).

To disable the Protection/XPIC interface on an PTP 850EX, enter the following CLI command:

```
root>platform management protection interface set disable
```

To enable the Protection/XPIC interface, enter the following CLI command:

```
root>platform management protection interface set enable
```

Changing Your Password

It is recommended to change your default Admin password as soon as you have logged into the system. If the default Admin password is not changed within ten days after the first unit boot up, or the first unit boot up after upgrading to System Release 12.0 or higher from an earlier System Release version, an alarm is raised:

- 5051 – 'admin' user password needs to be changed (Alarm)

Note

If the system reboots within ten days, the 10 day count starts over.

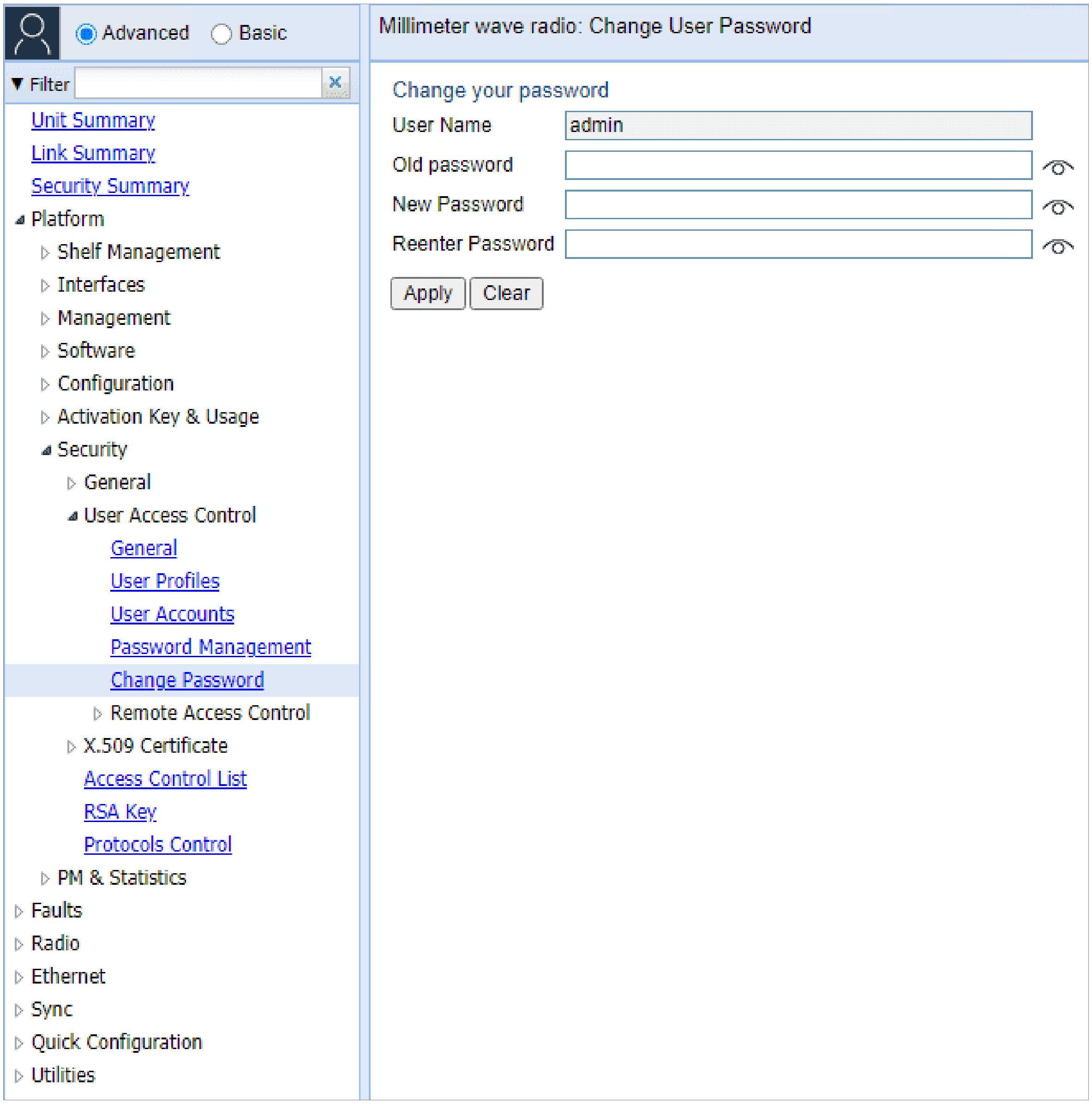
In addition to the Admin password, there is an additional password protected user account, “root user”, which is configured in the system. The root user password and instructions for changing this password are available from Cambium Customer Support. It is strongly recommended to change this password.

To change your password, click 👤 on the upper left of any Web EMS screen and select **Change Your Password**.

In Advanced mode, you can also change your password as follows:

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

Figure 18 *Change User Password Page*



Millimeter wave radio: Change User Password

Change your password

User Name: admin

Old password:

New Password:

Reenter Password:

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

3. 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.
    - 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*.

4. Click **Apply**.

Applying a Pre-Defined Configuration File

PTP 850 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 850 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
  - LAG
  - Unit Redundancy
  - Advanced radio configuration
- Services configuration
  - Management
  - Point-to-Point
  - Multipoint

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

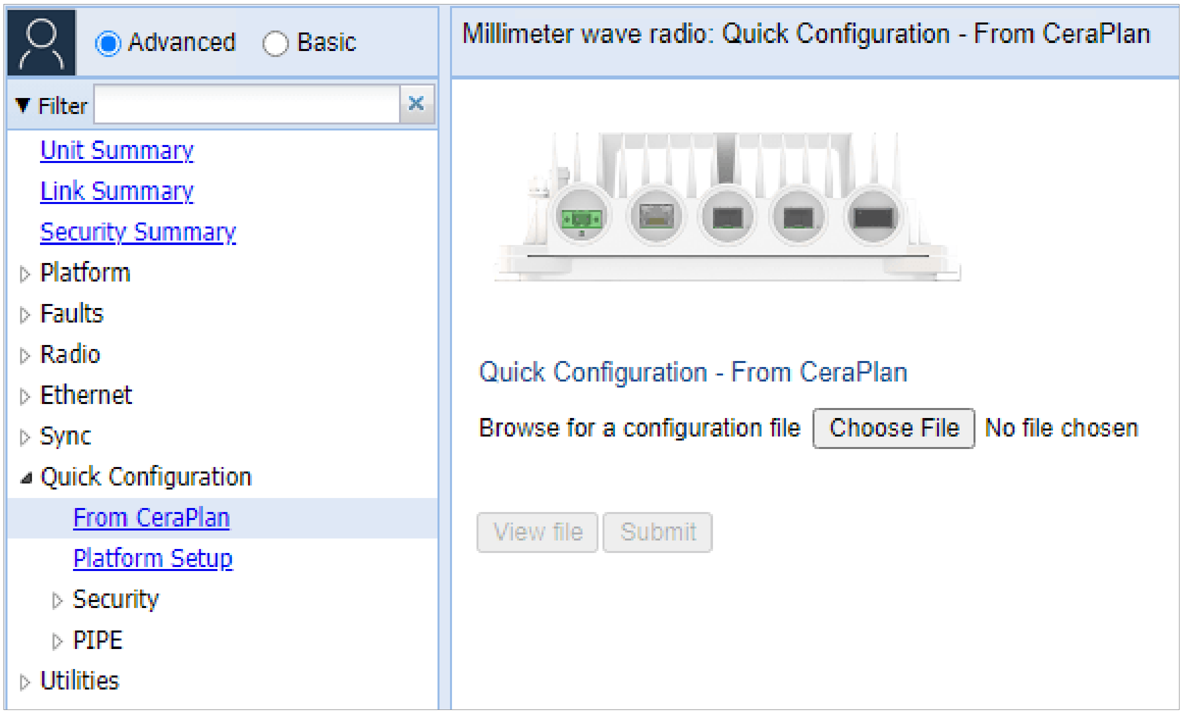
The pre-defined configuration file must be compatible with the System Release version the PTP 850 device is running. Configuration files must also be compatible with the type of device.

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

You can apply a pre-defined configuration file from Advanced mode or Basic mode. To apply a pre-defined configuration file:

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

Figure 19 *Quick Configuration – From File Page*



● Advanced ○ Basic

Millimeter wave radio: Quick Configuration - From CeraPlan

Quick Configuration - From CeraPlan

Browse for a configuration file Choose File No file chosen

2. Click **Choose File**, and select the configuration file for your unit.
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 850 unit's new IP address.

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

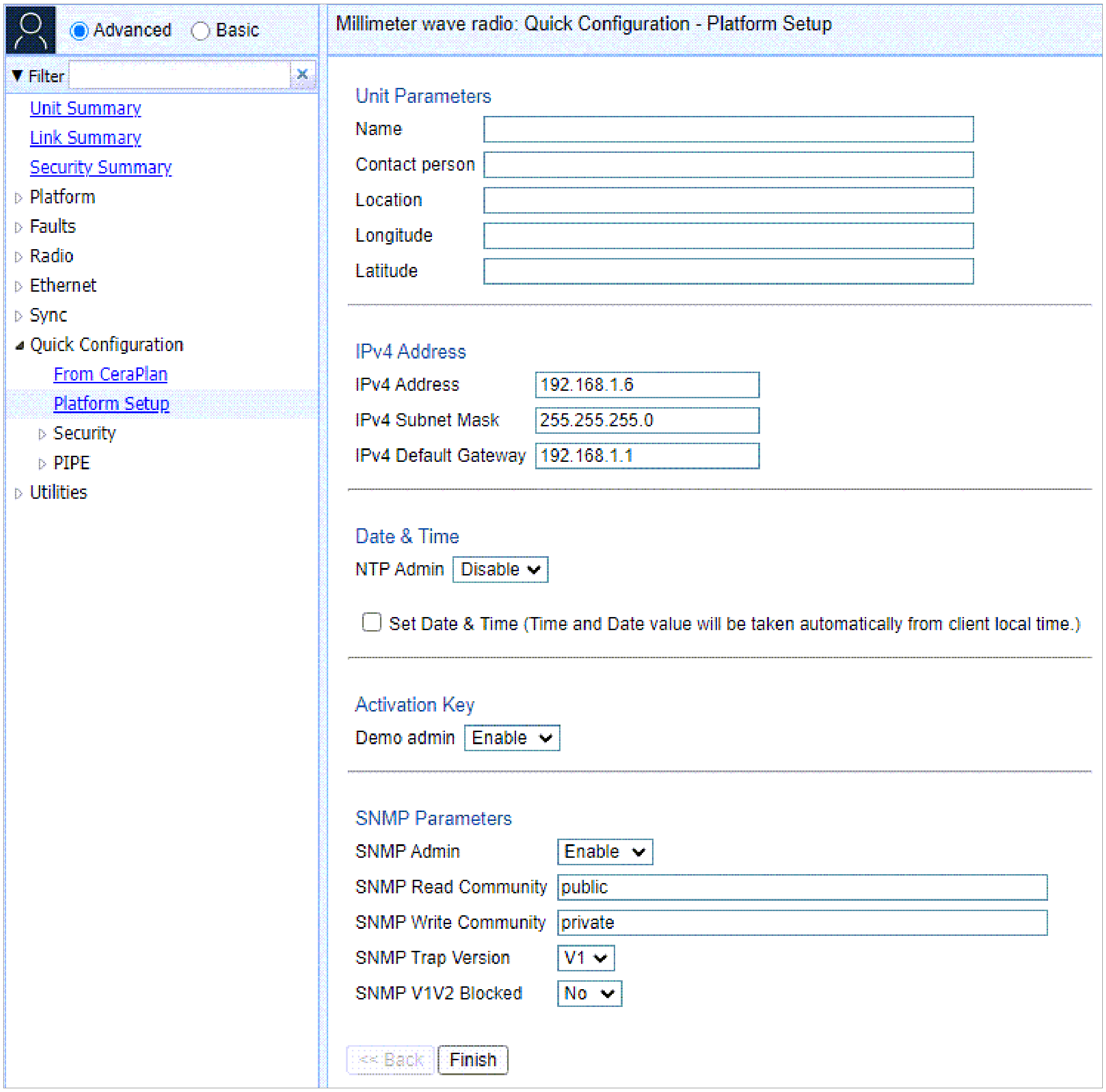
These items enable you to configure the basic platform parameters quickly, in a single Web EMS page. Combined with the quick link configuration wizards, this enables you to configure a new link in the field quickly and efficiently, to the point where the link is up and functioning and any necessary advanced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

> **Note**
>
> The Platform Setup page is only available in Advanced mode.

To use the Platform Setup page:

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

Figure 20 *Quick Configuration – Platform Setup Page*



Millimeter wave radio: Quick Configuration - Platform Setup

Unit Parameters

Name
Contact person
Location
Longitude
Latitude

IPv4 Address

IPv4 Address: 192.168.1.6
IPv4 Subnet Mask: 255.255.255.0
IPv4 Default Gateway: 192.168.1.1

Date & Time

NTP Admin: Disable

□ Set Date & Time (Time and Date value will be taken automatically from client local time.)

Activation Key

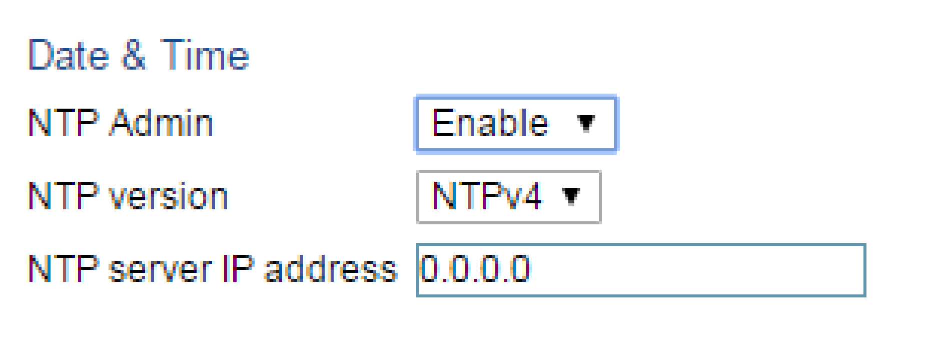
Demo admin: Enable

SNMP Parameters

SNMP Admin: Enable
SNMP Read Community: public
SNMP Write Community: private
SNMP Trap Version: V1
SNMP V1V2 Blocked: No

2. The Unit Parameters section is optional. For details on each field, see Configuring Unit Parameters.
3. 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.
4. 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.



Date & Time

NTP Admin: Enable

NTP version: NTPv4

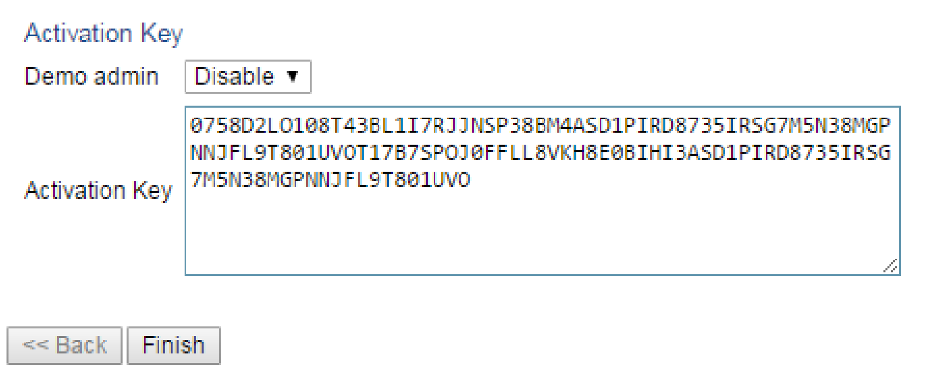
NTP server IP address: 0.0.0.0

Note

You can configure aqdditional NTP servers, up to four, in the NTP Configuration page. See Configuring NTP.

5. 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 Configuring the Activation Key.



Activation Key

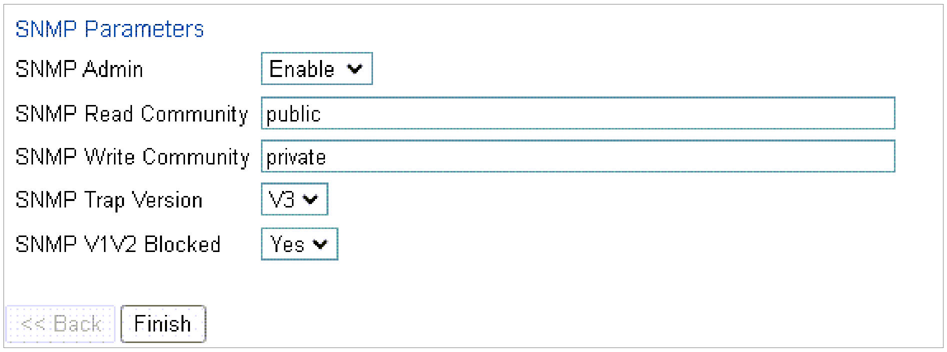
Demo admin: Disable

Activation Key:

```
0758D2LO108T43BL1I7RJJNSP38BM4ASD1PIRD8735IRSG7M5N38MGP
NNJFL9T801UVOT17B7SPOJ0FFLL8VKH8E0BIHI3ASD1PIRD8735IRSG
7M5N38MGPNNJFL9T801UVO
```

6. 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. For a full explanation of SNMP parameters, see

Configuring SNMP.

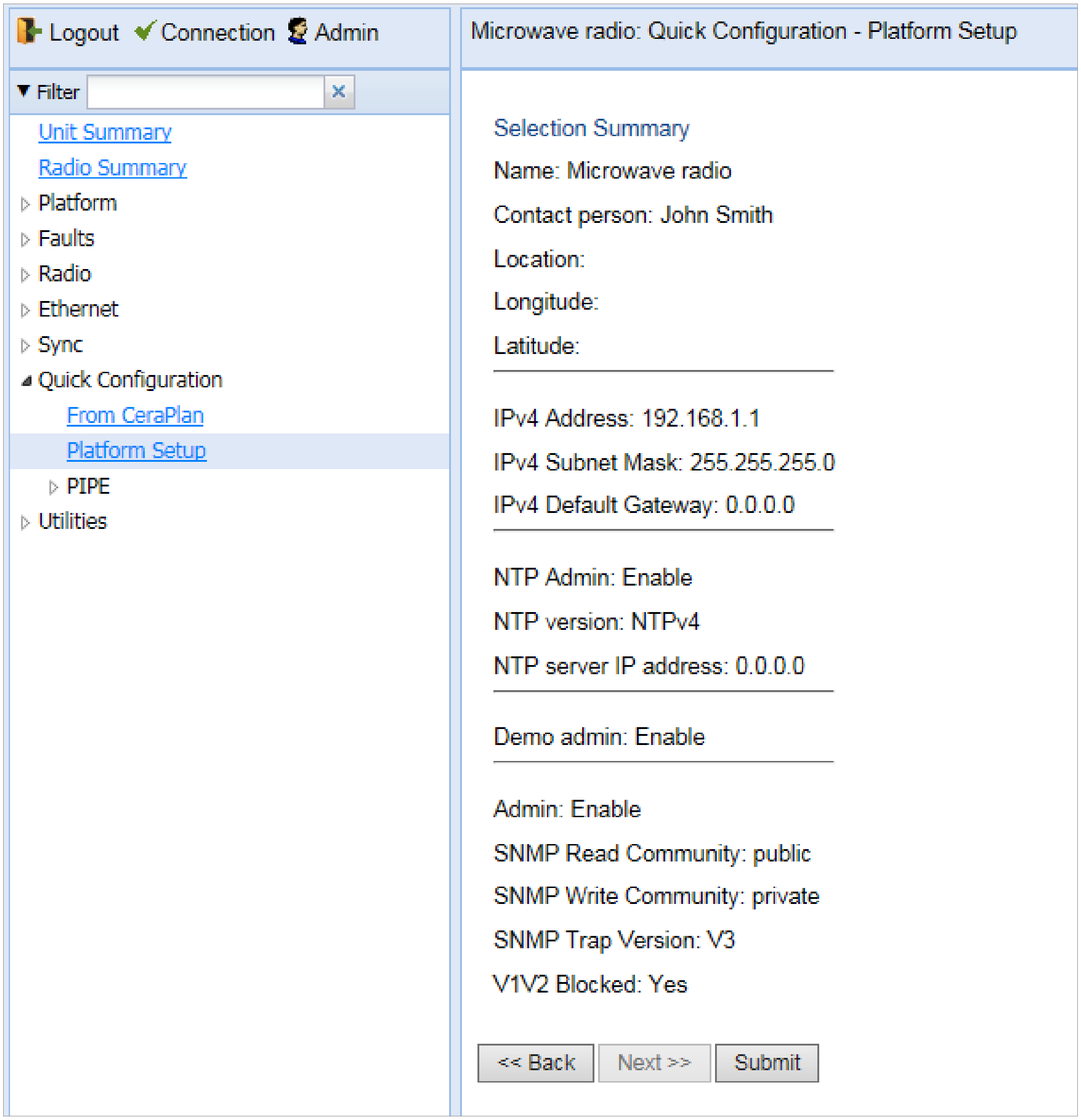


SNMP Parameters

SNMP Admin	Enable
SNMP Read Community	public
SNMP Write Community	private
SNMP Trap Version	V3
SNMP V1V2 Blocked	Yes

7. 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 21 *Quick Configuration – Platform Setup Summary Page*



Microwave radio: Quick Configuration - Platform Setup

Selection Summary

Name: Microwave radio

Contact person: John Smith

Location:

Longitude:

Latitude:

IPv4 Address: 192.168.1.1

IPv4 Subnet Mask: 255.255.255.0

IPv4 Default Gateway: 0.0.0.0

NTP Admin: Enable

NTP version: NTPv4

NTP server IP address: 0.0.0.0

Demo admin: Enable

Admin: Enable

SNMP Read Community: public

SNMP Write Community: private

SNMP Trap Version: V3

V1V2 Blocked: Yes

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 listed in Configuration Tips.

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

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.

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

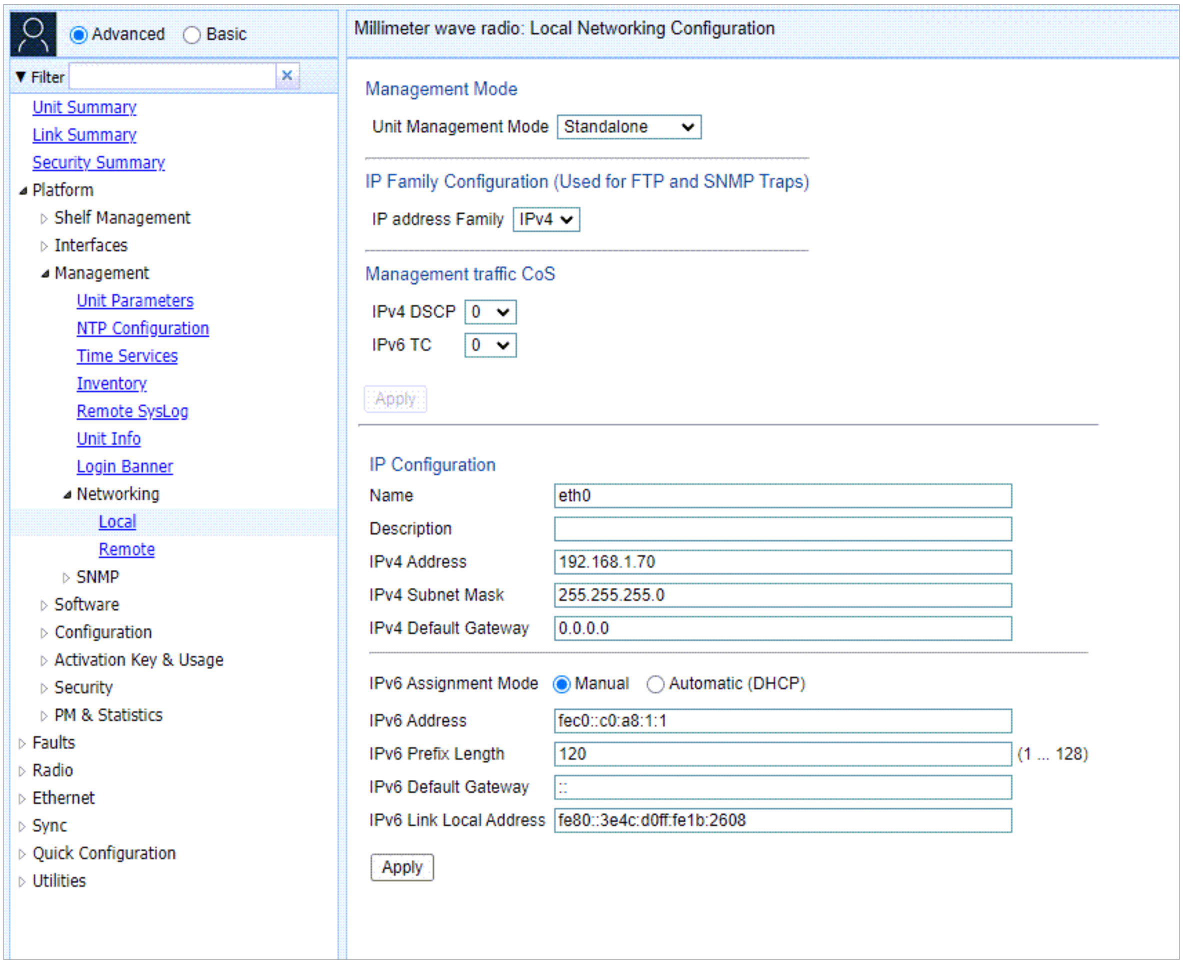
To change the management IP address of the local unit in Advanced mode:

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

   Note

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

Figure 22 *Local Networking Configuration Page*



Millimeter wave radio: Local Networking Configuration

Management Mode

Unit Management Mode: Standalone

IP Family Configuration (Used for FTP and SNMP Traps)

IP address Family: IPv4

Management traffic CoS

IPv4 DSCP: 0

IPv6 TC: 0

Apply

IP Configuration

Name	eth0
Description	
IPv4 Address	192.168.1.70
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	0.0.0.0
IPv6 Assignment Mode	● Manual ○ Automatic (DHCP)
IPv6 Address	fec0::c0:a8:1:1
IPv6 Prefix Length	120 (1 ... 128)
IPv6 Default Gateway	::
IPv6 Link Local Address	fe80::3e4c:d0ff:fe1b:2608

Apply

2. In the **Unit Management Mode** field, leave the default value of Standalone unless you are managing the device via RAON.

Note

For instructions on configuring and using RAON to manage PTP 850 devices with PTP 850FX200, refer to the User Guide for RAON.

3. Optionally, in the **Name** field, enter a name for the unit.
4. Optionally, in the **Description** field, enter descriptive information about the unit.
5. 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 Addres**s field. The unit will receive communications whether they are sent to its IPv4 address or its IPv6 address.
6. If you entered an IPv4 address, in the **IPv4 Subnet mask** field, enter the subnet mask.
7. Optionally, in the **IPv4 Default gateway** field, enter the default gateway address.
8. 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.

9. 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.
10. If you entered an IPv6 address, enter the IPv6 prefix length in the IPv6 Prefix-Length field.
11. Optionally, if you entered an IPv6 address, enter the default gateway in IPv6 format in the IPv6 Default Gateway field.
12. Click **Apply**.

Note

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

Enabling Dynamic IPv6 Addresses Via DHCPv6

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.

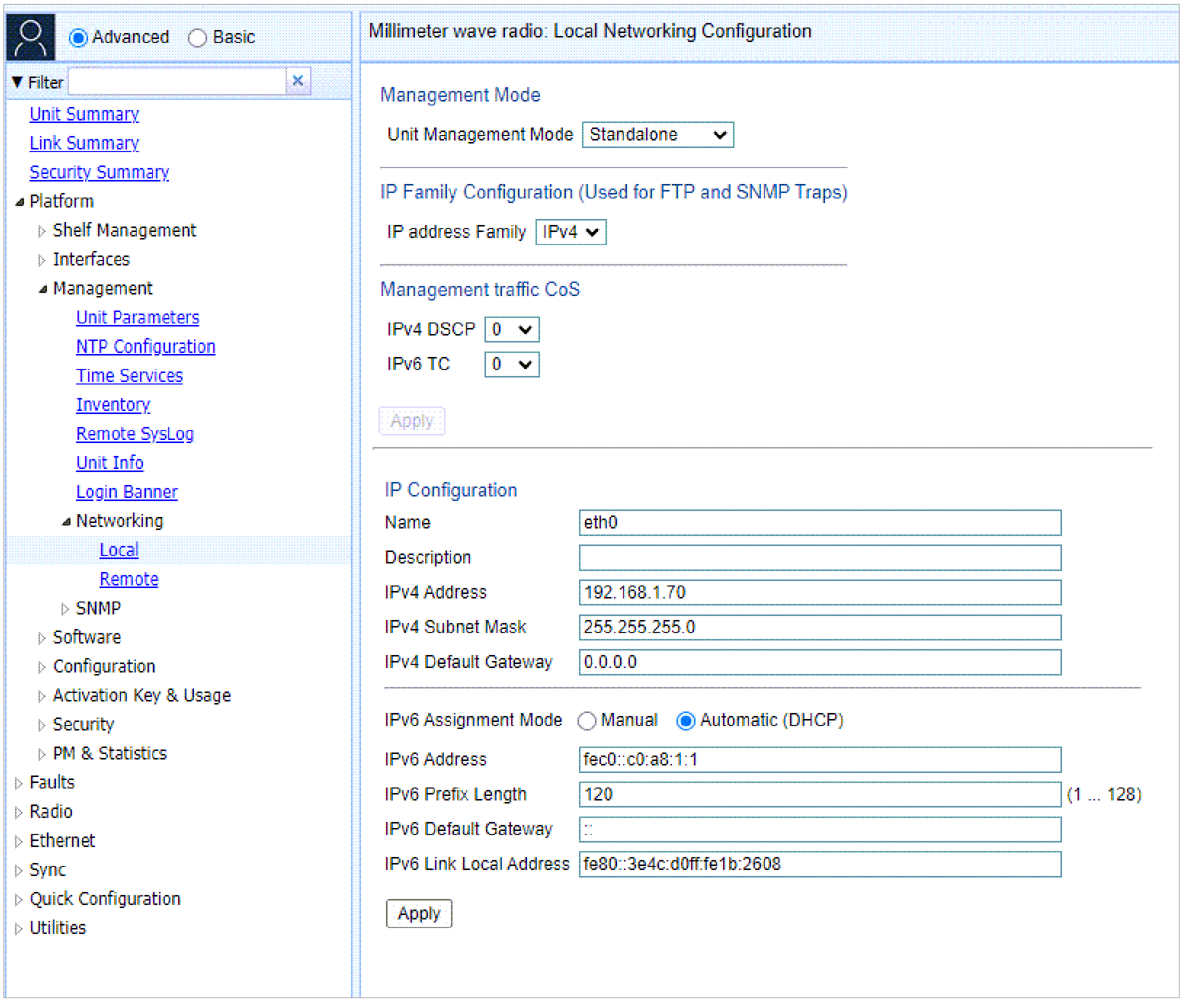
To enable IPv6 Automatic mode:

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 23 *Local Networking Configuration Page (IPv6 Automatic Mode)*



Millimeter wave radio: Local Networking Configuration

Management Mode

Unit Management Mode: Standalone

IP Family Configuration (Used for FTP and SNMP Traps)

IP address Family: IPv4

Management traffic CoS

IPv4 DSCP: 0

IPv6 TC: 0

IP Configuration

Name	eth0
Description	
IPv4 Address	192.168.1.70
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	0.0.0.0
IPv6 Assignment Mode	○ Manual ● Automatic (DHCP)
IPv6 Address	fec0::c0:a8:1:1
IPv6 Prefix Length	120 (1 ... 128)
IPv6 Default Gateway	::
IPv6 Link Local Address	fe80::3e4c:d0ff:fe1b:2608

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.

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. See Configuring Ingress Path Classification on a Logical Interface.
- For the management service, the CoS Mode must be set to Preserve-SP-COS-Decision. See Adding an Ethernet Service.

To configure DSCP/TC for management:

1. Select **Platform** > **Management** > **Networking** > **Local**. The Local Networking Configuration page opens (Changing the Management IP Address).
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.

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

Activation Key Overview

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.

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. For further information about Smart Activation Key management, refer to the *Smart Activation Key User Guide*.

Note

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

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.

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.

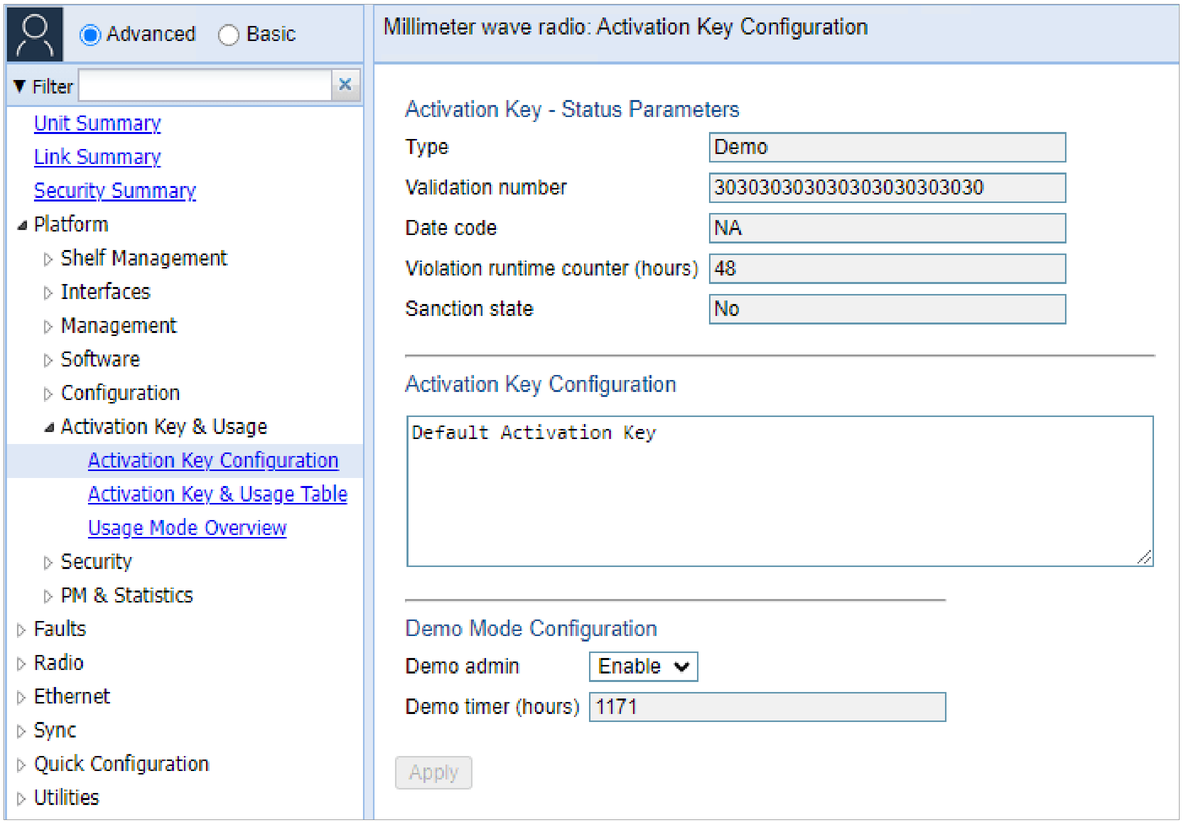
Viewing the Activation Key Status Parameters

To display the current activation key status parameters in Advanced mode:

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

   Note
   To display the same page in Basic mode, select Platform > Activation Key.

Figure 24 *Activation Key Configuration Page*



Millimeter wave radio: Activation Key Configuration

Activation Key - Status Parameters

Type	Demo
Validation number	303030303030303030303030
Date code	NA
Violation runtime counter (hours)	48
Sanction state	No

Activation Key Configuration

```
Default Activation Key
```

Demo Mode Configuration

Demo admin	Enable
Demo timer (hours)	1171

Table 9 *Activation Key Status Parameters*

Parameter	Definition
Type	Displays the current activation key type.
Validation number	Displays a random, system-generated validation number. This number is required when reclaiming an activation key. See Activation Key Reclaim.
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.

Entering the Activation Key

To enter a new activation key:

1. Select **Platform** > **Activation Key & Usage** > **Activation Key Configuration** in Advanced mode or **Platform** > **Activation Key** in Basic mode. The Activation Key Configuration page opens (Activation Key Configuration Page).
2. Enter the activation key cipher you have received from the vendor in the **Activation Key Configuration** field. The activation key cipher is a string that enables all features and capacities that have been purchased for the unit.
3. 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 Demo Mode

To activate demo mode:

1. Select **Platform** > **Activation Key & Usage** > **Activation Key Configuration** in Advanced mode or **Platform** > **Activation Key** in Basic mode. The Activation Key Configuration page opens (Activation Key Configuration Page).
2. In the **Demo admin** field, select **Enable**.
3. Click **Apply**.

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

Activation Key Reclaim

If it is necessary to deactivate an PTP 850 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.

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*.

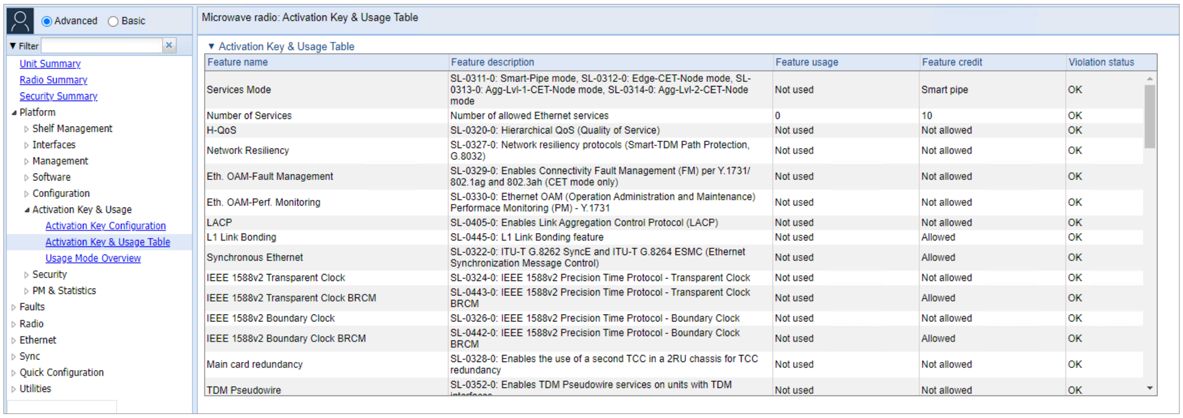
Displaying a List of Activation-Key-Enabled Features

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

1. In Advanced mode, select Platform > Activation Key & Usage > Activation Key & Usage Table. The Activation Key & Usage Table page opens.

Note
To display this information in Basic mode, select Platform > Activation Key and click Show Activation Key & Usage Table at the bottom of the Activation Key page.

Figure 25 *Activation Key & Usage Table Page*



Microwave radio: Activation Key & Usage Table

▼ Activation Key & Usage Table

Feature name	Feature description	Feature usage	Feature credit	Violation status
Services Mode	SL-0311-0: Smart-Pipe mode, SL-0312-0: Edge-CET-Node mode, SL-0313-0: Agg-Lvl-1-CET-Node mode, SL-0314-0: Agg-Lvl-2-CET-Node mode	Not used	Smart pipe	OK
Number of Services	Number of allowed Ethernet services	0	10	OK
H-QoS	SL-0320-0: Hierarchical QoS (Quality of Service)	Not used	Not allowed	OK
Network Resiliency	SL-0327-0: Network resiliency protocols (Smart-TDM Path Protection, G.8032)	Not used	Not allowed	OK
Eth. OAM-Fault Management	SL-0329-0: Enables Connectivity Fault Management (FM) per Y.1731/ 802.1ag and 802.3ah (CET mode only)	Not used	Not allowed	OK
Eth. OAM-Perf. Monitoring	SL-0330-0: Ethernet OAM (Operation Administration and Maintenance) Performace Monitoring (PM) - Y.1731	Not used	Not allowed	OK
LACP	SL-0405-0: Enables Link Aggregation Control Protocol (LACP)	Not used	Not allowed	OK
L1 Link Bonding	SL-0445-0: L1 Link Bonding feature	Not used	Allowed	OK
Synchronous Ethernet	SL-0322-0: ITU-T G.8262 SyncE and ITU-T G.8264 ESMC (Ethernet Synchronization Message Control)	Not used	Allowed	OK
IEEE 1588v2 Transparent Clock	SL-0324-0: IEEE 1588v2 Precision Time Protocol - Transparent Clock	Not used	Not allowed	OK
IEEE 1588v2 Transparent Clock BRCM	SL-0443-0: IEEE 1588v2 Precision Time Protocol - Transparent Clock BRCM	Not used	Allowed	OK
IEEE 1588v2 Boundary Clock	SL-0326-0: IEEE 1588v2 Precision Time Protocol - Boundary Clock	Not used	Not allowed	OK
IEEE 1588v2 Boundary Clock BRCM	SL-0442-0: IEEE 1588v2 Precision Time Protocol - Boundary Clock BRCM	Not used	Allowed	OK
Main card redundancy	SL-0328-0: Enables the use of a second TCC in a 2RU chassis for TCC redundancy	Not used	Not allowed	OK
TDM Pseudowire	SL-0352-0: Enables TDM Pseudowire services on units with TDM interfaces	Not used	Not allowed	OK

The Activation Key & Usage Table 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. Activation Key-Enabled-Features Description describes the available activation keys, as displayed in the Activation Key & Usage Table page.

Note

Some of the features listed in the Activation Key & Usage Table page and described in Activation Key-Enabled-Features Description may not be supported in the currently installed software version. For details on feature support, refer to the Release Notes or Technical Description for the System Release release you are using.

Table 10 *Activation Key-Enabled-Features Table Parameters*

Parameter	Definition
Feature name	The name of the feature.
Feature description	A description of the feature.
Feature usage	Indicates whether the activation-key-enabled feature is actually being used.
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 11 *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.

Activation Key Name	Description
	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. 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	Not relevant for PTP 850EX.
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 release.
LACP	Enables Link Aggregation Control Protocol (LACP). One activation key is required per device. **Note:** Support for LACP is planned for future release.
L1 Link Bonding	Not relevant for PTP 850EX.
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	Enables IEEE-1588 Transparent Clock. One activation key is required per device.
IEEE 1588v2 Transparent Clock BRCM	Not relevant for PTP 850EX.
IEEE 1588v2 Boundary Clock	Enables IEEE-1588 Boundary Clock. One activation key is required per device.
IEEE 1588v2	Not relevant for PTP 850EX.

Activation Key Name	Description
Boundary Clock BRCM	
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.
Ethernet traffic ports – 25GbE	Enables the use of 25GbE ports. A separate activation key is required per port.
Ethernet traffic ports – 40GbE	Not relevant for PTP 850EX.
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. **Note:** Support for XPIC with PTP 850EX is planned for future release.
Millimeter Wave XPIC (NA)	Not relevant for PTP 850EX.
Multi Carrier ABC	Multi-Carrier ABC. A separate activation key is required per radio member.

Activation Key Name	Description
	Not relevant for PTP 850EX.
MIMO	Not relevant for PTP 850EX.
SD	Space Diversity. A separate activation key is required per radio member. Not relevant for PTP 850EX.
ASD	Not relevant for PTP 850EX.
AFR 1+0	Not relevant for PTP 850EX.
ACMB	Adaptive Coding Modulation Channel Bandwidth. A separate activation key is required per radio.
AES Encryption	Planned for future release.
2nd RX Core Activation	Not relevant for PTP 850EX.
2nd Core Activation RFU-D	Not relevant for PTP 850EX.
2nd Core Activation HP	Not relevant for PTP 850EX.
2nd Modem Activation	Not relevant for PTP 850EX.
RFU Port Activation	Not relevant for PTP 850EX.
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	Displays the number of mmW radio carriers for which there is permission to use up to

Activation Key Name	**Description**
100Mbps	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.
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	Displays the number of radio carriers for which there is permission to use up to 500

Activation Key Name	Description
500Mbps	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.
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.
mmW Capacity	Displays the number of radio carriers for which there is permission to use up to 9

Activation Key Name	Description
9Gbps	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	Planned for future release.
Anti-Theft	Not relevant for PTP 850EX.
Web customer view	Planned for future release.
Front Panel RFU Activation	Not relevant for PTP 850EX.
Advanced Security Key	Enables Syslog Encryption and NTP Authentication.
E-Stabilizer Advanced Features	Enables activation of automatic tracking mode and performance monitoring (PTP 850EX only)

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 with the correct time.

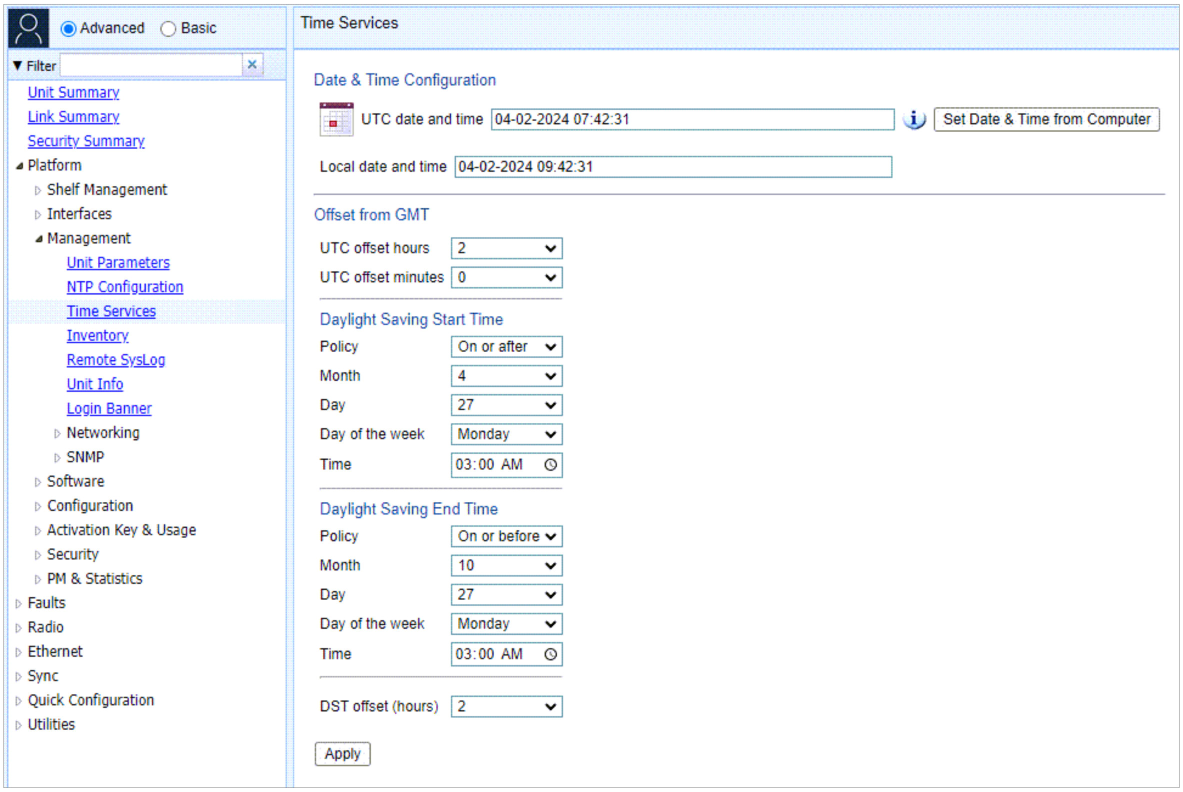
Note

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 display and configure the UTC parameters:

1. Select **Platform** > **Management** > **Time Services** in Advanced mode or **Platform** > **Time Services** in Basic mode. The Time Services page opens.

Figure 26 *Time Services Page*



Time Services

Date & Time Configuration

UTC date and time: 04-02-2024 07:42:31

Local date and time: 04-02-2024 09:42:31

Offset from GMT

UTC offset hours: 2

UTC offset minutes: 0

Daylight Saving Start Time

Policy: On or after

Month: 4

Day: 27

Day of the week: Monday

Time: 03:00 AM

Daylight Saving End Time

Policy: On or before

Month: 10

Day: 27

Day of the week: Monday

Time: 03:00 AM

DST offset (hours): 2

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

Table 12 *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.
	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	Policy	Enables you to create a rule for the beginning of Daylight Saving Time

	Parameter	Definition
Saving Start 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 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.

	Parameter	Definition
		- 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. 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.
	DST offset	The required offset, in hours, for Daylight Savings Time. Only positive offset is supported.
Date & Time Configuration	UTC Date and Time	The UTC date and time.
	Local Current Date and Time	Read-only. 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.
	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	Month	The month when Daylight Savings Time begins.
	Day	The date in the month when Daylight Savings Time begins.
Daylight Saving End Time	Month	The month when Daylight Savings Time ends.
	Day	The date in the month when Daylight Savings Time ends.
	DST Offset (Hours)	The required offset, in hours, for Daylight Savings Time. Only positive offset is supported.

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.

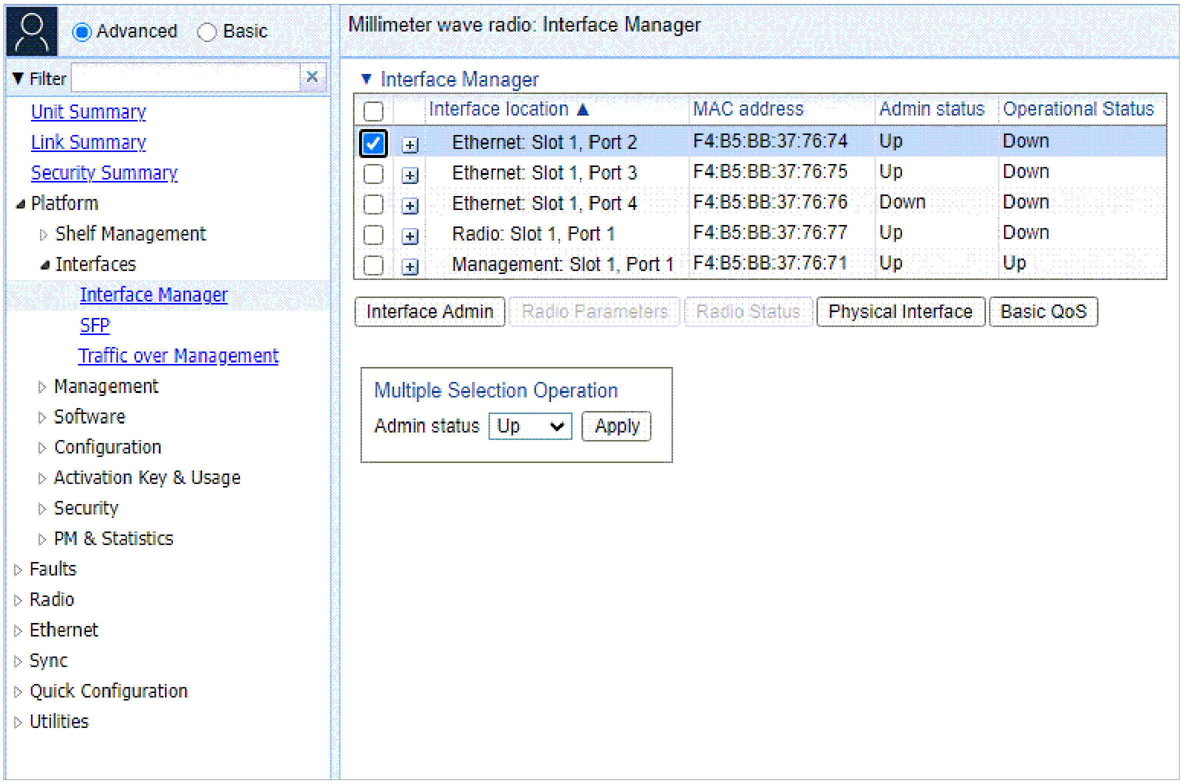
> **Note**
>
> For PTP 850EX, Ethernet Slot 1, Ports 2, 3, and 4 are supported. Management Slot 1 Port 1 is also supported for management.
>
> For PTP 850EX, support for traffic with the Management port is planned for future release.

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.

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

Figure 27 *Interface Manager Page (PTP 850EX)*



Millimeter wave radio: Interface Manager

▼ Interface Manager

□		Interface location ▲	MAC address	Admin status	Operational Status
☑	+	Ethernet: Slot 1, Port 2	F4:B5:BB:37:76:74	Up	Down
□	+	Ethernet: Slot 1, Port 3	F4:B5:BB:37:76:75	Up	Down
□	+	Ethernet: Slot 1, Port 4	F4:B5:BB:37:76:76	Down	Down
□	+	Radio: Slot 1, Port 1	F4:B5:BB:37:76:77	Up	Down
□	+	Management: Slot 1, Port 1	F4:B5:BB:37:76:71	Up	Up

Multiple Selection Operation

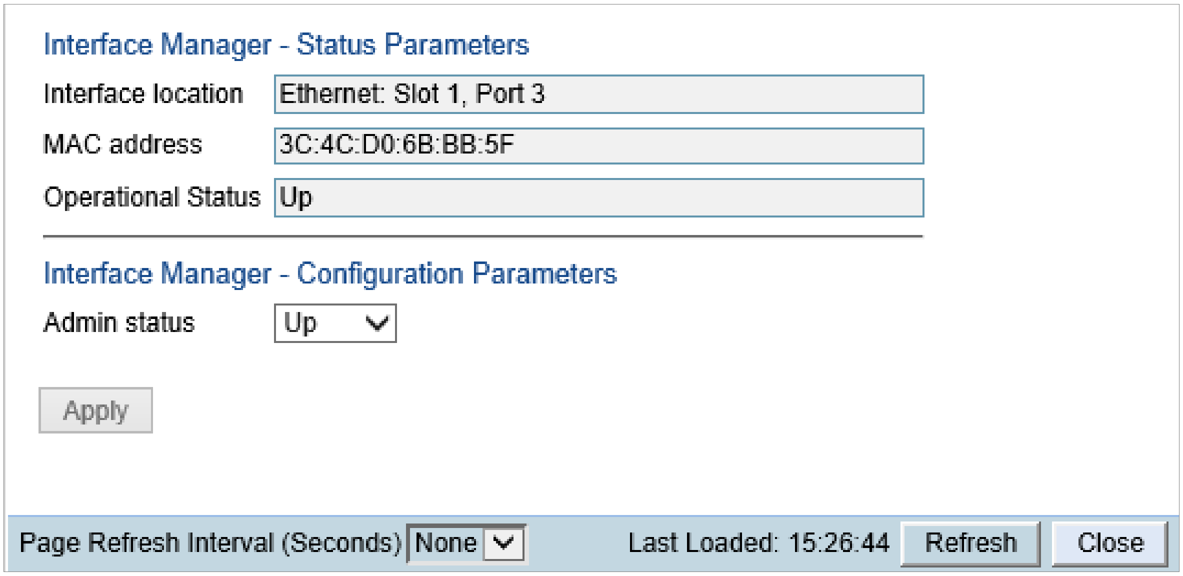
Admin status: Up ▾ Apply

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.

To enable or disable an individual interface:

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

   Figure 28 *Interface Manager – Edit Page*



Interface Manager - Status Parameters

Interface location: Ethernet: Slot 1, Port 3

MAC address: 3C:4C:D0:6B:BB:5F

Operational Status: Up

Interface Manager - Configuration Parameters

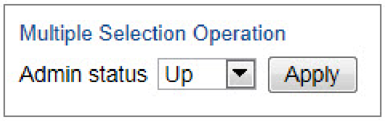
Admin status: Up

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 29 *Multiple Selection Operation Section (Interface Manager Page)*



Multiple Selection Operation

Admin status: Up

3. Click **Apply**.

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

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**.

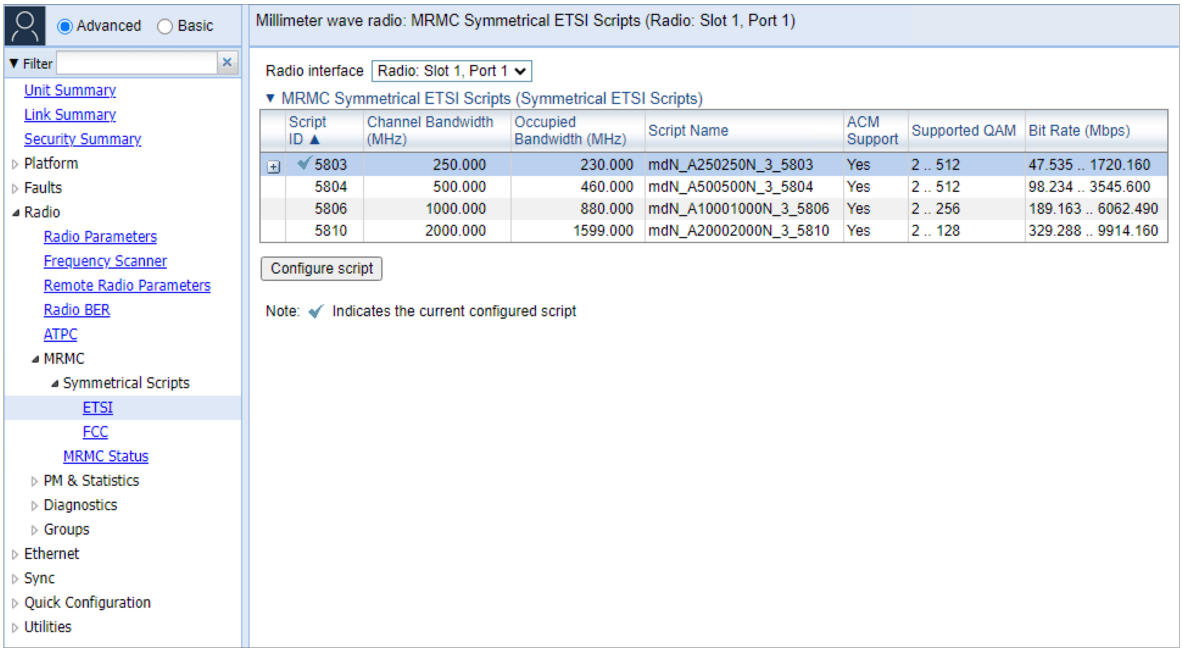
    The MRMC Symmetrical Scripts page opens. For a description of the parameters displayed in the MRMC Symmetrical Scripts page, see Configuring the Radio (MRMC) Script(s).

    Note

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

    This page is only available in Advanced mode. However, MRMC scripts can also be configured during link configuration with a Quick Configuration wizard. See Configuring a Link Using the Quick Configuration Wizard.

    Figure 30 *MRMC Symmetrical Scripts Page (PTP 850EX)*



Millimeter wave radio: MRMC Symmetrical ETSI Scripts (Radio: Slot 1, Port 1)

Radio interface: Radio: Slot 1, Port 1

▼ MRMC Symmetrical ETSI Scripts (Symmetrical ETSI Scripts)

	Script ID ▲	Channel Bandwidth (MHz)	Occupied Bandwidth (MHz)	Script Name	ACM Support	Supported QAM	Bit Rate (Mbps)
+	✓ 5803	250.000	230.000	mdN_A250250N_3_5803	Yes	2 .. 512	47.535 .. 1720.160
	5804	500.000	460.000	mdN_A500500N_3_5804	Yes	2 .. 512	98.234 .. 3545.600
	5806	1000.000	880.000	mdN_A10001000N_3_5806	Yes	2 .. 256	189.163 .. 6062.490
	5810	2000.000	1599.000	mdN_A20002000N_3_5810	Yes	2 .. 128	329.288 .. 9914.160

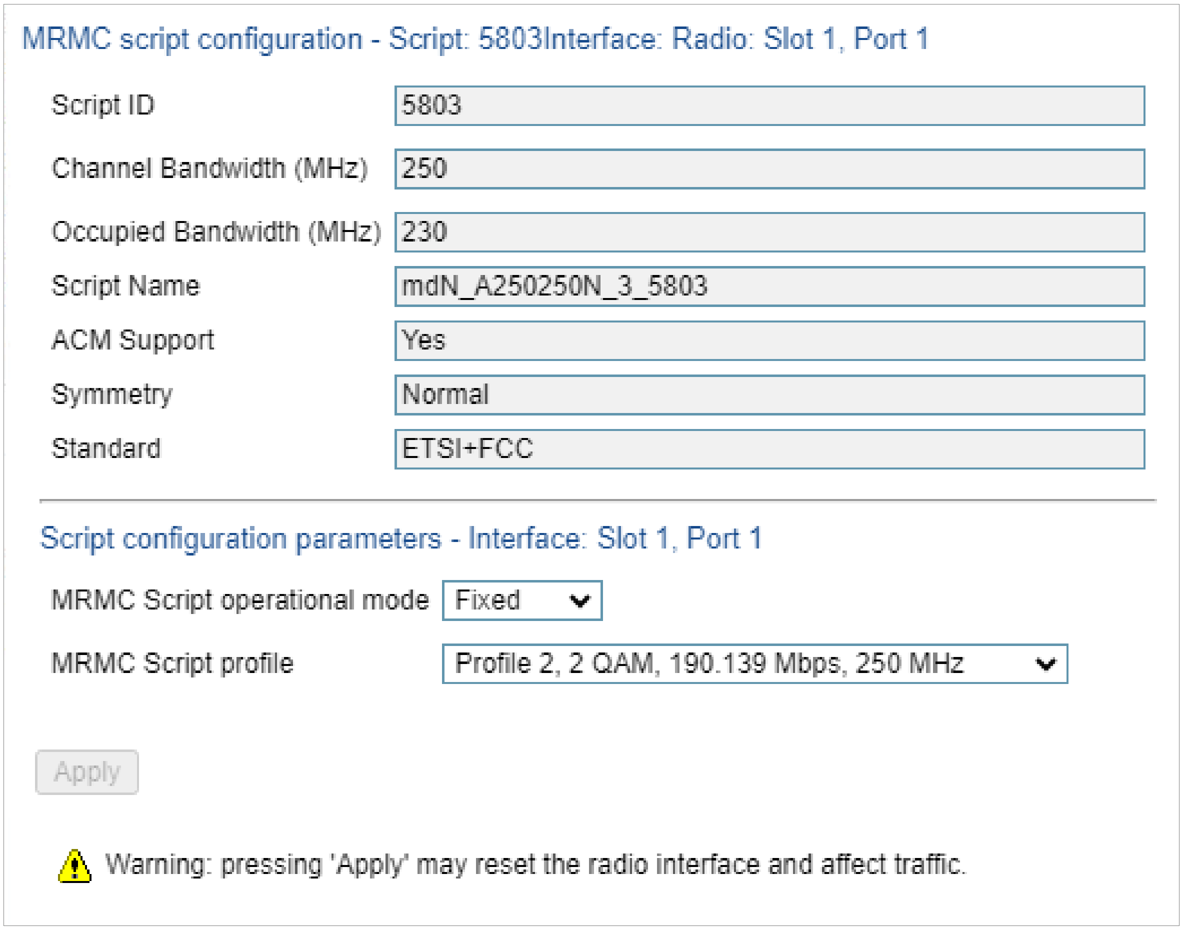
Configure script

Note: ✓ Indicates the current configured script

2. Select the script you want to assign to the radio. The currently-assigned script is marked by a check mark.

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

Figure 31 *MRMC Symmetrical Scripts Page – Configuration (PTP 850EX, Fixed Mode)*



MRMC script configuration - Script: 5803Interface: Radio: Slot 1, Port 1

Script ID	5803
Channel Bandwidth (MHz)	250
Occupied Bandwidth (MHz)	230
Script Name	mdN_A250250N_3_5803
ACM Support	Yes
Symmetry	Normal
Standard	ETSI+FCC

Script configuration parameters - Interface: Slot 1, Port 1

MRMC Script operational mode	Fixed
MRMC Script profile	Profile 2, 2 QAM, 190.139 Mbps, 250 MHz

⚠ Warning: pressing 'Apply' may reset the radio interface and affect traffic.

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.

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.

Refer to Radio Profiles for PTP 850EX for a list of available radio profiles.

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 14: MRMC Symmetrical Scripts Page Parameters describes the MRMC Symmetrical Scripts page parameters.

Table 14: 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 850 scripts support ACM.
Supported QAM	The supported range of modulations.
Latency Level	Always displays Normal.
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.

Parameter	Definition
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 0.

Radio Profiles for PTP 850EX

Note

The maximum vary per script. For details, refer to the Release Notes for the System Release version you are using.

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 13 *Available Radio Profiles*

Profile	Modulation – Script 5803 (250 MHz)	Modulation – Script 5804 (500 MHz)	Modulation – Script 5806 (1000 MHz)	Modulation – Script 5810 (2000 MHz)
Profile 0	BPSK (¼ channel spacing)	BPSK (¼ channel spacing)	BPSK (¼ channel spacing)	BPSK (¼ channel spacing)
Profile 1	BPSK (½ channel spacing)	BPSK (½ channel spacing)	BPSK (½ channel spacing)	BPSK (½ channel spacing)
Profile 2	BPSK (full channel spacing)	BPSK (full channel spacing)	BPSK (full channel spacing)	BPSK (full channel spacing)
Profile 3	4 QAM	4 QAM	4 QAM	4 QAM
Profile 4	8 QAM	8 QAM	8 QAM	8 QAM
Profile 5	16 QAM	16 QAM	16 QAM	16 QAM
Profile 6	32 QAM	32 QAM	32 QAM	32 QAM
Profile 7	64 QAM	64 QAM	64 QAM	64 QAM
Profile	128 QAM	128 QAM	128 QAM	128 QAM

Profile	Modulation – Script 5803 (250 MHz)	Modulation – Script 5804 (500 MHz)	Modulation – Script 5806 (1000 MHz)	Modulation – Script 5810 (2000 MHz)
8				
Profile 9	256 QAM	256 QAM	256 QAM	n/a
Profile 10	512 QAM	512 QAM	512 QAM	n/a
Profile 11	1024 QAM	1024 QAM	n/a	n/a

Configuring the Radio Parameters

In order to establish a radio link, you must:

- Verify that the radio is muted (the TX 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.
- 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.

- Set TX Mute to Unmute.
- Click **Apply** to apply the unmute.
- 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.

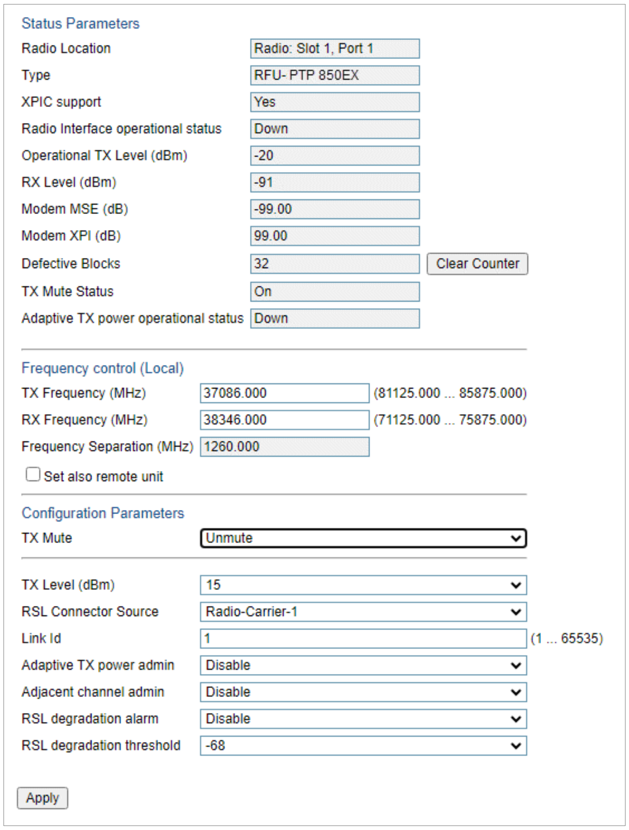
To configure the radio parameters:

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 850E, the Radio Parameters page opens right away.

Figure 32 *Radio Parameters Page*



Status Parameters

Radio Location	Radio: Slot 1, Port 1	
Type	RFU- PTP 850EX	
XPIC support	Yes	
Radio Interface operational status	Down	
Operational TX Level (dBm)	-20	
RX Level (dBm)	-91	
Modem MSE (dB)	-99.00	
Modem XPI (dB)	99.00	
Defective Blocks	32	Clear Counter
TX Mute Status	On	
Adaptive TX power operational status	Down	

Frequency control (Local)

TX Frequency (MHz)	37086.000	(81125.000 ... 85875.000)
RX Frequency (MHz)	38346.000	(71125.000 ... 75875.000)
Frequency Separation (MHz)	1260.000	

□ Set also remote unit

Configuration Parameters

TX Mute	Unmute	
TX Level (dBm)	15	
RSL Connector Source	Radio-Carrier-1	
Link Id	1	(1 ... 65535)
Adaptive TX power admin	Disable	
Adjacent channel admin	Disable	
RSL degradation alarm	Disable	
RSL degradation threshold	-68	

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

   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. 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.

   d. Optionally, select Set also remote unit to apply the frequency settings to the remote unit as well as the local unit.

> **Note**
>
> 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:

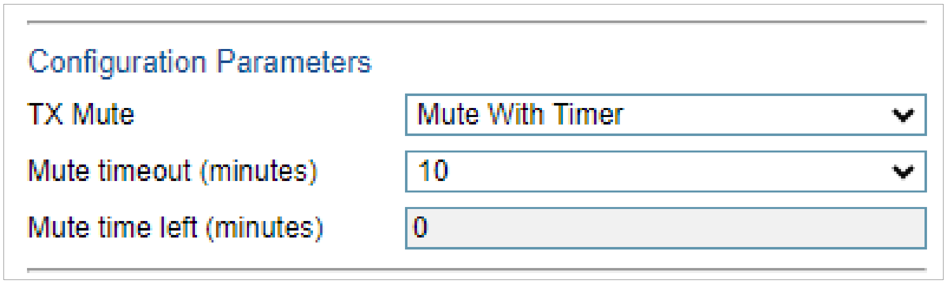
i. To mute the TX output of the radio carrier, select Mute in the TX Mute field. To unmute the TX output of the radio carrier, select Unmute. To configure a timed mute, select Mute with Timer.

If you select Mute with Timer, two additional fields appear:

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.

Mute time left (minutes) – Displays how much time is left until the mute timer expires.

Figure 33 *Radio Parameters – Configuration Parameters*



Configuration Parameters

TX Mute	Mute With Timer
Mute timeout (minutes)	10
Mute time left (minutes)	0

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. 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.

iv. 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.

v. 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 850EX.

For a description of the read-only parameters in the **Status parameters** section, see Viewing the Radio Status and Settings.

Creating Service(s) for Traffic

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

Configuration Guide

This section lists the basic PTP 850EX system configurations, with links to configuration instructions.

Note

In addition to the configurations listed below and described in this manual, PTP 850EX can be used in Layer 1 Link Bonding configurations with PTP 820N or PTP 820A. For more information about Link Bonding configurations with PTP 820N and PTP 820A, refer to the *User Guide for PTP 820N and PTP 820A*. For instructions how to configure the PTP 850EX for Link Bonding using a Quick Configuration wizard, see Configuring PTP 850EX as an Attached Unit in a Layer 1 Link Bonding Group.

Table 14 *System Configurations*

Configuration	Supported Products	Link to Configuration Instructions
1+0	PTP 850EX	Configuring a 1+0 Link Using the Quick Configuration Wizard
Link Aggregation (LAG)	PTP 850EX	Configuring Link Aggregation (LAG)

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:

- Configuring an PTP 850 Unit Using Basic Mode – Enables you to create Ethernet services.
- Configuring an PTP 850 Unit Using Basic Mode – Includes options to display current alarms and the event log.
- Configuring an PTP 850 Unit Using Basic Mode – Enables you to display radio and Ethernet PMs.
- Configuring an PTP 850 Unit Using Basic Mode – Enables you to perform diagnostics, troubleshooting, and configuration management.
- Configuring an PTP 850 Unit Using Basic Mode – 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 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.

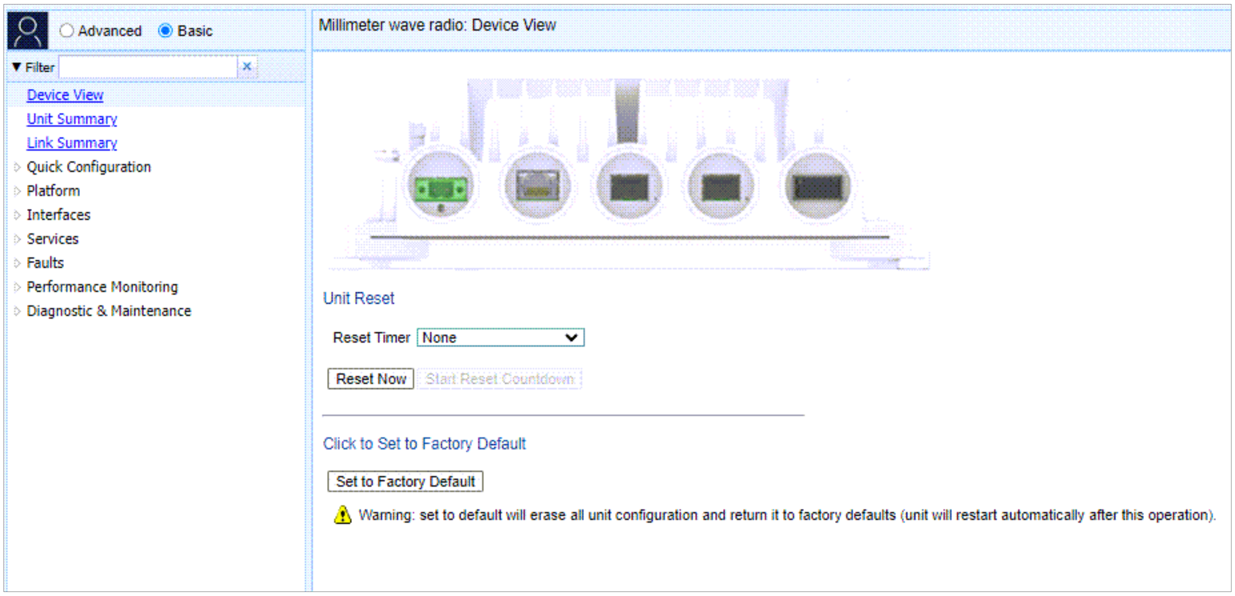
Device View

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 Unit Reset.

Set the unit to its default factory configuration settings. See Setting the Unit to the Factory Default Configuration.

Figure 34 *Basic Mode – Device View Page*



Millimeter wave radio: Device View

Unit Reset

Reset Timer: None

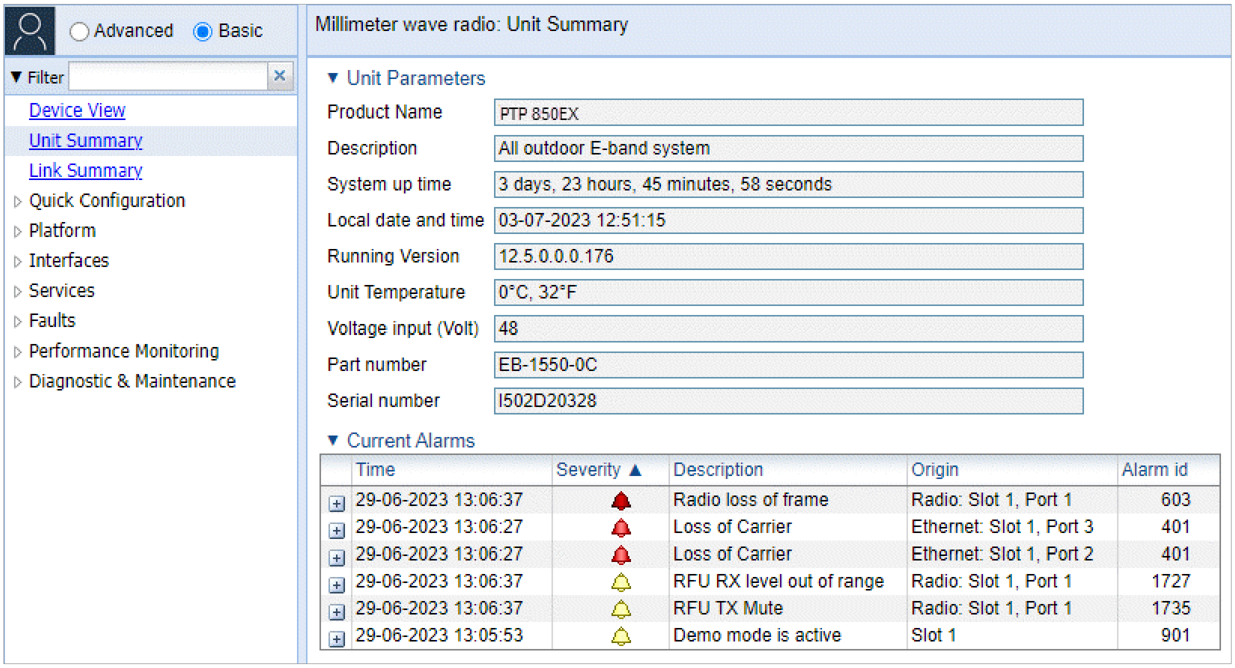
Click to Set to Factory Default

⚠ Warning: set to default will erase all unit configuration and return it to factory defaults (unit will restart automatically after this operation).

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 35 *Basic Mode – Unit Summary Page*



Millimeter wave radio: Unit Summary

▼ Unit Parameters

Product Name	PTP 850EX
Description	All outdoor E-band system
System up time	3 days, 23 hours, 45 minutes, 58 seconds
Local date and time	03-07-2023 12:51:15
Running Version	12.5.0.0.0.176
Unit Temperature	0°C, 32°F
Voltage input (Volt)	48
Part number	EB-1550-0C
Serial number	I502D20328

▼ Current Alarms

	Time	Severity ▲	Description	Origin	Alarm id
⊞	29-06-2023 13:06:37	●	Radio loss of frame	Radio: Slot 1, Port 1	603
⊞	29-06-2023 13:06:27	●	Loss of Carrier	Ethernet: Slot 1, Port 3	401
⊞	29-06-2023 13:06:27	●	Loss of Carrier	Ethernet: Slot 1, Port 2	401
⊞	29-06-2023 13:06:37	○	RFU RX level out of range	Radio: Slot 1, Port 1	1727
⊞	29-06-2023 13:06:37	○	RFU TX Mute	Radio: Slot 1, Port 1	1735
⊞	29-06-2023 13:05:53	○	Demo mode is active	Slot 1	901

Quick Configuration

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

- **From NMS** – Enables you apply a pre-defined configuration file. See Applying a Pre-Defined Configuration File.
- **PIPE Wizards** – Opens a sub-menu from which you can access a Quick Configuration wizard that guides you through the process of configuring PTP 850EX links See Configuring a Link Using the Quick Configuration Wizard.

Platform

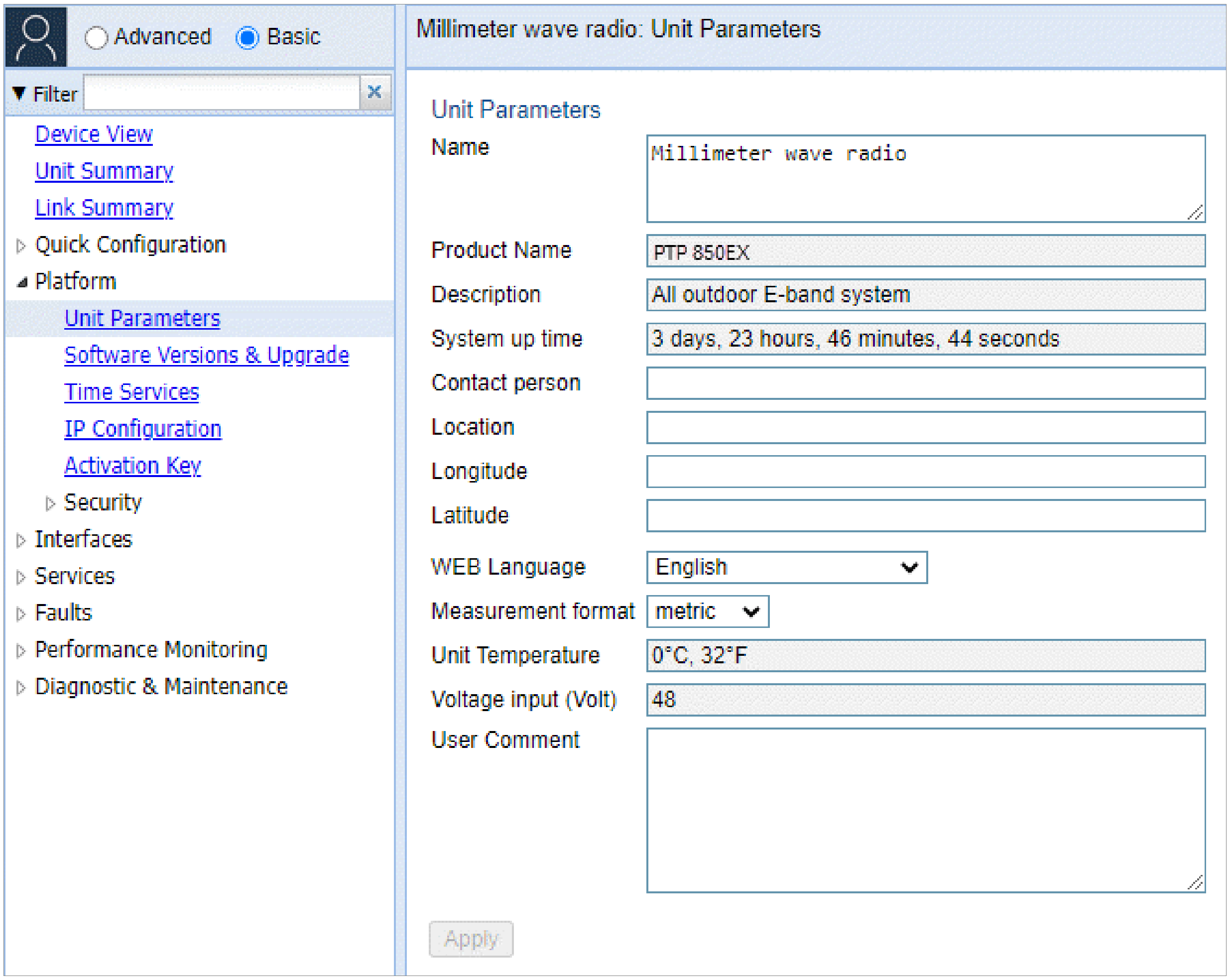
From the Platform menu, you can access pages that enable you to configure the unit, including:

- 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 access 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 36 *Basic Mode – Unit Parameters Page*



Millimeter wave radio: Unit Parameters

Unit Parameters

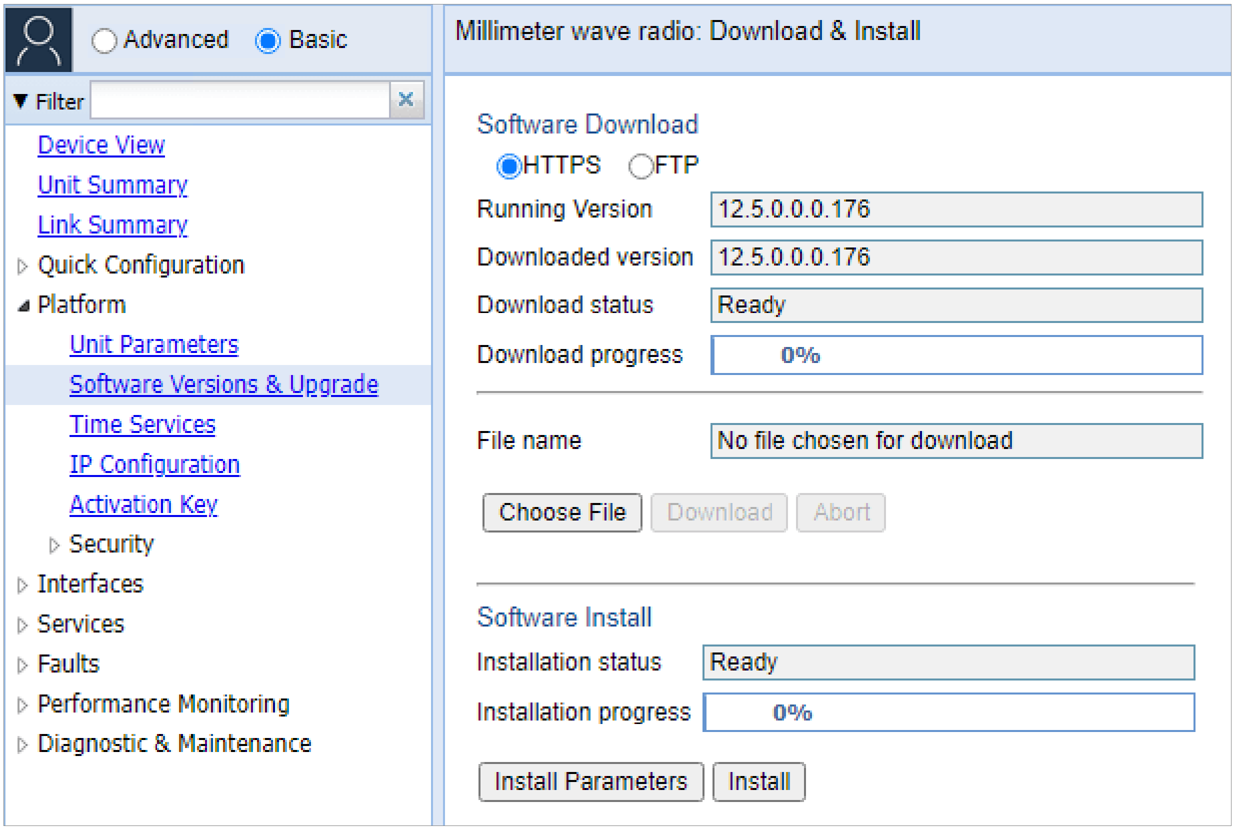
Name	Millimeter wave radio
Product Name	PTP 850EX
Description	All outdoor E-band system
System up time	3 days, 23 hours, 46 minutes, 44 seconds
Contact person	
Location	
Longitude	
Latitude	
WEB Language	English
Measurement format	metric
Unit Temperature	0°C, 32°F
Voltage input (Volt)	48
User Comment	

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 37 *Basic Mode – Software Versions & Upgrade Page*



○ Advanced ● Basic

Millimeter wave radio: Download & Install

Software Download

●HTTPS ○FTP

Running Version: 12.5.0.0.0.176

Downloaded version: 12.5.0.0.0.176

Download status: Ready

Download progress: 0%

File name: No file chosen for download

Software Install

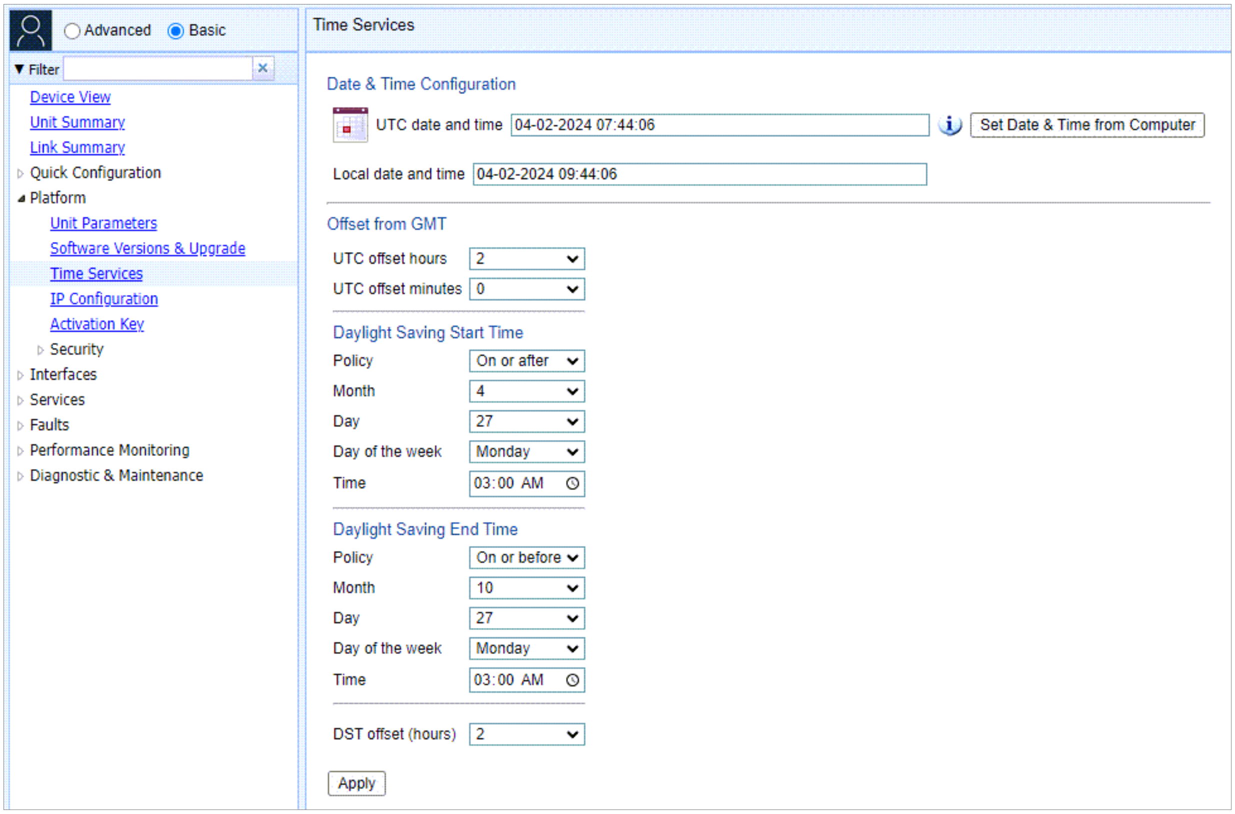
Installation status: Ready

Installation progress: 0%

Time Services Page

In the Time Services page, you can configure the unit's time and date settings. See Setting the Time and Date (Optional).

Figure 38 *Basic Mode – Time Services Page*



Time Services

Date & Time Configuration

UTC date and time: 04-02-2024 07:44:06

Local date and time: 04-02-2024 09:44:06

Offset from GMT

UTC offset hours: 2

UTC offset minutes: 0

Daylight Saving Start Time

Policy: On or after

Month: 4

Day: 27

Day of the week: Monday

Time: 03:00 AM

Daylight Saving End Time

Policy: On or before

Month: 10

Day: 27

Day of the week: Monday

Time: 03:00 AM

DST offset (hours): 2

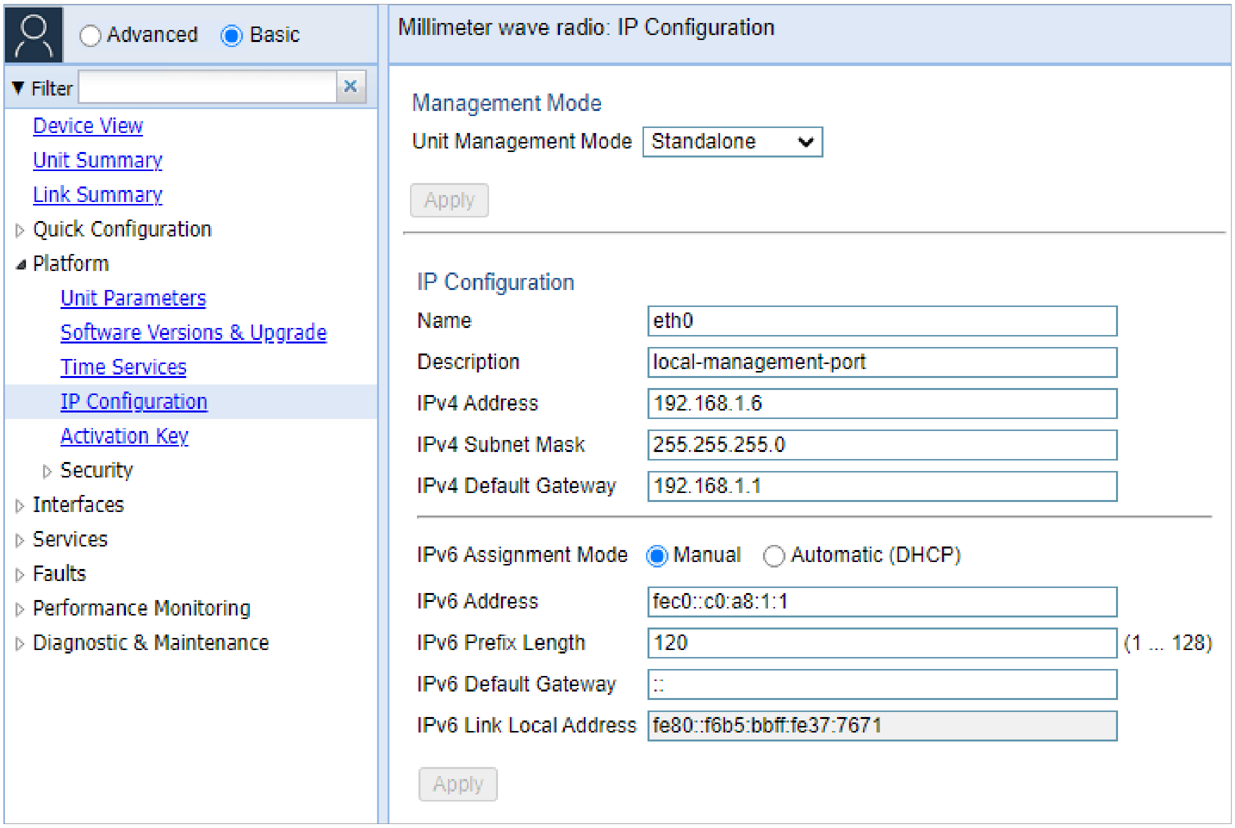
IP Configuration Page

In the IP Configuration page, you can configure the unit's IP address and related parameters. For an explanation of IP configuration, see Changing the Management IP Address.

Note

In the Unit Management Mode field, leave the default value of Standalone unless you are managing the device via RAON. For instructions on configuring and using RAON to manage PTP 850 devices with PTP 850FX200, refer to the User Guide for RAON.

Figure 39 *Basic Mode – IP Configuration Page*



Millimeter wave radio: IP Configuration

Management Mode

Unit Management Mode: Standalone

IP Configuration

Name	eth0
Description	local-management-port
IPv4 Address	192.168.1.6
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	192.168.1.1
IPv6 Assignment Mode	● Manual ○ Automatic (DHCP)
IPv6 Address	fec0::c0:a8:1:1
IPv6 Prefix Length	120 (1 ... 128)
IPv6 Default Gateway	::
IPv6 Link Local Address	fe80::f6b5:bbff:fe37:7671

Activation Key Page

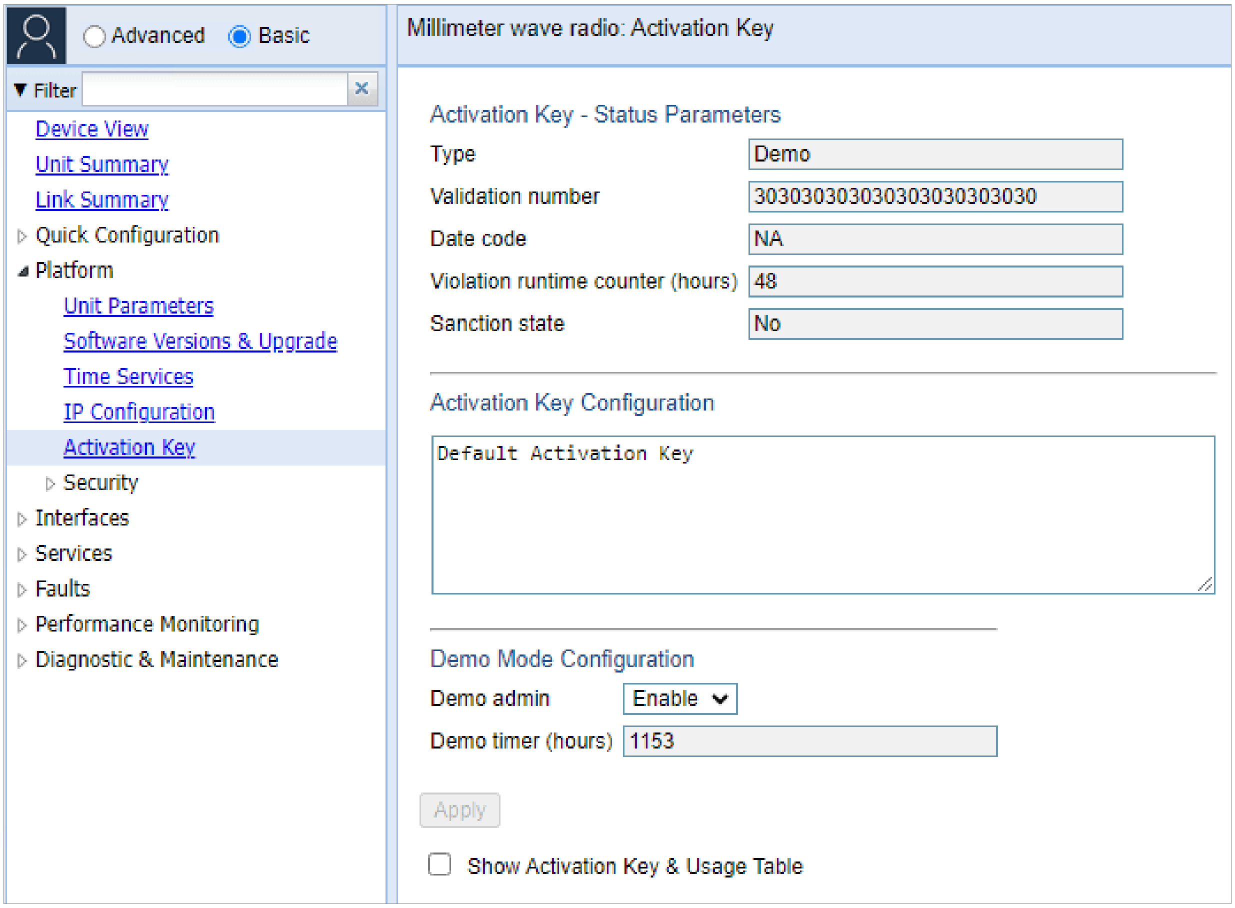
In the Activation Key page, you can configure the unit's activation key. You can also display the status of activation key coverage for features and capacities in the unit.

Note

To display the status of activation key coverage, select Show Activation Key & Usage Table. The status details appear at the bottom of the page, as shown in Basic Mode – Activation Key Page.

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

Figure 40 *Basic Mode – Activation Key Page*



Millimeter wave radio: Activation Key

Activation Key - Status Parameters

Type	Demo
Validation number	303030303030303030303030
Date code	NA
Violation runtime counter (hours)	48
Sanction state	No

Activation Key Configuration

```
Default Activation Key
```

Demo Mode Configuration

Demo admin: Enable

Demo timer (hours): 1153

□ Show Activation Key & Usage Table

Security Pages

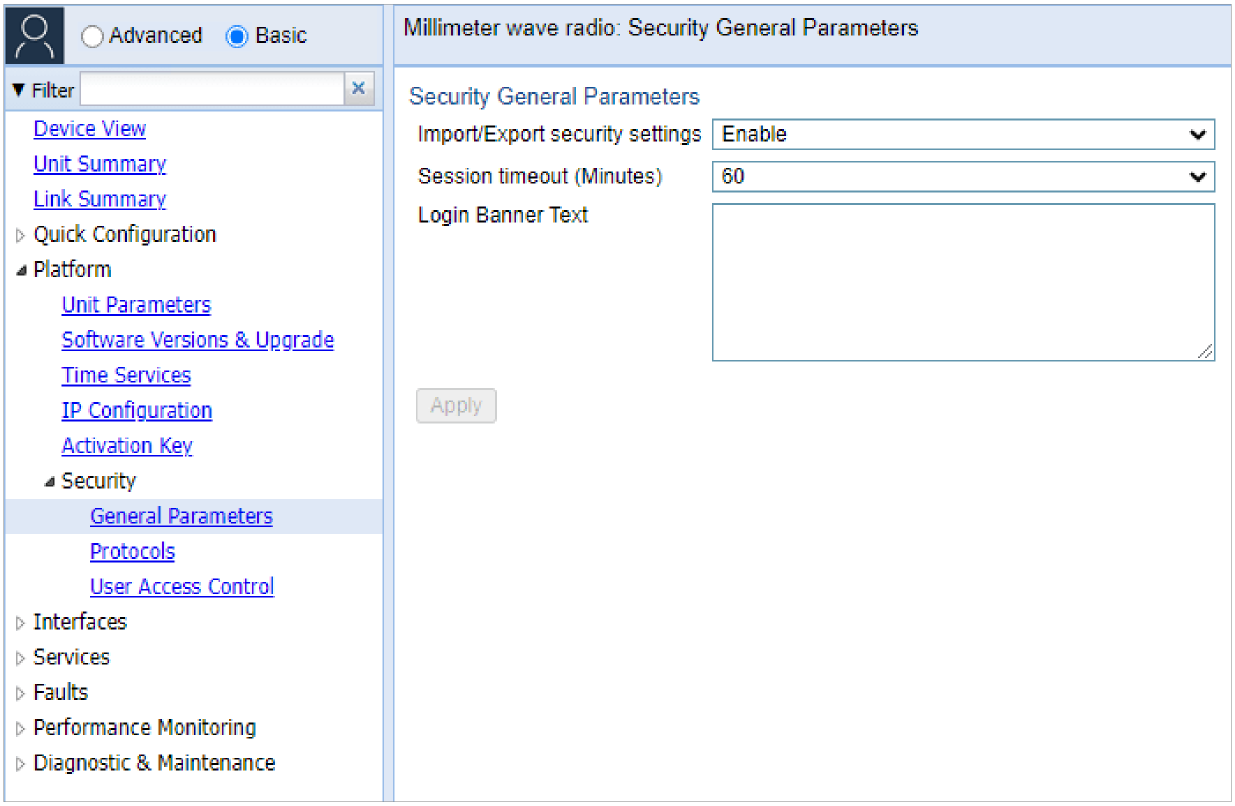
From the Security menu, you can access pages that enable you to configure the unit, including:

- 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 access, 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 41 *Basic Mode – Security – General Parameters Page*



Millimeter wave radio: Security General Parameters

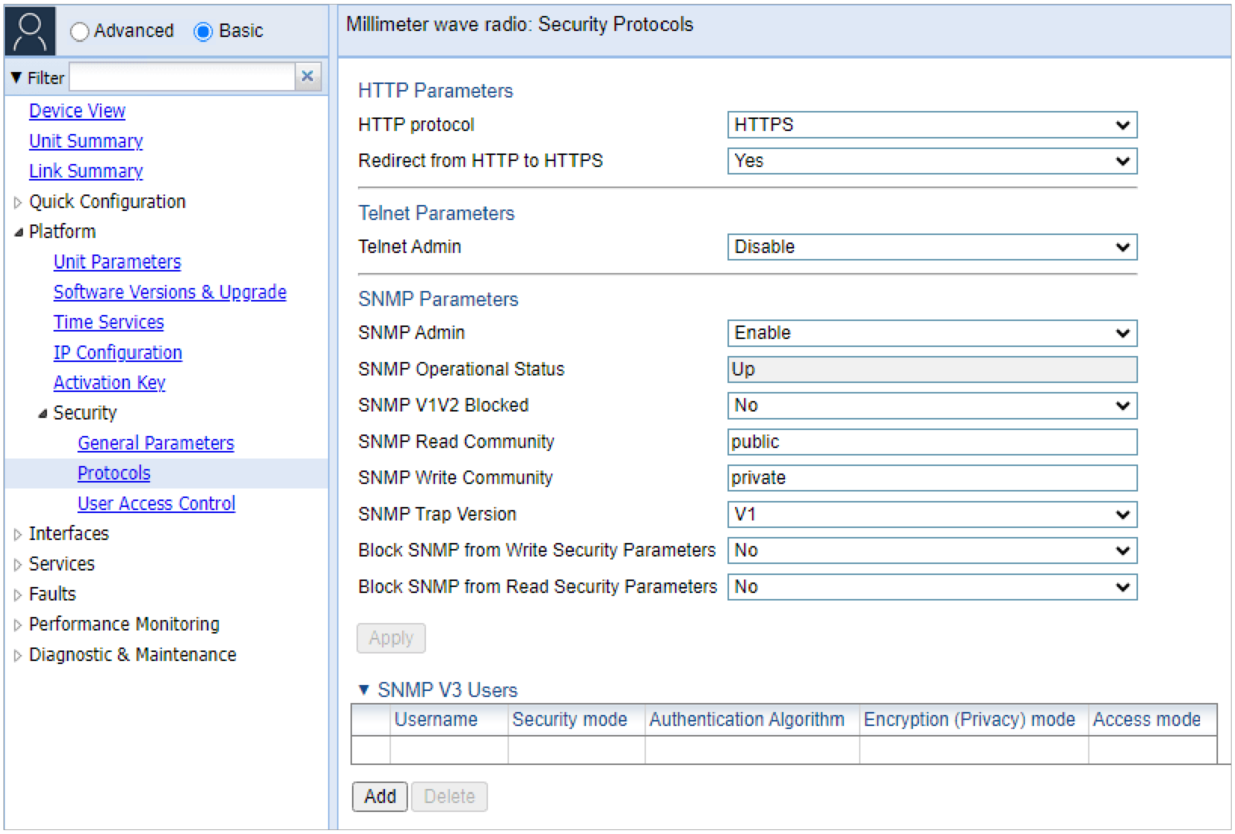
Security General Parameters

Import/Export security settings	Enable
Session timeout (Minutes)	60
Login Banner Text	

Protocols Page

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

Figure 42 *Basic Mode – Security – Protocols Page*



Millimeter wave radio: Security Protocols

HTTP Parameters

HTTP protocol	HTTPS
Redirect from HTTP to HTTPS	Yes

Telnet Parameters

Telnet Admin	Disable

SNMP Parameters

SNMP Admin	Enable
SNMP Operational Status	Up
SNMP V1V2 Blocked	No
SNMP Read Community	public
SNMP Write Community	private
SNMP Trap Version	V1
Block SNMP from Write Security Parameters	No
Block SNMP from Read Security Parameters	No

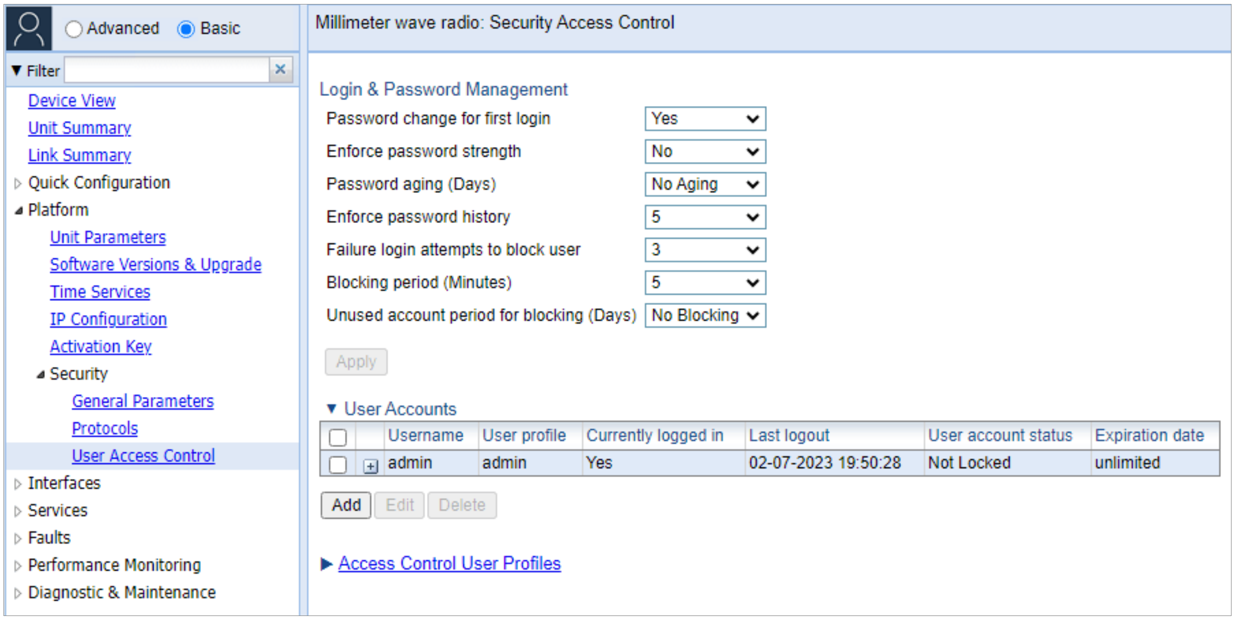
▼ SNMP V3 Users

	Username	Security mode	Authentication Algorithm	Encryption (Privacy) mode	Access mode

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 43 *Basic Mode – Security – Security Access Control Page*



Millimeter wave radio: Security Access Control

Login & Password Management

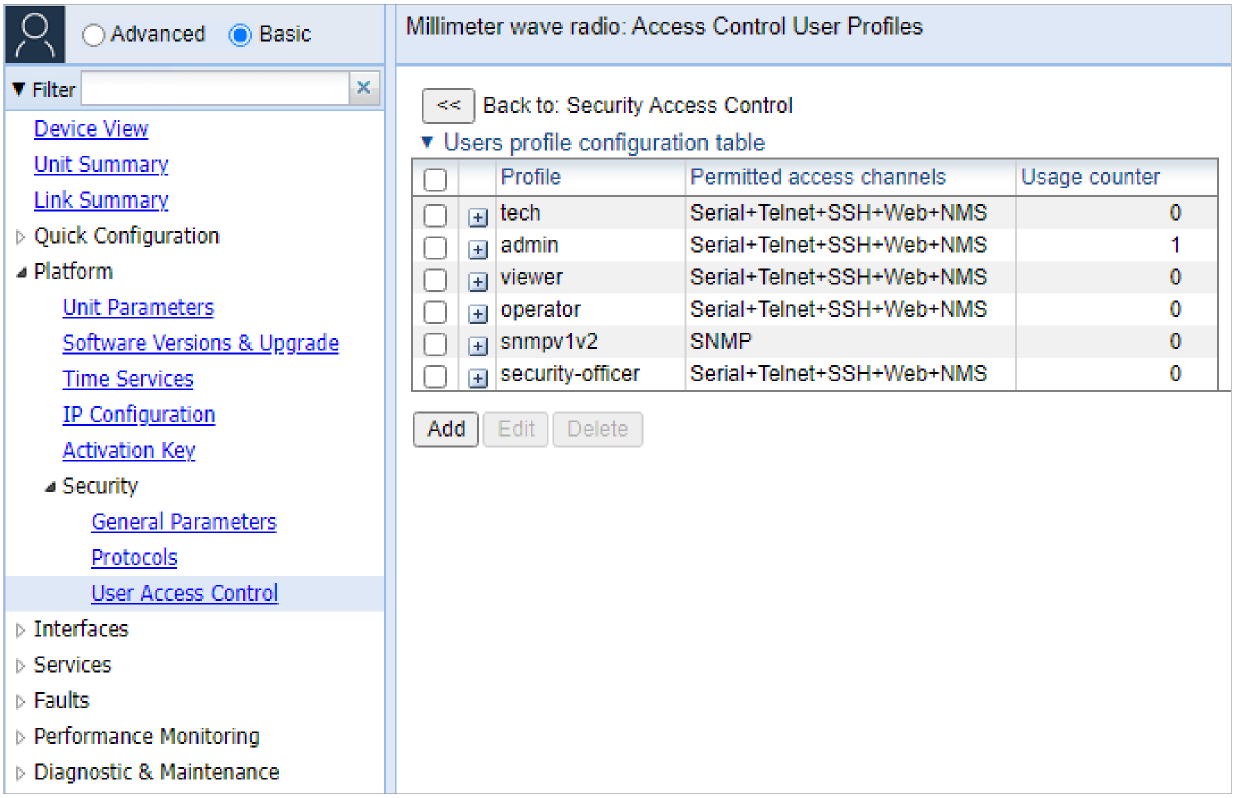
Password change for first login	Yes
Enforce password strength	No
Password aging (Days)	No Aging
Enforce password history	5
Failure login attempts to block user	3
Blocking period (Minutes)	5
Unused account period for blocking (Days)	No Blocking

▼ User Accounts

□	Username	User profile	Currently logged in	Last logout	User account status	Expiration date
□	⊞ admin	admin	Yes	02-07-2023 19:50:28	Not Locked	unlimited

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

Figure 44 *Basic Mode – Security – Access Control User Profiles Page*



Millimeter wave radio: Access Control User Profiles

Back to: Security Access Control

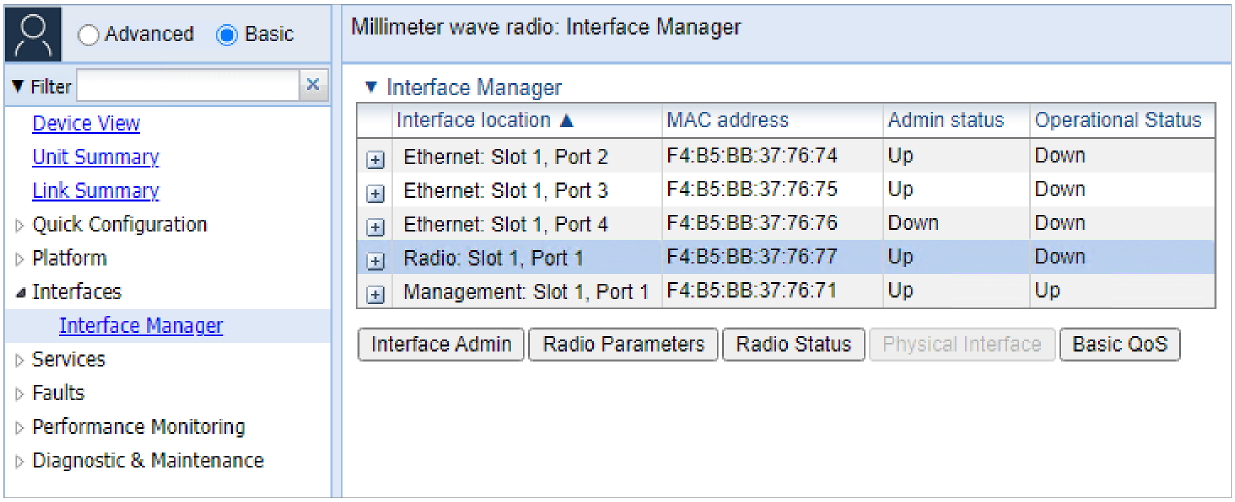
▼ Users profile configuration table

□	Profile	Permitted access channels	Usage counter
□	tech	Serial+Telnet+SSH+Web+NMS	0
□	admin	Serial+Telnet+SSH+Web+NMS	1
□	viewer	Serial+Telnet+SSH+Web+NMS	0
□	operator	Serial+Telnet+SSH+Web+NMS	0
□	snmpv1v2	SNMP	0
□	security-officer	Serial+Telnet+SSH+Web+NMS	0

Interfaces

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

Figure 45 *Basic Mode – Interface Manager Page (PTP 850EX)*



Millimeter wave radio: Interface Manager

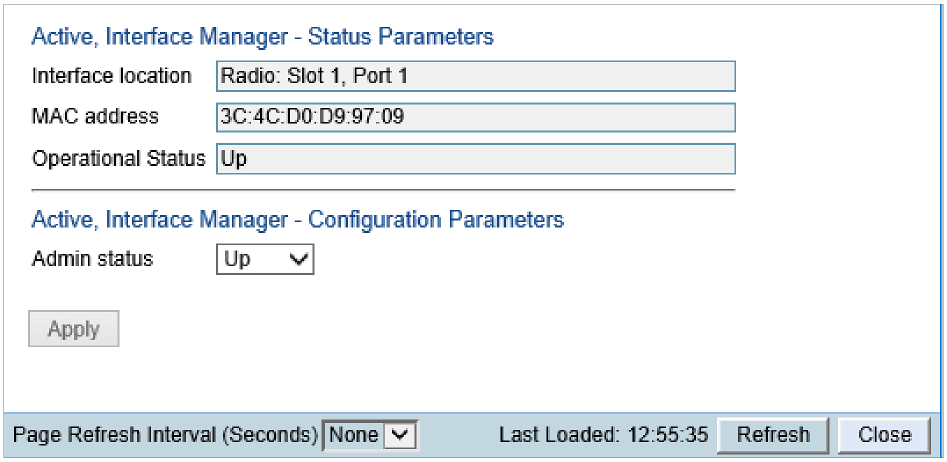
▼ Interface Manager

Interface location ▲	MAC address	Admin status	Operational Status
Ethernet: Slot 1, Port 2	F4:B5:BB:37:76:74	Up	Down
Ethernet: Slot 1, Port 3	F4:B5:BB:37:76:75	Up	Down
Ethernet: Slot 1, Port 4	F4:B5:BB:37:76:76	Down	Down
Radio: Slot 1, Port 1	F4:B5:BB:37:76:77	Up	Down
Management: Slot 1, Port 1	F4:B5:BB:37:76:71	Up	Up

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

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

Figure 46 *Basic Mode – Interface Manager Page – Interface Admin*



Active, Interface Manager - Status Parameters

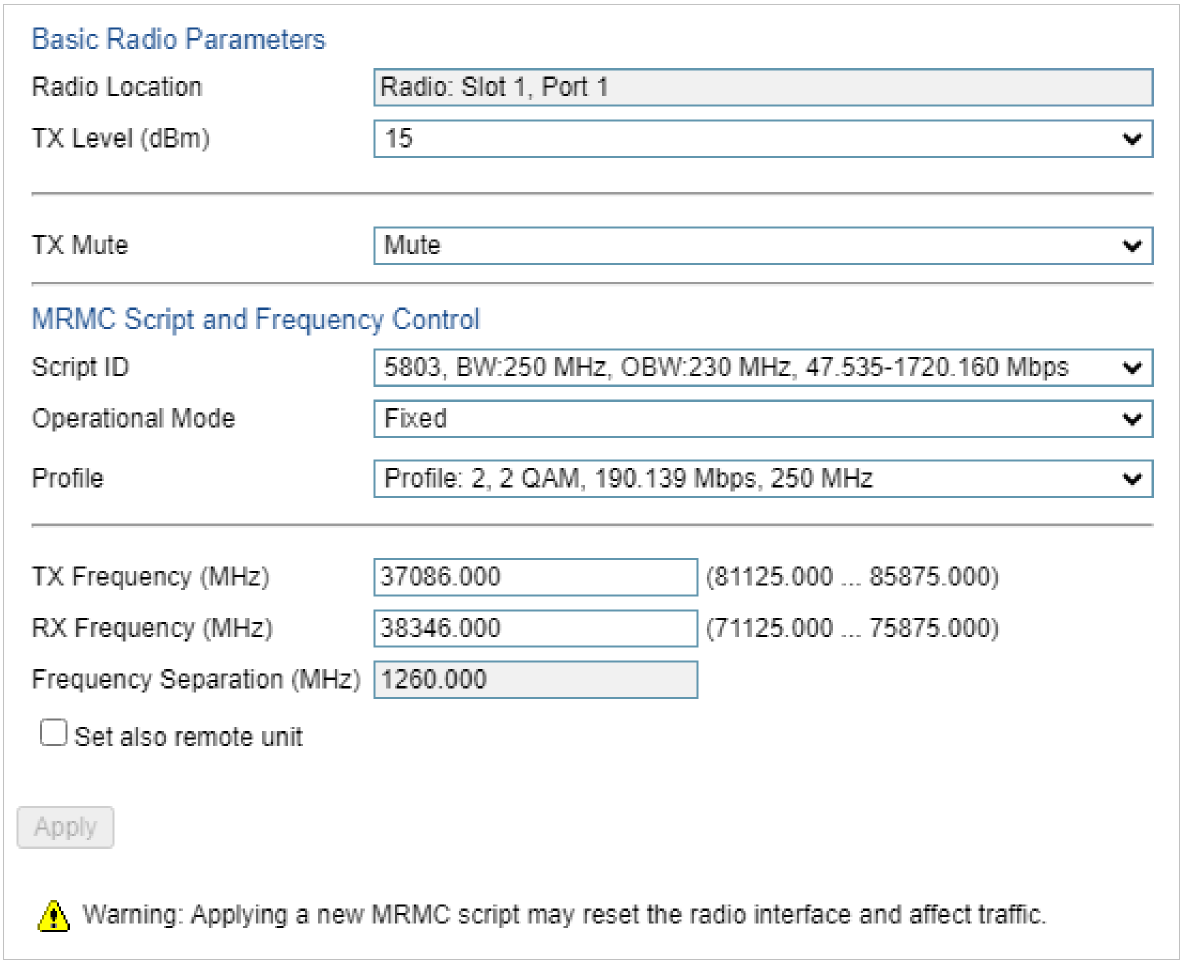
Interface location	Radio: Slot 1, Port 1
MAC address	3C:4C:D0:D9:97:09
Operational Status	Up

Active, Interface Manager - Configuration Parameters

Admin status: Up

- Configure the radio parameters and MRMC script of a radio interface – select the interface and click Radio Parameters. See Configuring the Radio Parameters and Configuring the Radio (MRMC) Script(s).

Figure 47 *Basic Mode – Interface Manager Page – Radio Parameters*



Basic Radio Parameters

Radio Location	Radio: Slot 1, Port 1
TX Level (dBm)	15
TX Mute	Mute

MRMC Script and Frequency Control

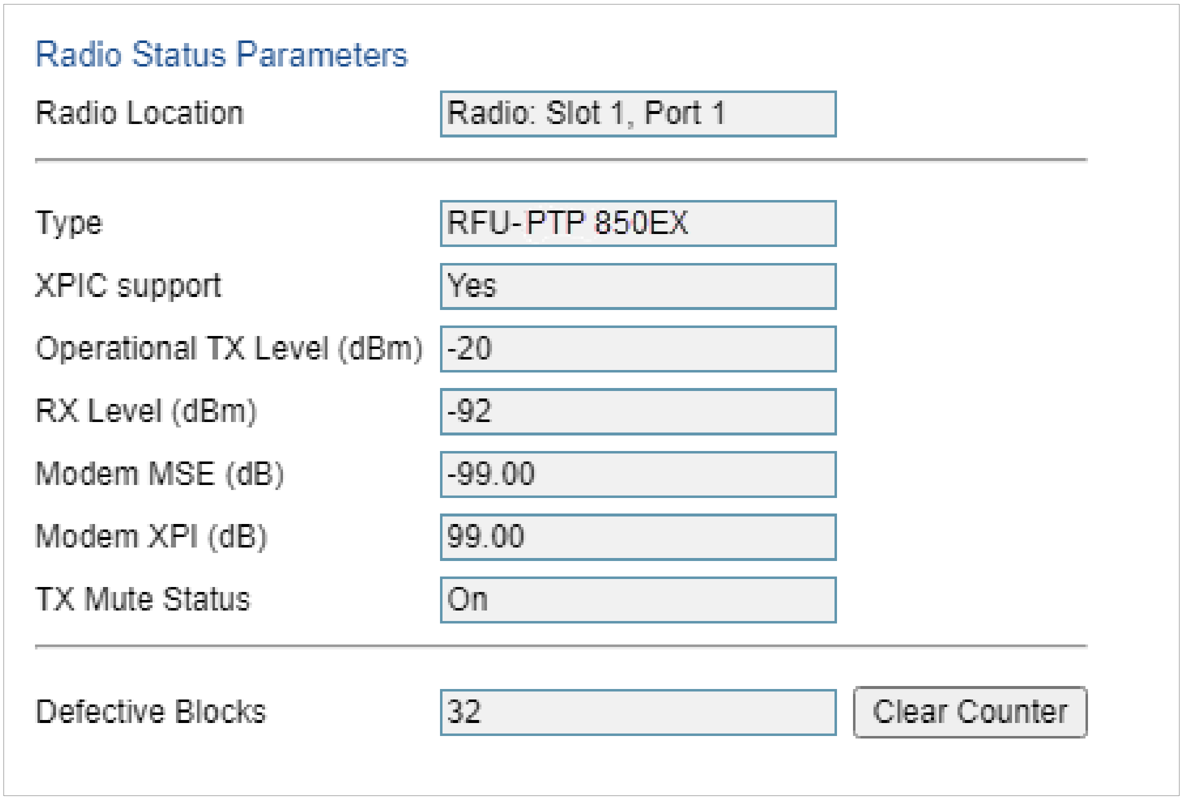
Script ID	5803, BW:250 MHz, OBW:230 MHz, 47.535-1720.160 Mbps	
Operational Mode	Fixed	
Profile	Profile: 2, 2 QAM, 190.139 Mbps, 250 MHz	
TX Frequency (MHz)	37086.000	(81125.000 ... 85875.000)
RX Frequency (MHz)	38346.000	(71125.000 ... 75875.000)
Frequency Separation (MHz)	1260.000	

☐ Set also remote unit

⚠ Warning: Applying a new MRMC script may reset the radio interface and affect traffic.

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

Figure 48 *Basic Mode – Interface Manager Page – Radio Status*

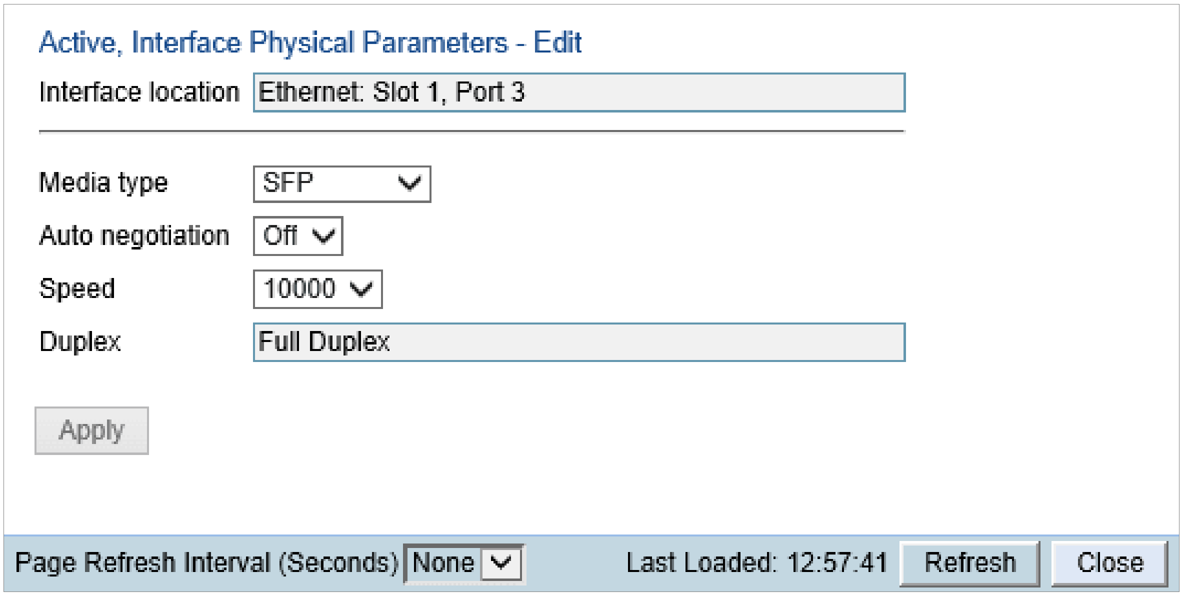


Radio Status Parameters

Radio Location	Radio: Slot 1, Port 1
Type	RFU-PTP 850EX
XPIC support	Yes
Operational TX Level (dBm)	-20
RX Level (dBm)	-92
Modem MSE (dB)	-99.00
Modem XPI (dB)	99.00
TX Mute Status	On
Defective Blocks	32

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

Figure 49 *Basic Mode – Interface Manager Page – Physical Interface*



Active, Interface Physical Parameters - Edit

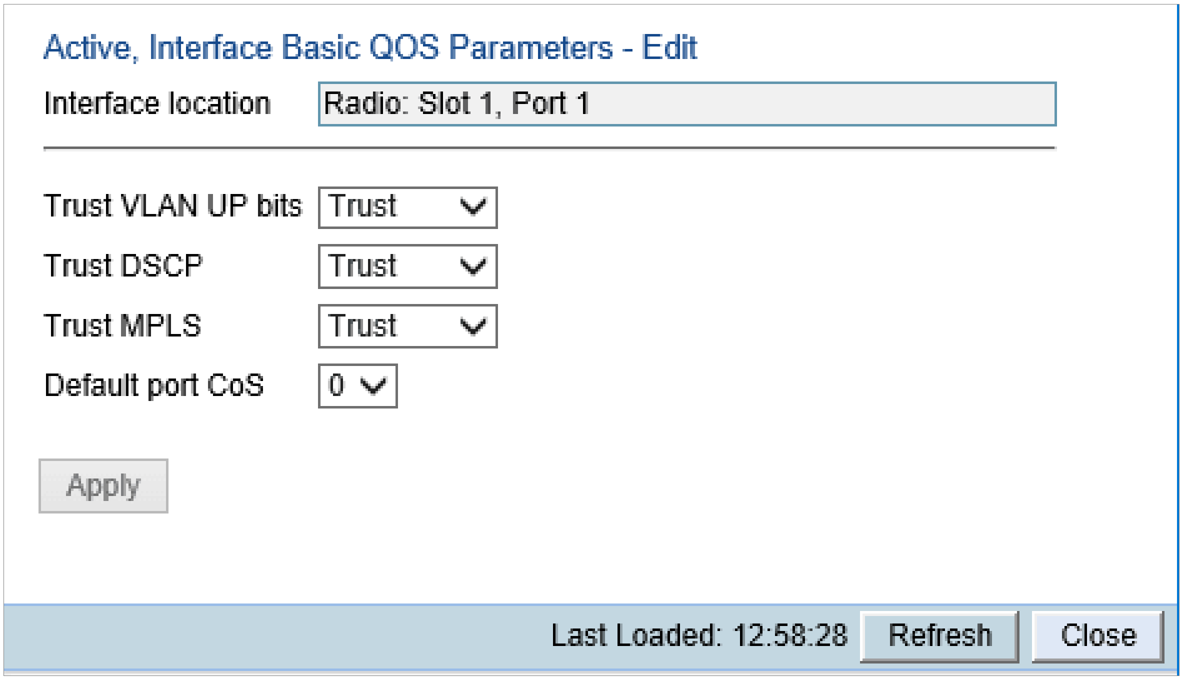
Interface location	Ethernet: Slot 1, Port 3
Media type	SFP
Auto negotiation	Off
Speed	10000
Duplex	Full Duplex

Page Refresh Interval (Seconds) None

Last Loaded: 12:57:41

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

Figure 50 *Basic Mode – Interface Manager Page – Basic QoS*



Active, Interface Basic QOS Parameters - Edit

Interface location: Radio: Slot 1, Port 1

Trust VLAN UP bits: Trust

Trust DSCP: Trust

Trust MPLS: Trust

Default port CoS: 0

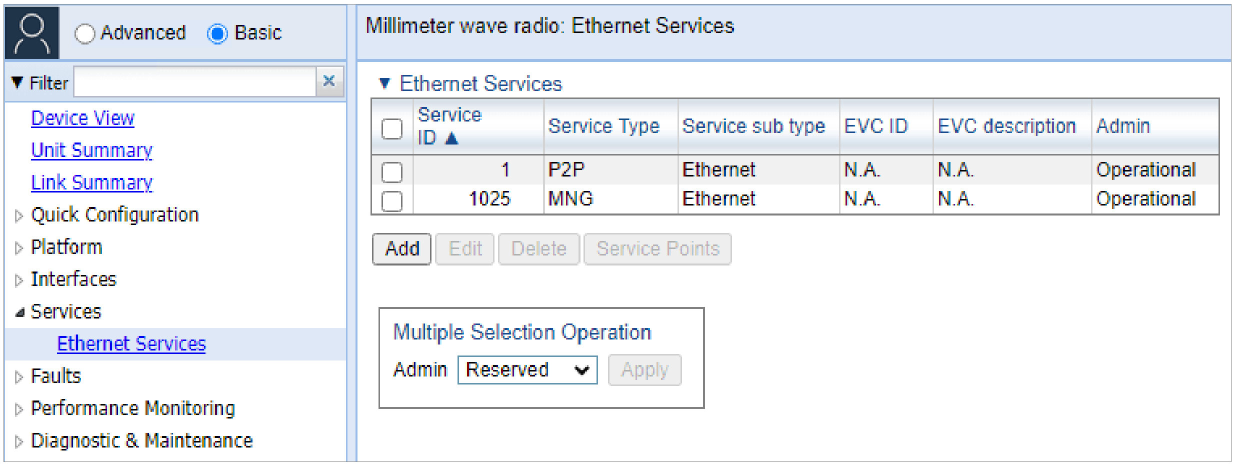
Last Loaded: 12:58:28

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 51 *Basic Mode – Ethernet Services*



Millimeter wave radio: Ethernet Services

▼ Ethernet Services

□	Service ID ▲	Service Type	Service sub type	EVC ID	EVC description	Admin
□	1	P2P	Ethernet	N.A.	N.A.	Operational
□	1025	MNG	Ethernet	N.A.	N.A.	Operational

Multiple Selection Operation

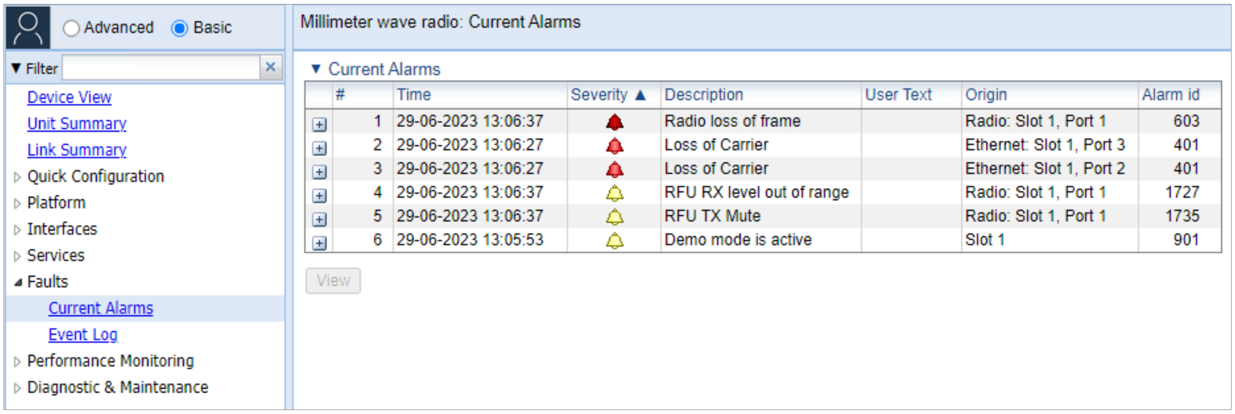
Admin: Reserved

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 52 *Basic Mode – Current Alarms*



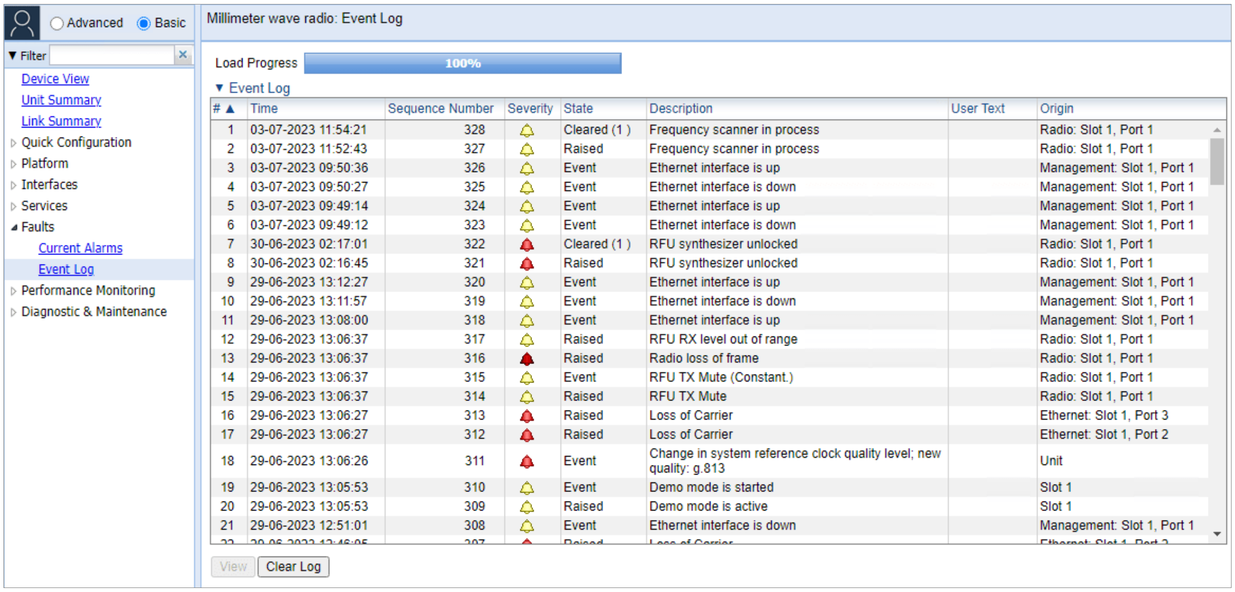
Millimeter wave radio: Current Alarms

▼ Current Alarms

	#	Time	Severity ▲	Description	User Text	Origin	Alarm id
⊞	1	29-06-2023 13:06:37	🔴	Radio loss of frame		Radio: Slot 1, Port 1	603
⊞	2	29-06-2023 13:06:27	🔴	Loss of Carrier		Ethernet: Slot 1, Port 3	401
⊞	3	29-06-2023 13:06:27	🔴	Loss of Carrier		Ethernet: Slot 1, Port 2	401
⊞	4	29-06-2023 13:06:37	🟡	RFU RX level out of range		Radio: Slot 1, Port 1	1727
⊞	5	29-06-2023 13:06:37	🟡	RFU TX Mute		Radio: Slot 1, Port 1	1735
⊞	6	29-06-2023 13:05:53	🟡	Demo mode is active		Slot 1	901

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

Figure 53 *Basic Mode – Event Log*



Millimeter wave radio: Event Log

Load Progress 100%

▼ Event Log

# ▲	Time	Sequence Number	Severity	State	Description	User Text	Origin
1	03-07-2023 11:54:21	328	🟡	Cleared (1)	Frequency scanner in process		Radio: Slot 1, Port 1
2	03-07-2023 11:52:43	327	🟡	Raised	Frequency scanner in process		Radio: Slot 1, Port 1
3	03-07-2023 09:50:36	326	🟡	Event	Ethernet interface is up		Management: Slot 1, Port 1
4	03-07-2023 09:50:27	325	🟡	Event	Ethernet interface is down		Management: Slot 1, Port 1
5	03-07-2023 09:49:14	324	🟡	Event	Ethernet interface is up		Management: Slot 1, Port 1
6	03-07-2023 09:49:12	323	🟡	Event	Ethernet interface is down		Management: Slot 1, Port 1
7	30-06-2023 02:17:01	322	🔴	Cleared (1)	RFU synthesizer unlocked		Radio: Slot 1, Port 1
8	30-06-2023 02:16:45	321	🔴	Raised	RFU synthesizer unlocked		Radio: Slot 1, Port 1
9	29-06-2023 13:12:27	320	🟡	Event	Ethernet interface is up		Management: Slot 1, Port 1
10	29-06-2023 13:11:57	319	🟡	Event	Ethernet interface is down		Management: Slot 1, Port 1
11	29-06-2023 13:08:00	318	🟡	Event	Ethernet interface is up		Management: Slot 1, Port 1
12	29-06-2023 13:06:37	317	🟡	Raised	RFU RX level out of range		Radio: Slot 1, Port 1
13	29-06-2023 13:06:37	316	🔴	Raised	Radio loss of frame		Radio: Slot 1, Port 1
14	29-06-2023 13:06:37	315	🟡	Event	RFU TX Mute (Constant.)		Radio: Slot 1, Port 1
15	29-06-2023 13:06:37	314	🟡	Raised	RFU TX Mute		Radio: Slot 1, Port 1
16	29-06-2023 13:06:27	313	🔴	Raised	Loss of Carrier		Ethernet: Slot 1, Port 3
17	29-06-2023 13:06:27	312	🔴	Raised	Loss of Carrier		Ethernet: Slot 1, Port 2
18	29-06-2023 13:06:26	311	🔴	Event	Change in system reference clock quality level; new quality: g.813		Unit
19	29-06-2023 13:05:53	310	🟡	Event	Demo mode is started		Slot 1
20	29-06-2023 13:05:53	309	🟡	Raised	Demo mode is active		Slot 1
21	29-06-2023 12:51:01	308	🟡	Event	Ethernet interface is down		Management: Slot 1, Port 1
22	29-06-2023 12:46:05	307	🔴	Raised	Loss of Carrier		Ethernet: Slot 1, Port 2

Performance Monitoring

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

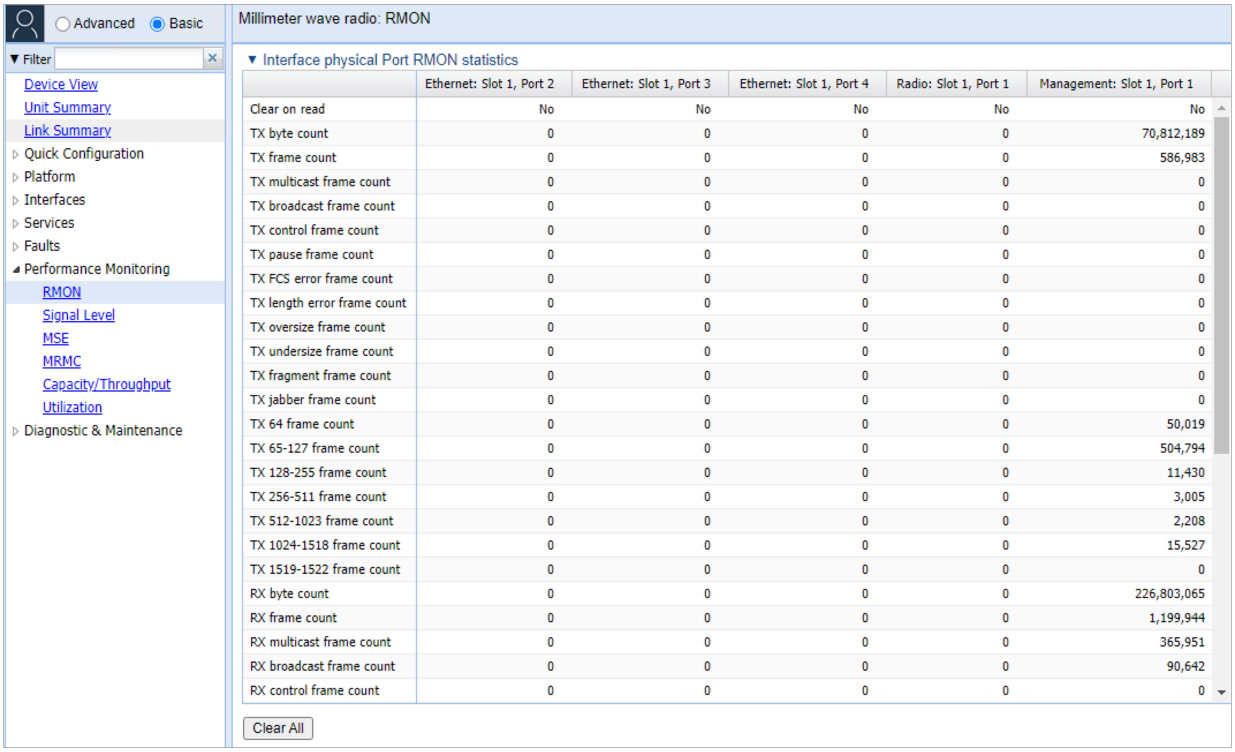
- RMON
- Signal Level
- MSE
- MRMC

- Capacity/Throughput
- Utilization

RMON

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

Figure 54 *Basic Mode – RMON Page*



Millimeter wave radio: RMON

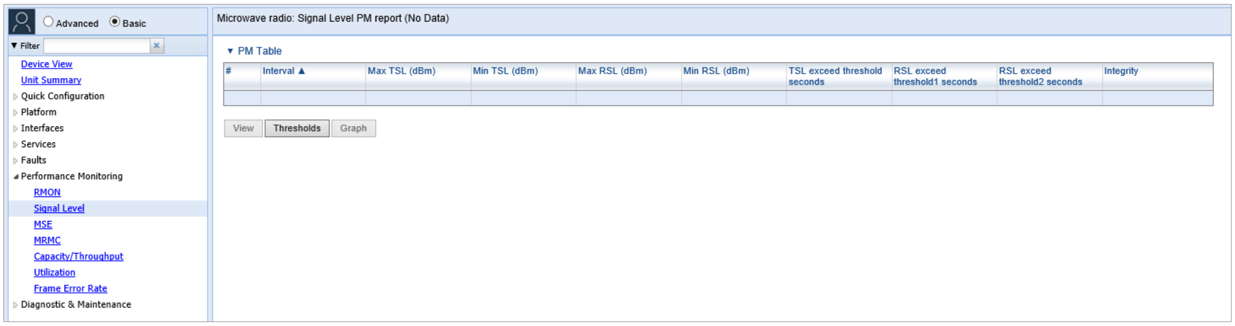
Interface physical Port RMON statistics

	Ethernet: Slot 1, Port 2	Ethernet: Slot 1, Port 3	Ethernet: Slot 1, Port 4	Radio: Slot 1, Port 1	Management: Slot 1, Port 1
Clear on read	No	No	No	No	No
TX byte count	0	0	0	0	70,812,189
TX frame count	0	0	0	0	586,983
TX multicast frame count	0	0	0	0	0
TX broadcast frame count	0	0	0	0	0
TX control frame count	0	0	0	0	0
TX pause frame count	0	0	0	0	0
TX FCS error frame count	0	0	0	0	0
TX length error frame count	0	0	0	0	0
TX oversize frame count	0	0	0	0	0
TX undersize frame count	0	0	0	0	0
TX fragment frame count	0	0	0	0	0
TX jabber frame count	0	0	0	0	0
TX 64 frame count	0	0	0	0	50,019
TX 65-127 frame count	0	0	0	0	504,794
TX 128-255 frame count	0	0	0	0	11,430
TX 256-511 frame count	0	0	0	0	3,005
TX 512-1023 frame count	0	0	0	0	2,208
TX 1024-1518 frame count	0	0	0	0	15,527
TX 1519-1522 frame count	0	0	0	0	0
RX byte count	0	0	0	0	226,803,065
RX frame count	0	0	0	0	1,199,944
RX multicast frame count	0	0	0	0	365,951
RX broadcast frame count	0	0	0	0	90,642
RX control frame count	0	0	0	0	0

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 55 *Basic Mode – Signal Level Page*



Microwave radio: Signal Level PM report (No Data)

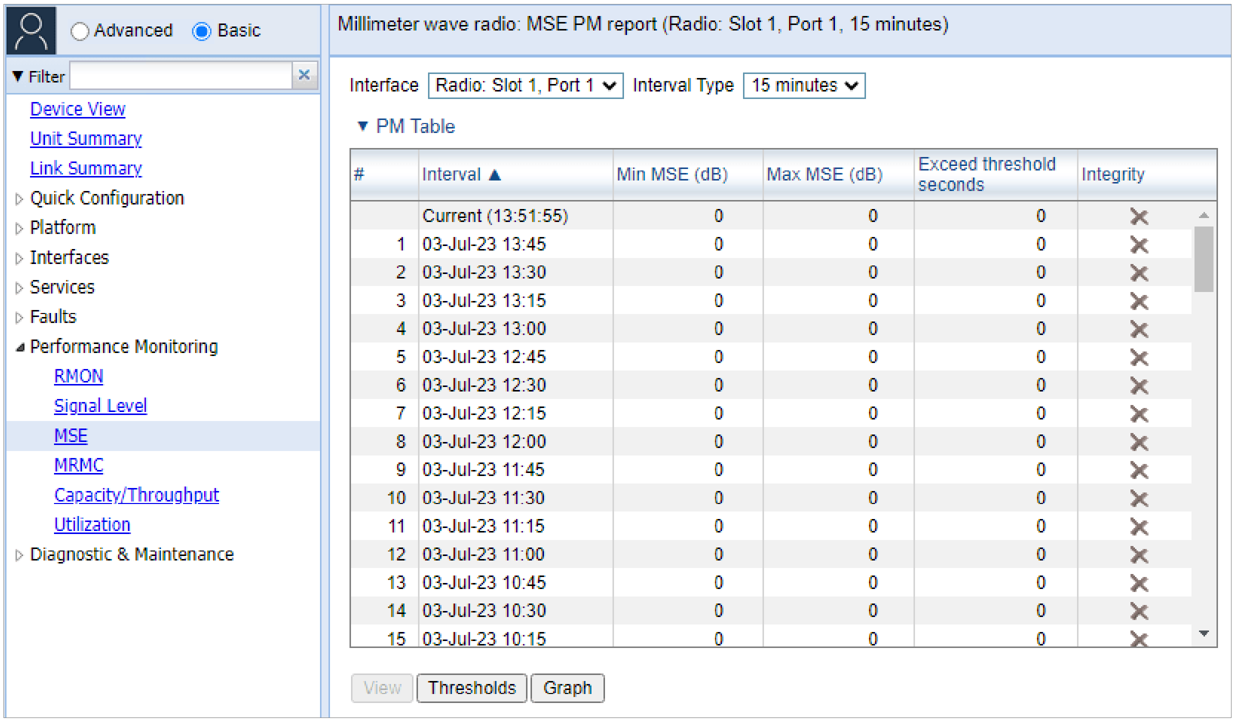
PM Table

#	Interval ▲	Max TSL (dBm)	Min TSL (dBm)	Max RSL (dBm)	Min RSL (dBm)	TSL exceed threshold seconds	RSL exceed threshold1 seconds	RSL exceed threshold2 seconds	Integrity

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 56 *Basic Mode – MSE Page*



Millimeter wave radio: MSE PM report (Radio: Slot 1, Port 1, 15 minutes)

Interface: Radio: Slot 1, Port 1 — Interval Type: 15 minutes

▼ PM Table

#	Interval ▲	Min MSE (dB)	Max MSE (dB)	Exceed threshold seconds	Integrity
	Current (13:51:55)	0	0	0	✗
1	03-Jul-23 13:45	0	0	0	✗
2	03-Jul-23 13:30	0	0	0	✗
3	03-Jul-23 13:15	0	0	0	✗
4	03-Jul-23 13:00	0	0	0	✗
5	03-Jul-23 12:45	0	0	0	✗
6	03-Jul-23 12:30	0	0	0	✗
7	03-Jul-23 12:15	0	0	0	✗
8	03-Jul-23 12:00	0	0	0	✗
9	03-Jul-23 11:45	0	0	0	✗
10	03-Jul-23 11:30	0	0	0	✗
11	03-Jul-23 11:15	0	0	0	✗
12	03-Jul-23 11:00	0	0	0	✗
13	03-Jul-23 10:45	0	0	0	✗
14	03-Jul-23 10:30	0	0	0	✗
15	03-Jul-23 10:15	0	0	0	✗

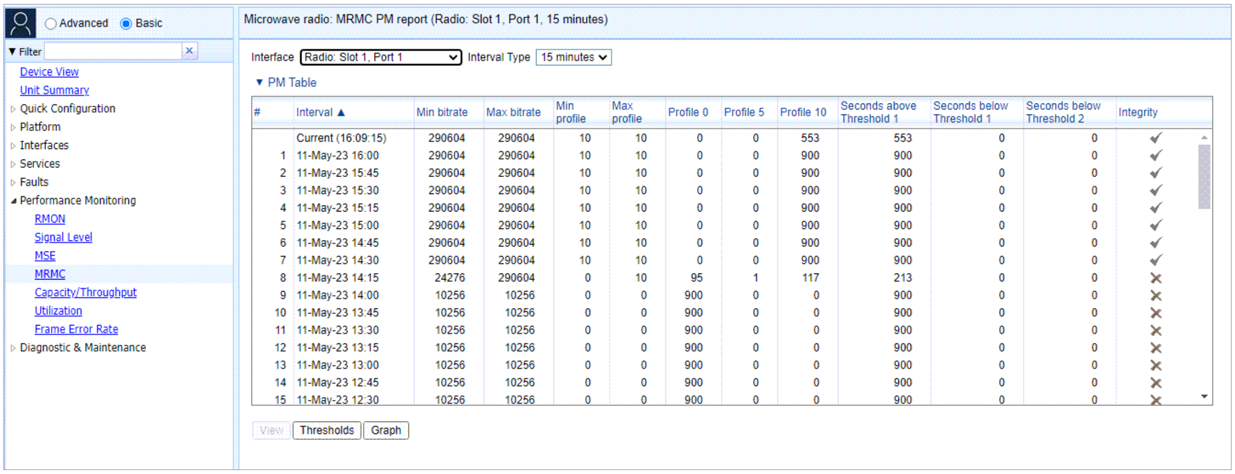
MRMC

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 display the number of seconds each carrier operated at each ACM profile for these 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 Thresholds.

Figure 57 *Basic Mode – MRMC Page*



Microwave radio: MRMC PM report (Radio: Slot 1, Port 1, 15 minutes)

Interface: Radio: Slot 1, Port 1 Interval Type: 15 minutes

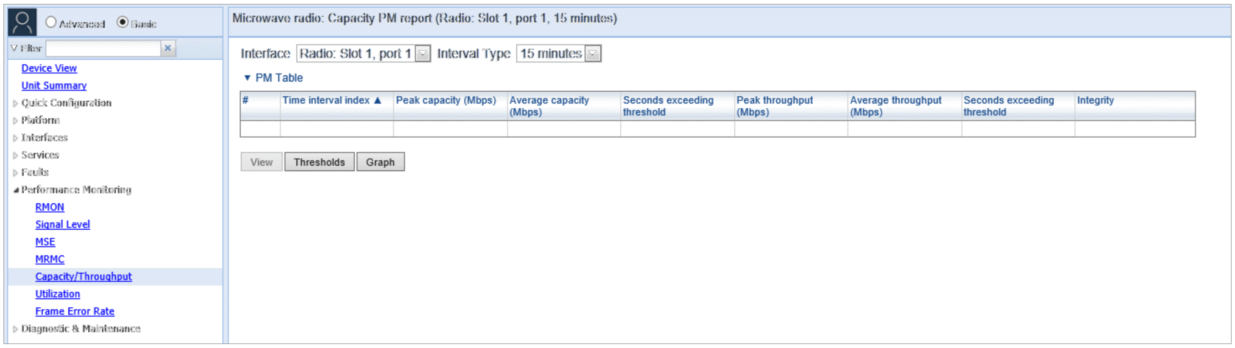
▼ PM Table

#	Interval ▲	Min bitrate	Max bitrate	Min profile	Max profile	Profile 0	Profile 5	Profile 10	Seconds above Threshold 1	Seconds below Threshold 1	Seconds below Threshold 2	Integrity
	Current (16:09:15)	290604	290604	10	10	0	0	553	553	0	0	✓
1	11-May-23 16:00	290604	290604	10	10	0	0	900	900	0	0	✓
2	11-May-23 15:45	290604	290604	10	10	0	0	900	900	0	0	✓
3	11-May-23 15:30	290604	290604	10	10	0	0	900	900	0	0	✓
4	11-May-23 15:15	290604	290604	10	10	0	0	900	900	0	0	✓
5	11-May-23 15:00	290604	290604	10	10	0	0	900	900	0	0	✓
6	11-May-23 14:45	290604	290604	10	10	0	0	900	900	0	0	✓
7	11-May-23 14:30	290604	290604	10	10	0	0	900	900	0	0	✓
8	11-May-23 14:15	24276	290604	0	10	95	1	117	213	0	0	✗
9	11-May-23 14:00	10256	10256	0	0	900	0	0	900	0	0	✗
10	11-May-23 13:45	10256	10256	0	0	900	0	0	900	0	0	✗
11	11-May-23 13:30	10256	10256	0	0	900	0	0	900	0	0	✗
12	11-May-23 13:15	10256	10256	0	0	900	0	0	900	0	0	✗
13	11-May-23 13:00	10256	10256	0	0	900	0	0	900	0	0	✗
14	11-May-23 12:45	10256	10256	0	0	900	0	0	900	0	0	✗
15	11-May-23 12:30	10256	10256	0	0	900	0	0	900	0	0	✗

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 58 *Basic Mode – Capacity/Throughput Page*



Microwave radio: Capacity PM report (Radio: Slot 1, port 1, 15 minutes)

Interface: Radio: Slot 1, port 1 Interval Type: 15 minutes

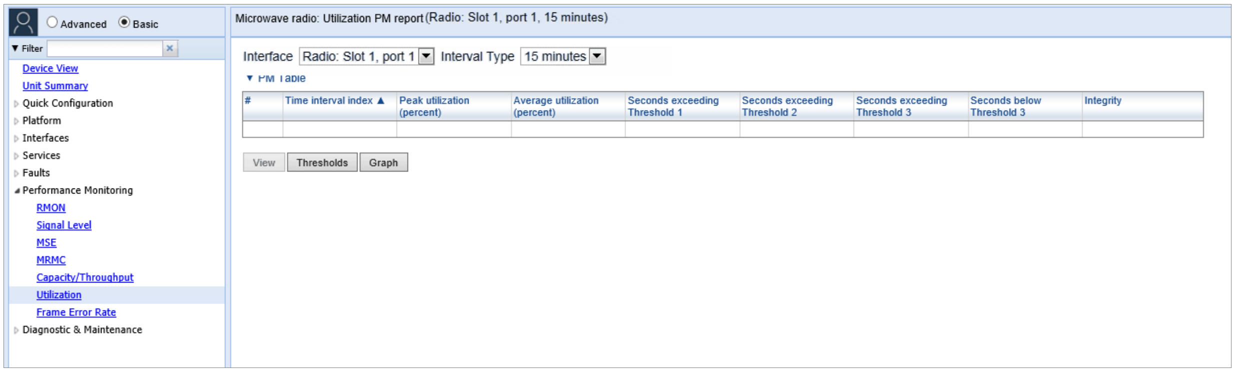
▼ PM Table

#	Time interval index ▲	Peak capacity (Mbps)	Average capacity (Mbps)	Seconds exceeding threshold	Peak throughput (Mbps)	Average throughput (Mbps)	Seconds exceeding threshold	Integrity

Utilization

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

Figure 59 *Basic Mode – Utilization Page*



Microwave radio: Utilization PM report (Radio: Slot 1, port 1, 15 minutes)

Interface: Radio: Slot 1, port 1 Interval Type: 15 minutes

▼ PM Table

#	Time interval index ▲	Peak utilization (percent)	Average utilization (percent)	Seconds exceeding Threshold 1	Seconds exceeding Threshold 2	Seconds exceeding Threshold 3	Seconds below Threshold 3	Integrity

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.

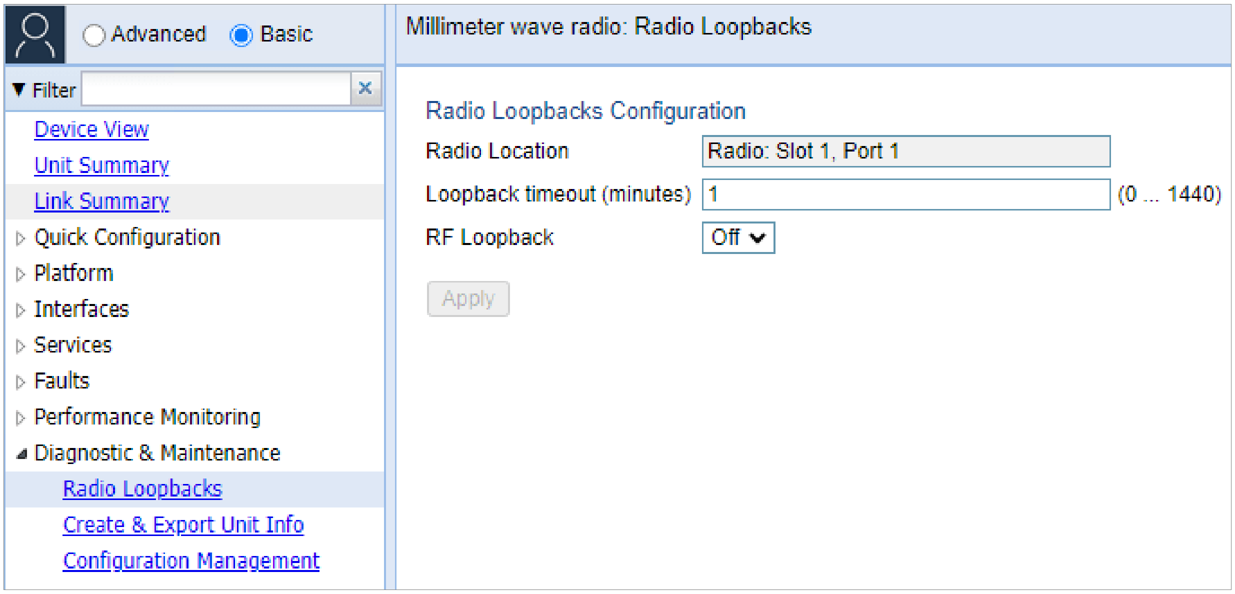
When performing RF loopback, the antenna port of the radio must be terminated.

Setting radio loopback, either RF or IF, will cause full loss of the end-to-end traffic and in-band management to remote units. 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 radio loopback, click Radio Loopback. For further information, see Performing Radio Loopback.

Figure 60 *Basic Mode – Radio Loopbacks Page*



Millimeter wave radio: Radio Loopbacks

Radio Loopbacks Configuration

Radio Location: Radio: Slot 1, Port 1

Loopback timeout (minutes): 1 (0 ... 1440)

RF Loopback: Off

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.

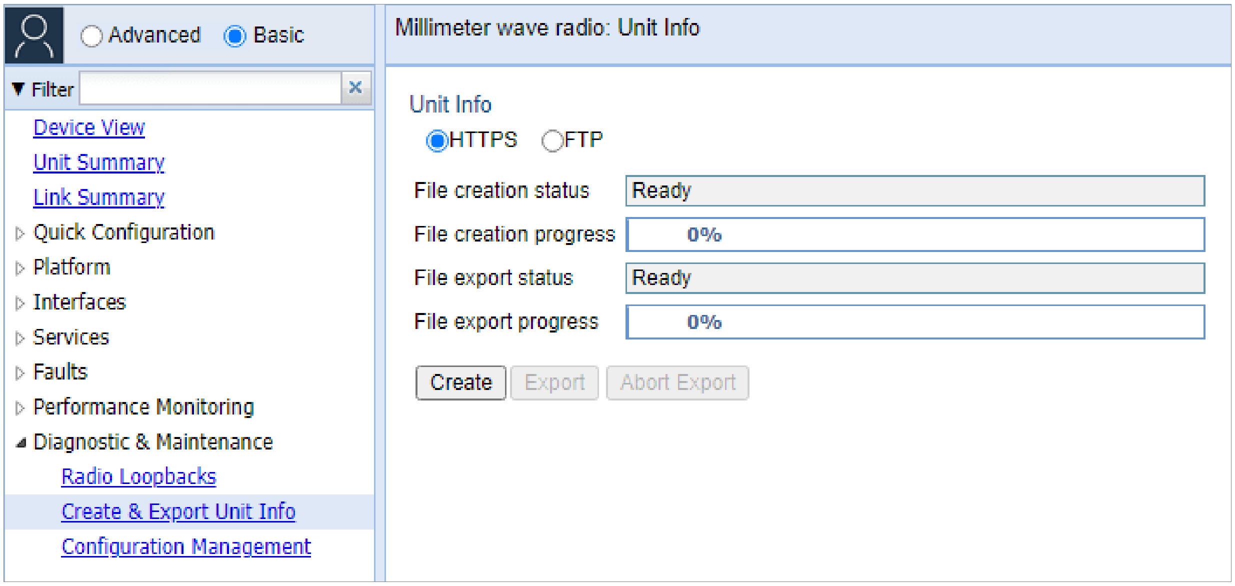
You can upload the Unit Information file using HTTP, HTTPS, FTP, or SFTP.

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.

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

Figure 61 *Basic Mode – Unit Info Page*



Millimeter wave radio: Unit Info

Unit Info

● HTTPS ○ FTP

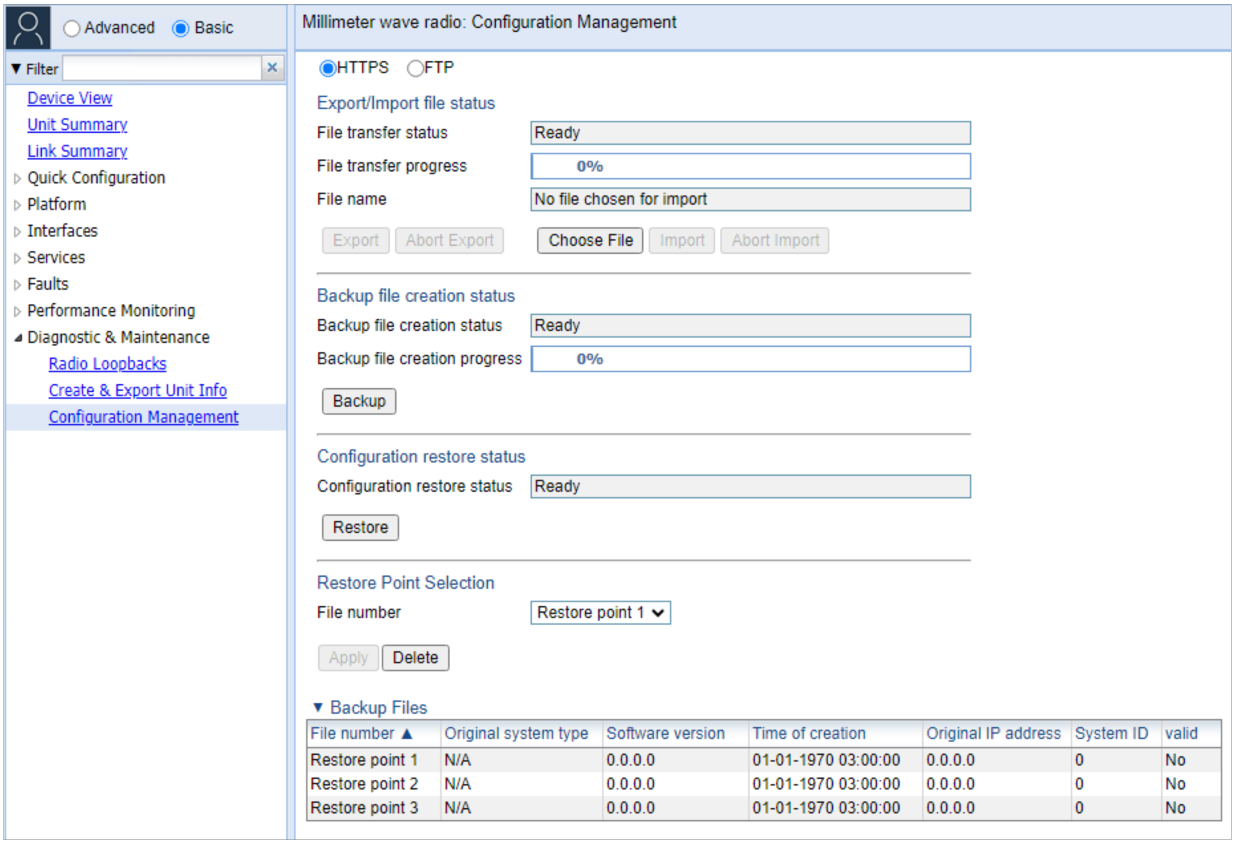
File creation status	Ready
File creation progress	0%
File export status	Ready
File export progress	0%

Configuration Management

You can import and export device configuration files. This enables you to copy the system configuration to multiple devices. 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 62 *Basic Mode – Configuration Management Page*



Millimeter wave radio: Configuration Management

● HTTPS ○ FTP

Export/Import file status

File transfer status: Ready

File transfer progress: 0%

File name: No file chosen for import

Backup file creation status

Backup file creation status: Ready

Backup file creation progress: 0%

Configuration restore status

Configuration restore status: Ready

Restore Point Selection

File number: Restore point 1

▼ Backup Files

File number ▲	Original system type	Software version	Time of creation	Original IP address	System ID	valid
Restore point 1	N/A	0.0.0.0	01-01-1970 03:00:00	0.0.0.0	0	No
Restore point 2	N/A	0.0.0.0	01-01-1970 03:00:00	0.0.0.0	0	No
Restore point 3	N/A	0.0.0.0	01-01-1970 03:00:00	0.0.0.0	0	No

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. See Configuring a 1+0 Link Using the Quick Configuration Wizard.
  This wizard can also be used to configure XPIC on the unit. See XPIC Overview.
- **Enhanced Multi-Carrier ABC** – Configures a 2 + 0 Multi-Carrier ABC group consisting of an Ethernet interface or LAG and the two radio interfaces. See Configuring a 2+0 Multi-Carrier ABC Link Using the Quick Configuration Wizard .
- **Layer 1 Link Bonding (Attached Unit)** – Configures an PTP 850EX that is an attached unit in a Link Bonding configuration that is an attached unit in a Link Bonding configuration with an PTP 850E. Although the Link Bonding group itself is configured on the main unit (PTP 850E), certain configurations are also required on the attached unit to support the Link Bonding configuration. This wizard also enables you to configure the radio, MRMC, and XPIC (optional) parameters on the attached unit. See Configuring PTP 850EX as an Attached Unit in a Layer 1 Link Bonding Group.

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. See Deleting a Service Point.

Note

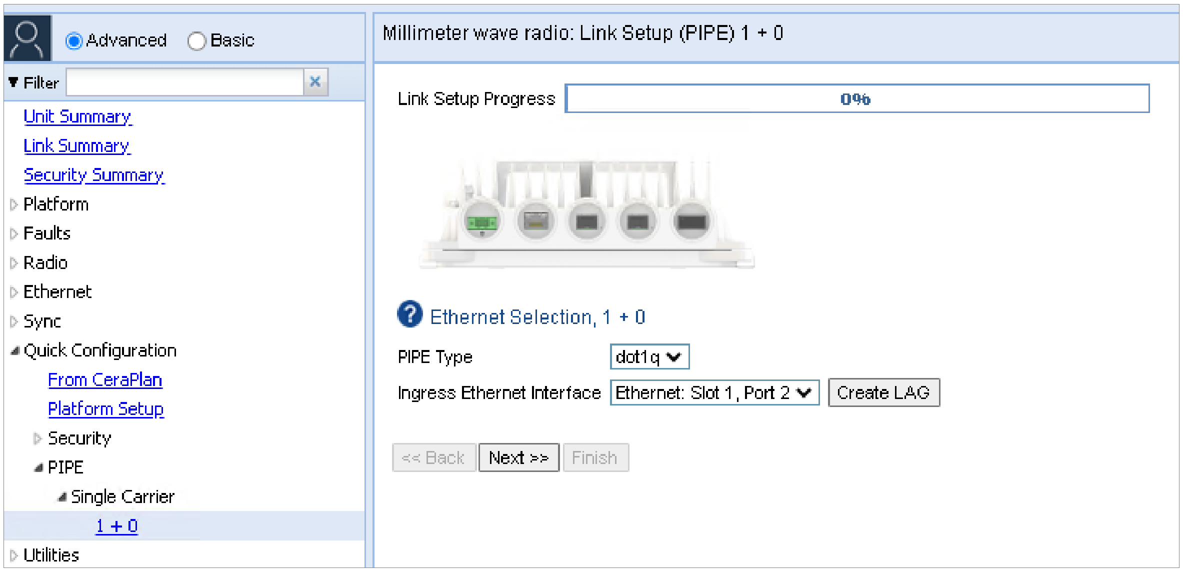
For all configurations, it is recommended that the MRMC script configurations be symmetric on both sides of the link, including the same script and minimum and maximum ACM profiles.

Configuring a 1+0 Link Using the Quick Configuration Wizard

To configure a 1+0 link using the Quick Configuration wizard:

1. Select **Quick Configuration** > **PIPE** > **Single Carrier** > **1+0**. The Ethernet Selection page of the 1+0 Quick Configuration wizard opens.

Figure 63 *1+0 Quick Configuration Wizard – Ethernet Selection*



Millimeter wave radio: Link Setup (PIPE) 1 + 0

Link Setup Progress 0%

Ethernet Selection, 1 + 0

PIPE Type: dot1q

Ingress Ethernet Interface: Ethernet: Slot 1, Port 2

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, see Configuring Ethernet Service(s).

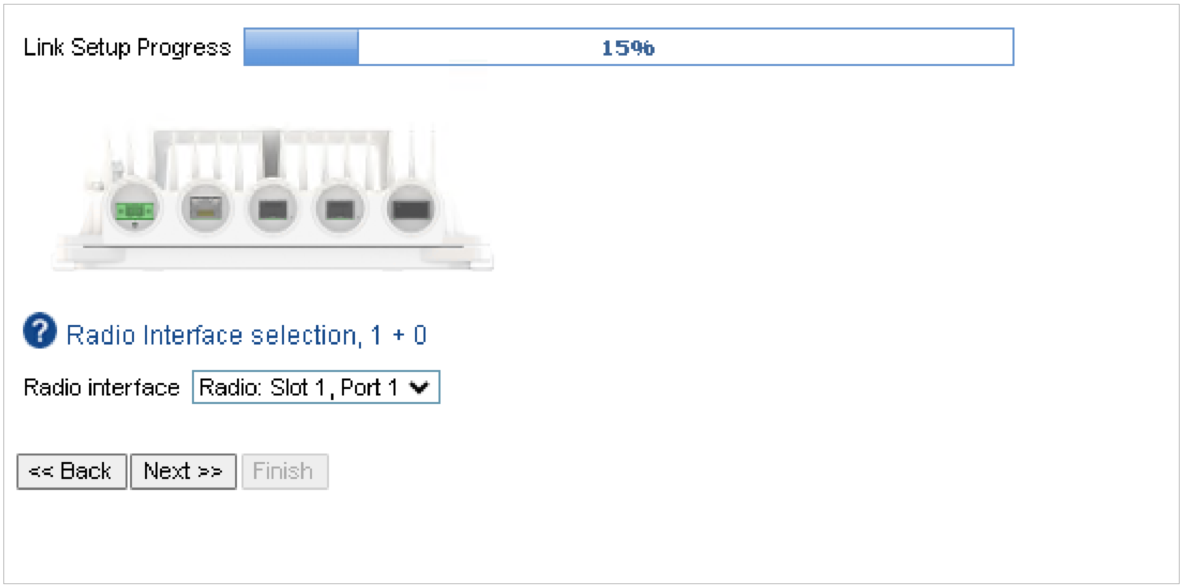
3. In the **Ingress Ethernet Interface** field, select an Ethernet interface or LAG for the link.

Note

To create a LAG, click Create LAG. The Create LAG Group page opens. For instructions on creating LAG groups, see Configuring Link Aggregation (LAG).

4. Click **Next**. The Radio Interface Selection page of the 1+0 Quick Configuration wizard opens.

Figure 64 *1+0 Quick Configuration Wizard – Radio Interface Selection*



Link Setup Progress 15%

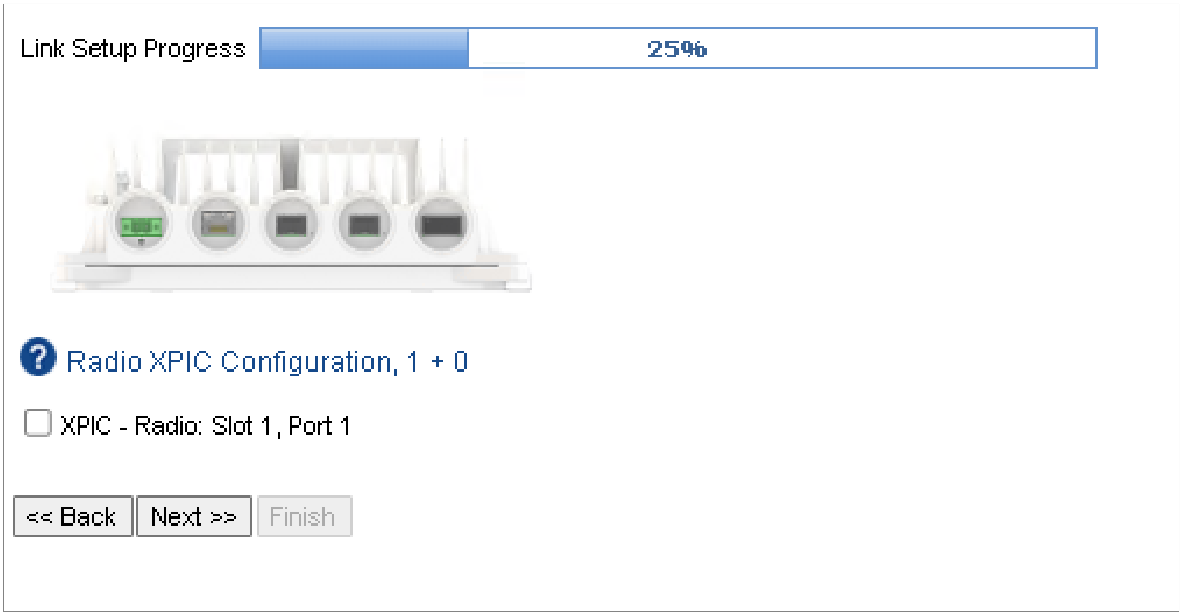
Radio Interface selection, 1 + 0

Radio interface: Radio: Slot 1, Port 1

5. In the **Radio Interface** field, select Radio: Slot 1, Port 1.

6. Click **Next**. The Radio XPIC Configuration page of the 1+0 Quick Configuration wizard opens.

Figure 65 *1+0 Quick Configuration Wizard – Radio XPIC Configuration*



Link Setup Progress 25%

Radio XPIC Configuration, 1 + 0

□ XPIC - Radio: Slot 1, Port 1

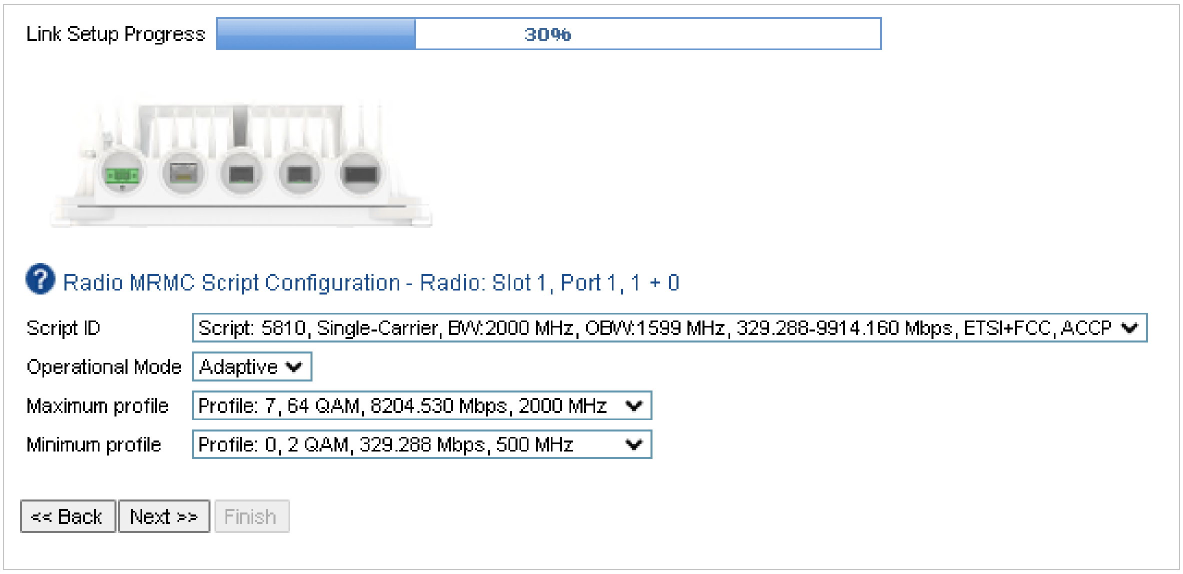
7. If the unit is part of an XPIC link, select XPIC.

Note

For PTP 850EX, XPIC is planned for future release.

8. Click **Next**. The MRMC Script Configuration page of the 1+0 Quick Configuration wizard opens.

Figure 66 *1+0 Quick Configuration Wizard – MRMC Script Configuration*



Link Setup Progress 30%

Radio MRMC Script Configuration - Radio: Slot 1, Port 1, 1 + 0

Script ID: Script: 5810, Single-Carrier, BW:2000 MHz, OBW:1599 MHz, 329.288-9914.160 Mbps, ETSI+FCC, ACCP

Operational Mode: Adaptive

Maximum profile: Profile: 7, 64 QAM, 8204.530 Mbps, 2000 MHz

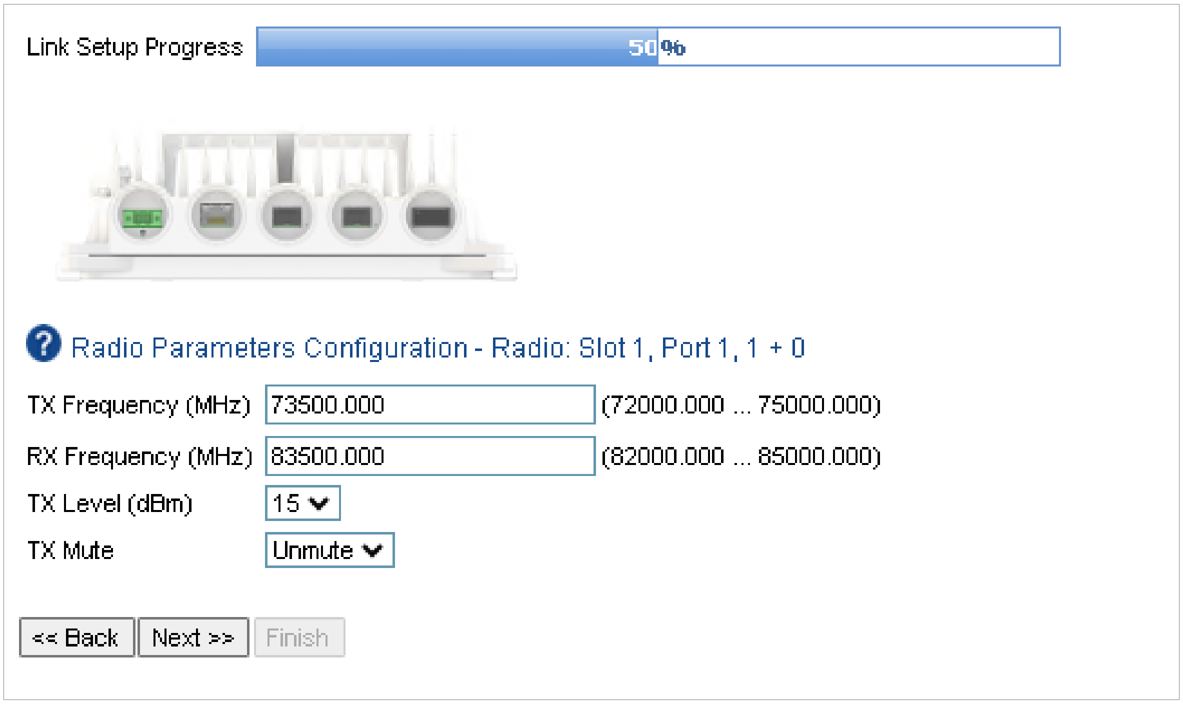
Minimum profile: Profile: 0, 2 QAM, 329.288 Mbps, 500 MHz

9. In the **Script ID** field, select an MRMC script.
10. 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.
11. 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).

        > **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.

12. Click **Next**. The Radio Parameters Configuration page of the 1+0 Quick Configuration wizard opens.

Figure 67 *1+0 Quick Configuration Wizard – Radio Parameters Configuration*



Link Setup Progress 50%

Radio Parameters Configuration - Radio: Slot 1, Port 1, 1 + 0

TX Frequency (MHz) 73500.000 (72000.000 ... 75000.000)

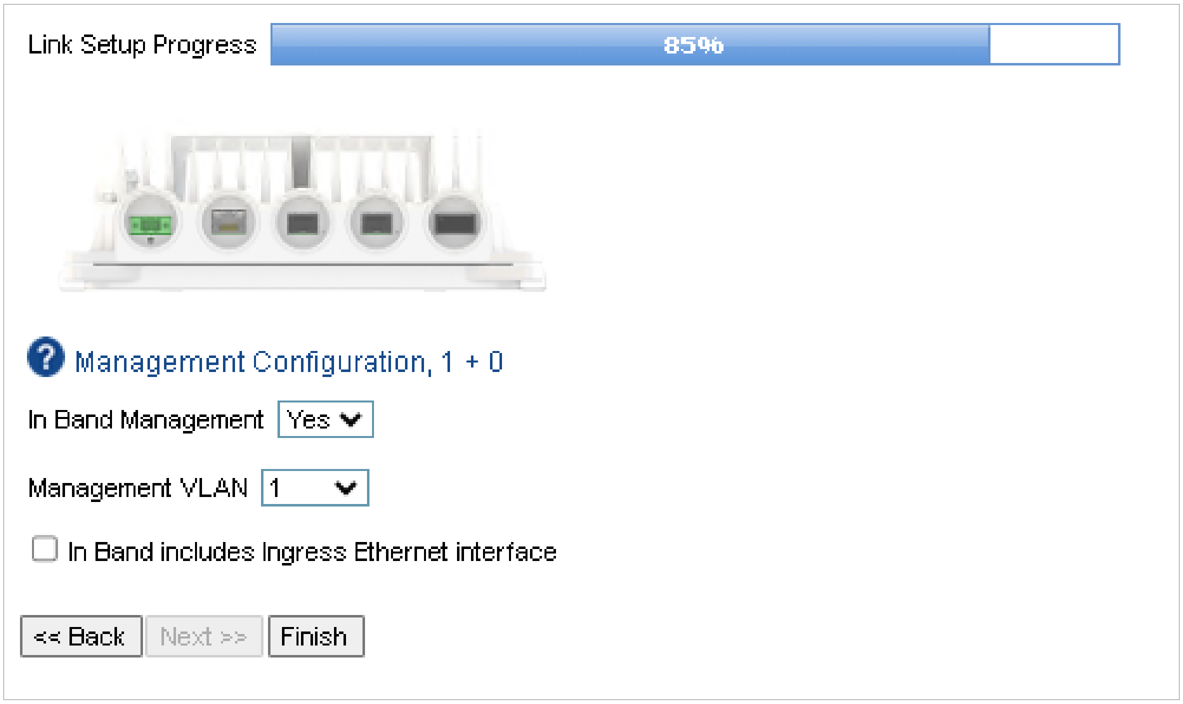
RX Frequency (MHz) 83500.000 (82000.000 ... 85000.000)

TX Level (dBm) 15

TX Mute Unmute

13. In the **TX Frequency (MHz)** field, set the transmission radio frequency in MHz.
14. In the **RX Frequency (MHz)** field, set the received radio frequency in MHz.
15. In the **TX Level (dBm)** field, enter the desired TX signal level (TSL). The range of values depends on the frequency and RFU type.
16. 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.
17. Click **Next**. The Management Configuration page of the 1+0 Quick Configuration wizard opens.

Figure 68 *1+0 Quick Configuration Wizard – Management Configuration*



Link Setup Progress 85%

Management Configuration, 1 + 0

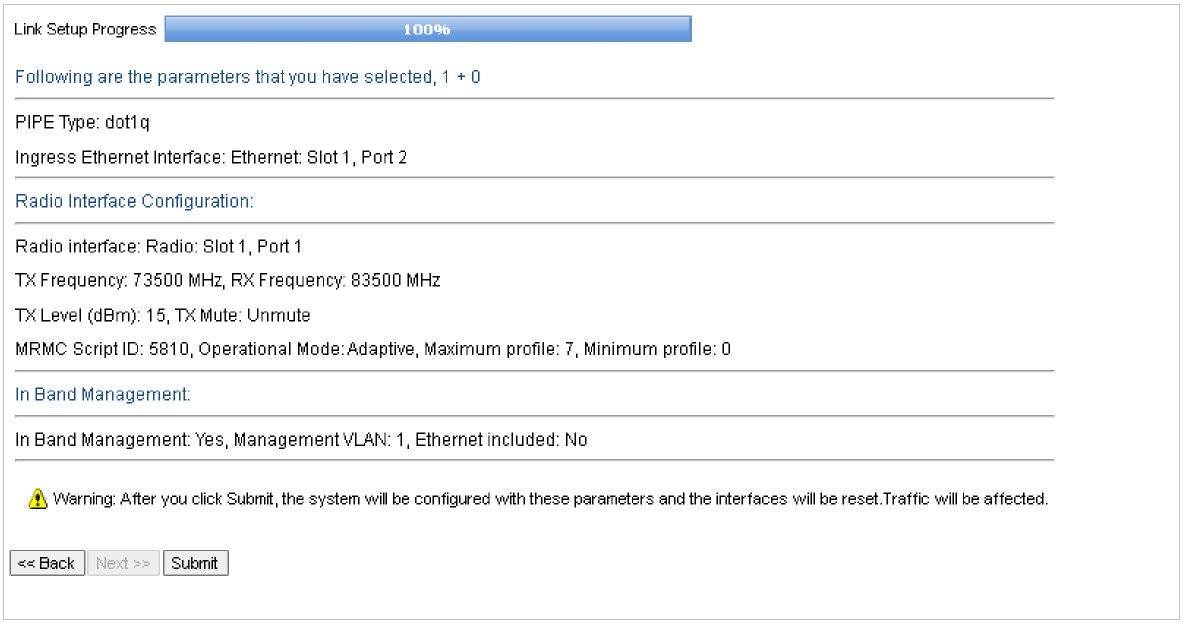
In Band Management: Yes

Management VLAN: 1

□ In Band includes Ingress Ethernet interface

18. 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.
19. If you selected Yes in the **In Band Management** field, select the management VLAN in the Management VLAN field.
20. If you want to use the Ethernet interface as well as the radio interface for in-band management, select In Band includes Ethernet interface.
21. Click **Finish**. The Summary page of the 1+0 Quick Configuration wizard opens. This page displays the parameters you have selected for the link.

Figure 69 *1+0 Quick Configuration Wizard –Summary Page*



Following are the parameters that you have selected, 1 + 0

PIPE Type: dot1q

Ingress Ethernet Interface: Ethernet: Slot 1, Port 2

Radio Interface Configuration:

Radio interface: Radio: Slot 1, Port 1

TX Frequency: 73500 MHz, RX Frequency: 83500 MHz

TX Level (dBm): 15, TX Mute: Unmute

MRMC Script ID: 5810, Operational Mode:Adaptive, Maximum profile: 7, Minimum profile: 0

In Band Management:

In Band Management: Yes, Management VLAN: 1, Ethernet included: No

⚠ Warning: After you click Submit, the system will be configured with these parameters and the interfaces will be reset.Traffic will be affected.

22. 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.

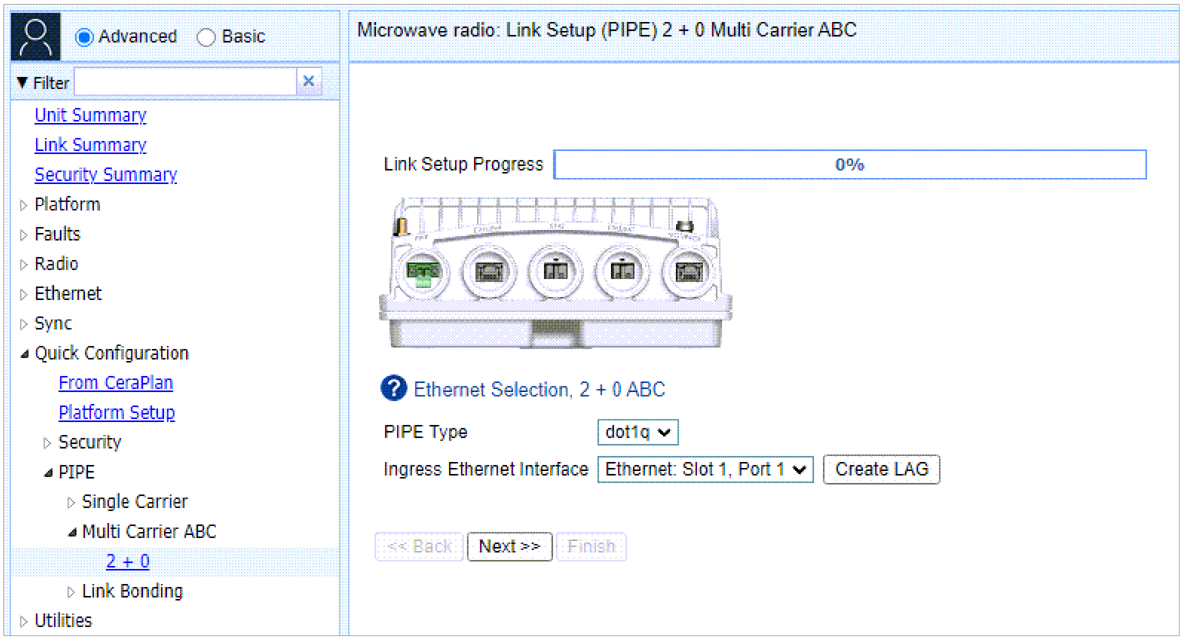
Configuring a 2+0 Multi-Carrier ABC Link Using the Quick Configuration Wizard

For important general information about Multi-Carrier ABC, see Configuring 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 70 *2 + 0 Multi Carrier ABC Quick Configuration Wizard – Ethernet Selection*



Microwave radio: Link Setup (PIPE) 2 + 0 Multi Carrier ABC

Link Setup Progress 0%

Ethernet Selection, 2 + 0 ABC

PIPE Type: dot1q

Ingress Ethernet Interface: Ethernet: Slot 1, Port 1

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, see Configuring Ethernet Service(s).

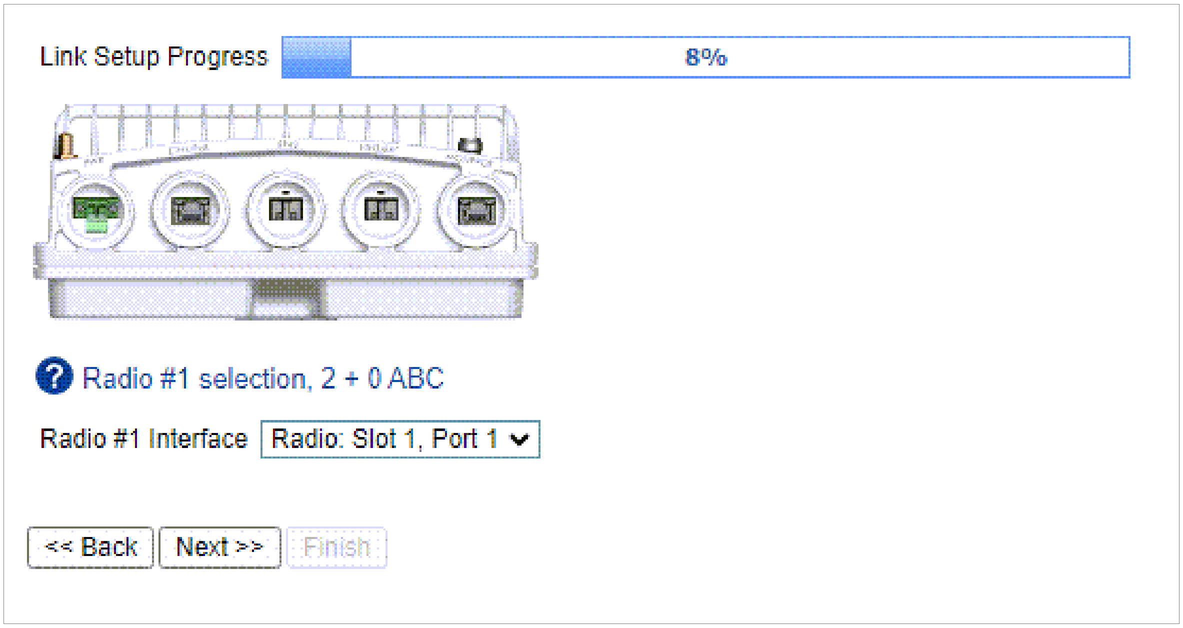
3. In the **Ethernet Interface** field, select an Ethernet interface or a LAG for the group.

Note

To create a LAG, click Create LAG. The Create LAG Group page opens. For instructions on creating LAG groups, see Configuring Link Aggregation (LAG).

4. Click **Next**. The Radio #1 Selection page opens.

Figure 71 *2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio #1 Selection Page*



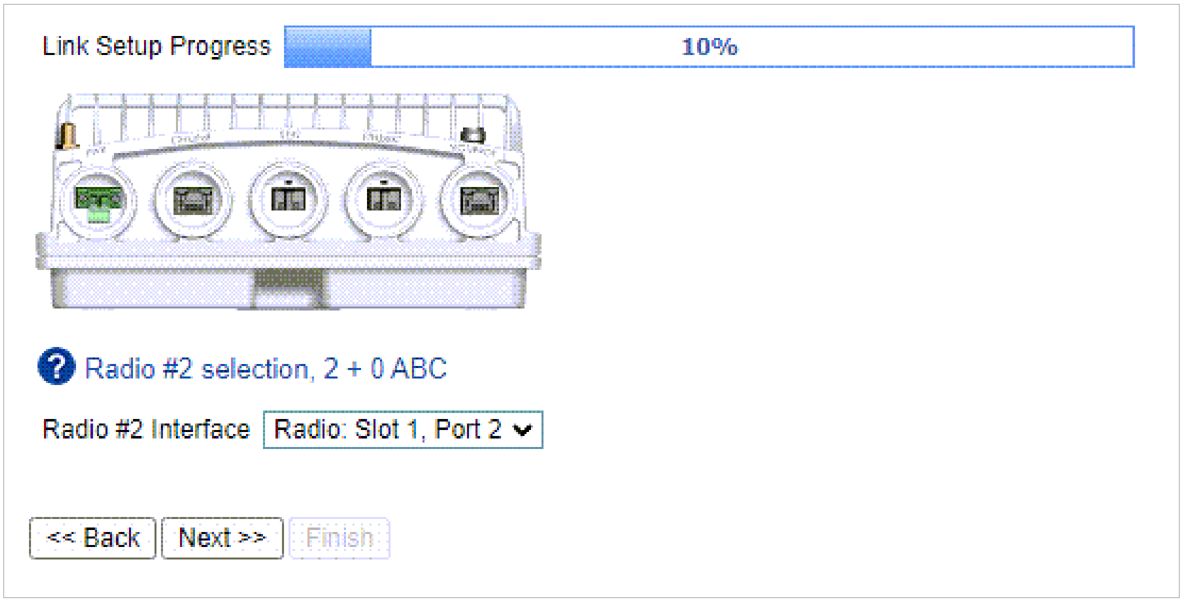
Link Setup Progress 8%

Radio #1 selection, 2 + 0 ABC

Radio #1 Interface: Radio: Slot 1, Port 1

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 72 *2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio #2 Selection Page*



Link Setup Progress 10%

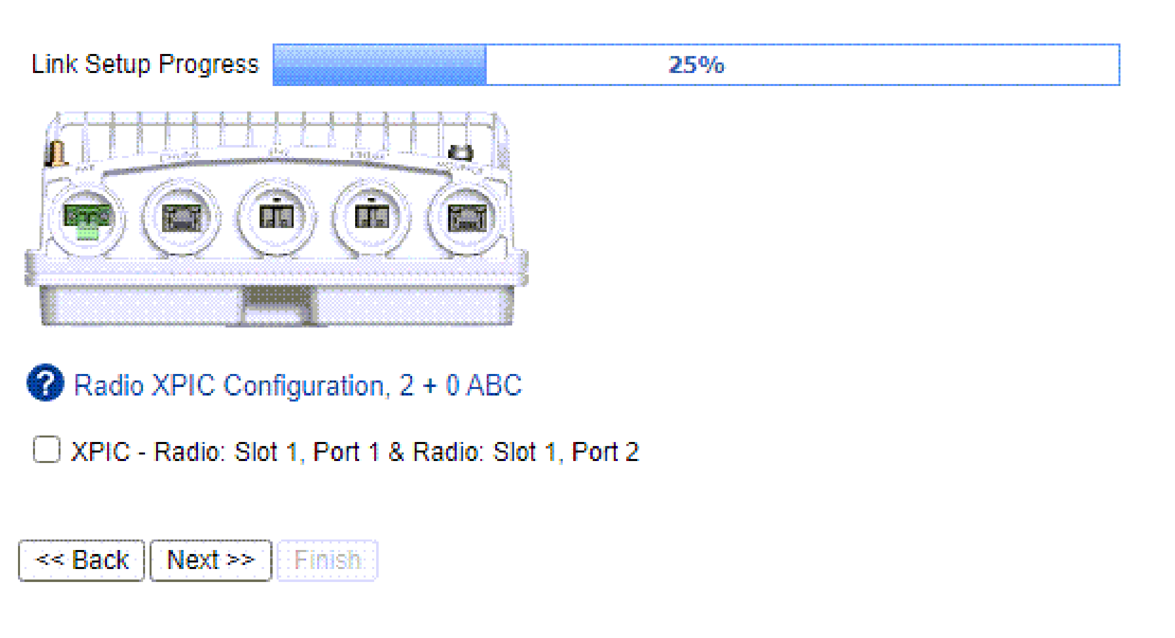
Radio #2 selection, 2 + 0 ABC

Radio #2 Interface: Radio: Slot 1, Port 2

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, see Configuring XPIC.

Figure 73 *2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio XPIC Configuration Page*



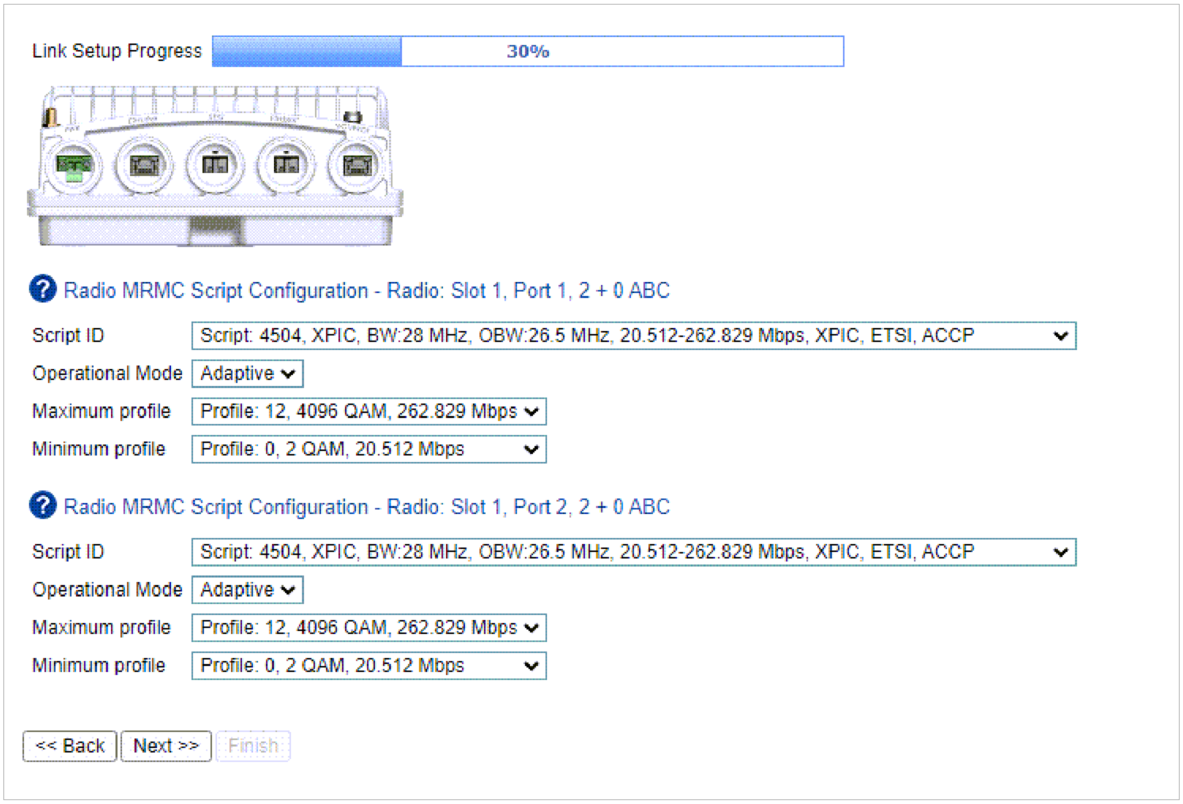
Link Setup Progress 25%

Radio XPIC Configuration, 2 + 0 ABC

□ XPIC - Radio: Slot 1, Port 1 & Radio: Slot 1, Port 2

9. 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 74 *2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio MRMC Script Configuration Page*



Link Setup Progress 30%

Radio MRMC Script Configuration - Radio: Slot 1, Port 1, 2 + 0 ABC

Script ID: Script: 4504, XPIC, BW:28 MHz, OBW:26.5 MHz, 20.512-262.829 Mbps, XPIC, ETSI, ACCP

Operational Mode: Adaptive

Maximum profile: Profile: 12, 4096 QAM, 262.829 Mbps

Minimum profile: Profile: 0, 2 QAM, 20.512 Mbps

Radio MRMC Script Configuration - Radio: Slot 1, Port 2, 2 + 0 ABC

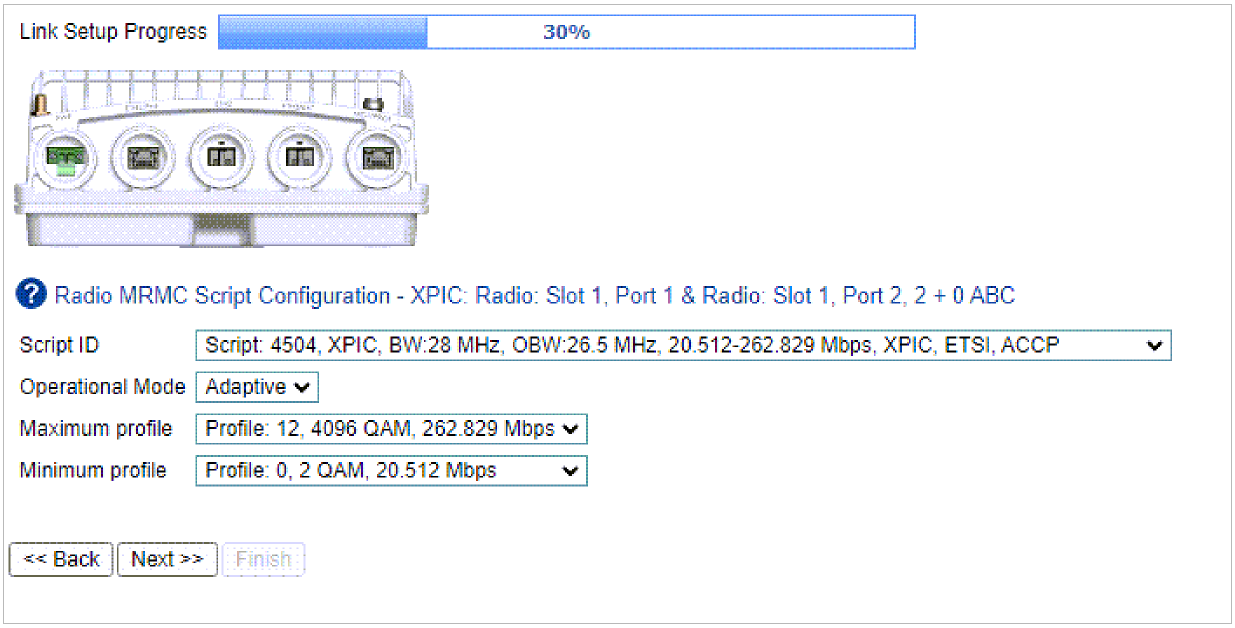
Script ID: Script: 4504, XPIC, BW:28 MHz, OBW:26.5 MHz, 20.512-262.829 Mbps, XPIC, ETSI, ACCP

Operational Mode: Adaptive

Maximum profile: Profile: 12, 4096 QAM, 262.829 Mbps

Minimum profile: Profile: 0, 2 QAM, 20.512 Mbps

Figure 75 *2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio MRMC Script Configuration Page – XPIC*



Link Setup Progress 30%

Radio MRMC Script Configuration - XPIC: Radio: Slot 1, Port 1 & Radio: Slot 1, Port 2, 2 + 0 ABC

Script ID: Script: 4504, XPIC, BW:28 MHz, OBW:26.5 MHz, 20.512-262.829 Mbps, XPIC, ETSI, ACCP

Operational Mode: Adaptive

Maximum profile: Profile: 12, 4096 QAM, 262.829 Mbps

Minimum profile: Profile: 0, 2 QAM, 20.512 Mbps

10. For each interface or XPIC group, configure the following MRMC script parameters.

11. 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, see Configuring the Radio (MRMC) Script(s).

12. 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.

13. Do one of the following:

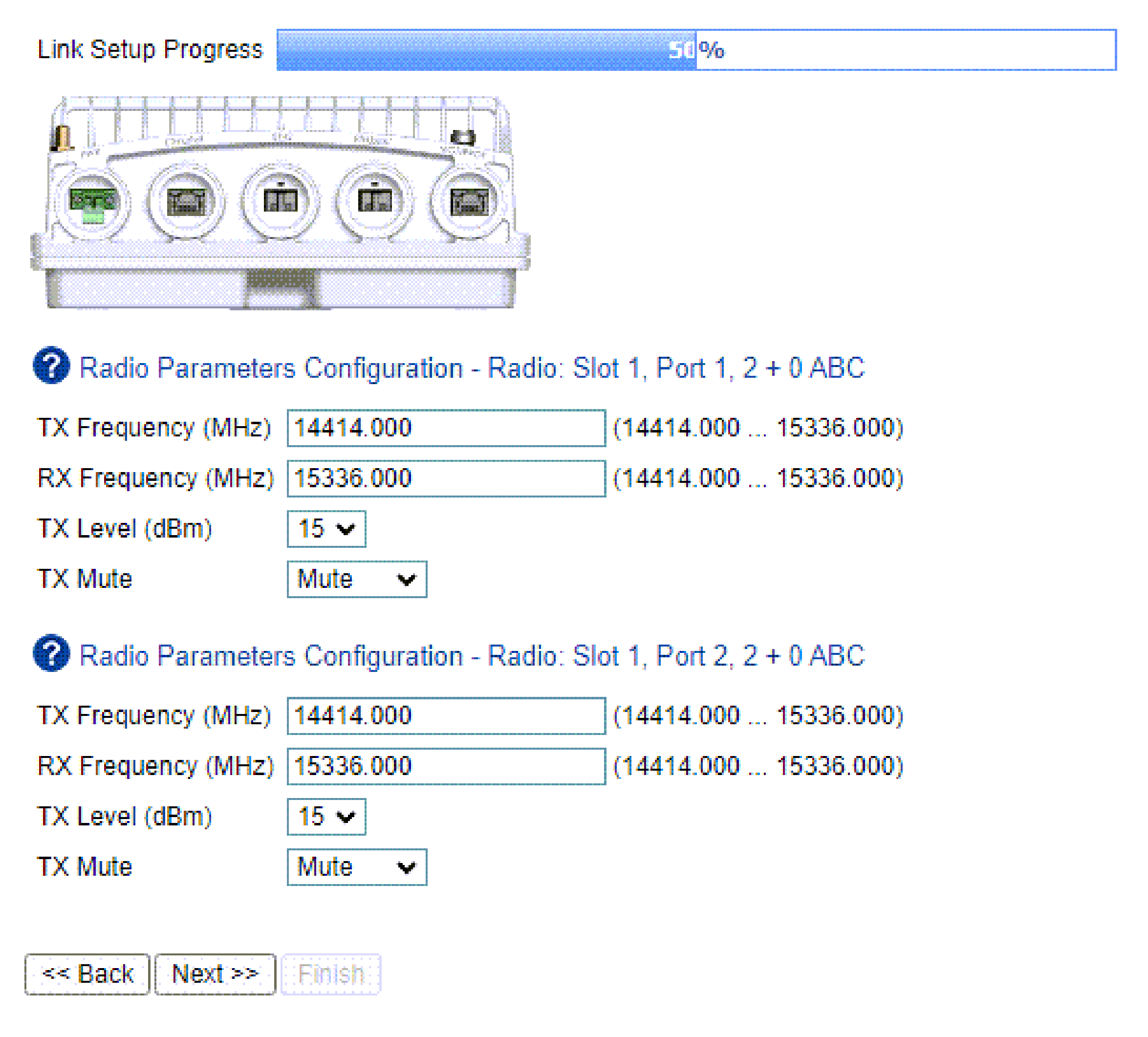
- If you selected **Fixed** in the **Operational Mode** field, the next field is Profile. Select the ACM profile in the **Profile** field.
- If you selected **Adaptive** in the **Operational Mode** field, the following two fields are displayed:
    - **Maximum profile** – Enter the maximum profile for the script. See Configuring the Radio (MRMC) Script(s).
    - **Minimum profile** – Enter the minimum profile for the script. See Configuring the Radio (MRMC) Script(s).

Note

The default minimum profile is 0.

14. 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 76 *2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio Parameters Configuration Page*



Link Setup Progress 50%

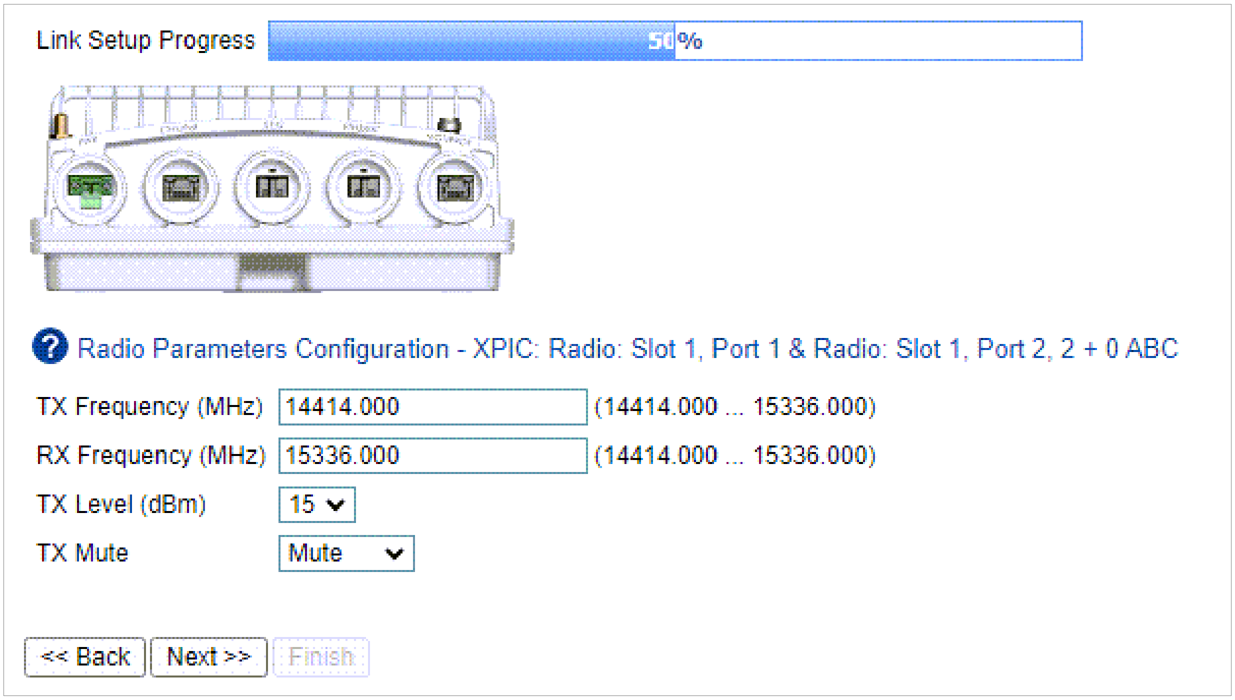
Radio Parameters Configuration - Radio: Slot 1, Port 1, 2 + 0 ABC

TX Frequency (MHz)	14414.000	(14414.000 ... 15336.000)
RX Frequency (MHz)	15336.000	(14414.000 ... 15336.000)
TX Level (dBm)	15	
TX Mute	Mute	

Radio Parameters Configuration - Radio: Slot 1, Port 2, 2 + 0 ABC

TX Frequency (MHz)	14414.000	(14414.000 ... 15336.000)
RX Frequency (MHz)	15336.000	(14414.000 ... 15336.000)
TX Level (dBm)	15	
TX Mute	Mute	

Figure 77 *2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio Parameters Configuration Page (XPIC)*



Link Setup Progress 50%

Radio Parameters Configuration - XPIC: Radio: Slot 1, Port 1 & Radio: Slot 1, Port 2, 2 + 0 ABC

TX Frequency (MHz) 14414.000 (14414.000 ... 15336.000)

RX Frequency (MHz) 15336.000 (14414.000 ... 15336.000)

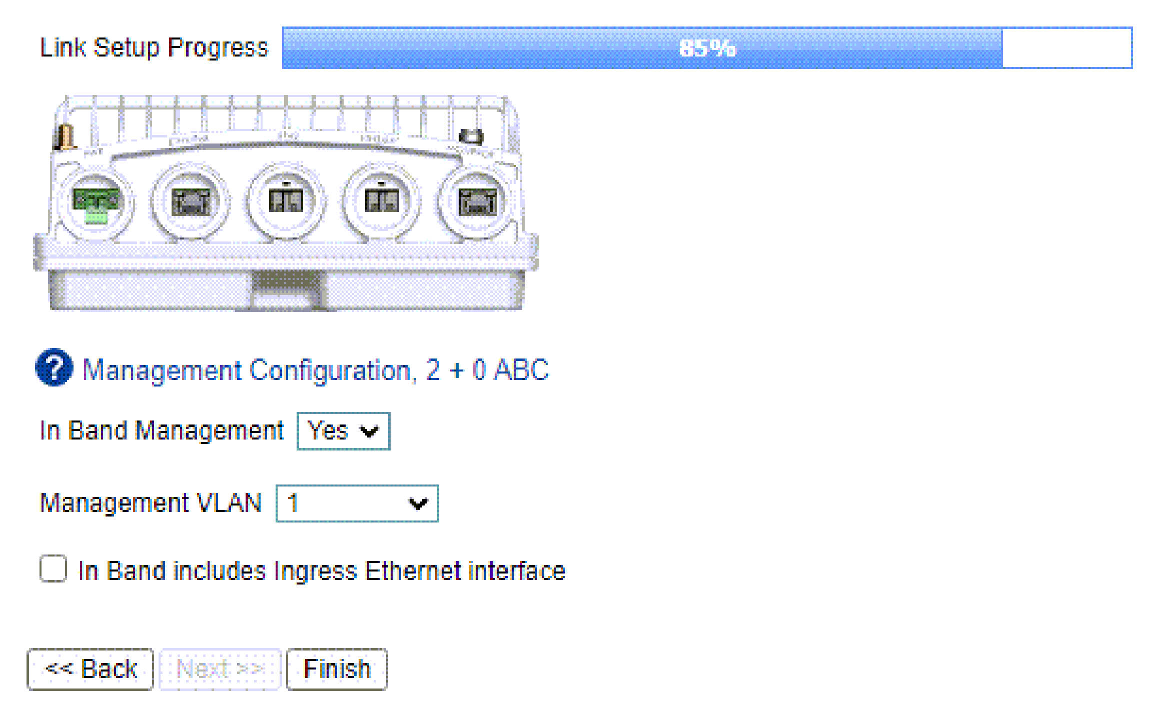
TX Level (dBm) 15

TX Mute Mute

15. For each interface or XPIC group, 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**. The Management Configuration page opens.

Figure 78 *2 + 0 Multi Carrier ABC Quick Configuration Wizard – Management Configuration Page*



Link Setup Progress 85%

Management Configuration, 2 + 0 ABC

In Band Management Yes

Management VLAN 1

□ In Band includes Ingress Ethernet interface

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.

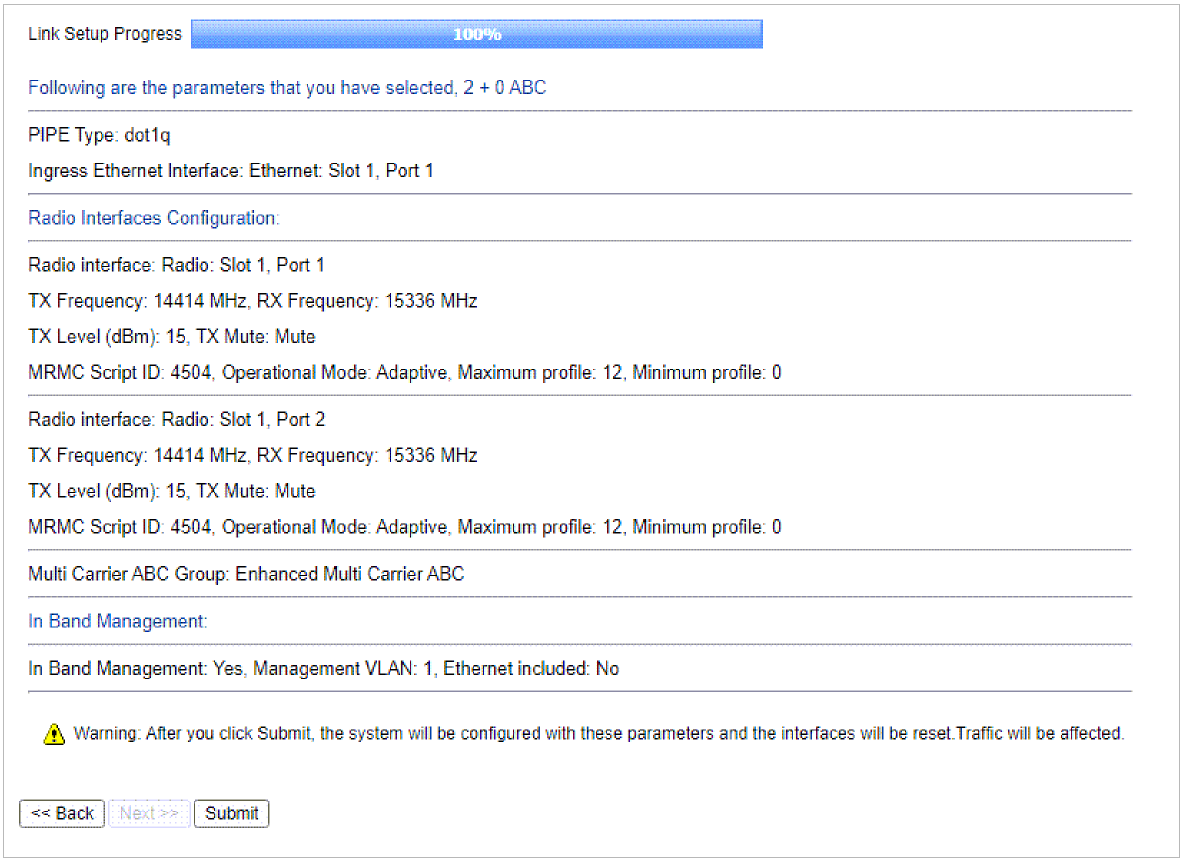
Note

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 79 *2 + 0 Multi Carrier ABC Quick Configuration Wizard –Summary Page*



Link Setup Progress 100%

Following are the parameters that you have selected, 2 + 0 ABC

PIPE Type: dot1q

Ingress Ethernet Interface: Ethernet: Slot 1, Port 1

Radio Interfaces Configuration:

Radio interface: Radio: Slot 1, Port 1

TX Frequency: 14414 MHz, RX Frequency: 15336 MHz

TX Level (dBm): 15, TX Mute: Mute

MRMC Script ID: 4504, Operational Mode: Adaptive, Maximum profile: 12, Minimum profile: 0

Radio interface: Radio: Slot 1, Port 2

TX Frequency: 14414 MHz, RX Frequency: 15336 MHz

TX Level (dBm): 15, TX Mute: Mute

MRMC Script ID: 4504, Operational Mode: Adaptive, Maximum profile: 12, Minimum profile: 0

Multi Carrier ABC Group: Enhanced Multi Carrier ABC

In Band Management:

In Band Management: Yes, Management VLAN: 1, Ethernet included: No

⚠ Warning: After you click Submit, the system will be configured with these parameters and the interfaces will be reset.Traffic will be affected.

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.

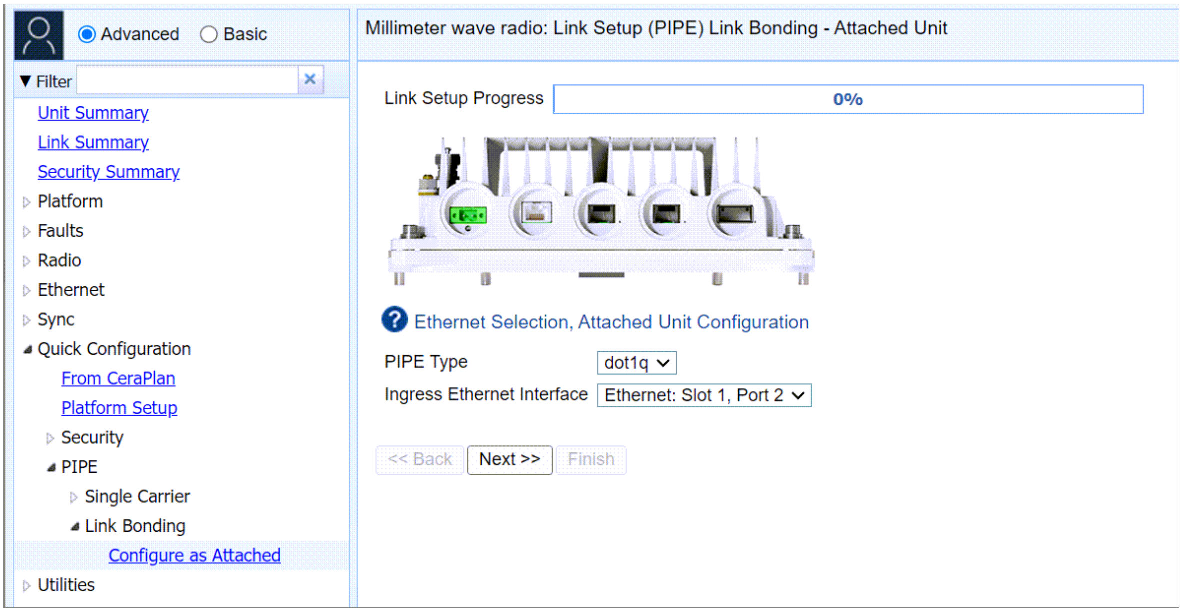
Configuring PTP 850EX as an Attached Unit in a Layer 1 Link Bonding Group

You can use the Link Bonding – Configure as Attached wizard to configure the radio and Link Bonding parameters of an PTP 850EX when configured as an attached unit in a Link Bonding group with an PTP 820N as the main unit.

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 80 *Link Bonding Attached Unit Quick Configuration Wizard – Ethernet Selection Page*



Millimeter wave radio: Link Setup (PIPE) Link Bonding - Attached Unit

Link Setup Progress 0%

Ethernet Selection, Attached Unit Configuration

PIPE Type: dot1q

Ingress Ethernet Interface: Ethernet: Slot 1, Port 2

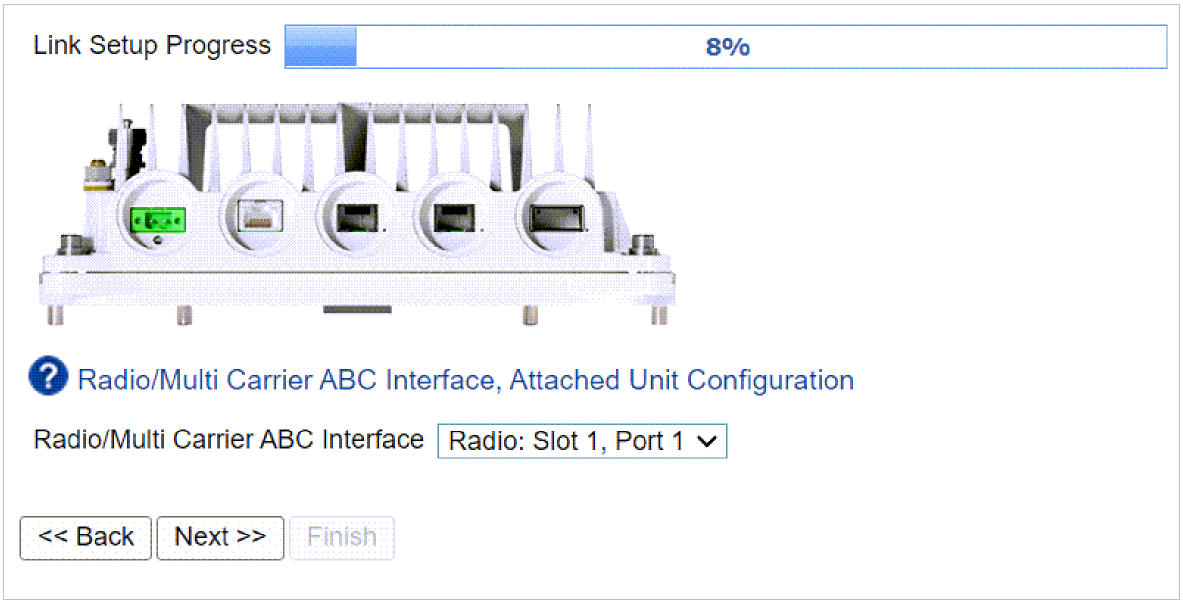
2. In the **Pipe Type** field, select the Attached Interface type for the service that will transport traffic between the main unit and the attached unit. The only available option is dot1q.

Note

For a full explanation of Ethernet Services, service types, and attached interface types, see Configuring Ethernet Service(s).

3. In the **Ingress Ethernet Interface** field, select the Ethernet interface on the attached unit connecting it to the main unit.
4. Click **Next**. The Radio Interface page of the Quick Configuration wizard opens.

Figure 81 *Link Bonding Attached Unit Quick Configuration Wizard – Radio Interface Page*



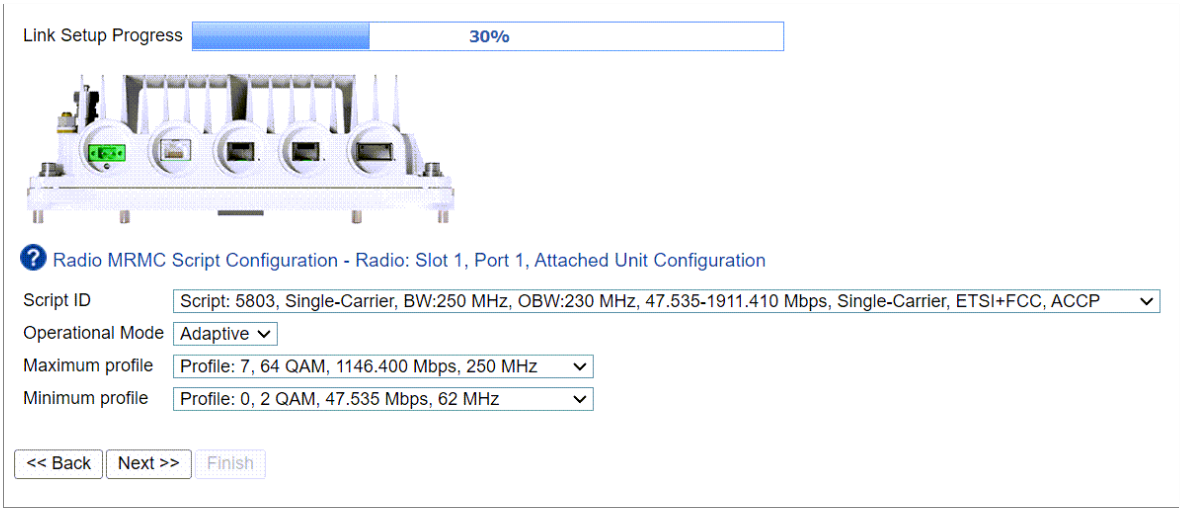
Link Setup Progress 8%

Radio/Multi Carrier ABC Interface, Attached Unit Configuration

Radio/Multi Carrier ABC Interface: Radio: Slot 1, Port 1

5. In the **Radio Interface** field, select the device's radio interface.
6. Click **Next**. The Radio MRMC Script Configuration page of the Quick Configuration wizard opens.

Figure 82 *Link Bonding Attached Unit Quick Configuration Wizard – Radio MRMC Script Configuration Page*



Link Setup Progress 30%

Radio MRMC Script Configuration - Radio: Slot 1, Port 1, Attached Unit Configuration

Script ID: Script: 5803, Single-Carrier, BW:250 MHz, OBW:230 MHz, 47.535-1911.410 Mbps, Single-Carrier, ETSI+FCC, ACCP

Operational Mode: Adaptive

Maximum profile: Profile: 7, 64 QAM, 1146.400 Mbps, 250 MHz

Minimum profile: Profile: 0, 2 QAM, 47.535 Mbps, 62 MHz

7. In the **Script ID** field, select the MRMC script you want to assign to the radio interface. For a full explanation of choosing an MRMC script, see Configuring the Radio (MRMC) Script(s).
8. In the **Operational Mode** field, select Adaptive. 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).

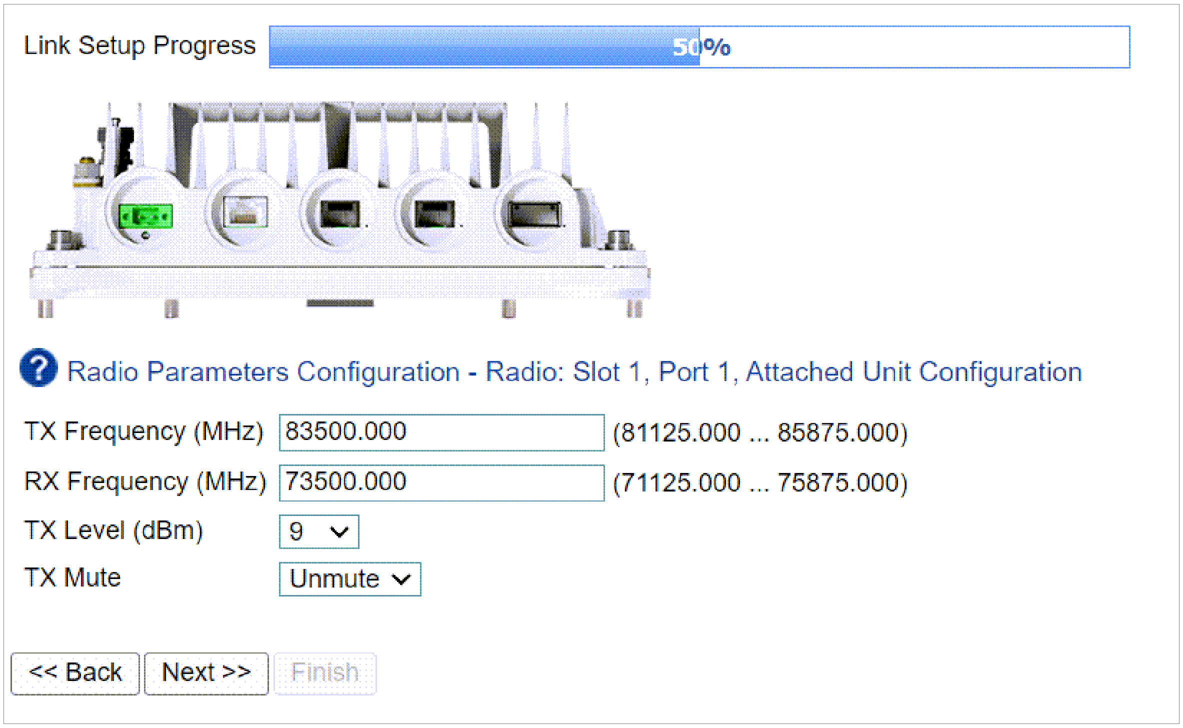
Note

Fixed mode is not supported for Multiband.

Make sure the Maximum profile and Minimum profile are set to different values. The default minimum profile is 0.

9. Click **Next**. The Radio Parameters Configuration page of the Quick Configuration wizard opens.

Figure 83 *Link Bonding Attached Unit Quick Configuration Wizard – Radio Parameters Configuration Page*



Link Setup Progress 50%

Radio Parameters Configuration - Radio: Slot 1, Port 1, Attached Unit Configuration

TX Frequency (MHz) 83500.000 (81125.000 ... 85875.000)

RX Frequency (MHz) 73500.000 (71125.000 ... 75875.000)

TX Level (dBm) 9

TX Mute Unmute

10. Configure the following radio parameters for the radio interface:

    a. In the TX Frequency (MHz) field, set the transmission radio frequency in MHz.

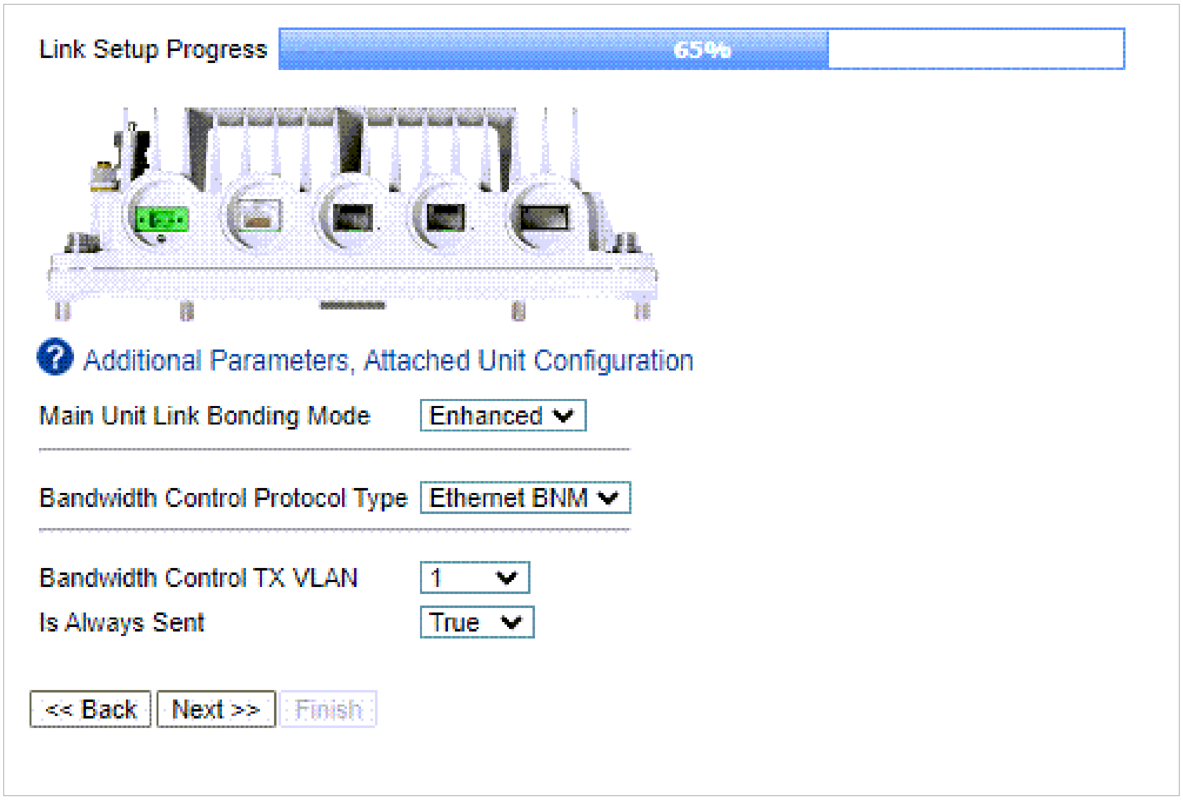
    b. In the RX Frequency (MHz) field, set the received radio frequency in MHz.

    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.

11. Click **Next**. The Additional Parameters page of the Quick Configuration wizard opens.

Figure 84 *Link Bonding Attached Unit Quick Configuration Wizard – Additional Parameters Page (Enhanced Link Bonding Mode)*



Link Setup Progress 65%

Additional Parameters, Attached Unit Configuration

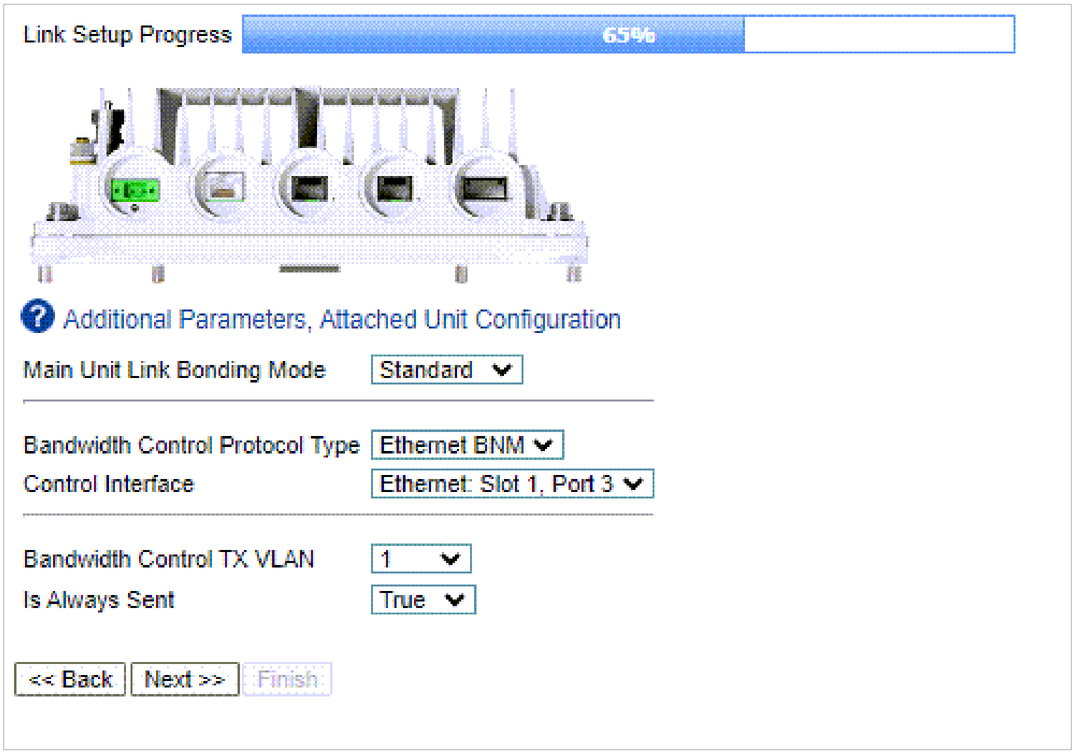
Main Unit Link Bonding Mode: Enhanced

Bandwidth Control Protocol Type: Ethernet BNM

Bandwidth Control TX VLAN: 1

Is Always Sent: True

Figure 85 *Link Bonding Attached Unit Quick Configuration Wizard – Additional Parameters Page (Standard Link Bonding Mode)*



Link Setup Progress 65%

Additional Parameters, Attached Unit Configuration

Main Unit Link Bonding Mode	Standard
Bandwidth Control Protocol Type	Ethernet BNM
Control Interface	Ethernet: Slot 1, Port 3
Bandwidth Control TX VLAN	1
Is Always Sent	True

12. 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.

13. In the **Bandwidth Control Protocol Type** field, select Ethernet BNM.

14. In the **Control Interface** field (Standard Mode only), select the port on the attached 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 In the Ingress Ethernet Interface field, select the Ethernet interface on the attached unit connecting it to the main unit..

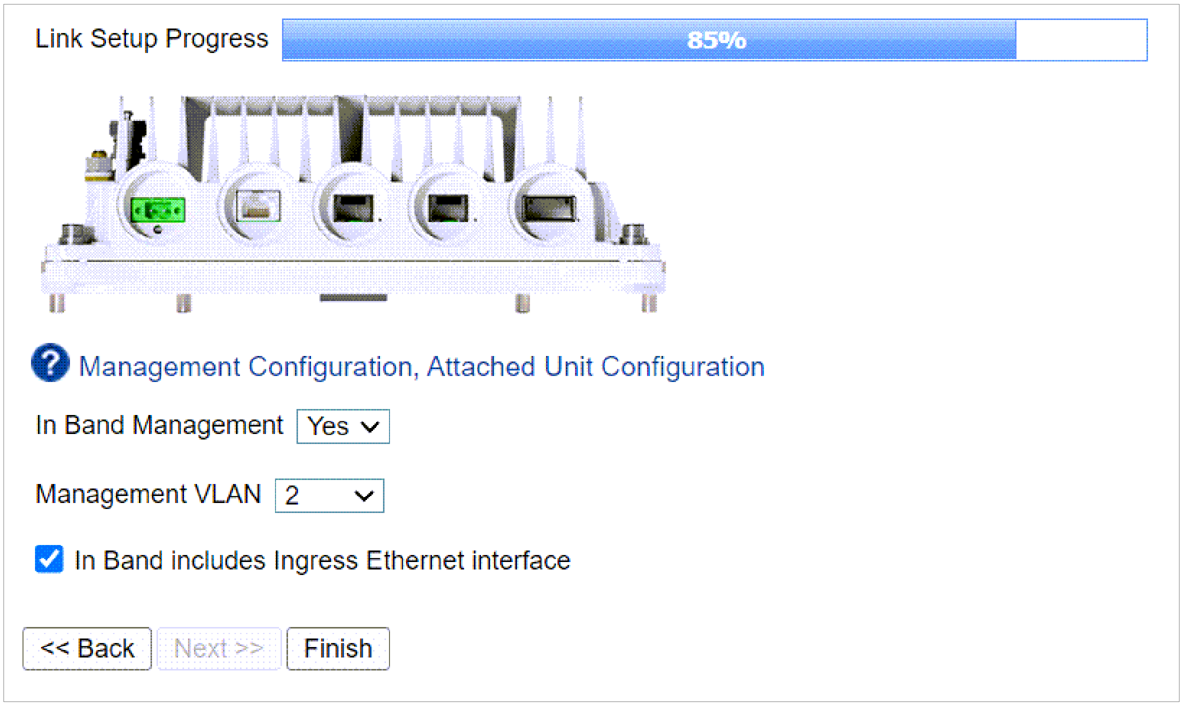
15. In the **Bandwidth Control TX VLAN** field, select a VLAN ID. You can use any available VLAN ID from 1 to 4090. This is the VLAN used to transfer protocol information between the two units. Make sure to use the same VLAN configured as the VLAN ID in BNM Packet in the main unit.

16. 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).

17. Click **Next**. The Management Configuration page of the Multiband Link Bonding Quick Configuration wizard opens.

Figure 86 *Multiband Link Bonding Quick Configuration Wizard – Management Configuration Page*



Link Setup Progress 85%

Management Configuration, Attached Unit Configuration

In Band Management: Yes

Management VLAN: 2

☑ In Band includes Ingress Ethernet interface

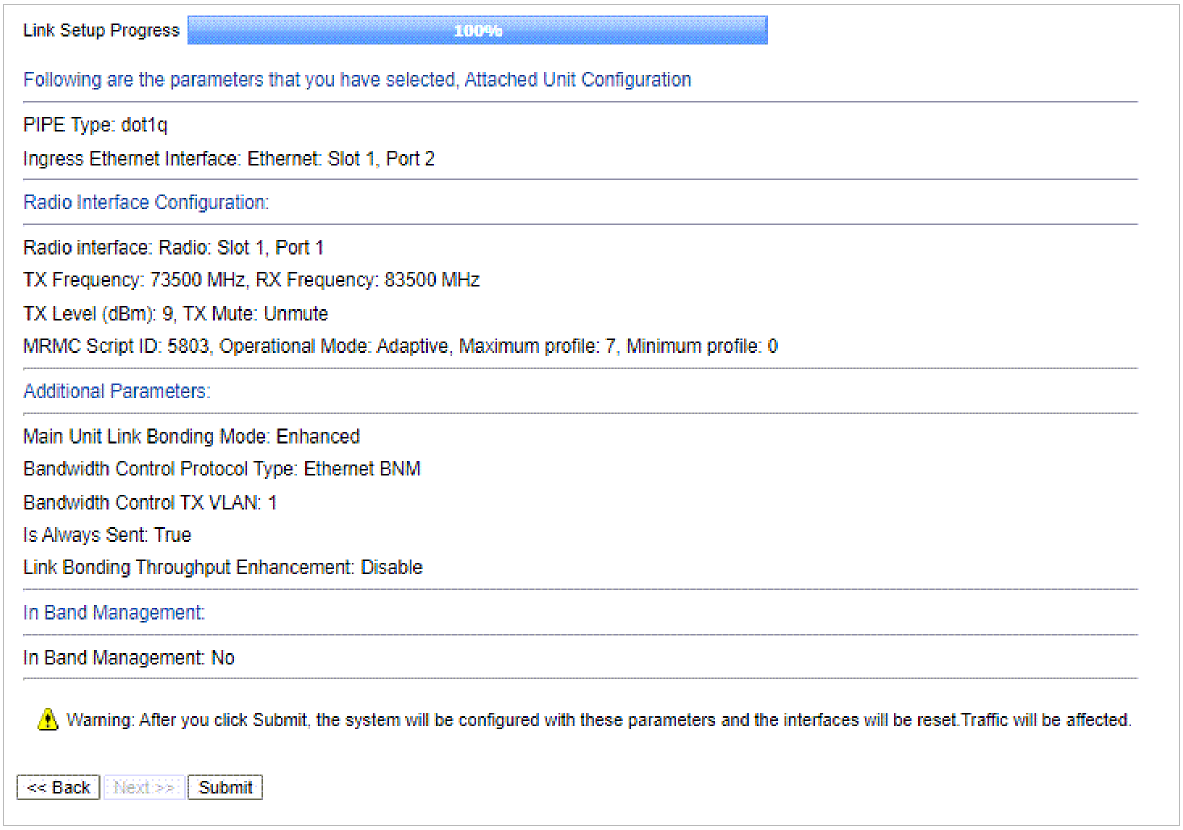
18. In the **In Band Management** field, select **Yes** to configure in-band management, or **No** if you do not need in-band management. If you select **Yes**, the **Management VLAN** field appears.

19. If you selected **Yes** in the **In Band Management** field, select the **management VLAN** in the Management VLAN field.

20. If you want to use the Ethernet interface as well as the radio interface for in-band management, select **In Band includes Ethernet interface**.

21. Click **Finish**. The Summary page opens. This page displays the parameters you have selected for the group.

Figure 87 *Multiband Quick Configuration Wizard – Summary Page*



Link Setup Progress 100%

Following are the parameters that you have selected, Attached Unit Configuration

PIPE Type: dot1q

Ingress Ethernet Interface: Ethernet: Slot 1, Port 2

Radio Interface Configuration:

Radio interface: Radio: Slot 1, Port 1

TX Frequency: 73500 MHz, RX Frequency: 83500 MHz

TX Level (dBm): 9, TX Mute: Unmute

MRMC Script ID: 5803, Operational Mode: Adaptive, Maximum profile: 7, Minimum profile: 0

Additional Parameters:

Main Unit Link Bonding Mode: Enhanced

Bandwidth Control Protocol Type: Ethernet BNM

Bandwidth Control TX VLAN: 1

Is Always Sent: True

Link Bonding Throughput Enhancement: Disable

In Band Management:

In Band Management: No

⚠ Warning: After you click Submit, the system will be configured with these parameters and the interfaces will be reset.Traffic will be affected.

22. To complete configuration of the attached unit, click **Submit**. If you want to go back and change any of the parameters, click **Back**.

Configuring Groups

This section provides instructions for configuring groups manually, using Advanced mode.

Most link configurations can be configured using Quick Configuration wizards, and it is recommended to do so whenever possible. See Configuring a Link Using the Quick Configuration Wizard.

This section includes:

- Configuring Multi-Carrier ABC
- Configuring XPIC
- Configuring Link Aggregation (LAG)

Configuring Multi-Carrier ABC

Note

Multi-Carrier ABC links can also be configured using the Quick Configuration wizard. It is recommended to use the wizard whenever possible. See Configuring a 2+0 Multi-Carrier ABC Link Using the Quick Configuration Wizard.

This section includes:

- Multi-Carrier ABC Overview
- Configuring a Multi-Carrier ABC Group
- Adding and Removing Group Members
- Deleting a Multi-Carrier ABC Group

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.

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.

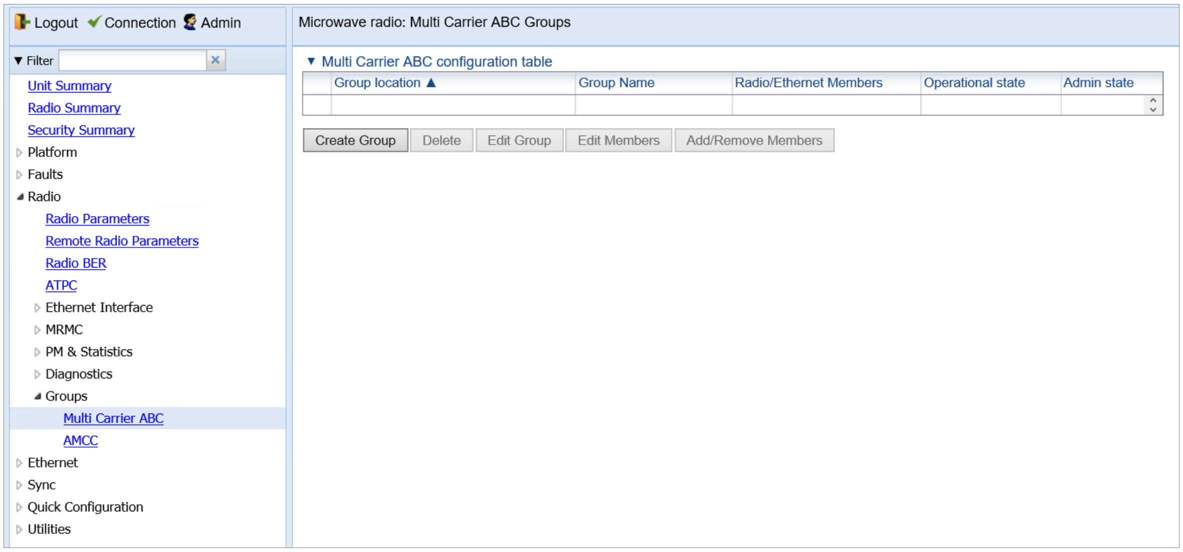
One Multi-Carrier ABC group that includes both radio interfaces can be configured per unit. It is recommended to use the same radio script and ACM settings on both radio carriers in the Multi-Carrier ABC group.

Configuring a Multi-Carrier ABC Group

To configure a Multi-Carrier ABC group:

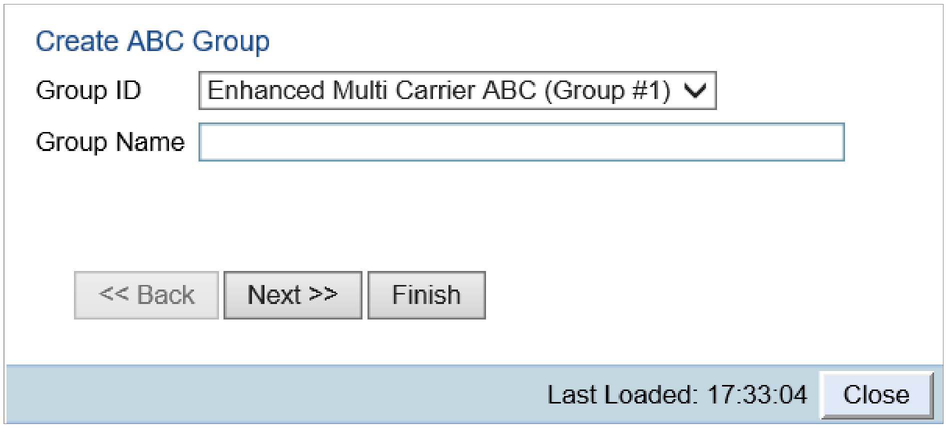
1. Select **Radio** > **Groups** > **Multi Carrier ABC**. The Multi Carrier ABC page opens.

   Figure 88 *Multi-Carrier ABC Group Page (Empty)*



2. Click **Create Group**. The first page of the Create ABC Group wizard opens.

   Figure 89 *Create ABC Group Wizard – Group Name*

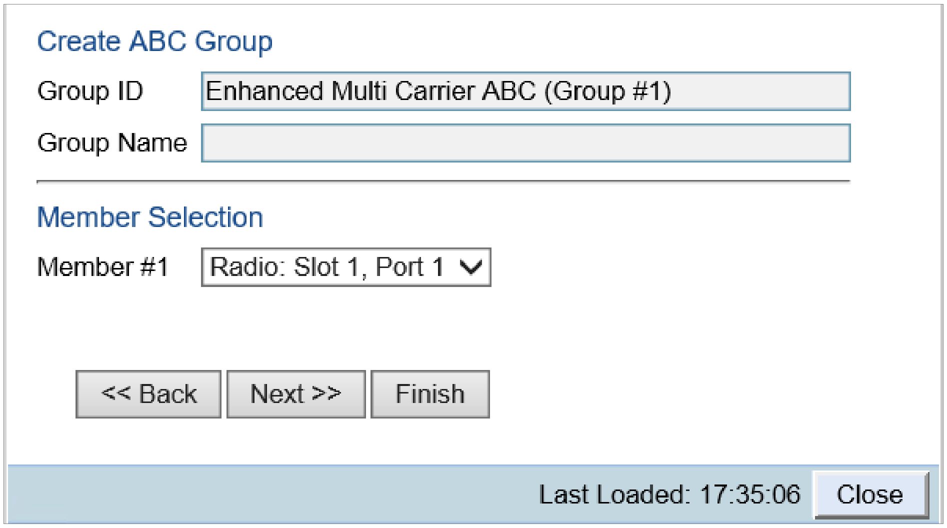

Create ABC Group

Group ID: Enhanced Multi Carrier ABC (Group #1)

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 90 *Create ABC Group Wizard – Member Selection 1*



Create ABC Group

Group ID: Enhanced Multi Carrier ABC (Group #1)

Group Name:

Member Selection

Member #1: Radio: Slot 1, Port 1

Last Loaded: 17:35:06

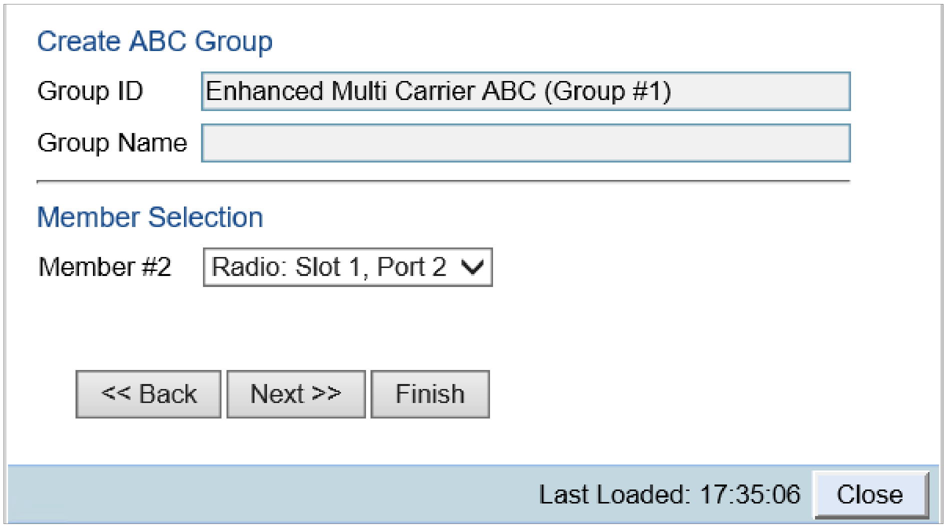
5. In the **Member 1** field, select a radio interface.

Note

Although you may select the Radio members in any order you wish, ABC configuration will not succeed unless Radio slot 1 port 1 is selected first and Radio slot 1 port 2 is selected second.

6. Click **Next**. The next page of the Create Group wizard opens.

Figure 91 *Create ABC Group Wizard – Member Selection 2*



Create ABC Group

Group ID: Enhanced Multi Carrier ABC (Group #1)

Group Name:

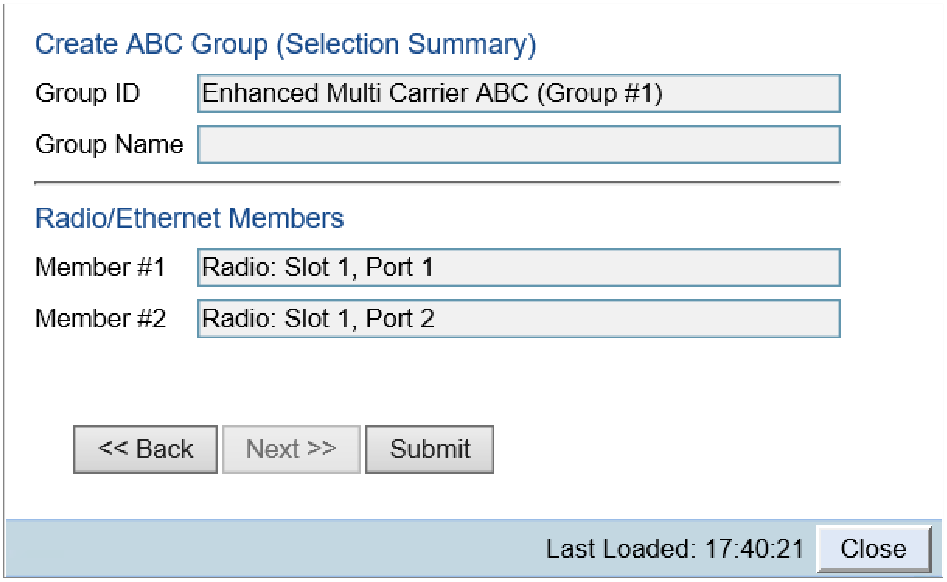
Member Selection

Member #2: Radio: Slot 1, Port 2

Last Loaded: 17:35:06

7. In the **Member 2** field, select a radio interface.
8. Click **Next**. A summary page opens.

Figure 92 *Create ABC Group Wizard – Summary Page*



Create ABC Group (Selection Summary)

Group ID: Enhanced Multi Carrier ABC (Group #1)

Group Name:

Radio/Ethernet Members

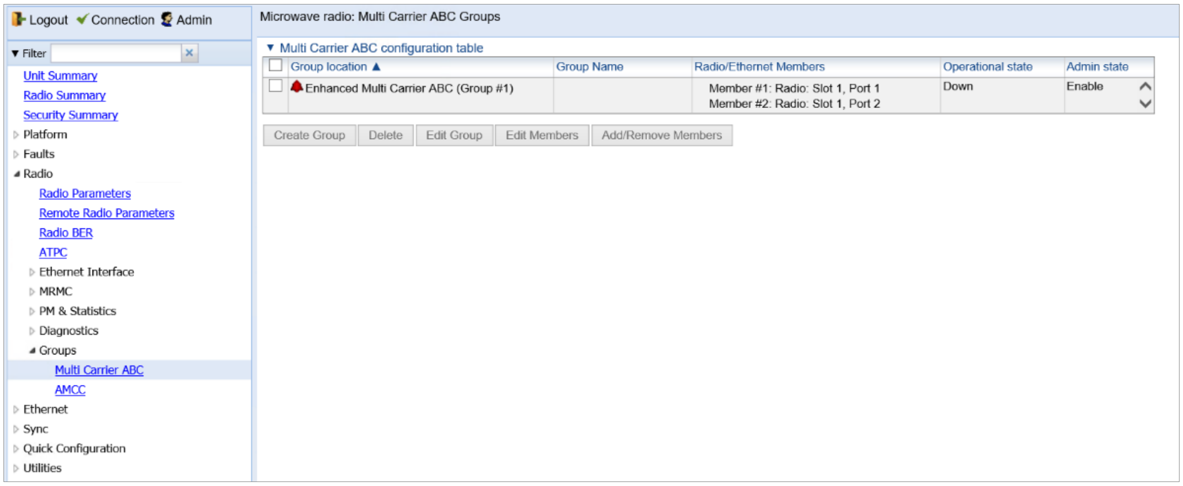
Member #1: Radio: Slot 1, Port 1

Member #2: Radio: Slot 1, Port 2

Last Loaded: 17:40:21

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 93 *Multi-Carrier ABC Group Page (Populated)*



Microwave radio: Multi Carrier ABC Groups

▼ Multi Carrier ABC configuration table

□	Group location ▲	Group Name	Radio/Ethernet Members	Operational state	Admin state
□	Enhanced Multi Carrier ABC (Group #1)		Member #1: Radio: Slot 1, Port 1 Member #2: Radio: Slot 1, Port 2	Down	Enable

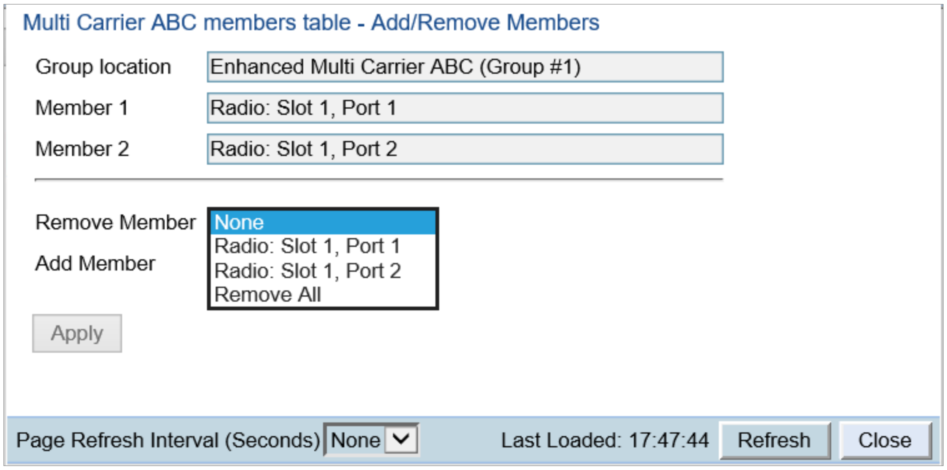
Adding and Removing Group Members

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 94 *Multi Carrier ABC Group - Add/Remove Members Page*



Multi Carrier ABC members table - Add/Remove Members

Group location: Enhanced Multi Carrier ABC (Group #1)

Member 1: Radio: Slot 1, Port 1

Member 2: Radio: Slot 1, Port 2

Remove Member: None

Page Refresh Interval (Seconds): None

Last Loaded: 17:47:44

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 (Multi-Carrier ABC Group Page (Empty)).
2. Select the group in the Multi-Carrier ABC table and click **Add/Remove Members**. The Add/Remove Members page opens (Multi Carrier ABC Group - Add/Remove Members Page).
3. Remove each member of the group.
4. Click **Close** to close the Multi Carrier ABC – Add/Remove Members page.
5. Select the group and click **Delete**.

Configuring XPIC

This section includes:

- *XPIC Overview*
- Configuring the Radio Carriers
- Deleting an AMCC (XPIC) Group
- Performing Antenna Alignment for XPIC
- XPIC Status and Troubleshooting

XPIC Overview

Note

For PTP 850EX, XPIC is planned for future release.

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.

XPIC is configured with the two carriers of a single unit on each side of the link.

XPIC enables links of up to 2 Gbps, consisting of 1 Gbps per carrier. XPIC can be installed in either of the following configurations:

- Direct Mount – The device is connected to the antenna via an OMT.
- Remote Mount – The device is connected to the antenna via two flexible waveguides. Some configurations also require an OMT.

To configure and enable XPIC:

- Install the IP-device in a dual polarization configuration.
- 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.

Note

Before performing any maintenance operation, such as performing an RF loopback, or setting the interface to Admin = Down, you must first either mute the radio to be disabled on both sides of the link or disable the XPIC group.

Configuring the Radio Carriers

Note

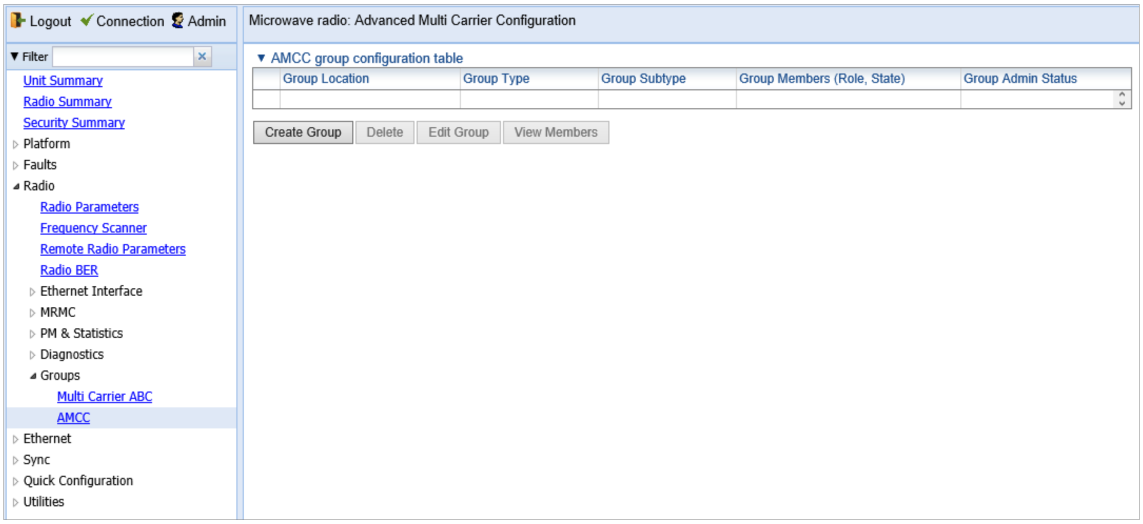
You can perform the entire configuration using the 1+0 Quick Configuration wizard. See Configuring a 1+0 Link Using the Quick Configuration Wizard.

To configure the radio carriers for XPIC:

1. Configure each radio carrier 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. To create an AMCC group:

a. Select **Radio** > **Groups** > **AMCC**. The Advanced Multi Carrier Configuration page opens.

Figure 95 *Advanced Multi Carrier Configuration Page*



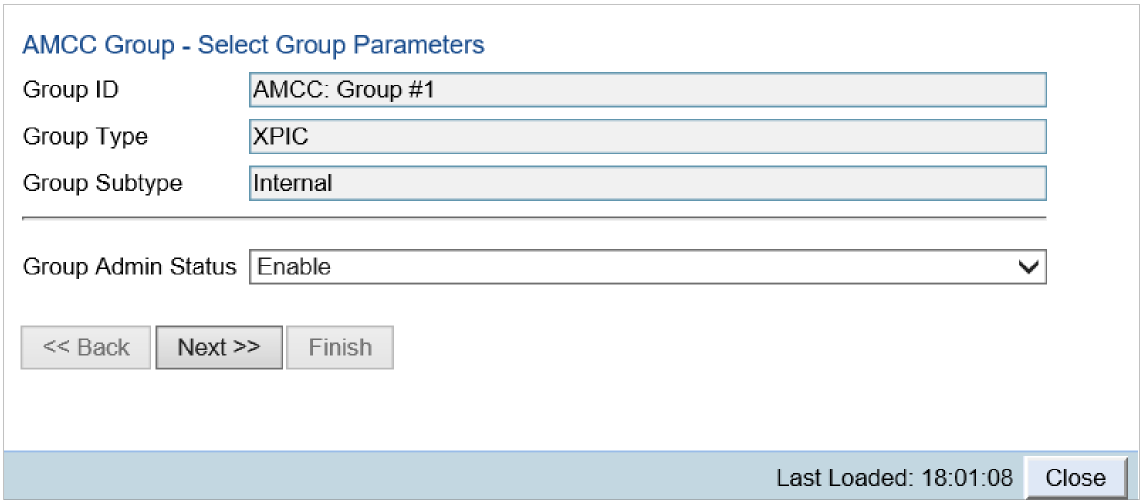
Microwave radio: Advanced Multi Carrier Configuration

AMCC group configuration table

Group Location	Group Type	Group Subtype	Group Members (Role, State)	Group Admin Status

b. Click **Create Group**. The AMCC Group – Select Group Parameters page opens.

Figure 96 *AMCC Group – Select Group Parameters Page*



AMCC Group - Select Group Parameters

Group ID: AMCC: Group #1

Group Type: XPIC

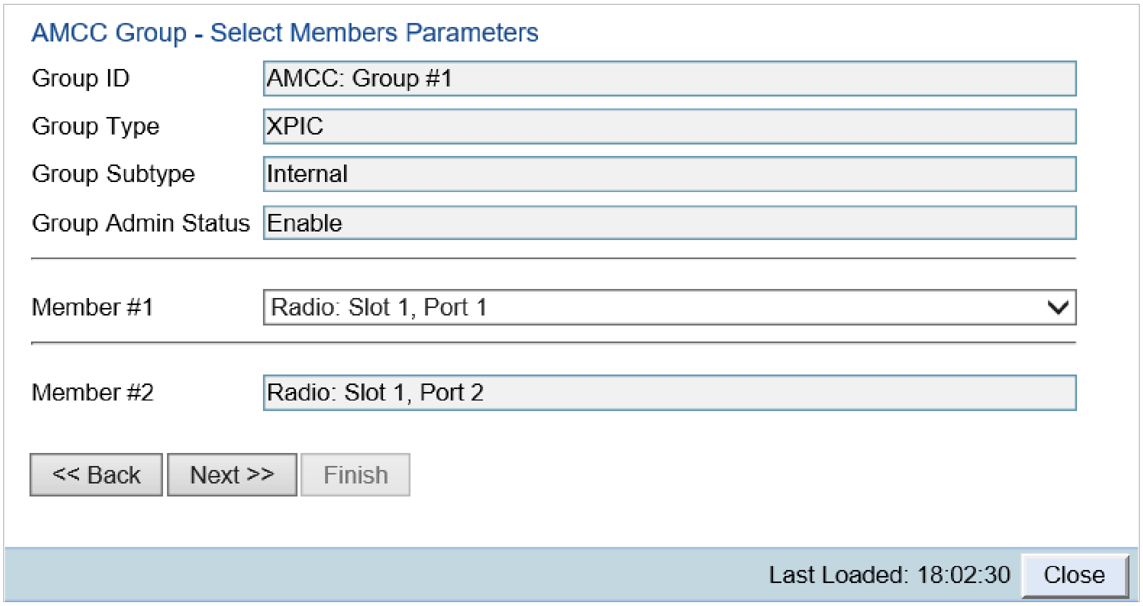
Group Subtype: Internal

Group Admin Status: Enable

c. In the **Group Admin Status** field, select **Enable**.

d. Click **Next**. The AMCC Group – Select Member Parameters page opens.

Figure 97 *AMCC Group – Select Member Parameters Page*



AMCC Group - Select Members Parameters

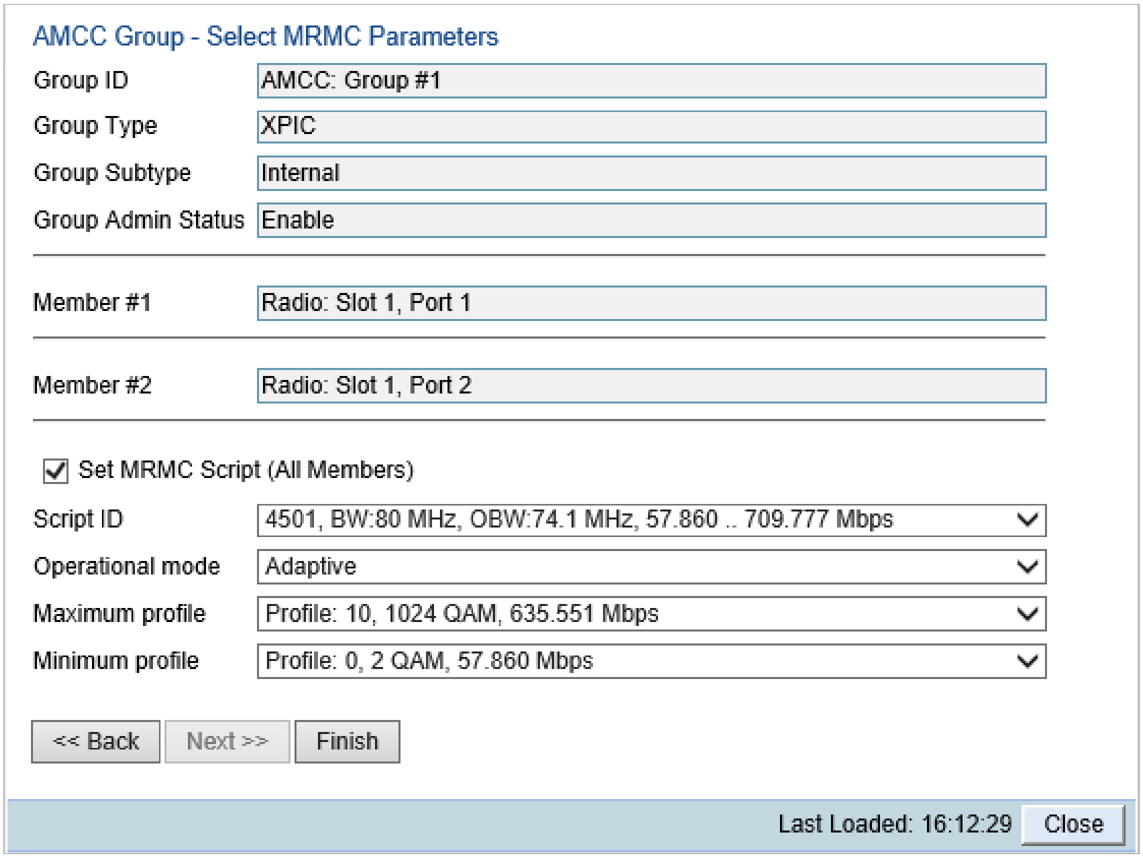
Group ID	AMCC: Group #1
Group Type	XPIC
Group Subtype	Internal
Group Admin Status	Enable
Member #1	Radio: Slot 1, Port 1
Member #2	Radio: Slot 1, Port 2

Last Loaded: 18:02:30

e. In the **Member #1** field, select a radio interface. The other interface automatically appears in the **Member #2** field. It does not matter which interface is Member 1 and which interface is Member 2. In any event, **Port 1** is the vertical radio carrier and **Port 2** is the horizontal radio carrier.

f. Click **Next**. The AMCC Group – Select MRMC Parameters page opens.

Figure 98 *AMCC Group – Select MRMC Parameters Page*


AMCC Group - Select MRMC Parameters

Group ID	AMCC: Group #1
Group Type	XPIC
Group Subtype	Internal
Group Admin Status	Enable
Member #1	Radio: Slot 1, Port 1
Member #2	Radio: Slot 1, Port 2

☑ Set MRMC Script (All Members)

Script ID	4501, BW:80 MHz, OBW:74.1 MHz, 57.860 .. 709.777 Mbps
Operational mode	Adaptive
Maximum profile	Profile: 10, 1024 QAM, 635.551 Mbps
Minimum profile	Profile: 0, 2 QAM, 57.860 Mbps

Last Loaded: 16:12:29

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, see Configuring the Radio (MRMC) Script(s).

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. See Configuring the Radio (MRMC) Script(s).
  - **Minimum profile** – Enter the minimum profile for the script. See Configuring the Radio (MRMC) Script(s).

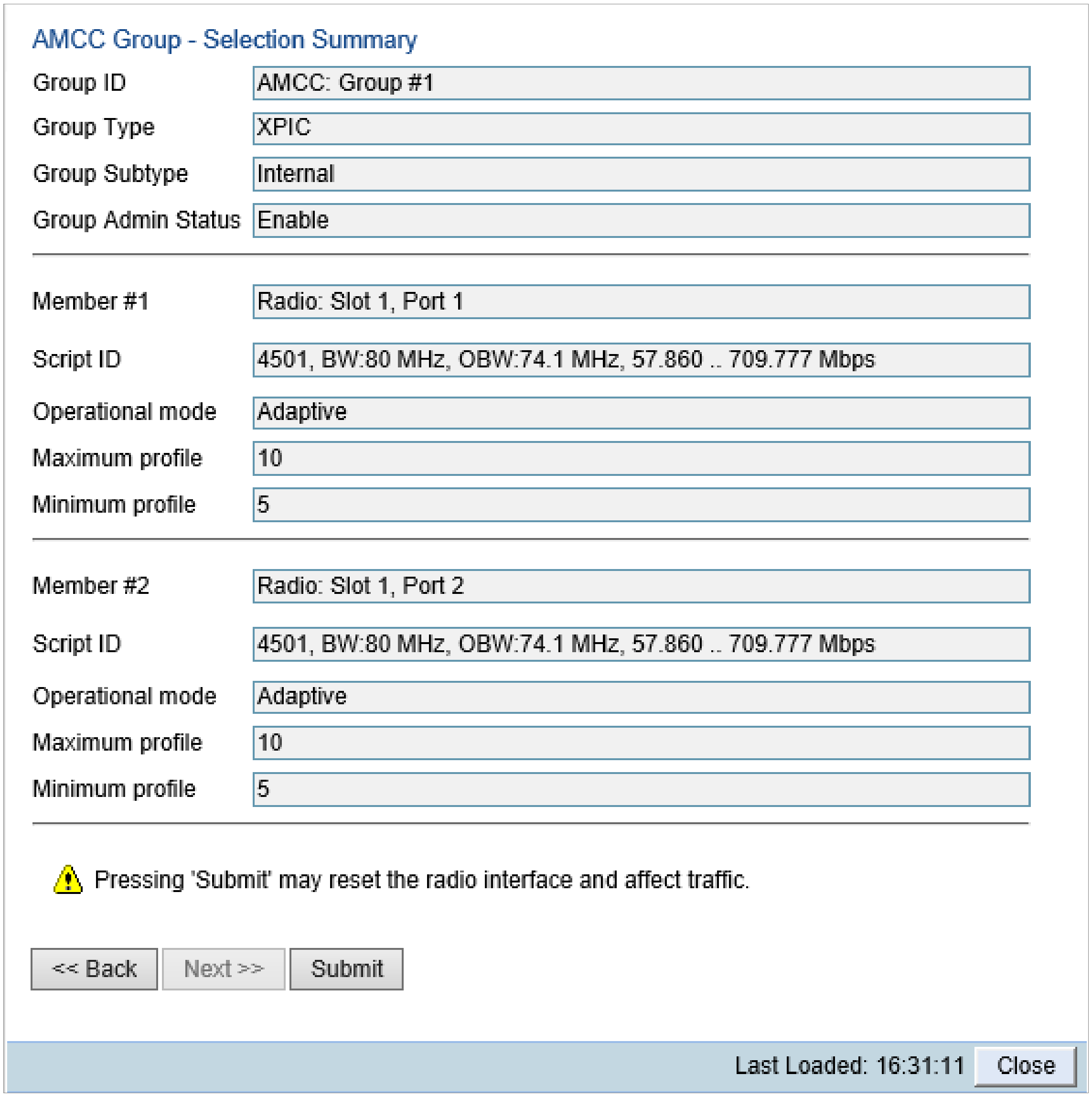
Note

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 99 *AMCC Group – Selection Summary Page*



AMCC Group - Selection Summary

Group ID	AMCC: Group #1
Group Type	XPIC
Group Subtype	Internal
Group Admin Status	Enable
Member #1	Radio: Slot 1, Port 1
Script ID	4501, BW:80 MHz, OBW:74.1 MHz, 57.860 .. 709.777 Mbps
Operational mode	Adaptive
Maximum profile	10
Minimum profile	5
Member #2	Radio: Slot 1, Port 2
Script ID	4501, BW:80 MHz, OBW:74.1 MHz, 57.860 .. 709.777 Mbps
Operational mode	Adaptive
Maximum profile	10
Minimum profile	5

⚠ Pressing 'Submit' may reset the radio interface and affect traffic.

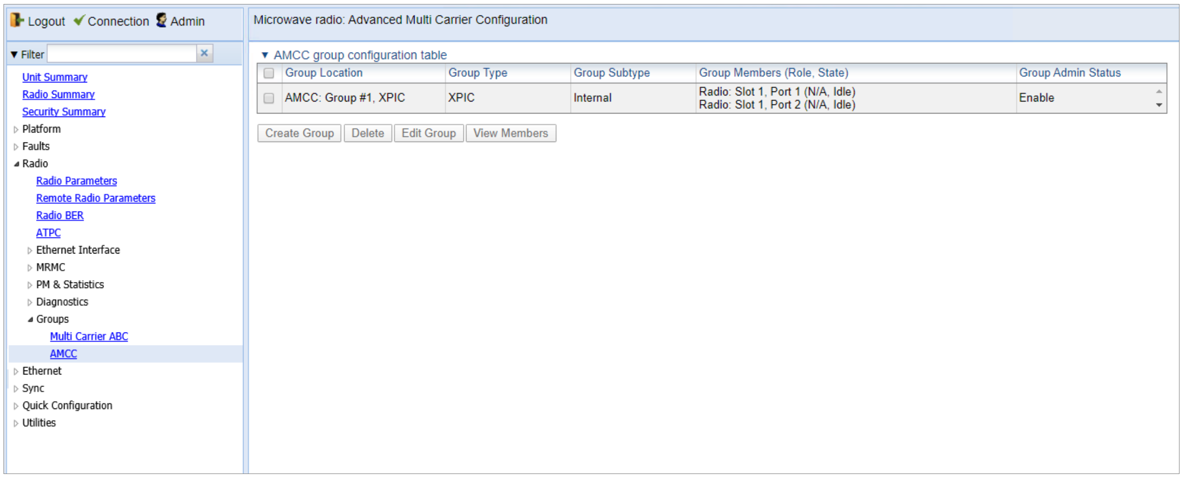
l. Review the parameters you have selected. If they are correct, click **Submit**. If you want to change any of the configurable parameters, click **Back**.

Deleting an AMCC (XPIC) Group

To delete an AMCC (XPIC) group:

1. Select **Radio** > **Groups** > **AMCC**. The Advanced Multi Carrier Configuration page opens.

Figure 100 *Advanced Multi Carrier Configuration Page (Populated)*



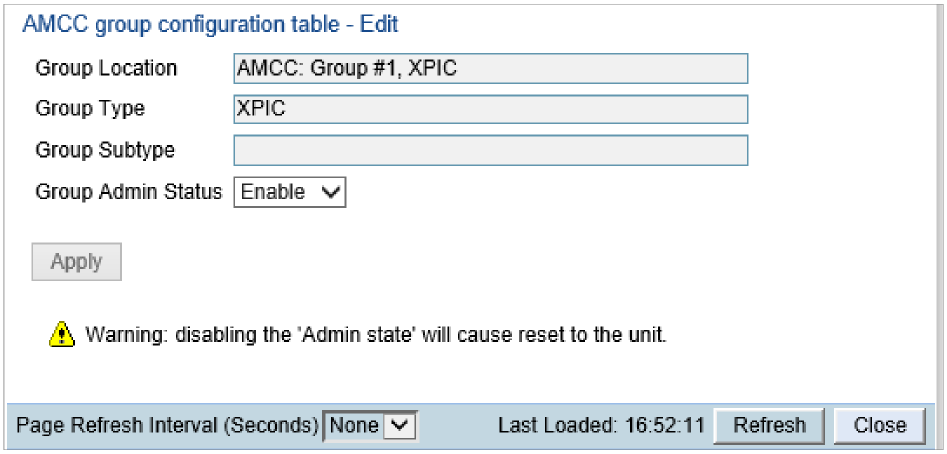
Microwave radio: Advanced Multi Carrier Configuration

AMCC group configuration table

	Group Location	Group Type	Group Subtype	Group Members (Role, State)	Group Admin Status
□	AMCC: Group #1, XPIC	XPIC	Internal	Radio: Slot 1, Port 1 (N/A, Idle) Radio: Slot 1, Port 2 (N/A, Idle)	Enable

2. Select the group and click **Edit Group**. The AMCC Group – Edit page opens.

Figure 101 *AMCC Group – Edit Page*



AMCC group configuration table - Edit

Group Location	AMCC: Group #1, XPIC
Group Type	XPIC
Group Subtype	
Group Admin Status	Enable

Warning: disabling the 'Admin state' will cause reset to the unit.

Last Loaded: 16:52:11

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 **Disable**.

Performing Antenna Alignment for XPIC

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 “RSLwanted”). This RSL should be no more than +/-2 dB from the expected level. Record the RSL of the first carrier as the “RSLwanted”).
3. Measure the RSL of the second carrier and record it as the “RSLunwanted”).

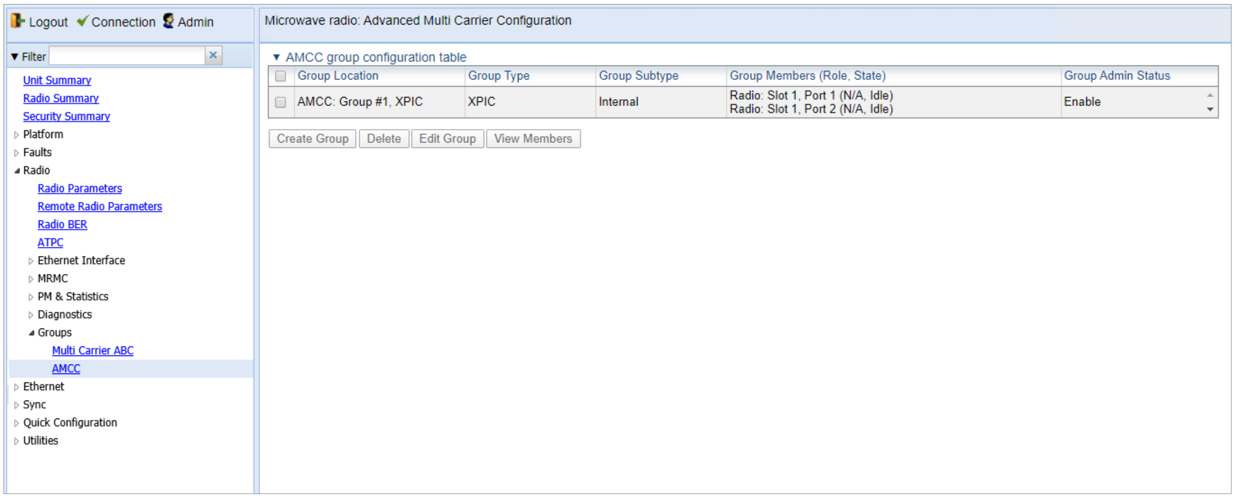
4. Determine the XPD by subtracting RSLunwanted from the RSLwanted.
5. The XPD should be at least 25dB. If it is not, you should adjust the OMT assembly on the back of the antenna at one side of the link until you achieve the highest XPD, which should be no less than 25dB. Adjust the OMT very slowly 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.

> **Note**
>
> 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 exceeds 25dB. A normal XPI level in clear sky conditions is between 25 and 30dB.

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 102 *Advanced Multi Carrier Configuration Page (Populated)*



☐	Group Location	Group Type	Group Subtype	Group Members (Role, State)	Group Admin Status
☐	AMCC: Group #1, XPIC	XPIC	Internal	Radio: Slot 1, Port 1 (N/A, Idle) Radio: Slot 1, Port 2 (N/A, Idle)	Enable

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.

Configuring Link Aggregation (LAG)

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.

Note

LACP is planned for future release.

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
- Deleting a LAG Group

LAG Overview

LAG can be used to provide redundancy for Ethernet interfaces, both on the same PTP 850 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.
- It is recommended not to include radio interfaces in a LAG group with Ethernet interfaces.
- 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 850 also supports Multi-Homing for ETH-BN and CSF messages. You can enable Multi-Homing when creating or editing a LAG. When Multi-Homing is enabled:

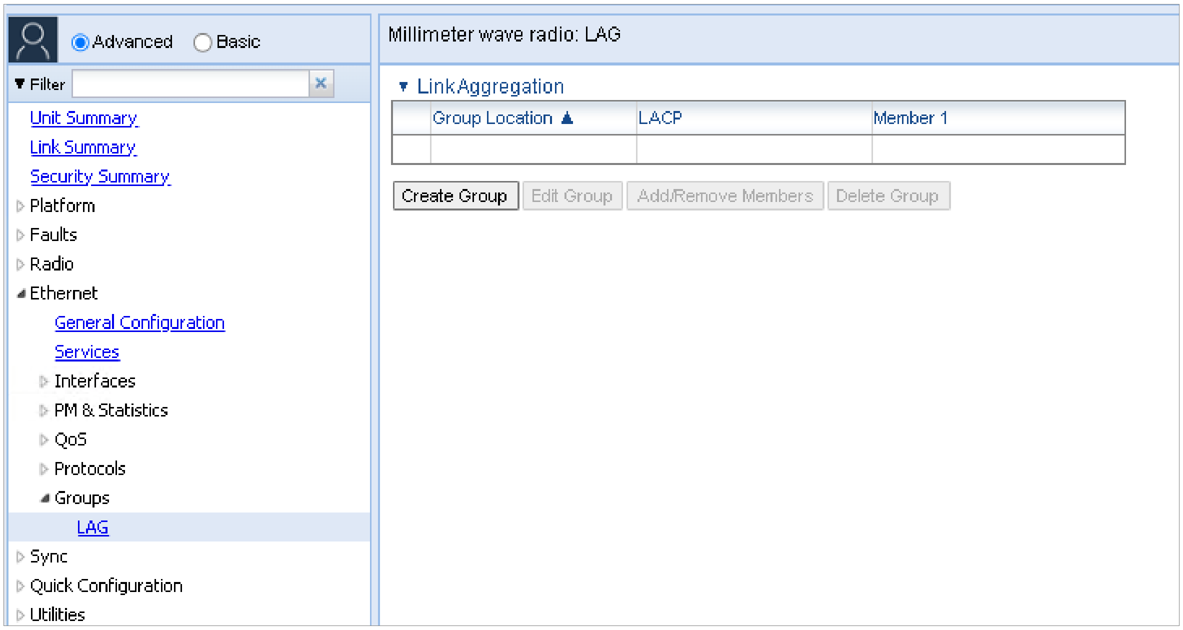
- If ETH-BN (Ethernet Bandwidth Notification) is enabled on one of the interfaces in the LAG, ETH-BN messages are sent simultaneously on all of the LAG members. See Configuring Ethernet Bandwidth Notification (ETH-BN).
- If ASP Management Safe Mode is enabled on one of the interfaces in the LAG, CSF messages are sent simultaneously on all of the LAG members. See Configuring Automatic State Propagation and Link Loss Forwarding.

Configuring a LAG Group

To create a LAG group:

1. Select **Ethernet** > **Groups** > **LAG**. The LAG page opens.

Figure 103 *LAG Page (Empty)*



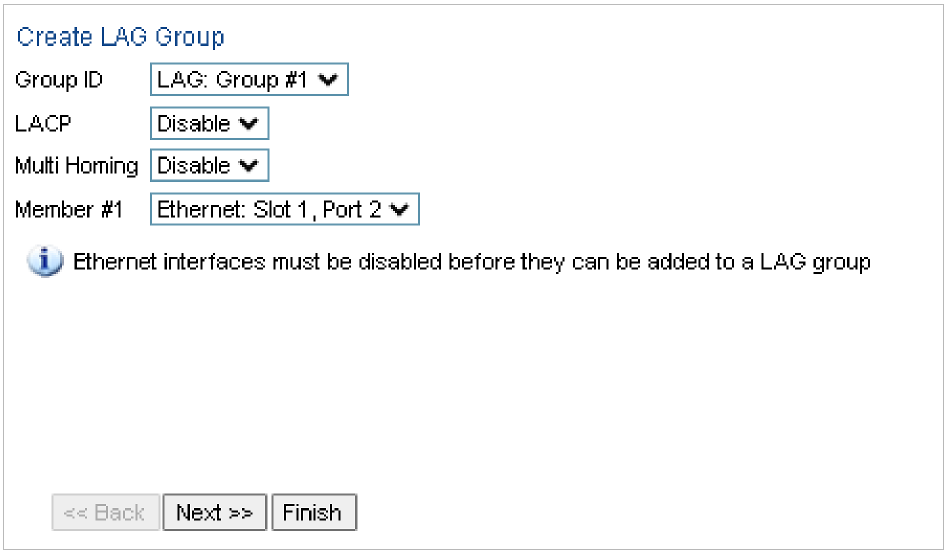
Millimeter wave radio: LAG

▾ LinkAggregation

Group Location ▲	LACP	Member 1

2. Click **Create Group** underneath the Link Aggregation table. The Create LAG Group page opens.

Figure 104 *Create LAG Group – Page 1*



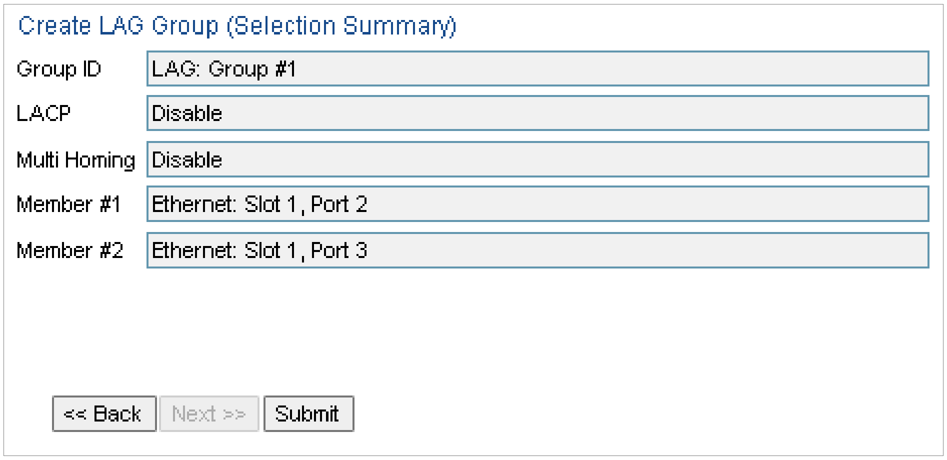
Create LAG Group

Group ID	LAG: Group #1
LACP	Disable
Multi Homing	Disable
Member #1	Ethernet: Slot 1 , Port 2

Ethernet interfaces must be disabled before they can be added to a LAG group

3. 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.
4. In the **LACP** field, select Disable. LACP is planned for future release.
5. In the **Multi Homing** field, select Enable to enable Multi-Homing on the LAG or Disable to disable Multi-Homing 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 105 *Create LAG Group – Summary Page*



Create LAG Group (Selection Summary)

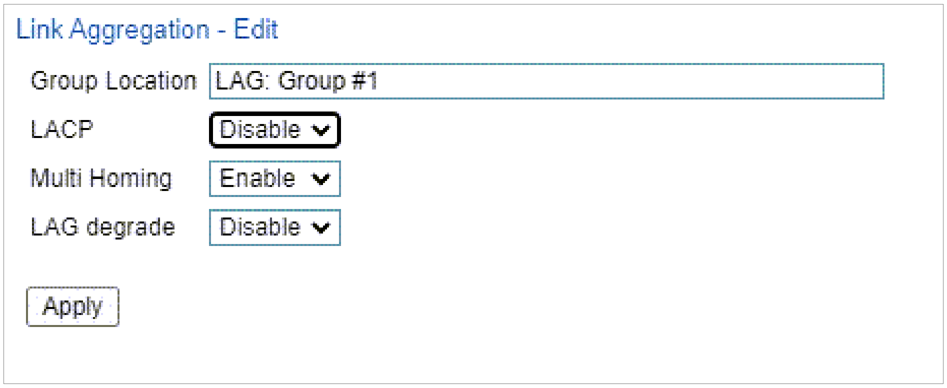
Group ID	LAG: Group #1
LACP	Disable
Multi Homing	Disable
Member #1	Ethernet: Slot 1, Port 2
Member #2	Ethernet: Slot 1, Port 3

11. 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.

To edit an existing LAG group:

1. Select **Ethernet** > **Groups** > **LAG**. The LAG page opens.
2. Select the LAG group you want to edit in the Link Aggregation table.
3. Click **Edit Group** underneath the Link Aggregation table. The Link Aggregation - Edit page opens.

   Figure 114: Link Aggregation - Edit Page



Link Aggregation - Edit

Group Location	LAG: Group #1
LACP	Disable
Multi Homing	Enable
LAG degrade	Disable

4. Do any of the following:
   - To enable or disable Multi-Homing, select **Enable** or **Disable** in the **Multi Homing** field. See LAG Overview for an explanation of Multi-Homing.
   - To enable or disable LAG Group Shutdown in case of Degradation Event, select **Enable** or **Disable** in the **LAG degrade** field. See Enabling and Disabling LAG Group Shutdown in Case of Degradation Event for restrictions.
5. 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.
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 Do any of the following:

Note

When removing an interface from a LAG group, the removed interface is assigned the default interface values.

For information about the **LAG degrade** field, see Enabling and Disabling LAG Group Shutdown in Case of Degradation Event .

Enabling and Disabling LAG Group Shutdown in Case of Degradation Event

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:

1. Select **Ethernet** > **Groups** > **LAG** to open the LAG page.
2. Select the LAG group in the Link Aggregation table.
3. Click **Edit Group** underneath the Link Aggregation table. The Link Aggregation - Edit page opens (Figure 114: Link Aggregation - Edit Page).
4. 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.
5. Click **Apply**.

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 and that all members of the LAG group are set to **Admin = Down**.

To delete one or more LAG groups:

1. Select **Ethernet** > **Groups** > **LAG**. The LAG page opens.
2. Select the LAG group or groups you want to delete in the Link Aggregation table, or select all the LAG groups by selecting the check box in the top row.
3. Click **Delete Group** underneath the Link Aggregation table. The LAG group or groups are deleted.

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 Unit 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

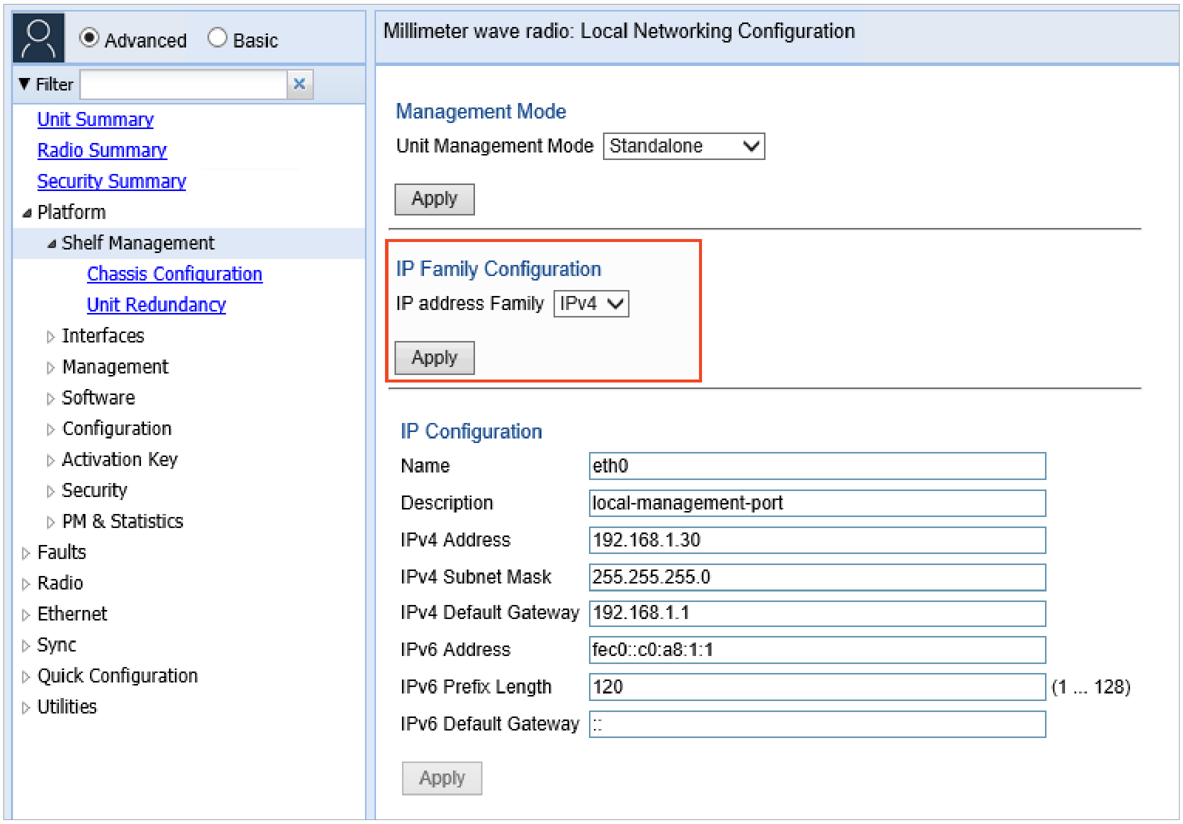
Defining the IP Protocol Version for Initiating Communications

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 106 *Local Networking Configuration Page (IP Family Configuration)*



Millimeter wave radio: Local Networking Configuration

Management Mode

Unit Management Mode: Standalone

IP Family Configuration

IP address Family: IPv4

IP Configuration

Name	eth0
Description	local-management-port
IPv4 Address	192.168.1.30
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	192.168.1.1
IPv6 Address	fec0::c0:a8:1:1
IPv6 Prefix Length	120 (1 ... 128)
IPv6 Default Gateway	::

2. In the **IP Address Family** field, select the IP protocol the unit will use when initiating communications. The options are **IPv4** or **IPv6**.

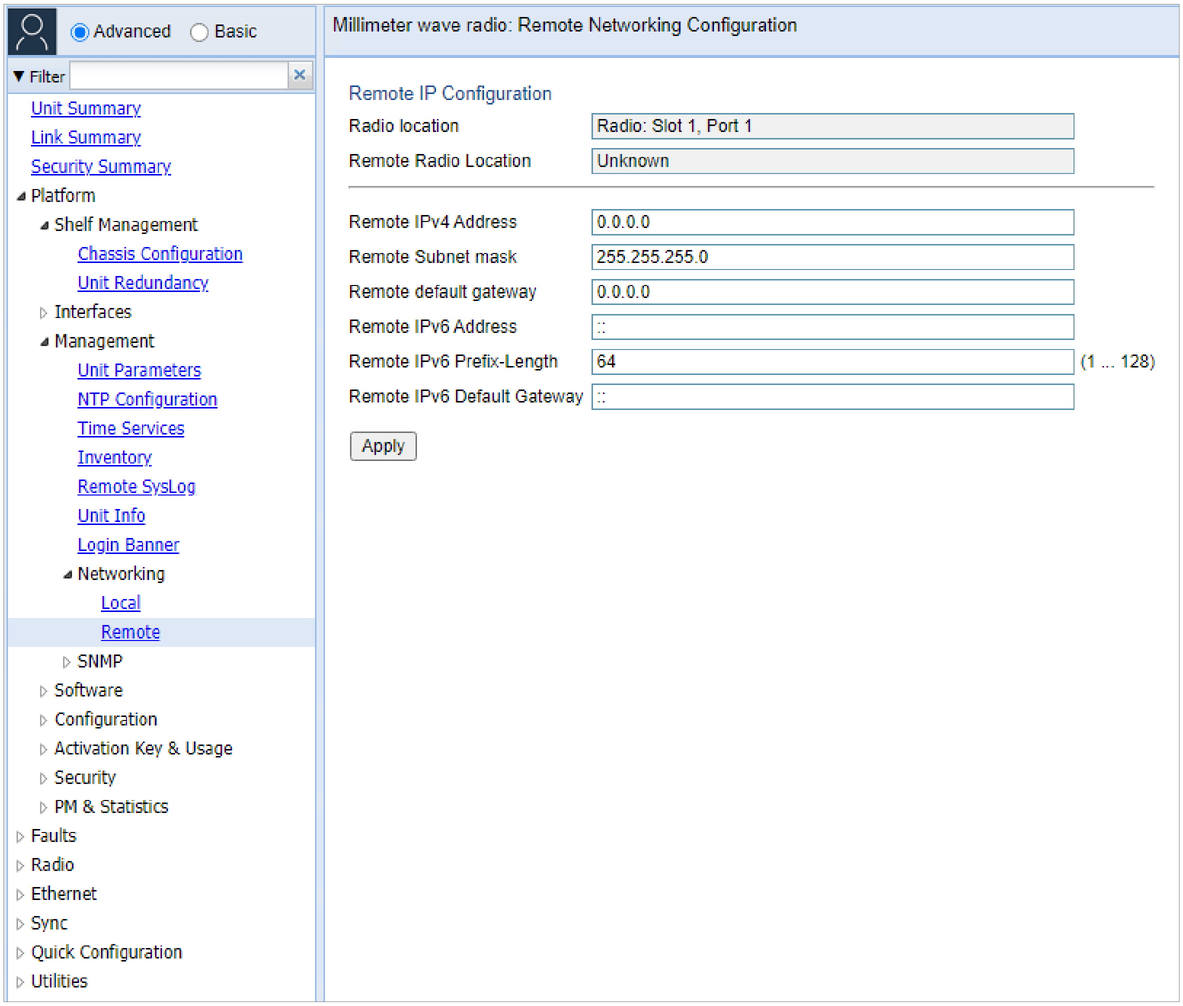
Configuring the Remote Unit's IP Address

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 107 *Remote Networking Configuration Page*



Millimeter wave radio: Remote Networking Configuration

Remote IP Configuration

Radio location	Radio: Slot 1, Port 1
Remote Radio Location	Unknown
Remote IPv4 Address	0.0.0.0
Remote Subnet mask	255.255.255.0
Remote default gateway	0.0.0.0
Remote IPv6 Address	::
Remote IPv6 Prefix-Length	64 (1 ... 128)
Remote IPv6 Default Gateway	::

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. For **IPv6 Assignment Mode**, select from the following options:

   - **Manual** – The IPv6 address is configured manually (default).
   - **Automatic** – The IPv6 address is obtained automatically from a DHCPv6 server.

     For additional information, see Enabling Dynamic IPv6 Addresses Via DHCPv6.

6. 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.

7. If you entered an IPv6 address, enter the IPv6 prefix length in the **Remote** IPv6 Prefix-Length field.
8. Optionally, if you entered an IPv6 address, enter the default gateway in IPv6 format in the **Remote IPv6 Default** Gateway field.
9. If the **IPv6 Assignment Mode** is **Automatic**, the **Remote IPv6 Link Local Address** can be used to reconnect to the device if the DHCPv6 server is unavailable.
10. Click **Apply**.

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.

Configuring SNMP

PTP 850 supports SNMP v1, V2c, and v3. You can set community strings for access to PTP 850 units.

PTP 850 supports the following MIBs:

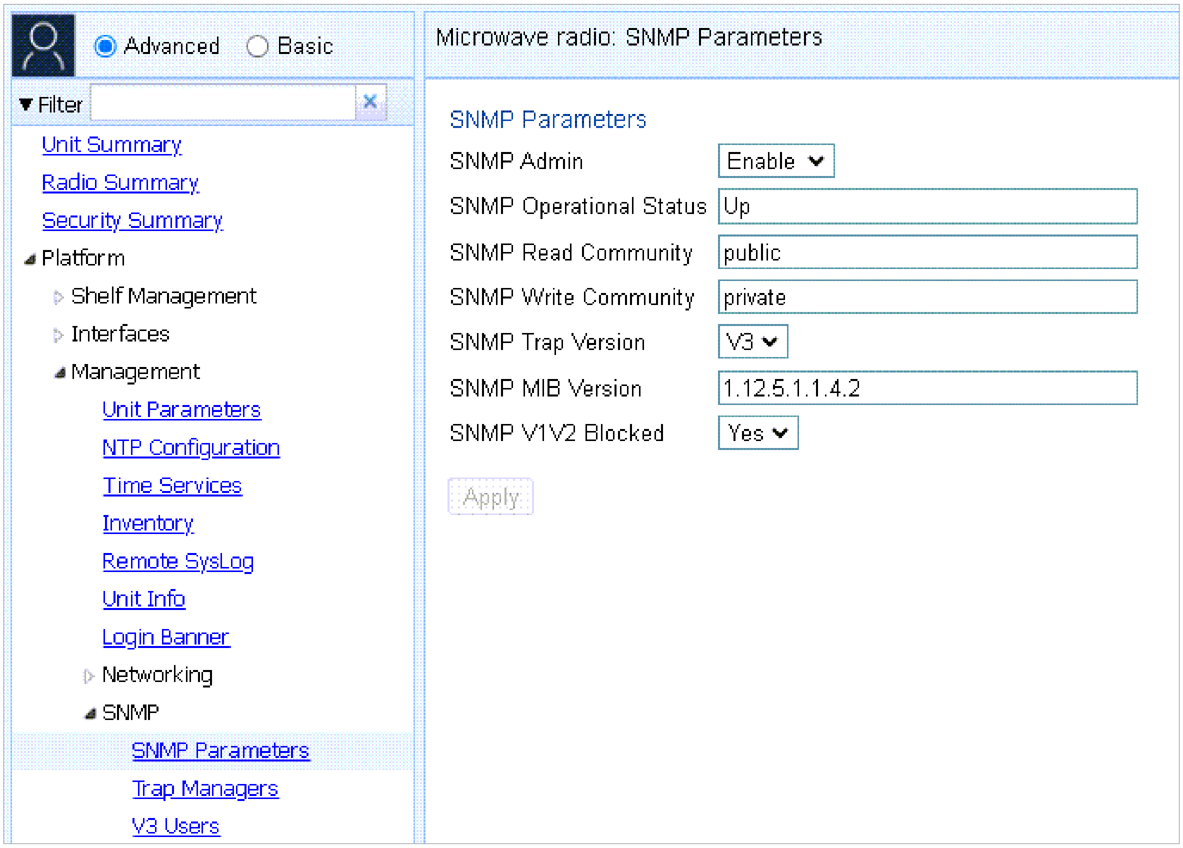
- RFC-1213 (MIB II).
- RMON MIB.
- Proprietary MIB.

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 108 *SNMP Parameters Page*



Microwave radio: SNMP Parameters

SNMP Parameters

SNMP Admin	Enable
SNMP Operational Status	Up
SNMP Read Community	public
SNMP Write Community	private
SNMP Trap Version	V3
SNMP MIB Version	1.12.5.1.1.4.2
SNMP V1V2 Blocked	Yes

2. In the **SNMP Admin** field, select **Enable** to enable SNMP monitoring, or **Disable** to disable SNMP monitoring.

> Note
>
> The **SNMP 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.

> **Note**
>
> The SNMP write community string must be different than the SNMP read community string. Otherwise, set commands will not take effect.

5. In the **SNMP Trap Version** field, select **V1, V2,** or **V3** to specify the SNMP version. By default, the **SNMP Trap Version** is **V3**.

> **Note**
>
> The SNMP MIB Version field displays the current SNMP MIB version the unit is using.

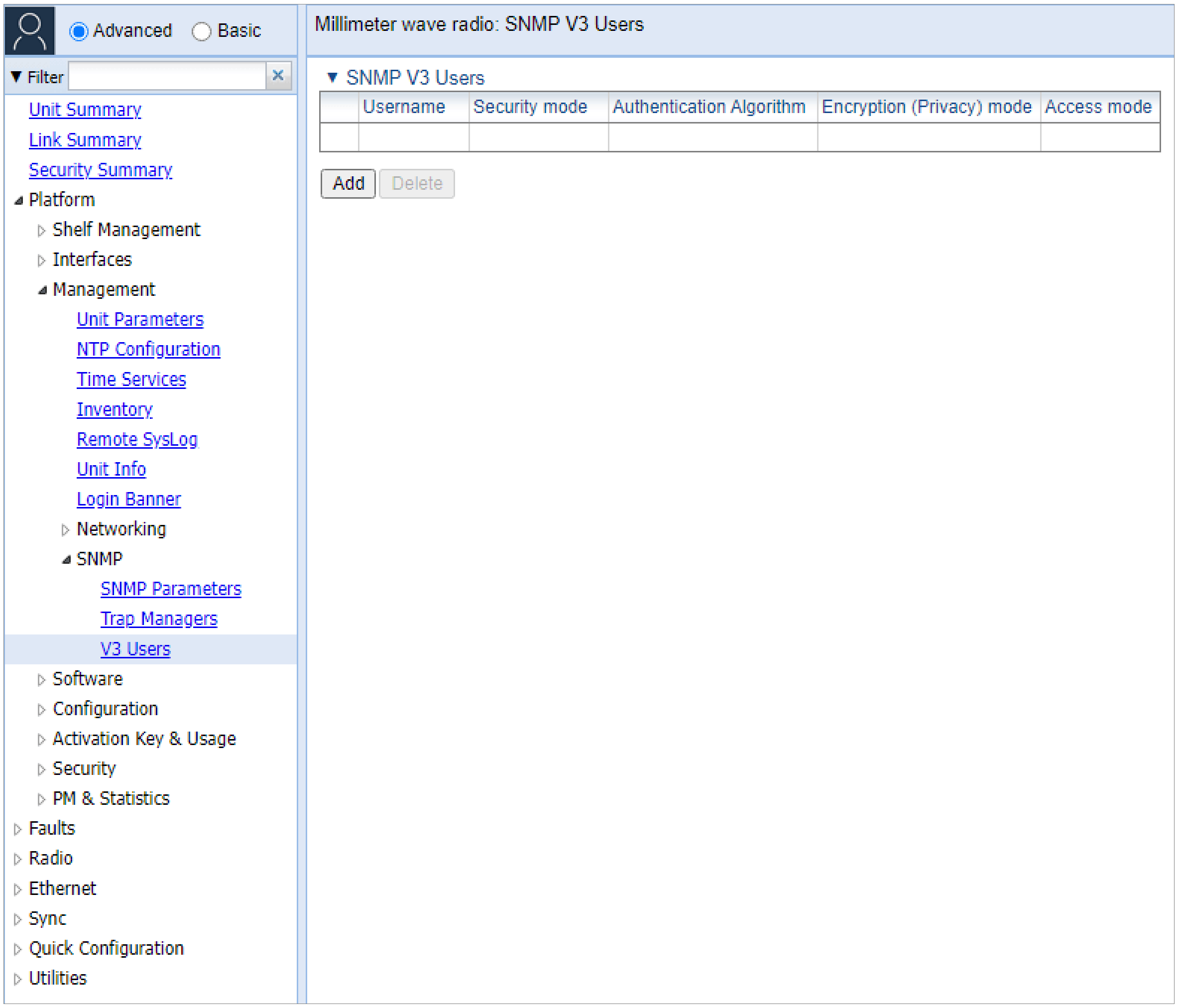
6. In the **SNMP V1V2 Blocked** field, select **Yes** if you want to block SNMPv1 and SNMPv2 access so that only SNMPv3 access will be enabled. By default, SNMPv1 and SNMPv2 are blocked.
7. Click **Apply**.

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 109 *SNMP V3 Users Page*



● Advanced ○ Basic

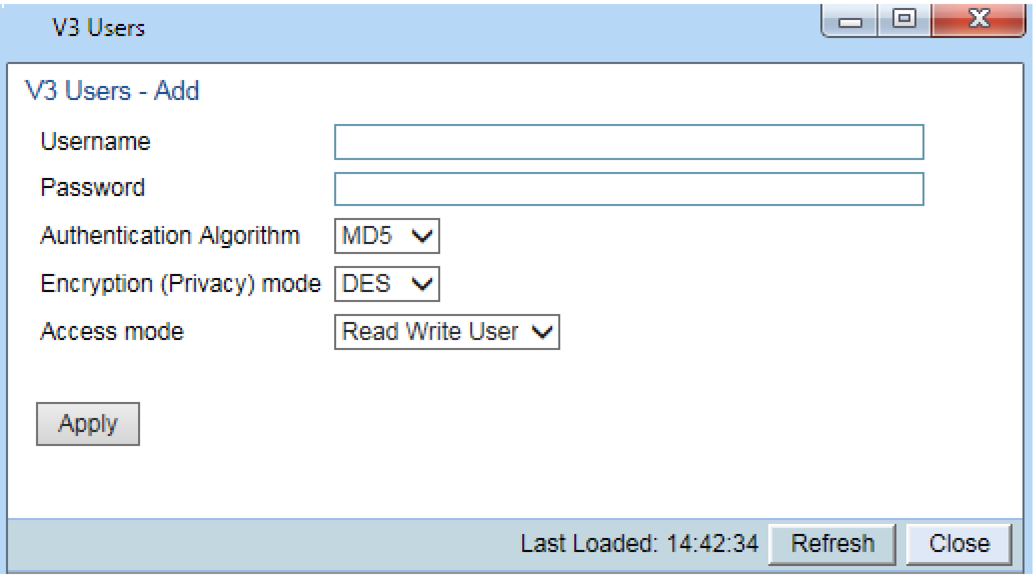
Millimeter wave radio: SNMP V3 Users

▼ SNMP V3 Users

	Username	Security mode	Authentication Algorithm	Encryption (Privacy) mode	Access mode

2. Click Add. The SNMP V3 Users - Add page opens.

Figure 110 *SNMP V3 Users - Add Page*



V3 Users

V3 Users - Add

Username

Password

Authentication Algorithm: MD5

Encryption (Privacy) mode: DES

Access mode: Read Write User

Last Loaded: 14:42:34

3. Configure the SNMP V3 User parameters, as described below.
4. Click **Apply**, then **Close**.

Table 15 *SNMP V3 User Parameters*

Parameter	Definition
Username	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**

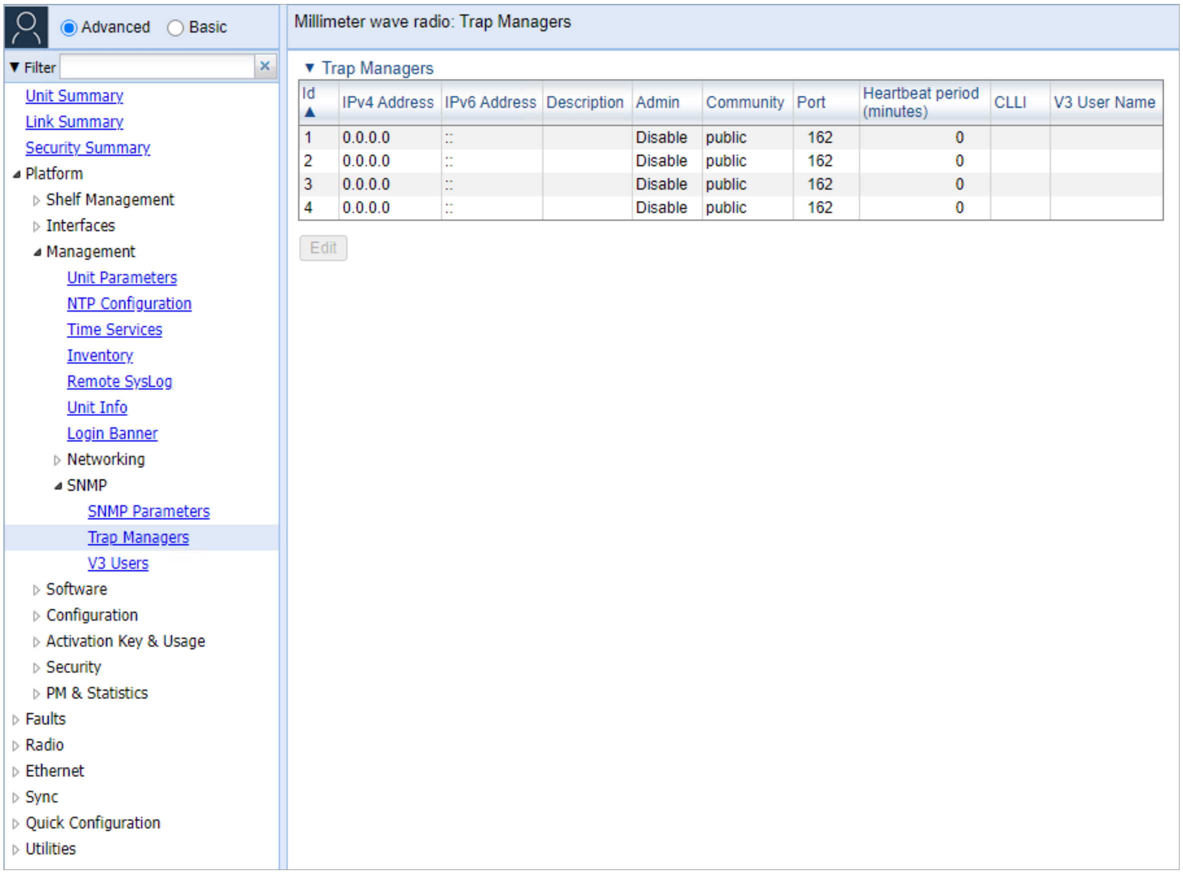
Configuring Trap Managers

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 111 *Trap Managers Page*



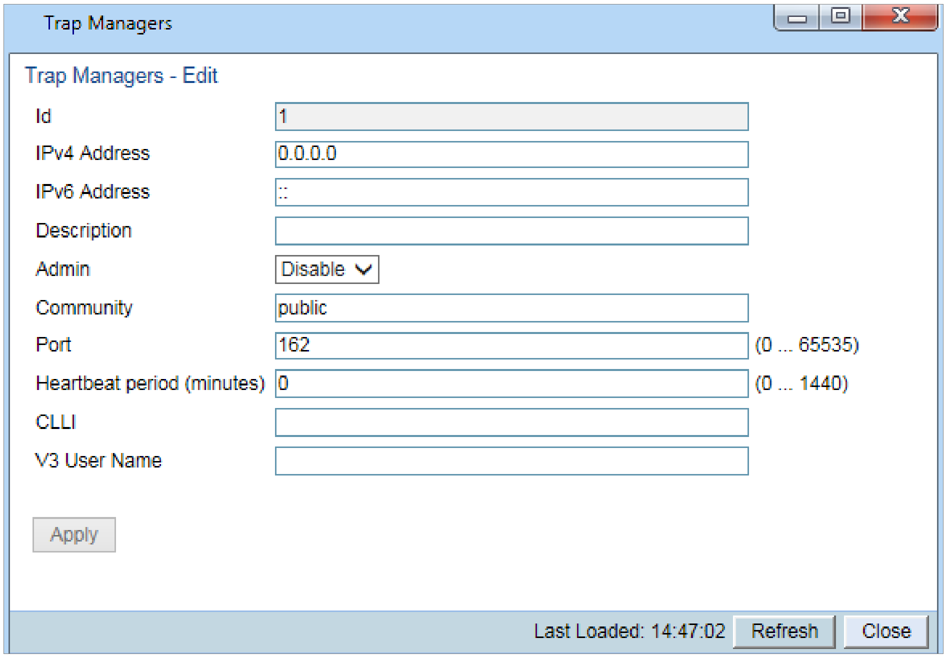
Millimeter wave radio: Trap Managers

▼ Trap Managers

Id ▲	IPv4 Address	IPv6 Address	Description	Admin	Community	Port	Heartbeat period (minutes)	CLLI	V3 User Name
1	0.0.0.0	::		Disable	public	162	0		
2	0.0.0.0	::		Disable	public	162	0		
3	0.0.0.0	::		Disable	public	162	0		
4	0.0.0.0	::		Disable	public	162	0		

2. Select a trap manager and click **Edit**. The Trap Managers Edit page opens.

Figure 112 *Trap Managers - Edit Page*



Trap Managers - Edit

Id	1
IPv4 Address	0.0.0.0
IPv6 Address	::
Description	
Admin	Disable
Community	public
Port	162 (0 ... 65535)
Heartbeat period (minutes)	0 (0 ... 1440)
CLLI	
V3 User Name	

3. Configure the trap manager parameters, as described in Trap Manager Parameters.

4. Click **Apply**, then **Close**.

Table 16 *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.
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.

Parameter	Definition
V3 User Name	If the SNMP Trap version selected in 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 SNMP V3 Users Page page. **Note**: Make sure that an identical V3 user is also defined on the manager's side.

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.

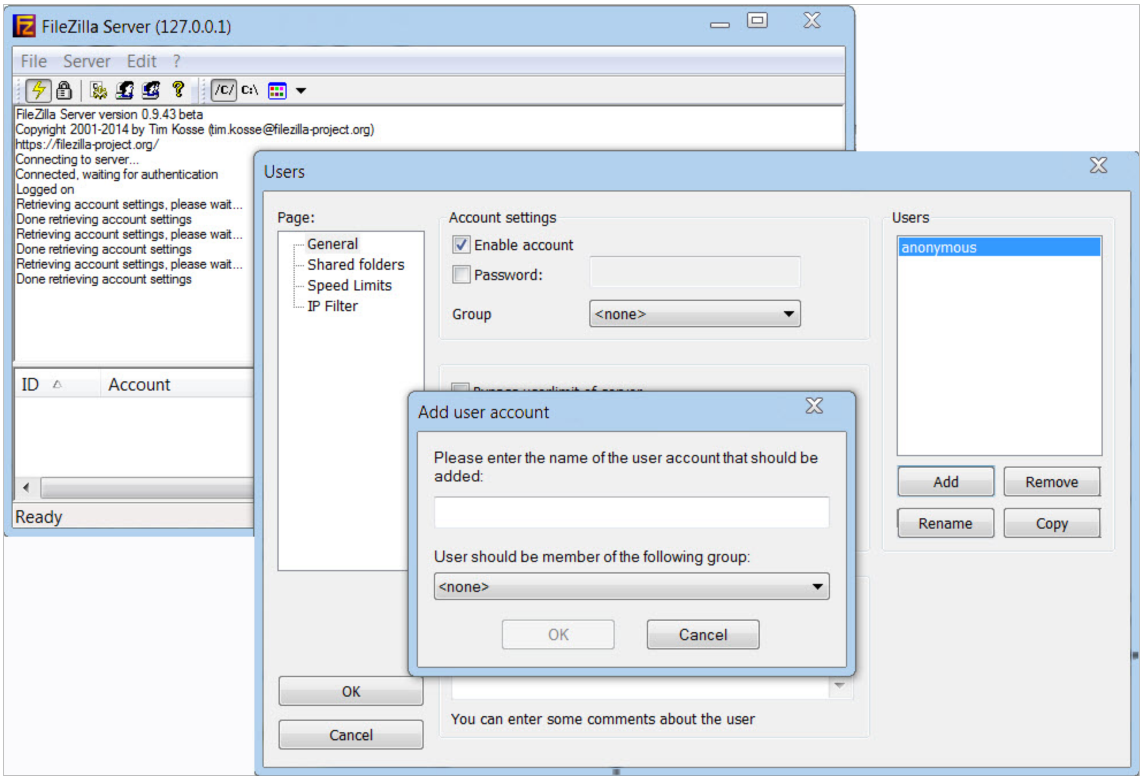
> **Note**
>
> For FTP, it is recommended to use FileZilla_Server software that can be downloaded from the web (freeware).
>
> For SFTP, it is recommended to use SolarWinds SFTP server 1.0.4.9 (freeware).

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:
   a. From the **Edit** menu, select **Users**.
   b. In the Users window, click **Add**.
   c. In the Add user account window, enter a user name and click **OK**.
   d. In the Users window, select **Enable account** and, optionally, select **Password** and enter a password.
   e. In the Users window, click **OK**.

Figure 113 *FileZilla Server User Configuration*



FileZilla Server (127.0.0.1)

```
FileZilla Server version 0.9.43 beta
Copyright 2001-2014 by Tim Kosse (tim.kosse@filezilla-project.org)
https://filezilla-project.org/
Connecting to server...
Connected, waiting for authentication
Logged on
Retrieving account settings, please wait...
Done retrieving account settings
Retrieving account settings, please wait...
Done retrieving account settings
Retrieving account settings, please wait...
Done retrieving account settings
```

Users

Account settings

☑ Enable account

□ Password:

Group <none>

Users: anonymous

Add user account

Please enter the name of the user account that should be added:

User should be member of the following group: <none>

You can enter some comments about the user

Ready

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:

    a. From the **Edit** menu, select **Users**.

    b. In the Users window, select **Shared folders**.

    c. Underneath the Shared folders section, click **Add** and browse for your shared FTP folder.

    d. Select the folder and click **OK**.

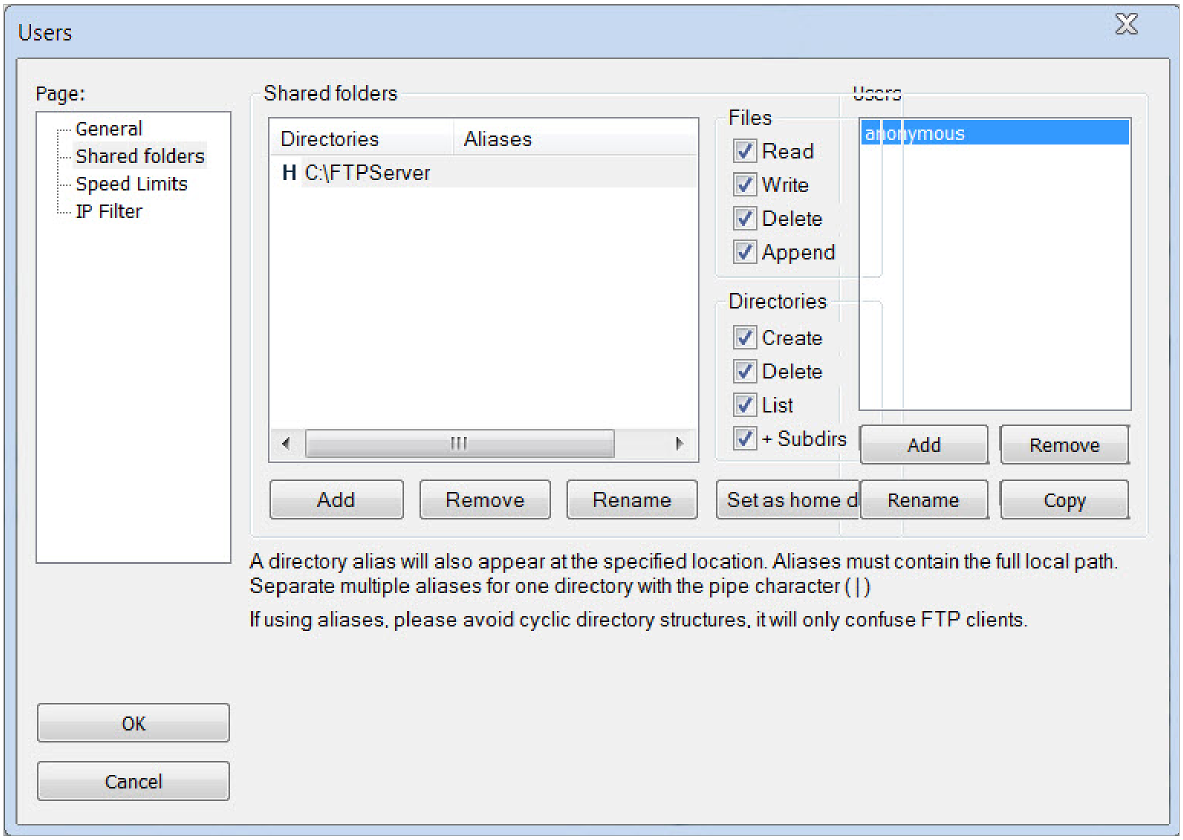
    e. In the Shared folders section, select your shared FTP folder.

    f. In the Files and Directories sections, select all of the permissions.

    g. Click **Set as home directory** to make the Shared folder the root directory for your FTP server.

    h. Click **OK** to close the Users window.

Figure 114 *FileZilla Server Shared Folder Setup*



H C:\FTPServer

Files: ☑ Read ☑ Write ☑ Delete ☑ Append

Directories: ☑ Create ☑ Delete ☑ List ☑ + Subdirs

anonymous

A directory alias will also appear at the specified location. Aliases must contain the full local path. Separate multiple aliases for one directory with the pipe character (|)

If using aliases, please avoid cyclic directory structures, it will only confuse FTP clients.

Configuring the Internal Ports for FTP or SFTP

By default, the following 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):

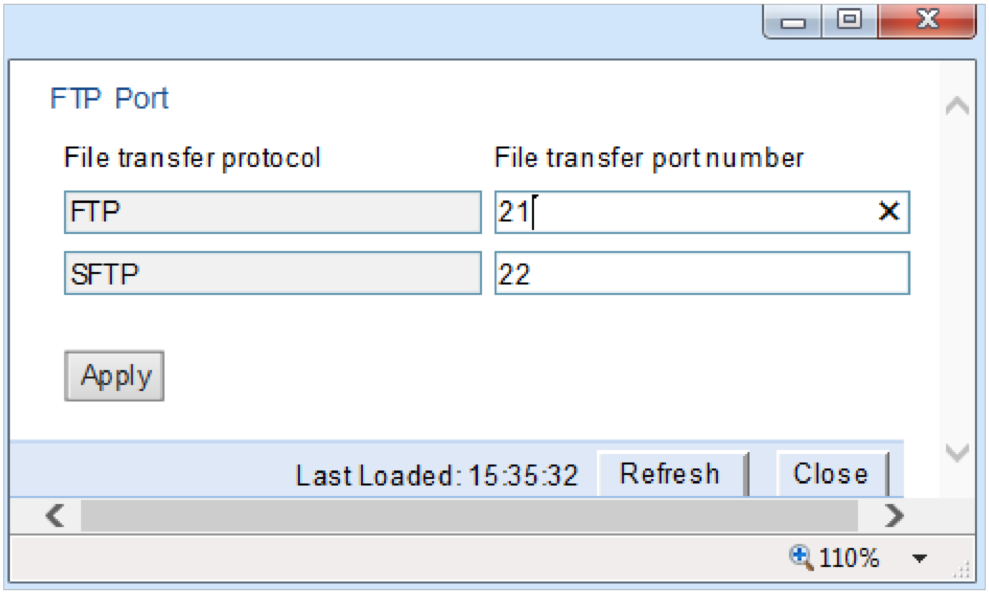
- FTP – 21
- SFTP – 22

You can change either or both of these ports from the following pages:

- Platform > Management > Unit Info
- Platform > 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
- Platform > Security > RSA Key

From any of these pages, click **FTP Port**. The FTP Port page opens.

Figure 115 *FTP Port Page*



FTP Port

File transfer protocol	File transfer port number
FTP	21
SFTP	22

Edit the **File transfer port number** for FTP and or SFTP and click **Apply**.

Note

Only SFTP is available in the X.509 Certificate pages and the RSA Key page.

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.

Note

Make sure to use the original System Release software file, without any modification. Otherwise the software download process will fail.

This section includes:

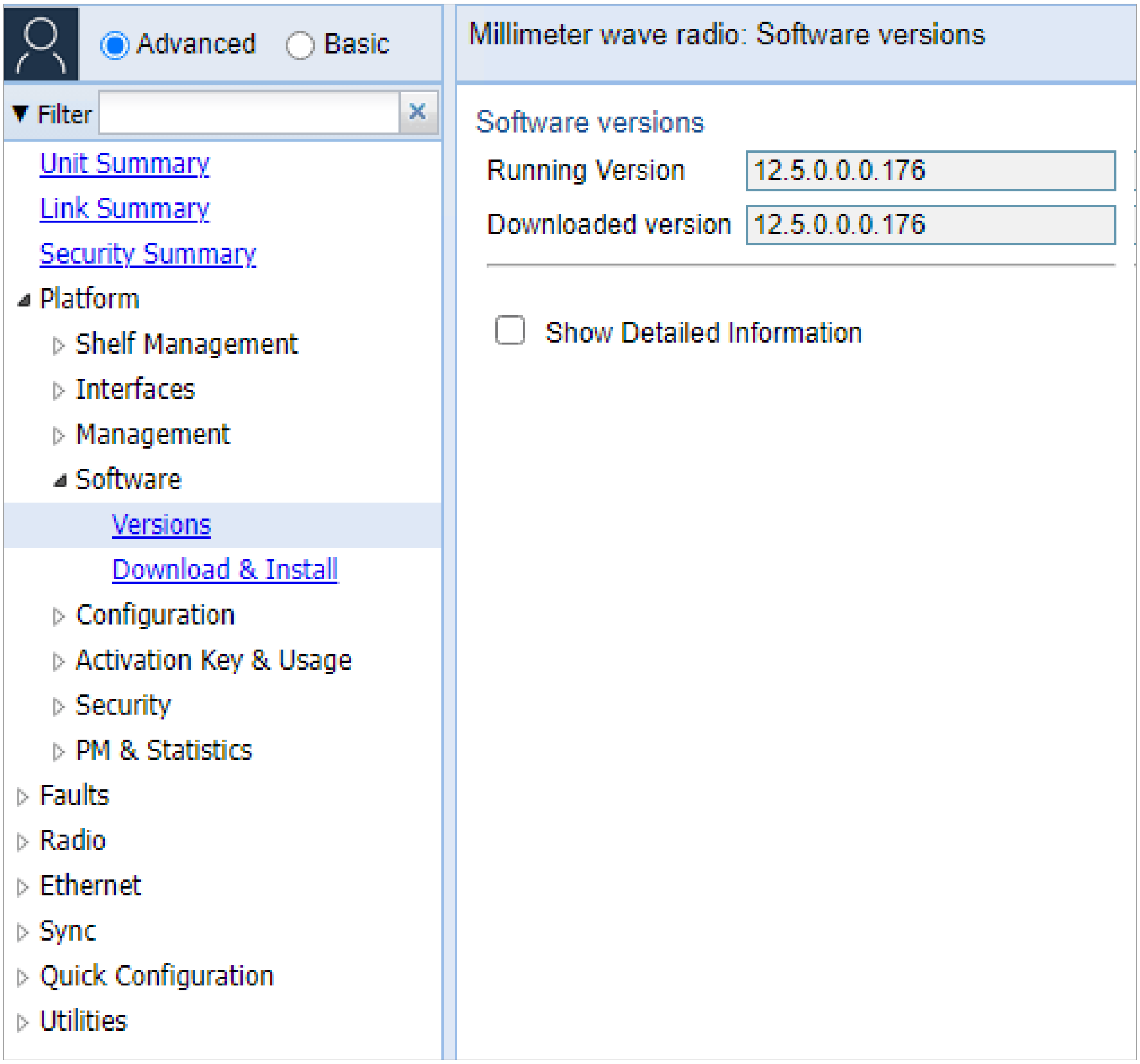
- Viewing Current Software Versions
- Software Upgrade Overview
- Downloading and Installing Software
- Configuring a Timed Installation

Viewing Current Software Versions

To display the software version running and downloaded on the unit:

1. Select **Platform** > **Software** > **Versions**. The Software Versions page opens, displaying the following:
   - **Running Version** – The software version currently running on the unit.
   - **Downloaded Version** – The version, if any, that has been downloaded from the server but not yet installed. Upon installation and reset, this version will become the Running Version.

Figure 116 *Software Versions Page*



● Advanced ○ Basic

Millimeter wave radio: Software versions

Software versions

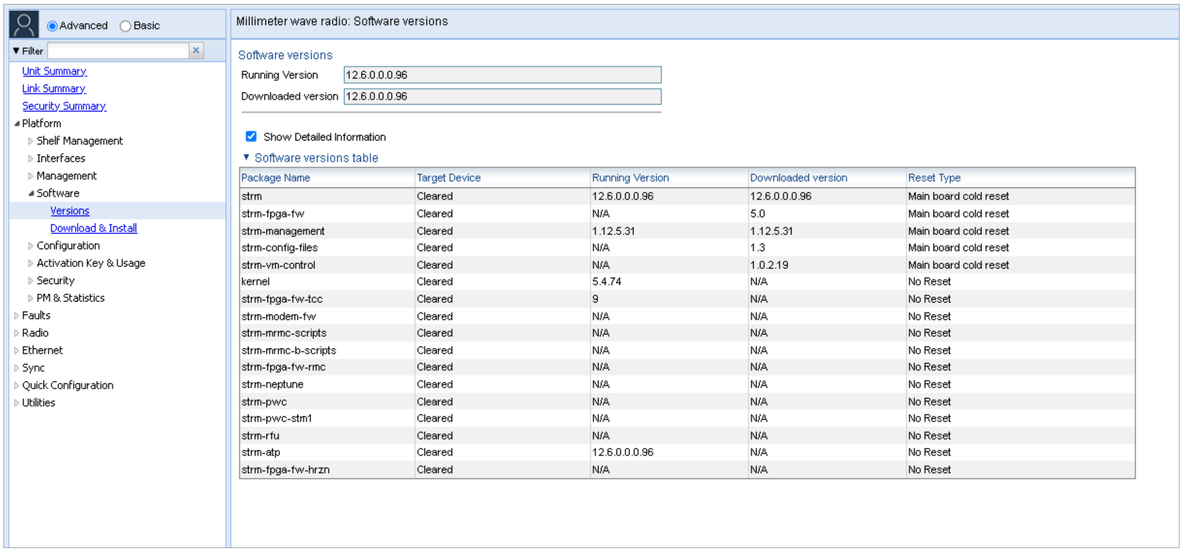
Running Version: 12.5.0.0.0.176

Downloaded version: 12.5.0.0.0.176

□ Show Detailed Information

2. To display more detailed information about software component versions, select Show Detailed Information. The Software Versions table opens in the Versions page. For a description of the information provided in the Software Versions table, see Software Versions Table Columns.

Figure 117 *Software Versions Table*



Millimeter wave radio: Software versions

Software versions

Running Version 12.6.0.0.0.96

Downloaded version 12.6.0.0.0.96

☑ Show Detailed Information

Software versions table

Package Name	Target Device	Running Version	Downloaded version	Reset Type
strm	Cleared	12.6.0.0.0.96	12.6.0.0.0.96	Main board cold reset
strm-fpga-fw	Cleared	N/A	5.0	Main board cold reset
strm-management	Cleared	1.12.5.31	1.12.5.31	Main board cold reset
strm-config-files	Cleared	N/A	1.3	Main board cold reset
strm-vm-control	Cleared	N/A	1.0.2.19	Main board cold reset
kernel	Cleared	5.4.74	N/A	No Reset
strm-fpga-fw-tcc	Cleared	9	N/A	No Reset
strm-modem-fw	Cleared	N/A	N/A	No Reset
strm-mrmc-scripts	Cleared	N/A	N/A	No Reset
strm-mrmc-b-scripts	Cleared	N/A	N/A	No Reset
strm-fpga-fw-rmc	Cleared	N/A	N/A	No Reset
strm-neptune	Cleared	N/A	N/A	No Reset
strm-pwc	Cleared	N/A	N/A	No Reset
strm-pwc-stm1	Cleared	N/A	N/A	No Reset
strm-rfu	Cleared	N/A	N/A	No Reset
strm-atp	Cleared	12.6.0.0.0.96	N/A	No Reset
strm-fpga-fw-hrzn	Cleared	N/A	N/A	No Reset

Table 17 *Software Versions Table 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.
Downloaded Version	The version, if any, that has been downloaded from the server but not yet installed. Upon installation, this version will become the Running 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.

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.

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).

When upgrading a node with Unit Redundancy, upgrade the standby unit first, then the active unit.

Downloading and Installing Software

Note

For HTTPS and SFTP downloads, be aware that only certain ciphers are supported. For a list of supported ciphers, refer to Annex A – Supported Ciphers for Secured Communication Protocols in the Release Notes for the product and System Release version you are using.

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.

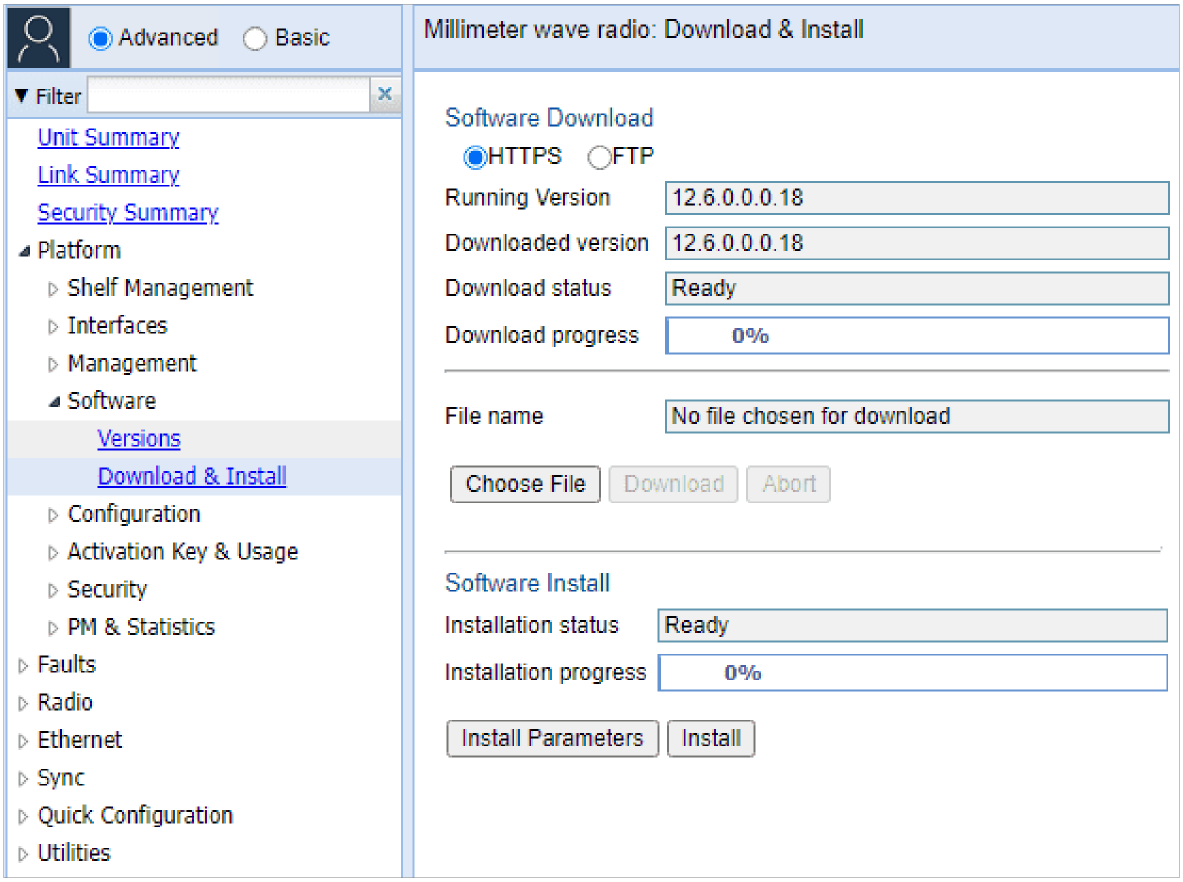
When downloading software via FTP or SFTP, the PTP 850 functions as an FTP or SFTP client. You must install FTP or SFTP server software on the PC or laptop you are using to perform the software upgrade. For details, see Installing and Configuring an FTP or SFTP Server.

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. See Setting the Time and Date (Optional).
2. In the PTP 850's Web EMS, select **Platform** > **Software** > **Download & Install**. The Download & Install page opens.

Figure 118 *Download & Install Page – HTTP/HTTPS Download – No File Selected*



Millimeter wave radio: Download & Install

Software Download

● HTTPS ○ FTP

Running Version: 12.6.0.0.0.18

Downloaded version: 12.6.0.0.0.18

Download status: Ready

Download progress: 0%

File name: No file chosen for download

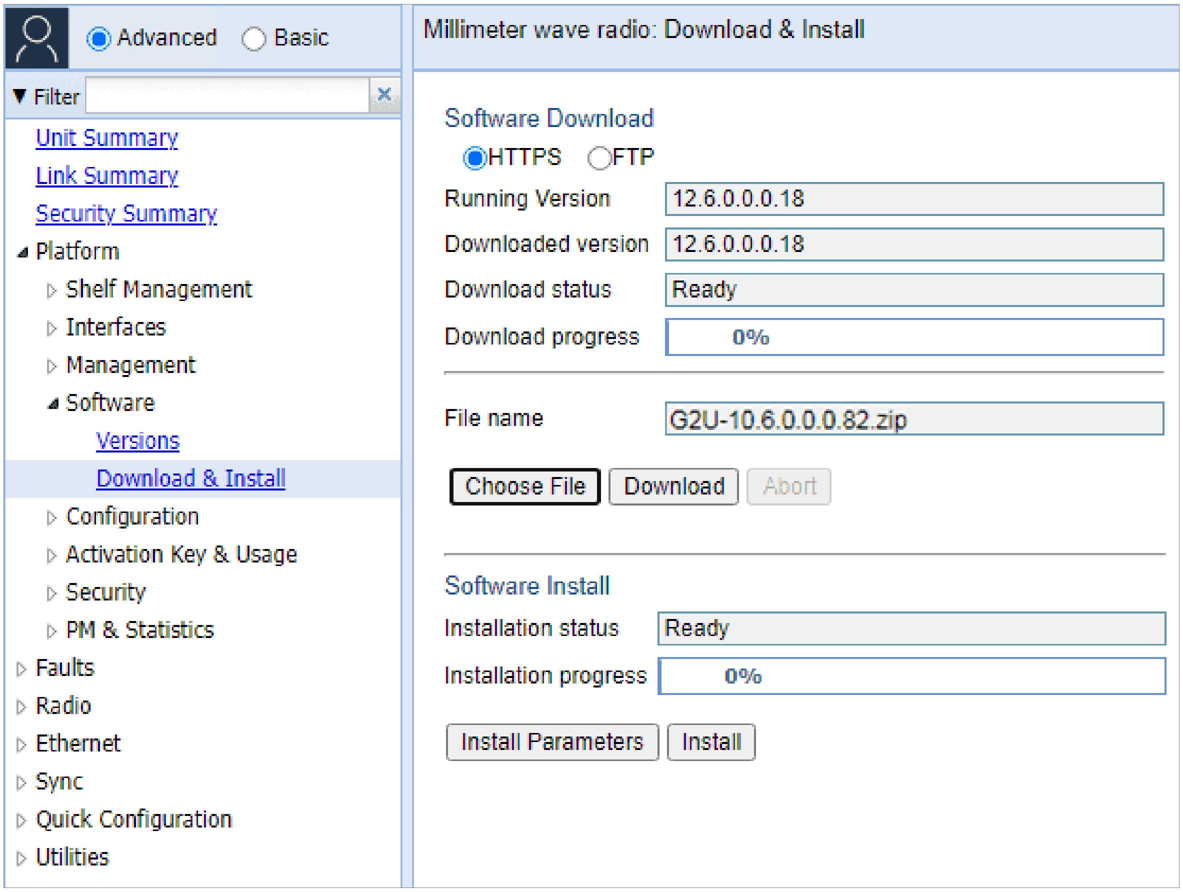
Software Install

Installation status: Ready

Installation progress: 0%

3. Select **HTTPS**.
4. Click **Choose File**. A browse window opens.
5. Navigate to the directory in which the software file is located and select 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 119 *Download & Install Page – HTTP/HTTPS Download –File Selected*



Millimeter wave radio: Download & Install

Software Download

● HTTPS ○ FTP

Running Version	12.6.0.0.0.18
Downloaded version	12.6.0.0.0.18
Download status	Ready
Download progress	0%
File name	G2U-10.6.0.0.0.82.zip

Software Install

Installation status	Ready
Installation progress	0%

7. Click **Download**. The download begins. You can view the status of the download in the **Download Status** field. See Download & Install Status Parameters.

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.

Downloading Software Via FTP or SFTP

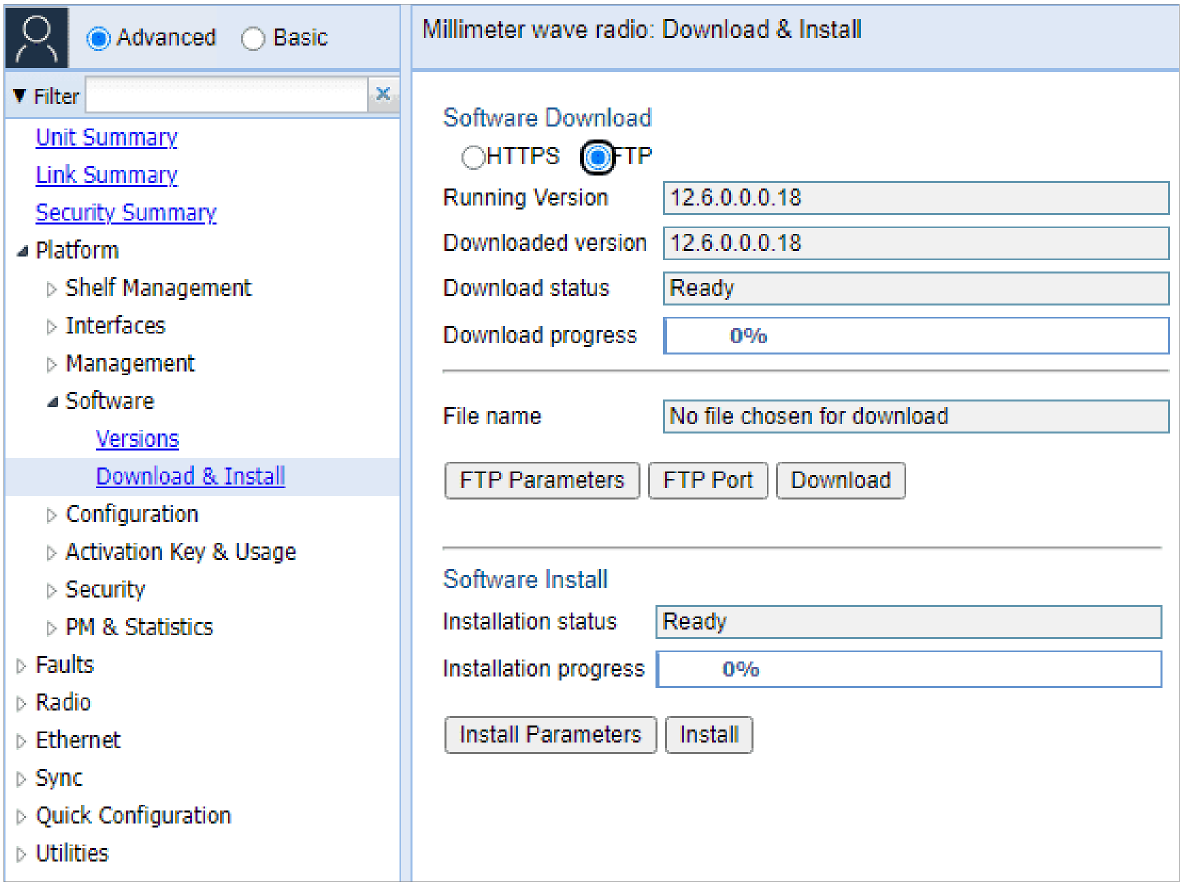
To download and install a new software version using FTP or SFTP:

1. Before performing a software upgrade, it is important to verify that the system date and time are correct. See Setting the Time and Date (Optional).
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 120 *Download & Install Page – FTP*



● Advanced ○ Basic

Millimeter wave radio: Download & Install

Software Download

○ HTTPS ● FTP

Running Version: 12.6.0.0.0.18

Downloaded version: 12.6.0.0.0.18

Download status: Ready

Download progress: 0%

File name: No file chosen for download

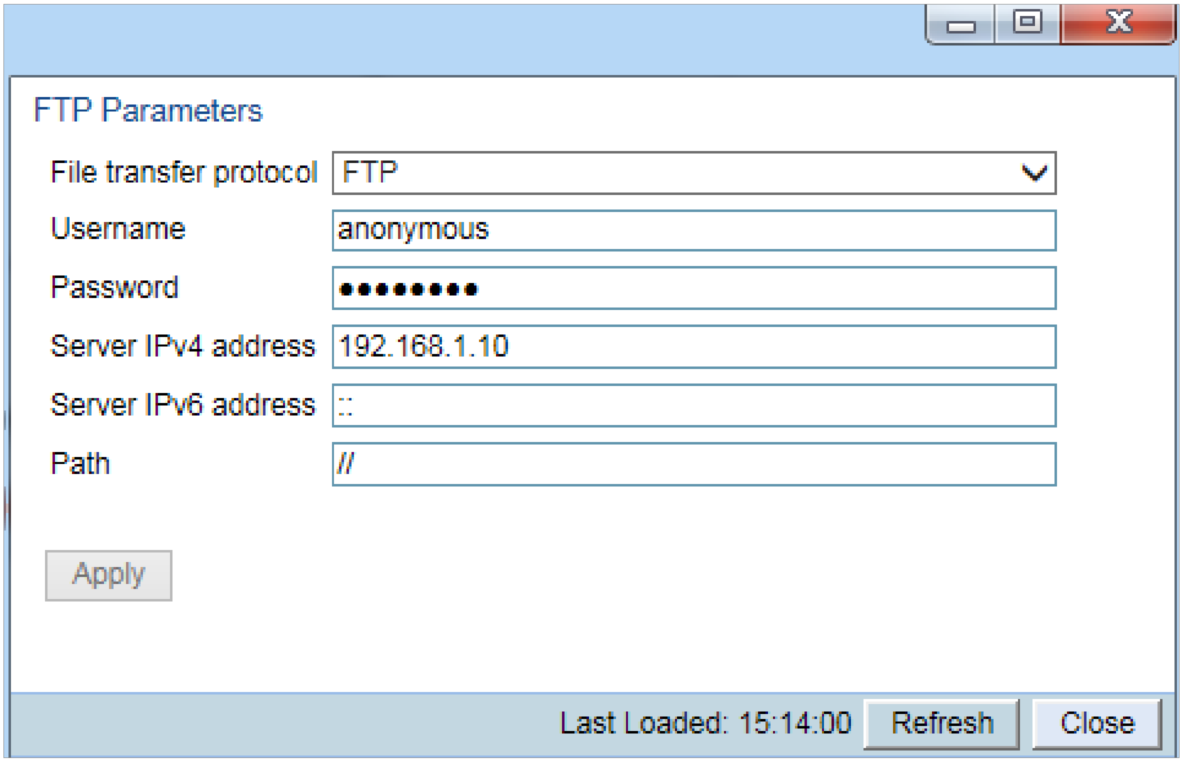
Software Install

Installation status: Ready

Installation progress: 0%

6. Click **FTP Parameters** to display the FTP Parameters page.

Figure 121 *FTP Parameters Page*



FTP Parameters

File transfer protocol: FTP

Username: anonymous

Password: ●●●●●●●●●

Server IPv4 address: 192.168.1.10

Server IPv6 address: ::

Path: //

Last Loaded: 15:14:00

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, then **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. See 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.

Installing Software

Note

For instructions 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 (Download & Install Page – FTP).
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 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 18 *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	Displays the progress of the current software download.

Parameter	Definition
progress	
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.
Install progress	Displays the progress of the current software installation.

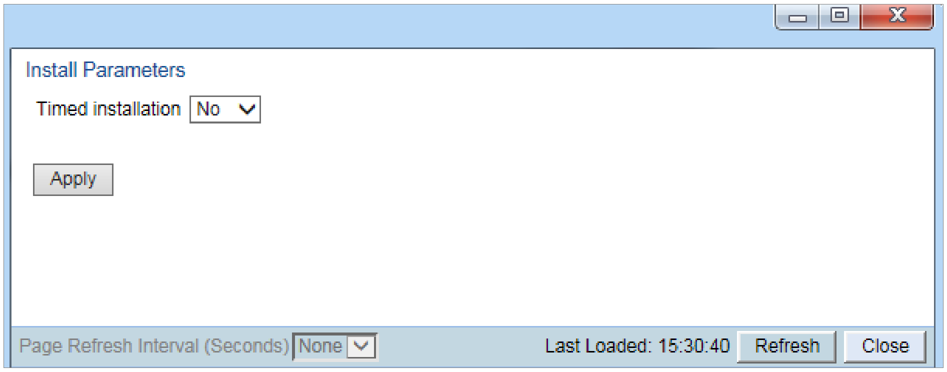
Configuring a Timed Installation

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 (Download & Install Page – FTP).
3. Click **Install Parameters**. The Install Parameters page opens.

   Figure 122 *Install Parameters Page*

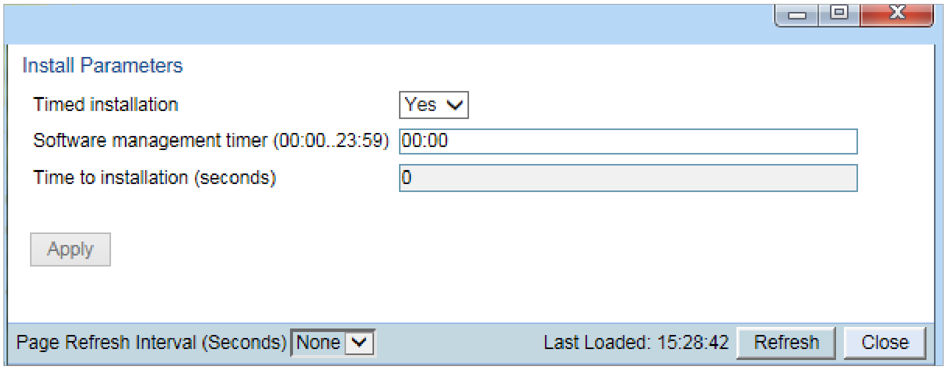


Install Parameters

Timed installation: No

4. Select **Yes** in the **Timed installation** field.
5. Click **Apply**. The **Software management timer field** appears.

Figure 123 *Install Parameters Page*



Install Parameters

Timed installation: Yes

Software management timer (00:00..23:59): 00:00

Time to installation (seconds): 0

6. In the **Software management timer** field, enter the amount of time, in hours and minutes, you want to defer the installation. For example, in Install Parameters Page, 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. In the Download & Install page (Download & Install Page – FTP), click **Install**.

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 850EX to PTP 850EX.

Importing and exporting configuration files can be done using HTTP, HTTPS, FTP, or SFTP.

This section includes:

- Configuration Management Overview
- Viewing Current Backup Files
- Setting the FTP/SFTP Configuration Management Parameters
- Exporting a Configuration File
- Importing a Configuration File
- Deleting a Configuration File
- Backing Up the Current Configuration
- Restoring a Saved Configuration
- Editing CLI Scripts

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.

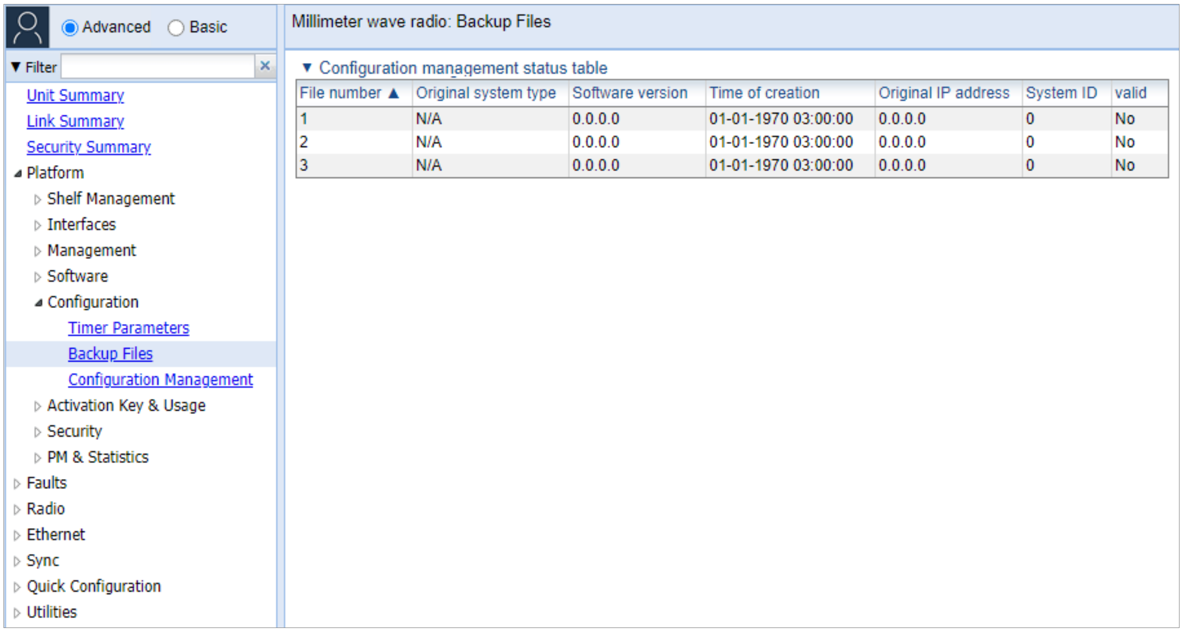
Viewing Current Backup Files

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 Backup Files Page Columns.

Figure 124 *Backup Files Page*



Millimeter wave radio: Backup Files

▼ Configuration management status table

File number ▲	Original system type	Software version	Time of creation	Original IP address	System ID	valid
1	N/A	0.0.0.0	01-01-1970 03:00:00	0.0.0.0	0	No
2	N/A	0.0.0.0	01-01-1970 03:00:00	0.0.0.0	0	No
3	N/A	0.0.0.0	01-01-1970 03:00:00	0.0.0.0	0	No

Table 19 *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.

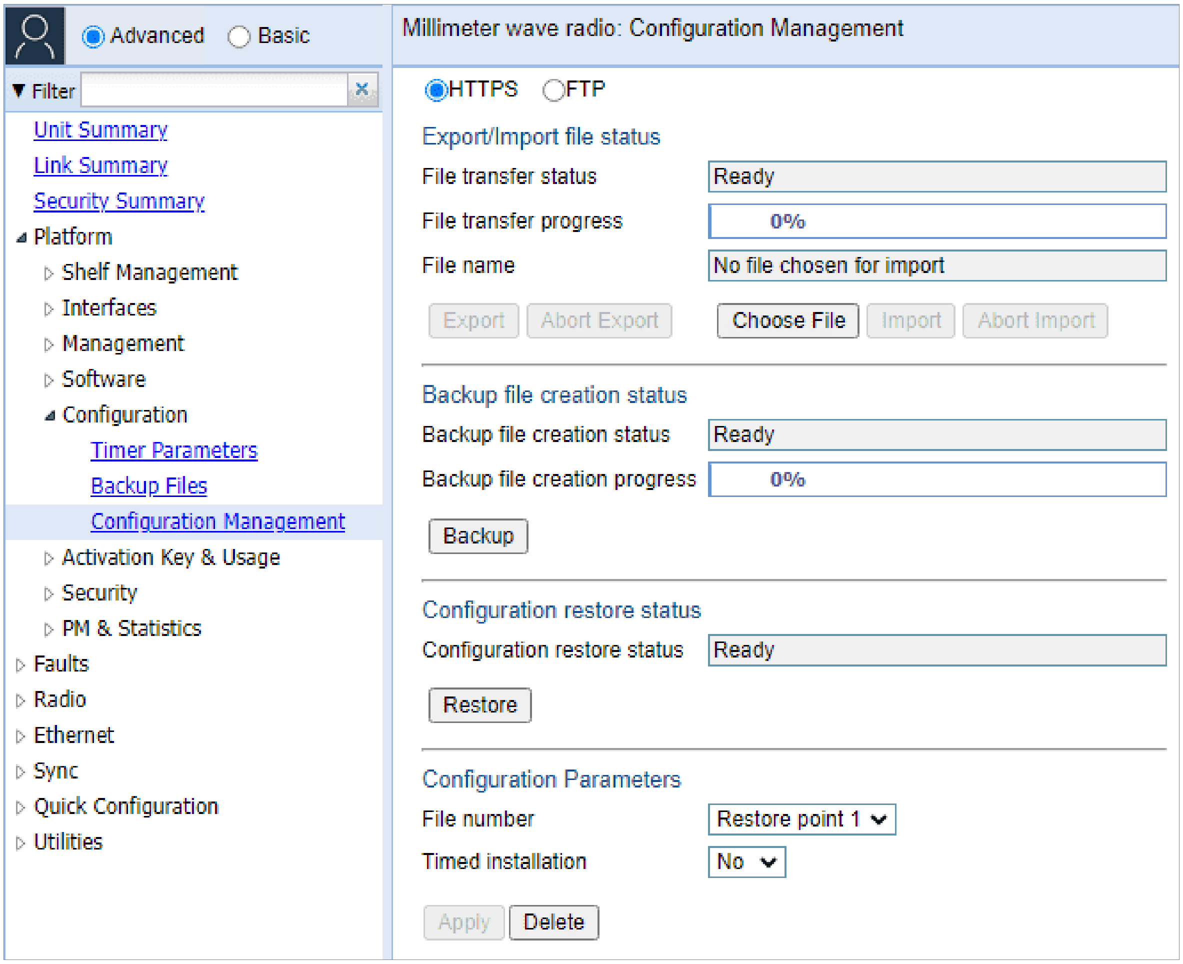
Setting the FTP/SFTP Configuration Management Parameters

When importing and exporting configuration files 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 import or export. For details, see Installing and Configuring an FTP or SFTP Server.

Before importing or exporting a configuration file via FTP or SFTP, you must perform the following steps:

1. Verify that the system date and time are correct. See Setting the Time and Date (Optional).
2. Install and configure an FTP server on the PC or laptop you are using to perform the import or export. See Installing and Configuring an FTP or SFTP Server.
3. In the PTP 850 Web EMS, select **Platform** > **Configuration** > **Configuration Management**. The Configuration Management page opens.
4. In the Configuration Management page, select **FTP**.

Figure 125 *Configuration Management Page – FTP/SFTP*



● Advanced ○ Basic

Millimeter wave radio: Configuration Management

● HTTPS ○ FTP

Export/Import file status

File transfer status	Ready
File transfer progress	0%
File name	No file chosen for import

Backup file creation status

Backup file creation status	Ready
Backup file creation progress	0%

Configuration restore status

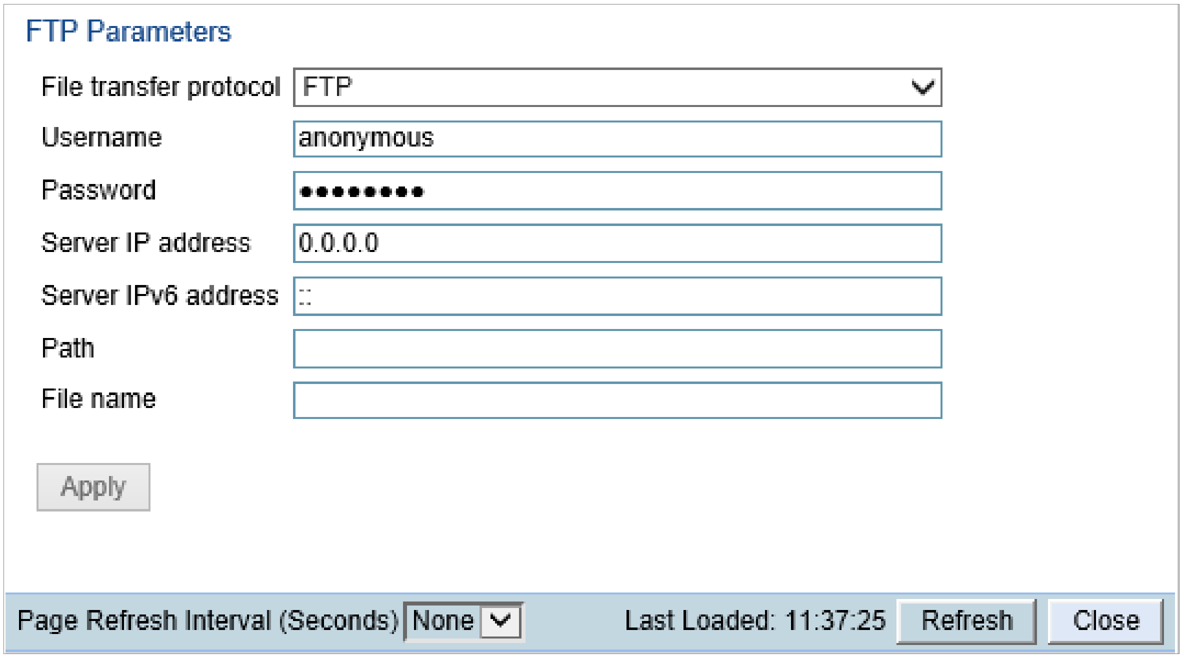
Configuration restore status	Ready

Configuration Parameters

File number	Restore point 1
Timed installation	No

5. Click **FTP Parameters** to display the FTP Parameters page.

Figure 126 *FTP Parameters Page (Configuration Management)*



FTP Parameters

File transfer protocol	FTP
Username	anonymous
Password	●●●●●●●●●
Server IP address	0.0.0.0
Server IPv6 address	::
Path	
File name	

6. In the **File transfer protocol** field, select FTP or SFTP.
7. In the **Username** field, enter the user name you configured in the FTP server.
8. 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.
9. 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.
10. 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.
11. In the **Path** field, enter the location of the file you are importing, or the location to which you want to export the file. 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 "//".
12. 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.

13. Click **Apply**, then **Close**, to save the FTP parameters and return to the Configuration Management page.

Exporting a Configuration File

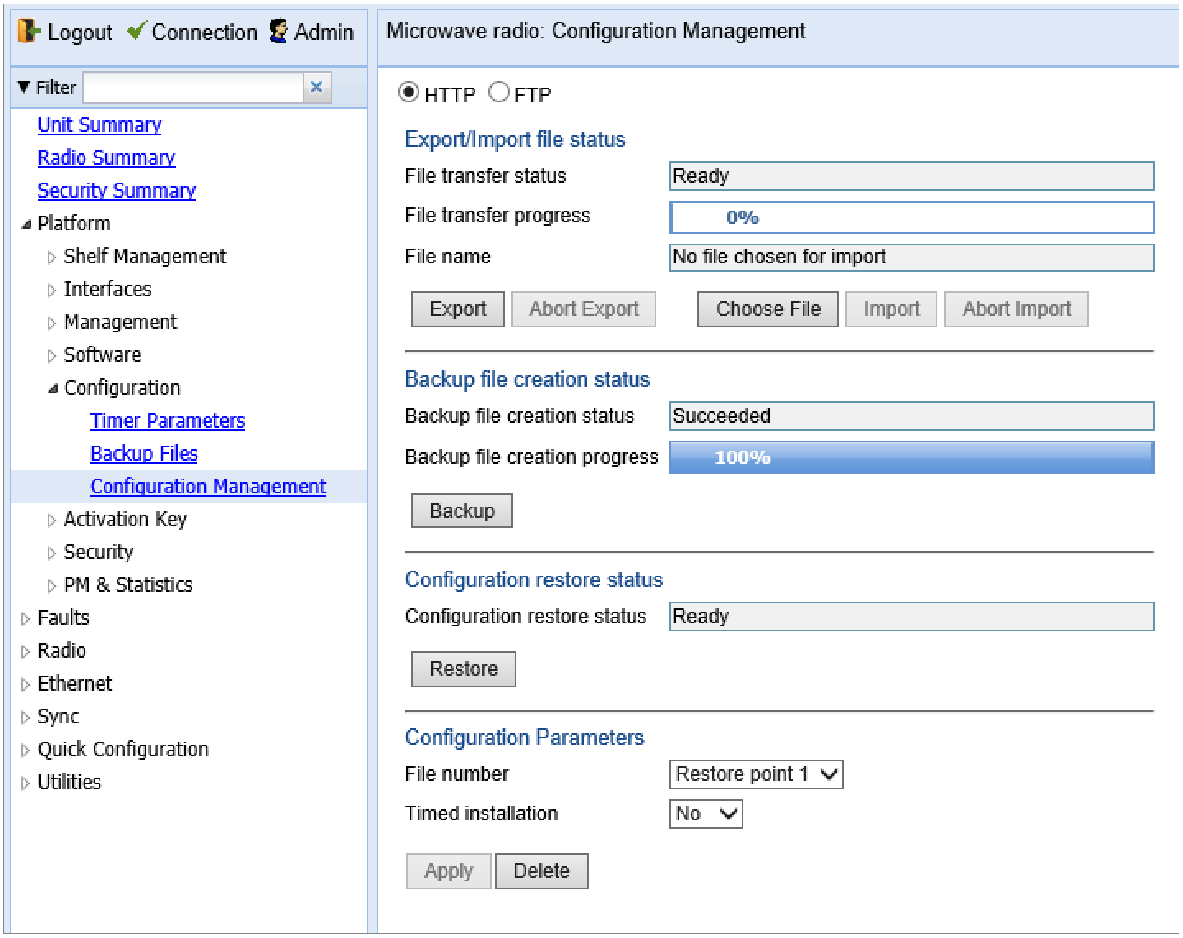
You can export a saved configuration file from one of the system's three restore points to a PC or laptop. You can use FTP, SFTP, HTTP, or HTTPS to export a configuration file.

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 127 *Configuration Management Page – HTTP/HTTPS*



● HTTP ○ FTP

File transfer status: Ready

File transfer progress: 0%

File name: No file chosen for import

Backup file creation status: Succeeded

Backup file creation progress: 100%

Configuration restore status: Ready

File number: Restore point 1

Timed installation: No

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 (Configuration Management Page – FTP/SFTP).
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**.

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.

Importing 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 (Configuration Management Page – HTTP/HTTPS).
2. Select **HTTP**.
3. Select **Choose File** and from your directory, select the file you want to import.
4. 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.
5. Click **Apply** to save your settings.
6. 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:

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 (Configuration Management Page – FTP/SFTP).
3. Select FTP.
4. 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.
5. Click Apply to save your settings.
6. 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**

When the import or export is complete, one of the following status indications appears: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.

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 (Configuration Management Page – FTP/SFTP).
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.

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 (Configuration Management Page – FTP/SFTP).
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.

   - Succeeded
   - Failure

The next time the system is reset, the **Backup file creation status** field returns to **Ready**.

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. Restoring a saved configuration does not change the unit's FIPS mode.

To restore a configuration file:

1. Select **Platform** > **Configuration** > **Configuration Management**. The Configuration Management page opens (Configuration Management Page – FTP/SFTP).
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.

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. See Backing Up the Current Configuration.
2. Export the configuration from the restore point to a PC or laptop. See Exporting a Configuration File.
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 a Configuration File.
7. Restore the imported configuration file. See Restoring a Saved Configuration. 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 command is executed. During initialization following the reset, execution of the CLI script continues from the following command.

Setting the Unit to the Factory Default Configuration

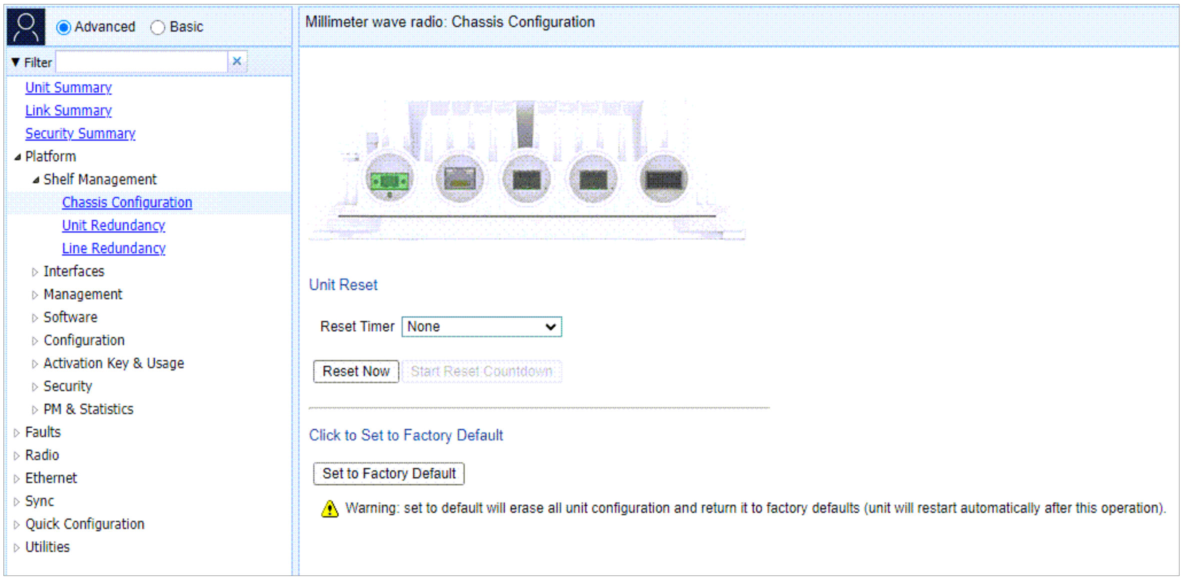
You can restore the unit to its factory default configuration, while retaining the unit's IP address settings and logs.

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 128 *Chassis Configuration Page*



Millimeter wave radio: Chassis Configuration

Unit Reset

Reset Timer: None

Click to Set to Factory Default

⚠ Warning: set to default will erase all unit configuration and return it to factory defaults (unit will restart automatically after this operation).

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.

Performing a Unit Reset

To initiate an immediate reset of the unit:

1. Select **Platform** > **Shelf Management** > **Chassis Configuration**. The Chassis Configuration page opens (Chassis Configuration Page).
2. Click **Reset Now**.
3. A prompt appears asking if you want to proceed with the reset. Click **Yes** to initiate the reset.

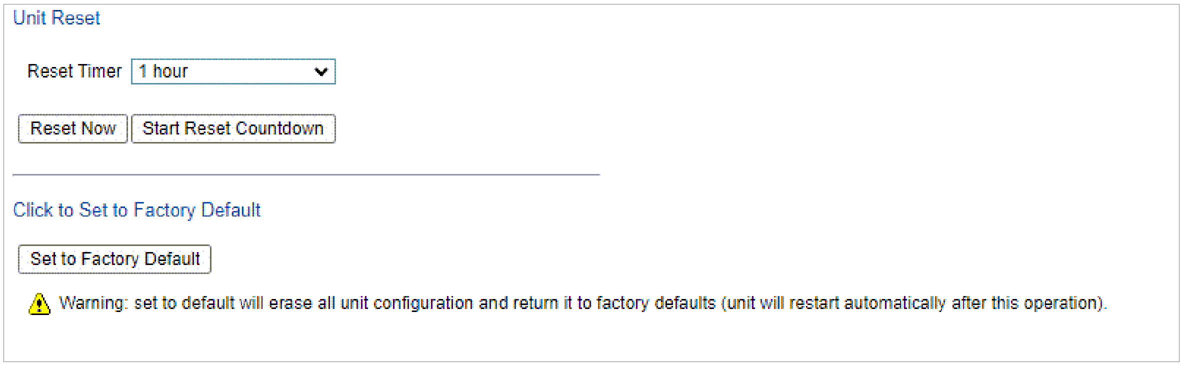
The unit is reset.

To configure a timed reset of the unit:

1. Select **Platform** > **Shelf Management** > **Chassis Configuration**. The Chassis Configuration page opens (Chassis Configuration Page).
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.



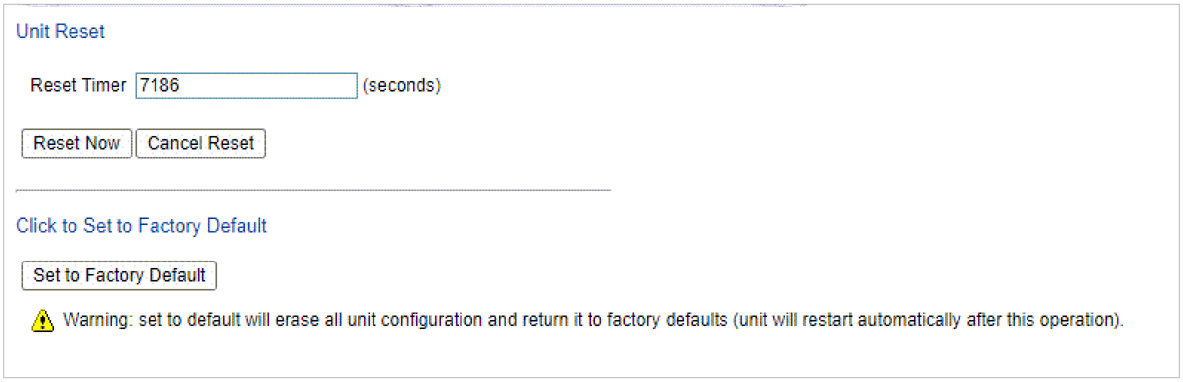
Unit Reset

Reset Timer: 1 hour

Click to Set to Factory Default

⚠ Warning: set to default will erase all unit configuration and return it to factory defaults (unit will restart automatically after this operation).

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**.



Unit Reset

Reset Timer: 7186 (seconds)

Click to Set to Factory Default

⚠ Warning: set to default will erase all unit configuration and return it to factory defaults (unit will restart automatically after this operation).

Note

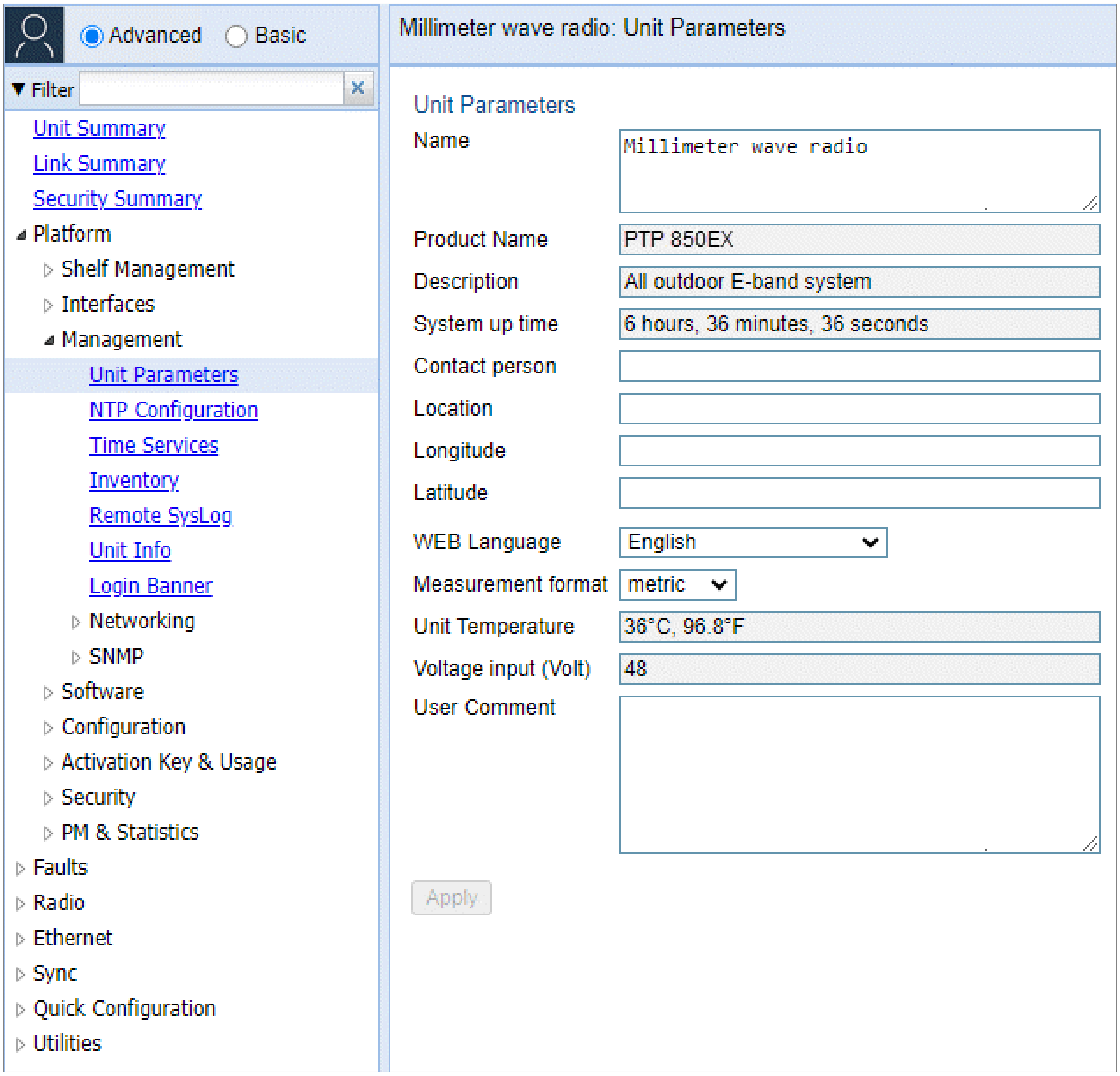
You can set a reset timer with granularity of one second and longer available timers via the CLI. See Performing a Unit Reset (CLI).

Configuring Unit Parameters

To view and configure system information:

1. Select **Platform** > **Management** > **Unit Parameters**. The Unit Parameters page opens. Unit Parameters describes the fields in the Unit Parameters page.

   Figure 129 *Unit Parameters Page*



Millimeter wave radio: Unit Parameters

Unit Parameters

Name	Millimeter wave radio
Product Name	PTP 850EX
Description	All outdoor E-band system
System up time	6 hours, 36 minutes, 36 seconds
Contact person	
Location	
Longitude	
Latitude	
WEB Language	English
Measurement format	metric
Unit Temperature	36°C, 96.8°F
Voltage input (Volt)	48
User Comment	

Table 20 *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.
Product Name	The product type.

Parameter	Definition
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.
Web Language	Enables you to select the language in which the Web EMS is displayed. 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. See Temperature Ranges.
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).

Configuring NTP

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.

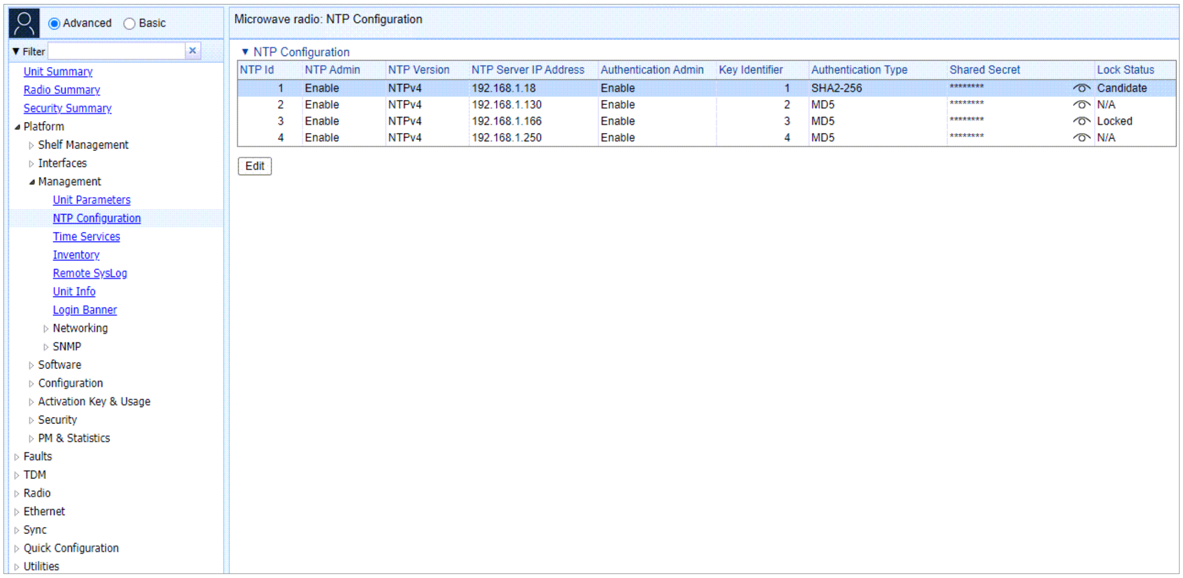
Optionally, for extra security you can enable NTP authentication, as defined in the NTP specification (IETF RFC 5905). NTP authentication enables the client to verify the authenticity of the NTP server before synchronizing its clock with the server’s time. This can help prevent man-in-the-middle attacks 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 view and configure the NTP Parameters:

1. Select **Platform** > **Management** > **NTP Configuration**. The NTP Configuration page opens.

Figure 130 *NTP Configuration Page*



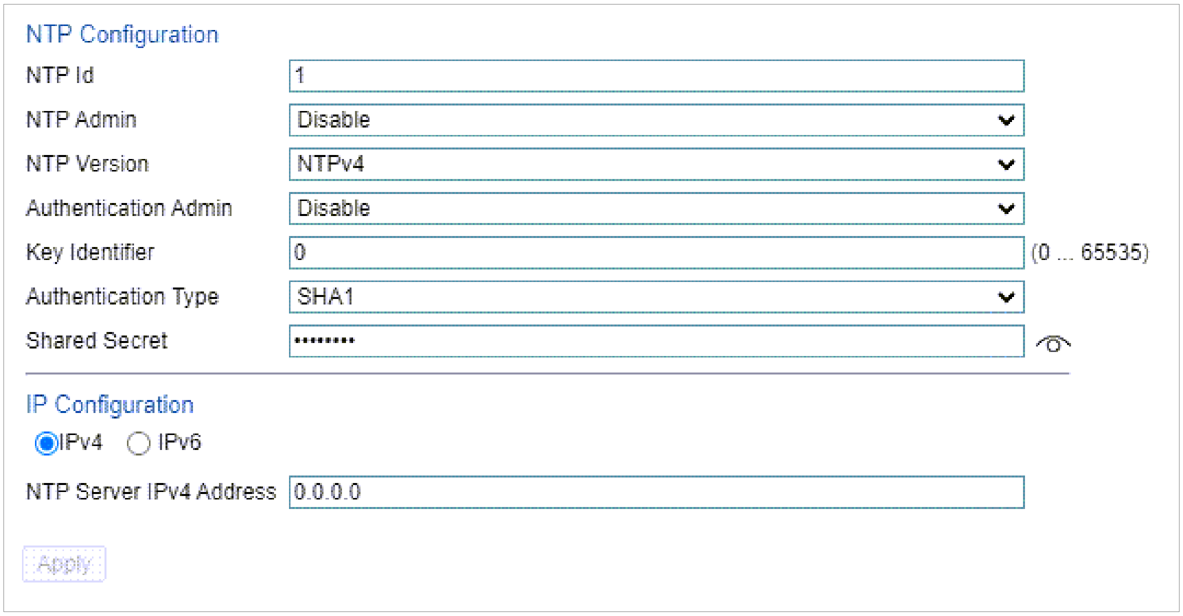
Microwave radio: NTP Configuration

▼ NTP Configuration

NTP Id	NTP Admin	NTP Version	NTP Server IP Address	Authentication Admin	Key Identifier	Authentication Type	Shared Secret	Lock Status
1	Enable	NTPv4	192.168.1.18	Enable	1	SHA2-256	********	Candidate
2	Enable	NTPv4	192.168.1.130	Enable	2	MD5	********	N/A
3	Enable	NTPv4	192.168.1.166	Enable	3	MD5	********	Locked
4	Enable	NTPv4	192.168.1.250	Enable	4	MD5	********	N/A

2. Select a row in the NTP Configuration table and click Edit. The NTP Configuration Edit page opens.

Figure 131 *NTP Configuration Edit Page (Disabled)*



NTP Configuration

NTP Id	1	
NTP Admin	Disable	
NTP Version	NTPv4	
Authentication Admin	Disable	
Key Identifier	0	(0 ... 65535)
Authentication Type	SHA1	
Shared Secret	********	

IP Configuration

● IPv4 ○ IPv6

NTP Server IPv4 Address: 0.0.0.0

3. In the **NTP Admin** field, select **Enable**.

4. 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.

5. In the **Authentication Admin** field, select **Enable** to enable NTP authentication or **Disable** to disable NTP authentication. By default, NTP authentication is disabled.

6. 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.

7. 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**.

8. 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

9. In the IP Configuration section, select IPv4 or IPv6.\

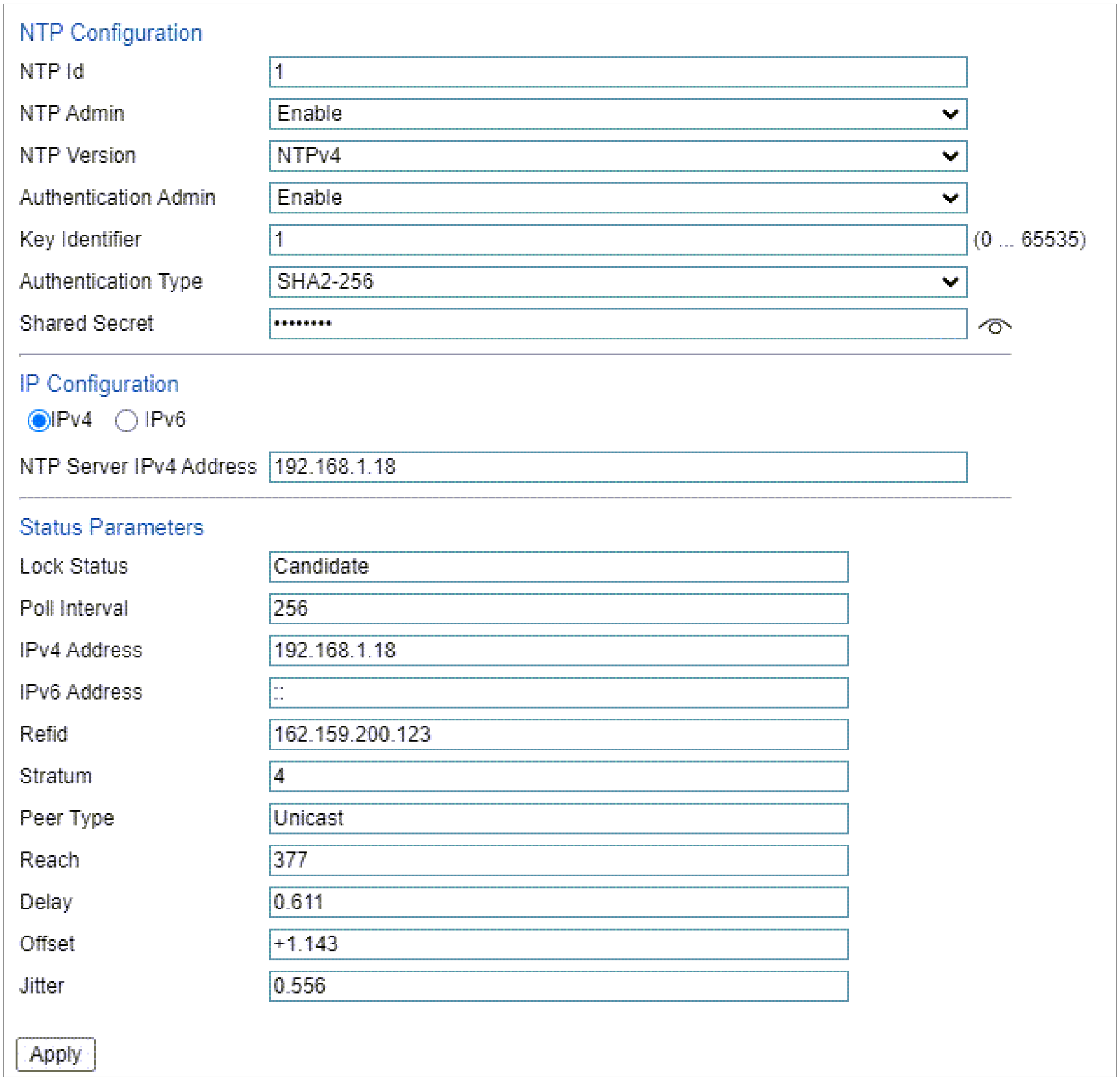
   Note

   For each NTP server, you can define an IPv4 address or an IPv6 address but not both.

10. In the **NTP server IPv4 address** or **NTP server IPv6 address** field, enter the IP address of the NTP server.

11. Click **Apply**. Once you click **Apply**, the NTP Status Parameters appear. NTP Status Parameters describes the NTP Status Parameters.

Figure 132 *NTP Configuration Edit Page (Enabled)*



NTP Configuration

NTP Id	1
NTP Admin	Enable
NTP Version	NTPv4
Authentication Admin	Enable
Key Identifier	1 (0 ... 65535)
Authentication Type	SHA2-256
Shared Secret	••••••••

IP Configuration

● IPv4 ○ IPv6

NTP Server IPv4 Address	192.168.1.18

Status Parameters

Lock Status	Candidate
Poll Interval	256
IPv4 Address	192.168.1.18
IPv6 Address	::
Refid	162.159.200.123
Stratum	4
Peer Type	Unicast
Reach	377
Delay	0.611
Offset	+1.143
Jitter	0.556

12. Repeat these steps for each NTP server you want to configure, up to four servers.

Table 21 *NTP Status Parameters*

Parameter	Definition
Lock status	Indicates the NTP status of the unit. Possible values are: • **LOCK** – The NTP client is locked on a remote server. • **LOCAL** – The NTP client is locked on the local system clock (free running clock). • **CANDIDATE** – The server is next in line to be selected if the currently locked server is discarded. • **N/A** – The NTP client is not locked on any clock or NTP is disabled.

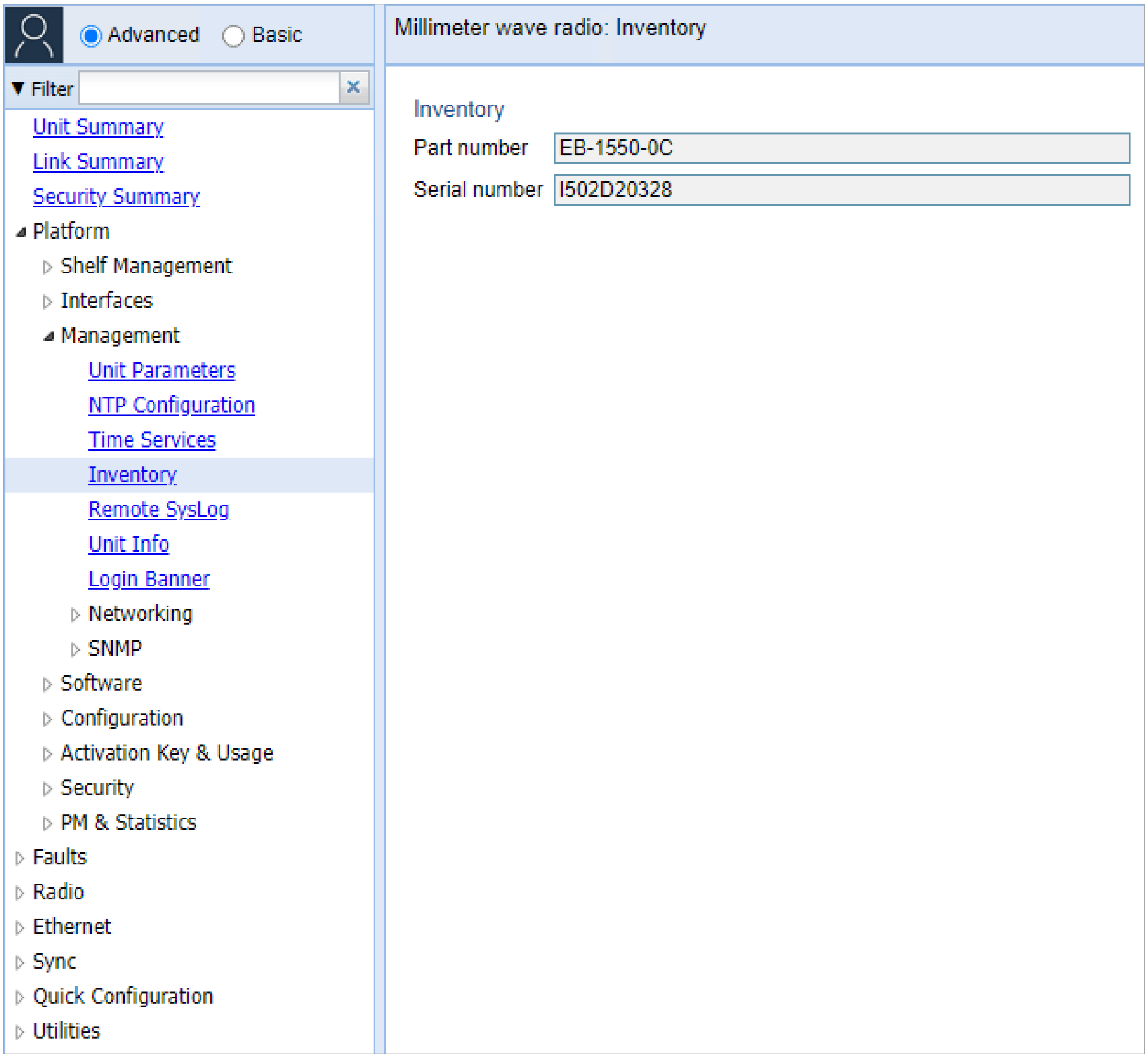
Parameter	Definition
Poll Interval	Seconds between polls.
IPv4 address	The IPv4 address of the NTP server (if configured).
IPv6 address	The IPv6 address of the NTP server (if configured).
Refid	The NTP client time server.
Stratum	The NTP client stratum.
Peer type	The server peer type.
Reach	The result 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.

Displaying Unit Inventory

To view the unit's part number and serial number:

1. Select **Platform** > **Management** > **Inventory**. The Inventory page opens, showing the unit's part number and serial number.

Figure 133 *Inventory Page*



Millimeter wave radio: Inventory

Inventory

Part number: EB-1550-0C

Serial number: I502D20328

Displaying SFP DDM and Inventory Information

Static and dynamic monitoring is available for all SFP, SFP+, and SFP28 modules used on PTP 850EX devices.

Dynamic monitoring (DDM) PMs are also available.

Note

DDM parameters are not relevant for electrical SFPs.

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.

These alarms are based on thresholds defined by the SFP module vendor, which are static. They also display the actual RX or TX values as of the time when the alarm was raised, which are dynamic. The dynamic values are not changed as long as the alarm is still raised. They are only updated if the alarm is cleared, then raised again.

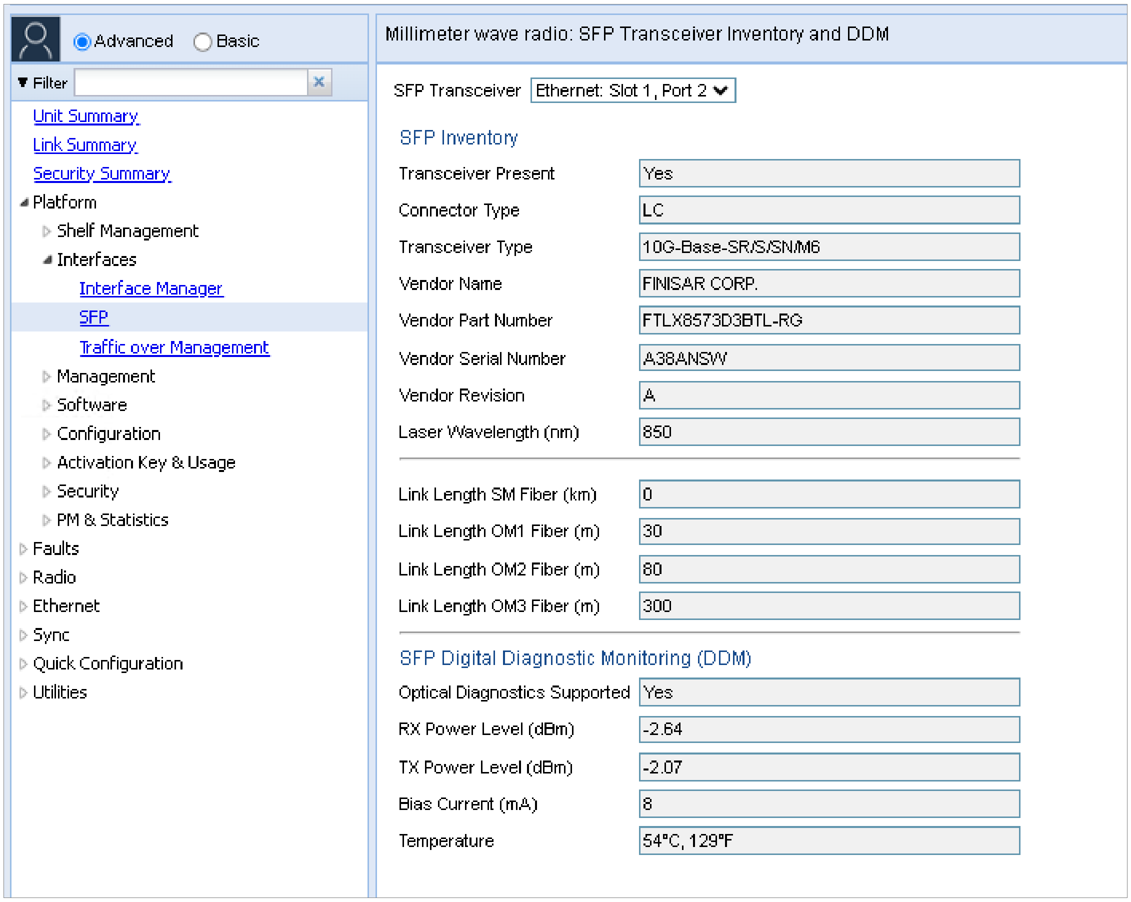
If there is no signal on the interface, a Loss of Carrier alarm (LOC) is raised, and this alarm masks the DDM alarms.

Displaying Information about an SFP Module

To display information about an SFP module:

1. Select **Platform** > **Interfaces** > SFP. The SFP Transceiver Inventory and DDM page opens.
    - The SFP Inventory section displays static information about the SFP module.
    - The SFP Digital Diagnostic Monitoring (DDM) section displays dynamic information about the current state of the SFP module.

Figure 134 *SFP Transceiver Inventory and DDM Page*



Millimeter wave radio: SFP Transceiver Inventory and DDM

SFP Transceiver: Ethernet: Slot 1, Port 2

SFP Inventory

Transceiver Present	Yes
Connector Type	LC
Transceiver Type	10G-Base-SR/S/SN/M6
Vendor Name	FINISAR CORP.
Vendor Part Number	FTLX8573D3BTL-RG
Vendor Serial Number	A38ANSW
Vendor Revision	A
Laser Wavelength (nm)	850
Link Length SM Fiber (km)	0
Link Length OM1 Fiber (m)	30
Link Length OM2 Fiber (m)	80
Link Length OM3 Fiber (m)	300

SFP Digital Diagnostic Monitoring (DDM)

Optical Diagnostics Supported	Yes
RX Power Level (dBm)	-2.64
TX Power Level (dBm)	-2.07
Bias Current (mA)	8
Temperature	54°C, 129°F

2. In the **SFP Transceiver** field, select the SFP interface about which you want to display information.

Table 22 *SFP Inventory Parameters*

Parameter	Description
Transceiver Present	Indicates whether an SFP module is attached to the interface.
Connector Type	Always displays LC.
Transceiver Type	Displays a description of the SFP module.
Vendor Name	Displays the name of the SFP's vendor.
Vendor Part Number	Displays the vendor's part number for the SFP module.
Vendor Serial Number	Displays the vendor's serial number for the SFP module.
Vendor Revision	Displays the revision number of the serial number provided by the vendor for the SFP module.
Laser Wavelength (nm)	Display's the SFP module's laser wavelength. For CSFP modules, 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 (m)	The maximum length of the cable (in meters) for OM3 multi-mode fiber cables.

Table 23 *SFP Digital Diagnostic Monitoring (DDM) Parameters*

Parameter	Description
Optical Diagnostics Supported	Displays whether the SFP module supports DDM monitoring. For modules that do not support DDM monitoring, the parameters below are not available.
RX Power Level (dBm)	The SFP module's current RX power signal strength (in dBm).
TX Power Level (dBm)	The SFP module's current TX power signal strength (in dBm).
Bias Current	The laser bias current of the SFP module (in mA)

Parameter	Description
(mA)	
Temperature	The current temperature of the SFP module (displayed in both C° and F°).

Note

Tx Power level DDM is not supported for QSFP (P5) – 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.

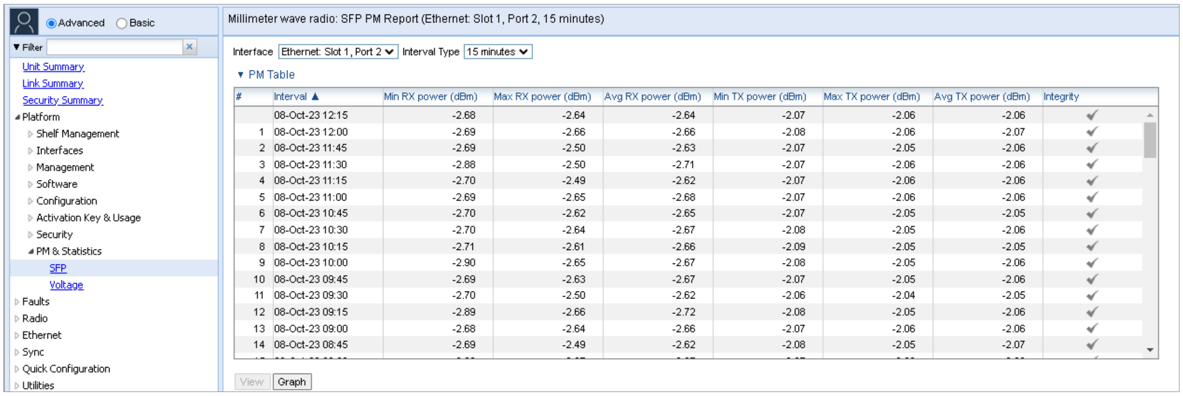
The Temperature is always shown as long as the SFP module is inserted in the port.

Displaying PMs about an SFP Module

To display DDM PMs:

1. Select **Platform** > **PM & Statistics** > **SFP**. The SFP PM Report page opens.

Figure 135 *SFP PM Report Page*



Millimeter wave radio: SFP PM Report (Ethernet: Slot 1, Port 2, 15 minutes)

Interface: Ethernet: Slot 1, Port 2 Interval Type: 15 minutes

#	Interval ▲	Min RX power (dBm)	Max RX power (dBm)	Avg RX power (dBm)	Min TX power (dBm)	Max TX power (dBm)	Avg TX power (dBm)	Integrity
	08-Oct-23 12:15	-2.68	-2.64	-2.64	-2.07	-2.06	-2.06	✓
1	08-Oct-23 12:00	-2.69	-2.66	-2.66	-2.08	-2.06	-2.07	✓
2	08-Oct-23 11:45	-2.69	-2.50	-2.63	-2.07	-2.05	-2.06	✓
3	08-Oct-23 11:30	-2.88	-2.50	-2.71	-2.07	-2.06	-2.06	✓
4	08-Oct-23 11:15	-2.70	-2.49	-2.62	-2.07	-2.06	-2.06	✓
5	08-Oct-23 11:00	-2.69	-2.65	-2.68	-2.07	-2.06	-2.06	✓
6	08-Oct-23 10:45	-2.70	-2.62	-2.65	-2.07	-2.05	-2.05	✓
7	08-Oct-23 10:30	-2.70	-2.64	-2.67	-2.08	-2.05	-2.06	✓
8	08-Oct-23 10:15	-2.71	-2.61	-2.66	-2.09	-2.05	-2.05	✓
9	08-Oct-23 10:00	-2.90	-2.65	-2.67	-2.08	-2.05	-2.06	✓
10	08-Oct-23 09:45	-2.69	-2.63	-2.67	-2.07	-2.05	-2.06	✓
11	08-Oct-23 09:30	-2.70	-2.50	-2.62	-2.06	-2.04	-2.05	✓
12	08-Oct-23 09:15	-2.89	-2.66	-2.72	-2.08	-2.05	-2.06	✓
13	08-Oct-23 09:00	-2.68	-2.64	-2.66	-2.07	-2.06	-2.06	✓
14	08-Oct-23 08:45	-2.69	-2.49	-2.62	-2.08	-2.05	-2.07	✓

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.

DDM PMs describes the DDM PMs.

Table 24 *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).
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.

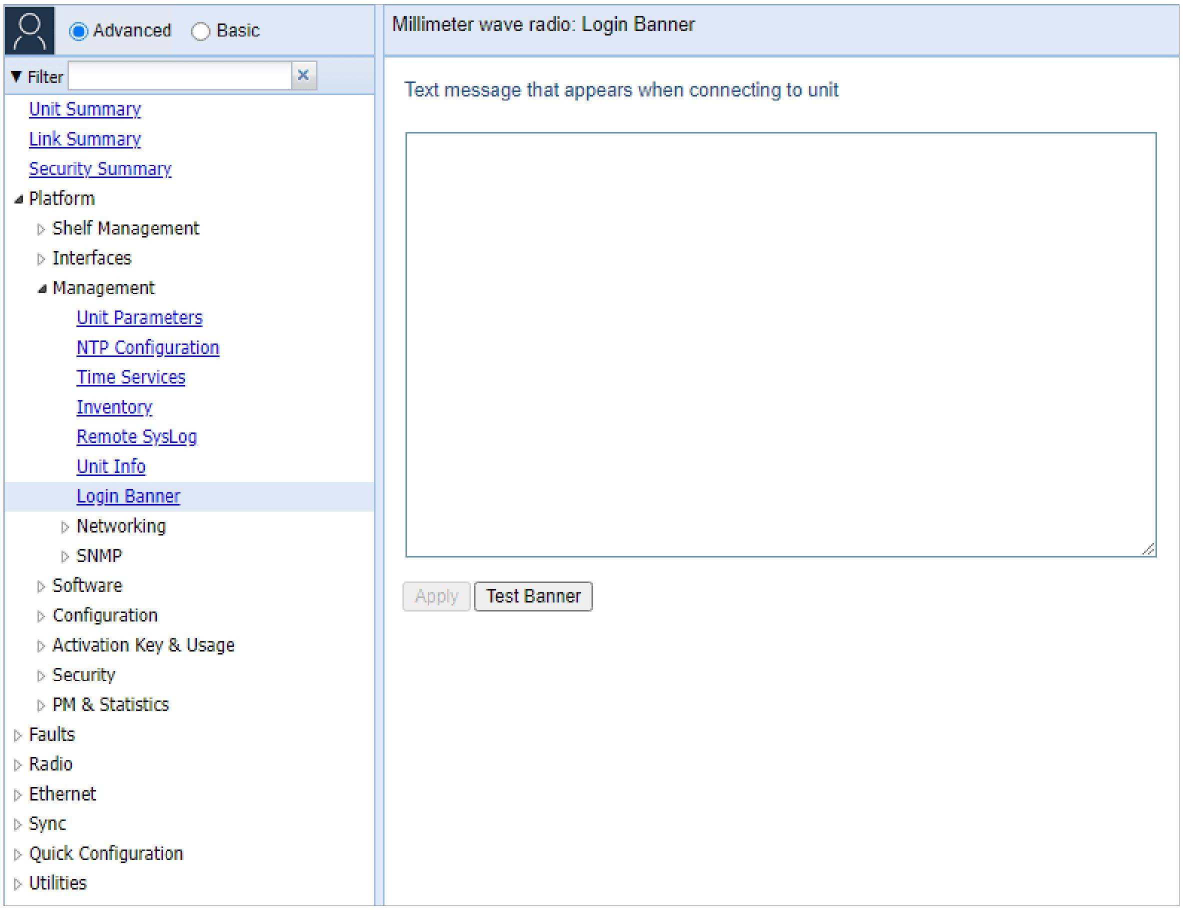
Defining a Login Banner

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 136 *Login Banner Page*



● Advanced ○ Basic

Millimeter wave radio: Login Banner

Text message that appears when connecting to unit

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**.

Radio Configuration

This section includes:

- Viewing the Radio Status and Settings
- Configuring the Remote Radio Parameters
- Configuring ATPC and ATPC Override Timer
- Configuring and Viewing Radio PMs and Statistics

Related topics:

- Configuring the Radio Parameters
- Configuring the Radio (MRMC) Script(s)
- Performing Radio Loopback

Viewing the Radio Status and Settings

You can configure the radios and display the radio parameters in the Radio Parameters page.

Note

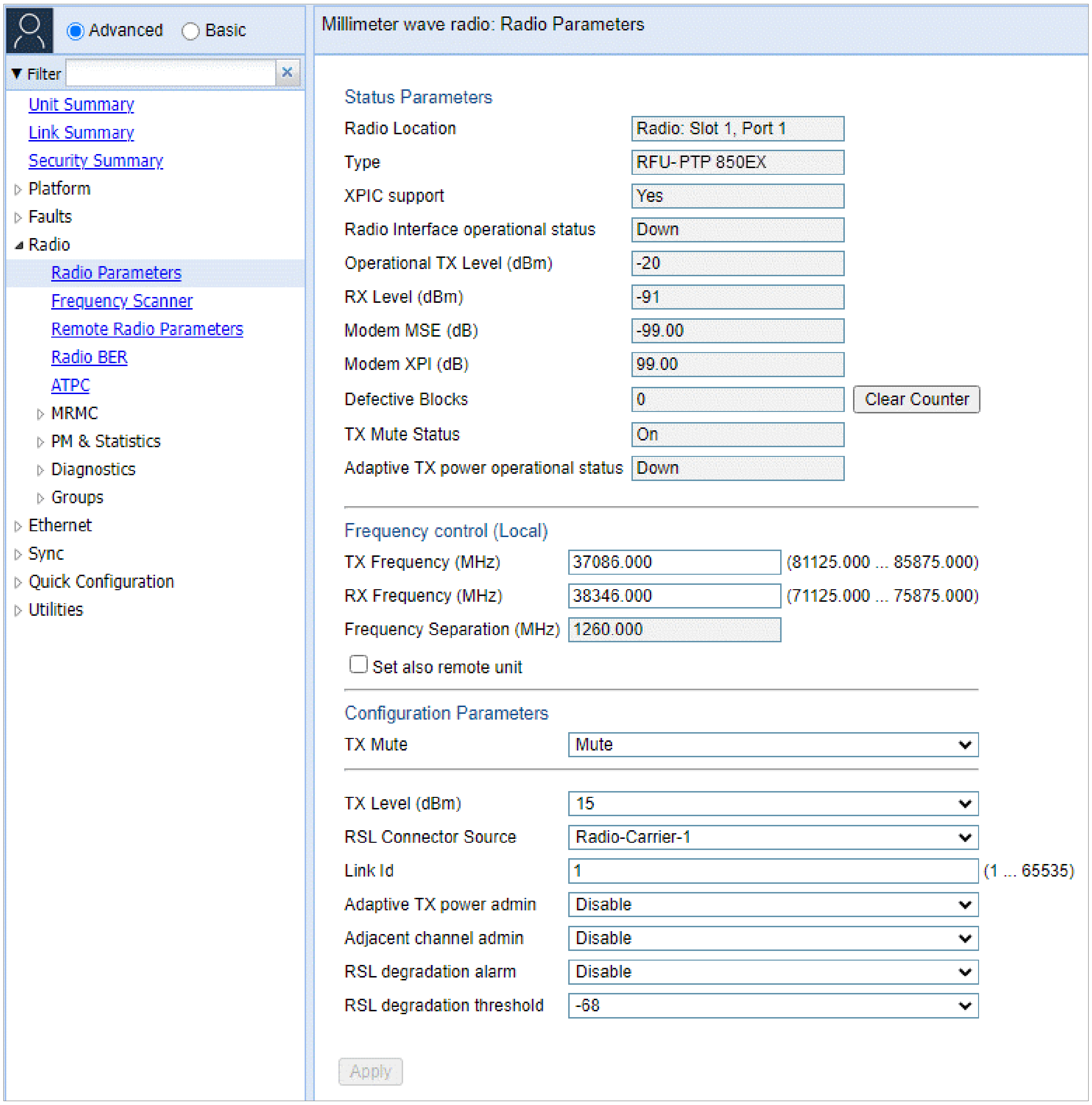
For instructions how to configure the radio parameters, see Configuring the Radio Parameters.

To display the radio parameters:

1. Select **Radio** > **Radio Parameters**:

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

Figure 137 *Radio Parameters Page*



Millimeter wave radio: Radio Parameters

Status Parameters

Radio Location	Radio: Slot 1, Port 1
Type	RFU-PTP 850EX
XPIC support	Yes
Radio Interface operational status	Down
Operational TX Level (dBm)	-20
RX Level (dBm)	-91
Modem MSE (dB)	-99.00
Modem XPI (dB)	99.00
Defective Blocks	0
TX Mute Status	On
Adaptive TX power operational status	Down

Frequency control (Local)

TX Frequency (MHz)	37086.000	(81125.000 ... 85875.000)
RX Frequency (MHz)	38346.000	(71125.000 ... 75875.000)
Frequency Separation (MHz)	1260.000	

□ Set also remote unit

Configuration Parameters

TX Mute	Mute	
TX Level (dBm)	15	
RSL Connector Source	Radio-Carrier-1	
Link Id	1	(1 ... 65535)
Adaptive TX power admin	Disable	
Adjacent channel admin	Disable	
RSL degradation alarm	Disable	
RSL degradation threshold	-68	

Radio Status Parameters lists and describes the parameters displayed in the **Status parameters** section of the Radio Parameters page. The configurable parameters are described in Configuring the Radio Parameters.

Table 25 *Radio Status Parameters*

Parameter	Description
Radio Location	The radio carrier.
Type	The RF module type.
XPIC Support	Indicates whether the carrier is operating in XPIC mode.

Parameter	Description
	Note: XPIC is planned for future release.
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.
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. See Configuring the Radio Parameters.
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. See Configuring the Radio Parameters.
Frequency Separation	The frequency separation, based on the configured TX and RX frequencies.

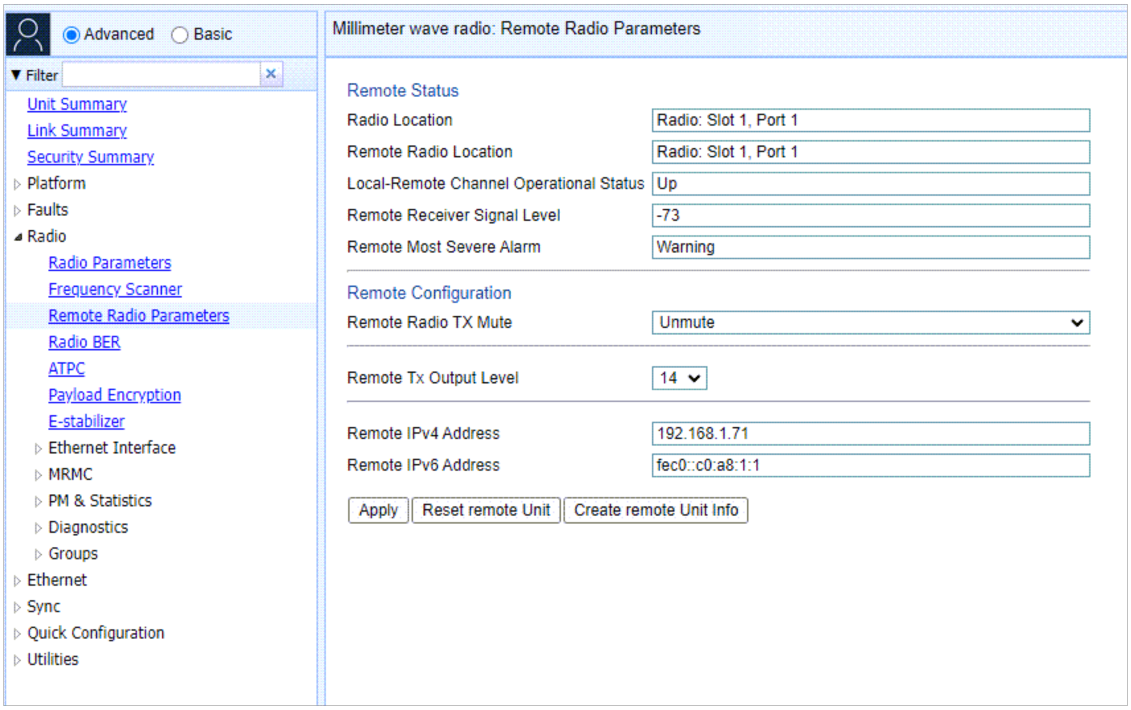
Configuring the Remote Radio Parameters

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**:
   - For PTP 850EX, the Remote Radio Parameters page opens right away.

   Figure 138 *Remote Radio Parameters Page*



Millimeter wave radio: Remote Radio Parameters

Remote Status

Radio Location	Radio: Slot 1, Port 1
Remote Radio Location	Radio: Slot 1, Port 1
Local-Remote Channel Operational Status	Up
Remote Receiver Signal Level	-73
Remote Most Severe Alarm	Warning

Remote Configuration

Remote Radio TX Mute	Unmute
Remote Tx Output Level	14
Remote IPv4 Address	192.168.1.71
Remote IPv6 Address	fec0::c0:a8:1:1

2. Configure the remote radio parameters. For a description of these parameters, see 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.Table 28: Remote Radio Parameters

   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. 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.Table 28: Remote Radio Parametersclick 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.Table 28: 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.

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.Table 28: 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 active (in a Unit Redundancy configuration) 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 Radio TX Mute	To mute the TX output of the remote radio, select **Mute**. To unmute the TX output of the remote radio, select **Unmute**. To mute with a timer, select **Mute With Timer**.
Remote mute timeout (minutes)	Only appears when the value displayed in the Remote Radio TX Mute field is **Mute With Timer**. Set the amount of time (in minutes) after which the remote radio will automatically be unmuted. The default value is 10 minutes. The value range is 1-1440 minutes (one day).
Remote mute time left (minutes)	Only appears when the value displayed in the Remote Radio TX Mute field is **Mute With Timer**. Read-only. The number of minutes left until the mute timer expires.
Remote Tx Output Level	Set the remote unit's Tx output level (in dBm).
Remote IP Address	The IPv4 IP address of the remote unit.
Remote IPv6 Address	The IPv6 IP address of the remote unit.

Configuring ATPC and ATPC Override Timer

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.

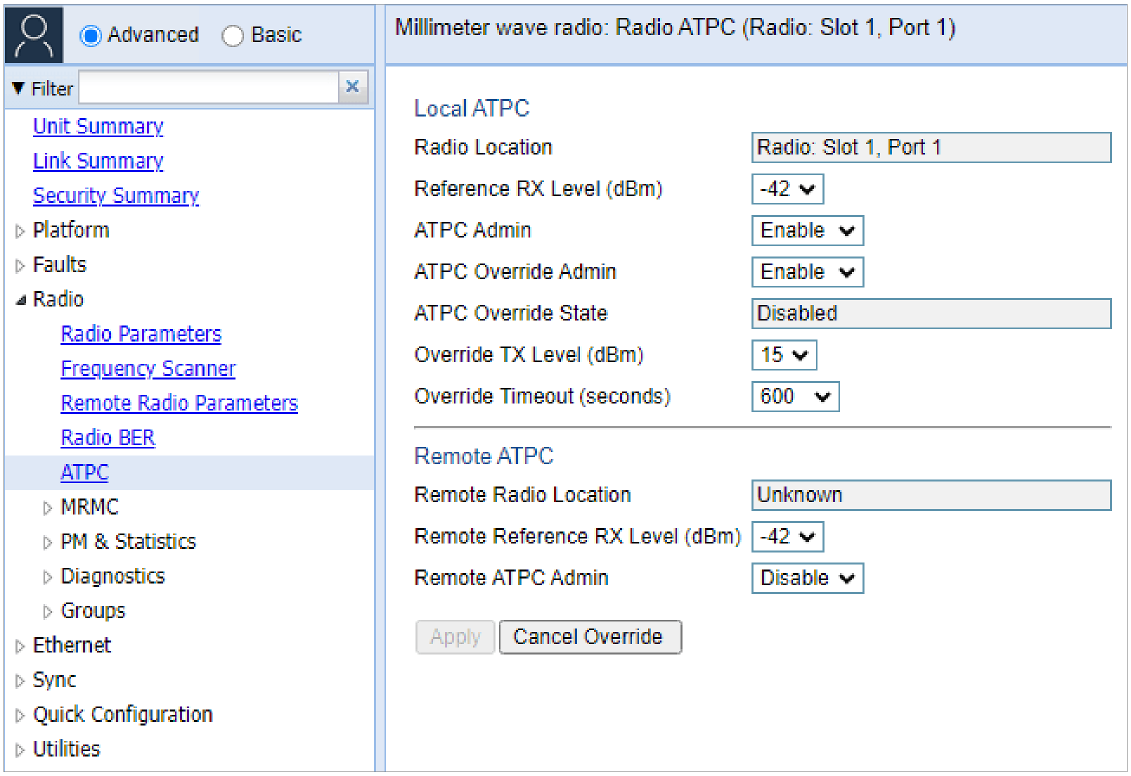
In a configuration with Unit Redundancy, the ATPC override state is propagated to the standby unit in the event of switchover.

> **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**:
   - For PTP 850EX, the ATPC page opens right away.

Figure 139 *ATPC Page*



Millimeter wave radio: Radio ATPC (Radio: Slot 1, Port 1)

Local ATPC

Radio Location	Radio: Slot 1, Port 1
Reference RX Level (dBm)	-42
ATPC Admin	Enable
ATPC Override Admin	Enable
ATPC Override State	Disabled
Override TX Level (dBm)	15
Override Timeout (seconds)	600

Remote ATPC

Remote Radio Location	Unknown
Remote Reference RX Level (dBm)	-42
Remote ATPC Admin	Disable

2. In the **ATPC Admin** field, select **Enable** to enable ATPC or **Disable** to disable ATPC.
3. Click **Apply**. If you selected **ATPC -Admin – Enable**, the **ATPC Override Admin** field is now displayed.
4. 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. It is recommended to set the ATPC Reference RX Level to a value that is 10 dB better than the RSL threshold for the maximum ACM profile configured for the radio, in order to account for normal fluctuations in the link quality.

5. 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.

6. Click **Apply**. If you selected **ATPC Override Admin – Enable**, the **ATPC Override State**, **Override TX Level**, and **ATPC Override Admin** fields are now displayed.
7. 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.
8. 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.
9. In the **Remote ATPC Admin** field, select **Enable** to enable ATPC or Disable to disable ATPC on the remote radio carrier.
10. Click **Apply**.
11. 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.
12. Click **Apply**.

To cancel an ATPC override state on the local unit, click **Cancel Override**.

Configuring and Viewing Radio PMs and Statistics

This section includes:

- Configuring BER Thresholds and Displaying Current BER
- Displaying MRMC Status
- Displaying MRMC PMs and Configuring ACM Profile Thresholds
- 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

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.

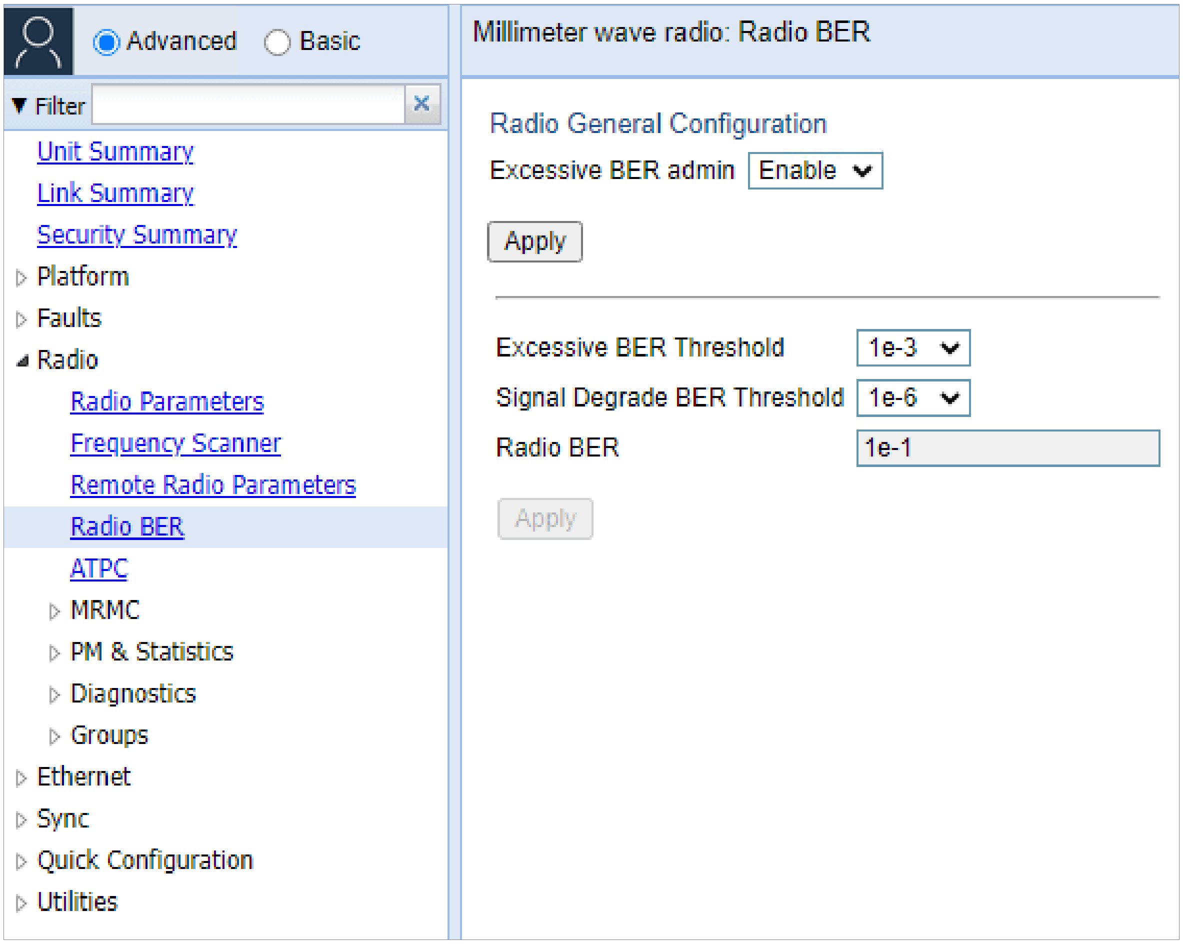
- Signal level PM thresholds, such as RX and TX level thresholds, are configured from the Signal Level PM Report page. See Displaying Signal Level PMs and Configuring Signal Level PM Thresholds.
- MSE PM thresholds are configured from the MSE PM Report page. See Displaying MSE PMs and Configuring MSE PM Thresholds.

You can also display the current BER level.

To configure the BER thresholds and Excessive BER Administration, and display current BER levels:

- For PTP 850EX, the Radio BER page opens right away.

Figure 140 *Radio BER Thresholds Page*



Millimeter wave radio: Radio BER

Radio General Configuration

Excessive BER admin: Enable

Apply

Excessive BER Threshold: 1e-3

Signal Degrade BER Threshold: 1e-6

Radio BER: 1e-1

Apply

The current BER level is displayed in the Radio BER field.

1. 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 unit 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.
2. In the **Excessive BER Threshold field**, select the level above which an excessive BER alarm is issued for errors detected over the radio link.
3. 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.
4. Click **Apply**, then **Close**.

Displaying MRMC Status

Related Topics:

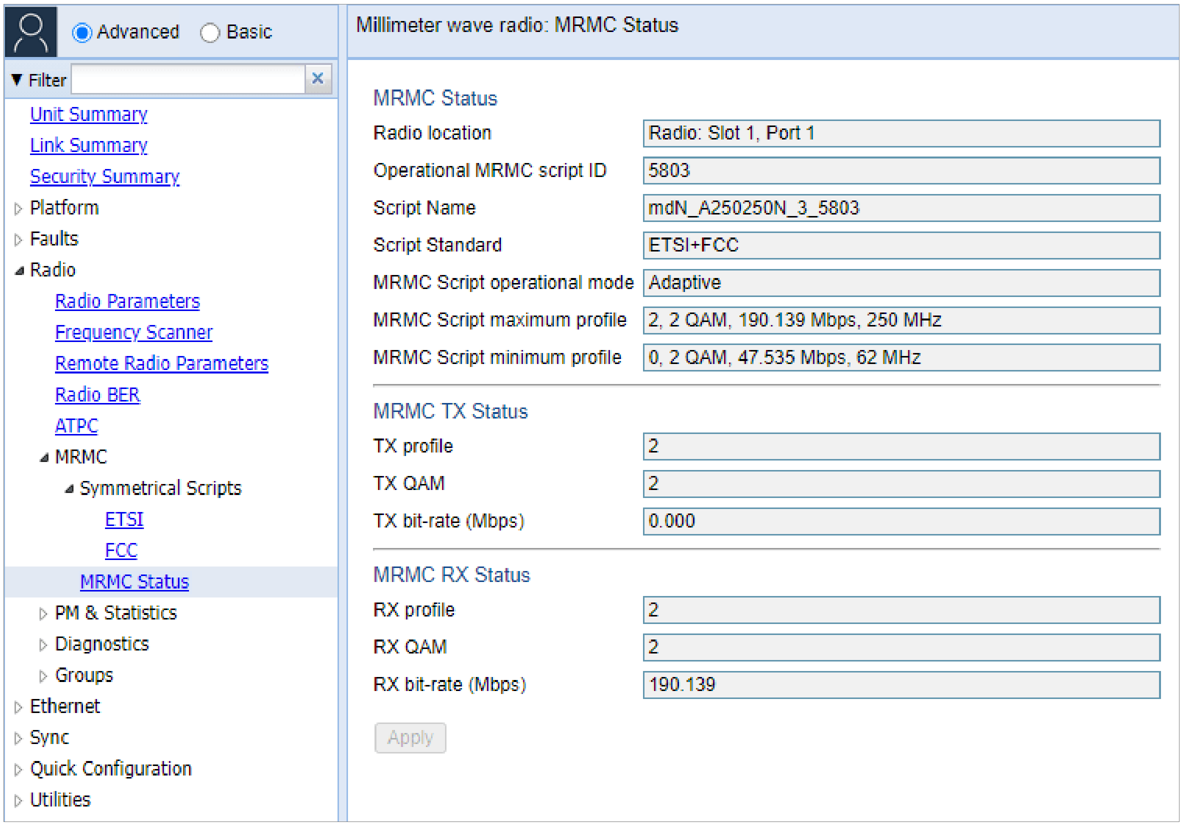
- Configuring the Radio (MRMC) Script(s)

To display the current modulation and bit rate per radio:

1. Select **Radio** > **MRMC** > **MRMC Status**:

- For PTP 850EX, the MRMC Status page opens right away.

Figure 141 *MRMC Status Page (PTP 850EX)*



Millimeter wave radio: MRMC Status

MRMC Status

Radio location	Radio: Slot 1, Port 1
Operational MRMC script ID	5803
Script Name	mdN_A250250N_3_5803
Script Standard	ETSI+FCC
MRMC Script operational mode	Adaptive
MRMC Script maximum profile	2, 2 QAM, 190.139 Mbps, 250 MHz
MRMC Script minimum profile	0, 2 QAM, 47.535 Mbps, 62 MHz

MRMC TX Status

TX profile	2
TX QAM	2
TX bit-rate (Mbps)	0.000

MRMC RX Status

RX profile	2
RX QAM	2
RX bit-rate (Mbps)	190.139

MRMC Status Parameters 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 26 *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 0.
TX profile	The current TX profile.
TX QAM	The current TX modulation.
TX bit-rate (Mbps)	The current TX bit-rate.
RX profile	The current RX profile.

Parameter	Definition
RX QAM	The current RX modulation.
RX bit-rate (Mbps)	The current RX bit-rate.

Displaying MRMC PMs and Configuring ACM Profile Thresholds

Related Topics:

- Configuring the Radio (MRMC) Script(s)

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 display the number of seconds each carrier operated at each ACM profile for these intervals.

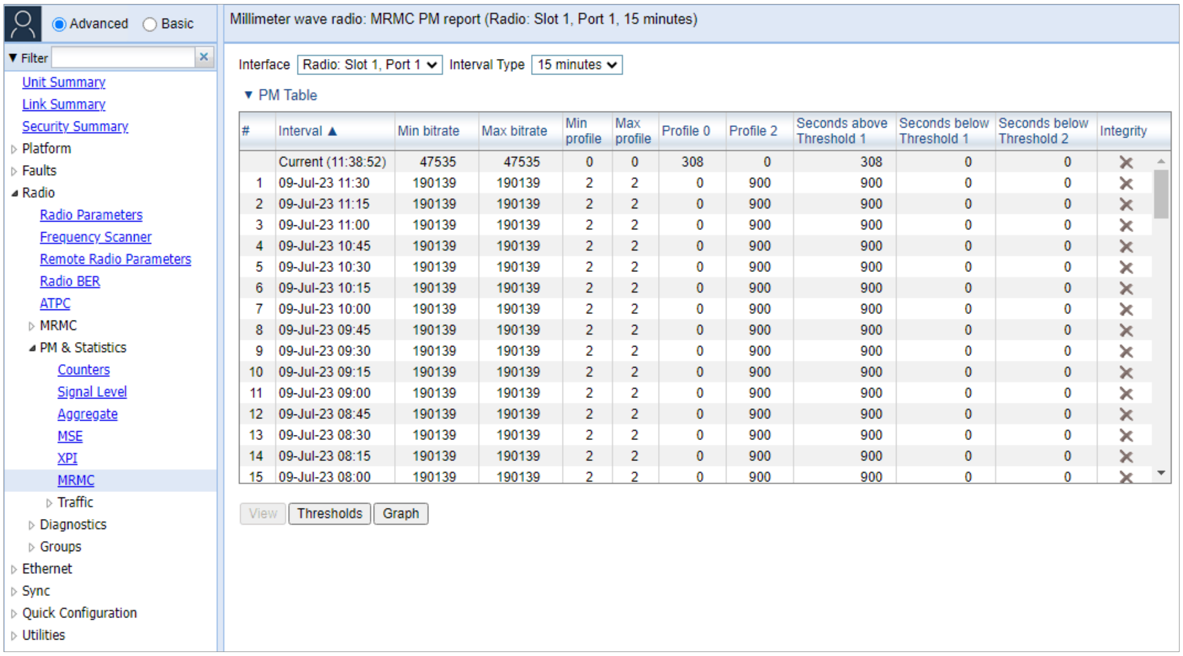
You can also define two ACM profile thresholds for each radio carrier, and display the number of seconds per interval that the radio's ACM profile was below each of these thresholds. These thresholds trigger the following alarms:

- **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 display Multi-Rate Multi-Constellation PMs, including information on ACM profile fluctuations per interval per radio:

1. Select **Radio** > **PM & Statistics** > **MRMC**. The MRMC PM Report page opens.

Figure 142 *MRMC PM Report Page*



Millimeter wave radio: MRMC PM report (Radio: Slot 1, Port 1, 15 minutes)

Interface: Radio: Slot 1, Port 1 Interval Type: 15 minutes

▼ PM Table

#	Interval ▲	Min bitrate	Max bitrate	Min profile	Max profile	Profile 0	Profile 2	Seconds above Threshold 1	Seconds below Threshold 1	Seconds below Threshold 2	Integrity
	Current (11:38:52)	47535	47535	0	0	308	0	308	0	0	✕
1	09-Jul-23 11:30	190139	190139	2	2	0	900	900	0	0	✕
2	09-Jul-23 11:15	190139	190139	2	2	0	900	900	0	0	✕
3	09-Jul-23 11:00	190139	190139	2	2	0	900	900	0	0	✕
4	09-Jul-23 10:45	190139	190139	2	2	0	900	900	0	0	✕
5	09-Jul-23 10:30	190139	190139	2	2	0	900	900	0	0	✕
6	09-Jul-23 10:15	190139	190139	2	2	0	900	900	0	0	✕
7	09-Jul-23 10:00	190139	190139	2	2	0	900	900	0	0	✕
8	09-Jul-23 09:45	190139	190139	2	2	0	900	900	0	0	✕
9	09-Jul-23 09:30	190139	190139	2	2	0	900	900	0	0	✕
10	09-Jul-23 09:15	190139	190139	2	2	0	900	900	0	0	✕
11	09-Jul-23 09:00	190139	190139	2	2	0	900	900	0	0	✕
12	09-Jul-23 08:45	190139	190139	2	2	0	900	900	0	0	✕
13	09-Jul-23 08:30	190139	190139	2	2	0	900	900	0	0	✕
14	09-Jul-23 08:15	190139	190139	2	2	0	900	900	0	0	✕
15	09-Jul-23 08:00	190139	190139	2	2	0	900	900	0	0	✕

2. In the Interval Type field:

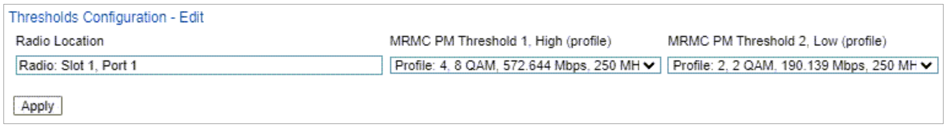
   - To display reports in 15-minute intervals, select 15 minutes.
   - To display reports in daily intervals, select 24 hours.

> **Note**
>
> To display the same parameters for a specific interval in a separate page, select the interval in the MRMC PM table and click View.

To set the ACM profile thresholds:

1. Click **Thresholds**. The MRMC Thresholds Configuration – Edit page opens.

Figure 143 *MRMC Thresholds Configuration – Edit Page (PTP 850EX)*



Thresholds Configuration - Edit

Radio Location	MRMC PM Threshold 1, High (profile)	MRMC PM Threshold 2, Low (profile)
Radio: Slot 1, Port 1	Profile: 4, 8 QAM, 572.644 Mbps, 250 MH	Profile: 2, 2 QAM, 190.139 Mbps, 250 MH

2. For each radio carrier, you can enter define two thresholds. In the MRMC PM Threshold 1 column, select the higher profile threshold. In the MRMC PM Threshold 2 column, select the lower profile threshold. The default value for each threshold is Profile 0.
3. Click **Apply**, then **Close**.

MRMC PMs describes the MRMC PMs.

Table 27 *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 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.
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.
Profile X	A column is displayed for each ACM profile at which the selected radio operated during the measured intervals. For each interval, this column displays the number of seconds during which the radio operated at that ACM profile during that interval.
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.
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 display the MRMC PM report for the selected radio in graph format, click **Graph**. The MRMC PM Report graphs page opens, offering three tabs:

- Min profile, Max profile
- Seconds above Thresholds, seconds below Thresholds
- Seconds per Profile

In each of the graphs, you can hide the display of a parameter in the graph by clicking it in the legend. An additional click un-hides the parameter.

Figure 144 *MRMC PM Report Graph – Min/Max Profile and Thresholds*

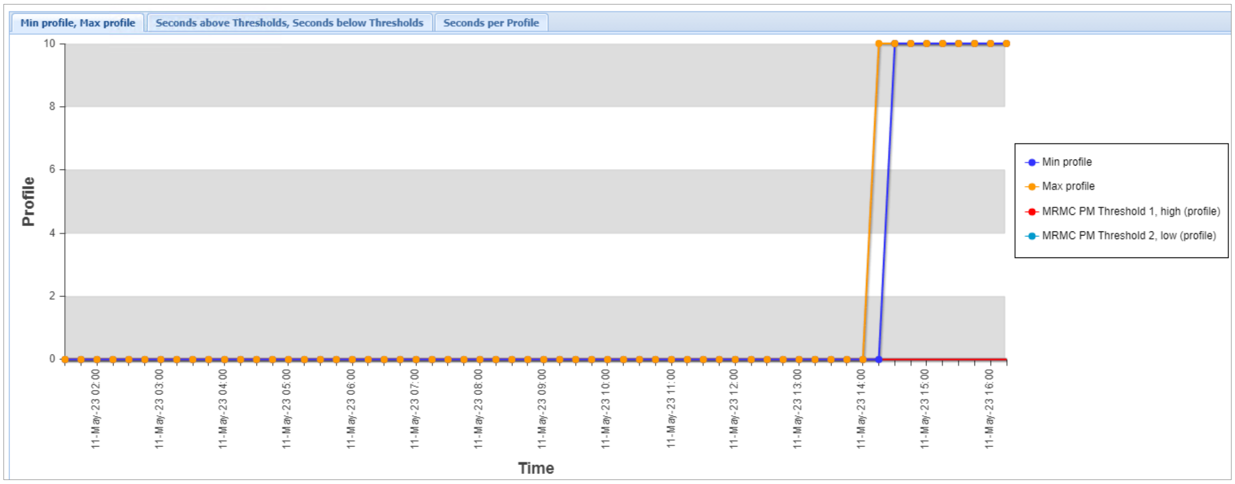


Figure 145 *MRMC PM Report Graph – Seconds Above/Below Thresholds*

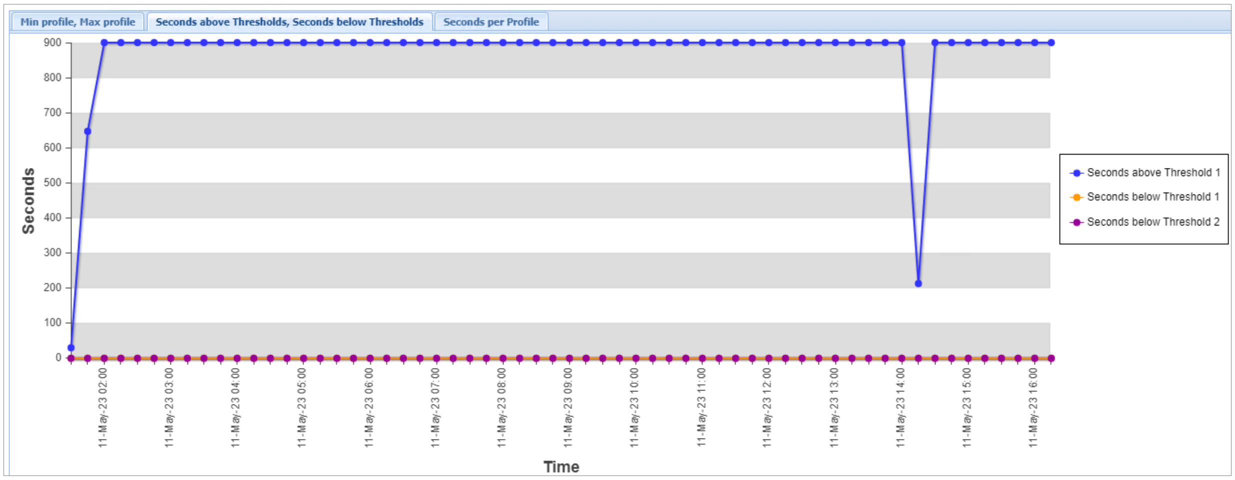
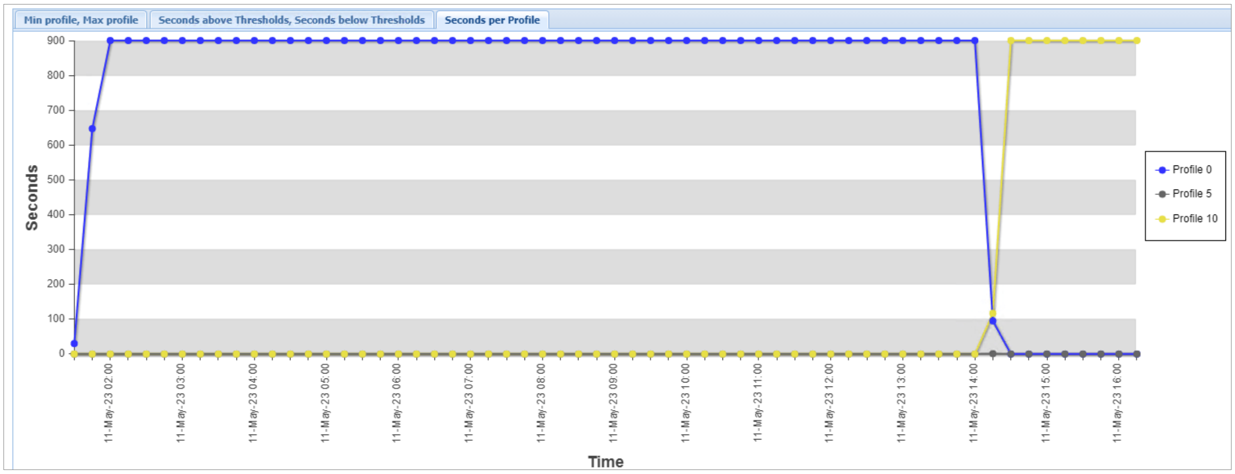


Figure 146 *MRMC PM Report Graph – Seconds Per Profile*



Displaying and Clearing Defective Block Counters

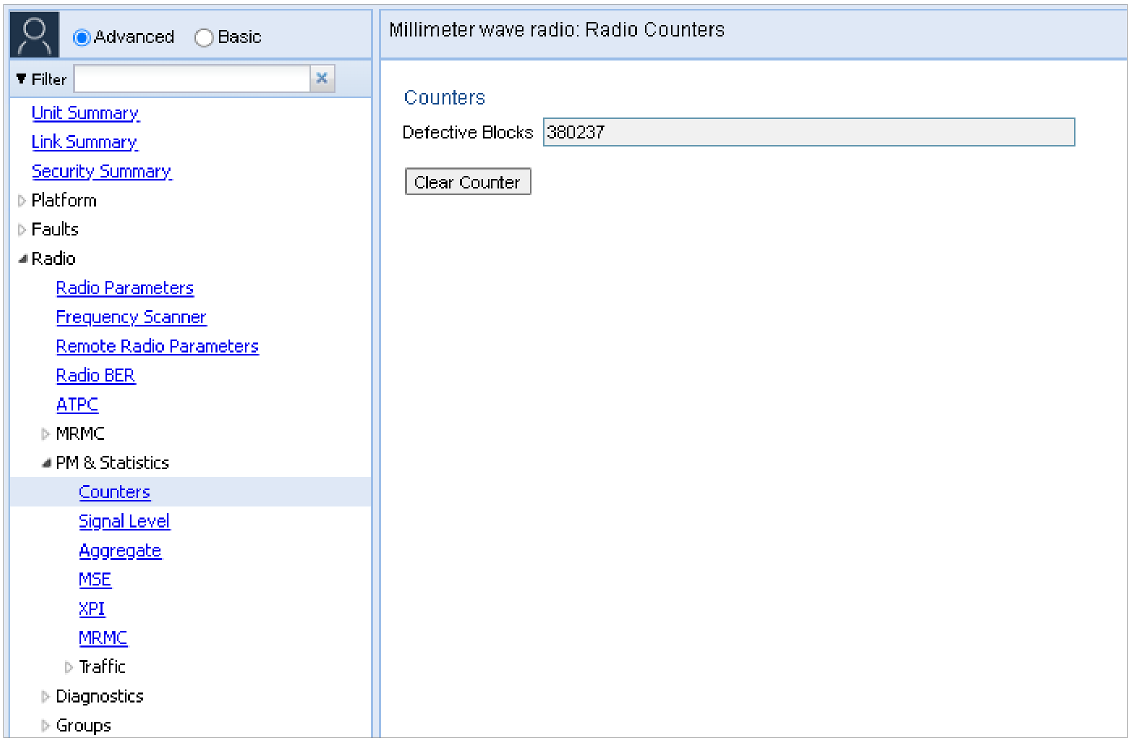
The Counters page displays the number of blocks in which errors were detected. The larger the amount, the poorer the radio link quality.

To display the number of blocks in which errors were detected per radio:

1. Select **Radio** > **PM & Statistics** > **Counters**:

    - For PTP 850EX, the Counters page opens right away.

    Figure 147 *Radio Counters Page (PTP 850EX)*



Millimeter wave radio: Radio Counters

Counters

Defective Blocks 380237

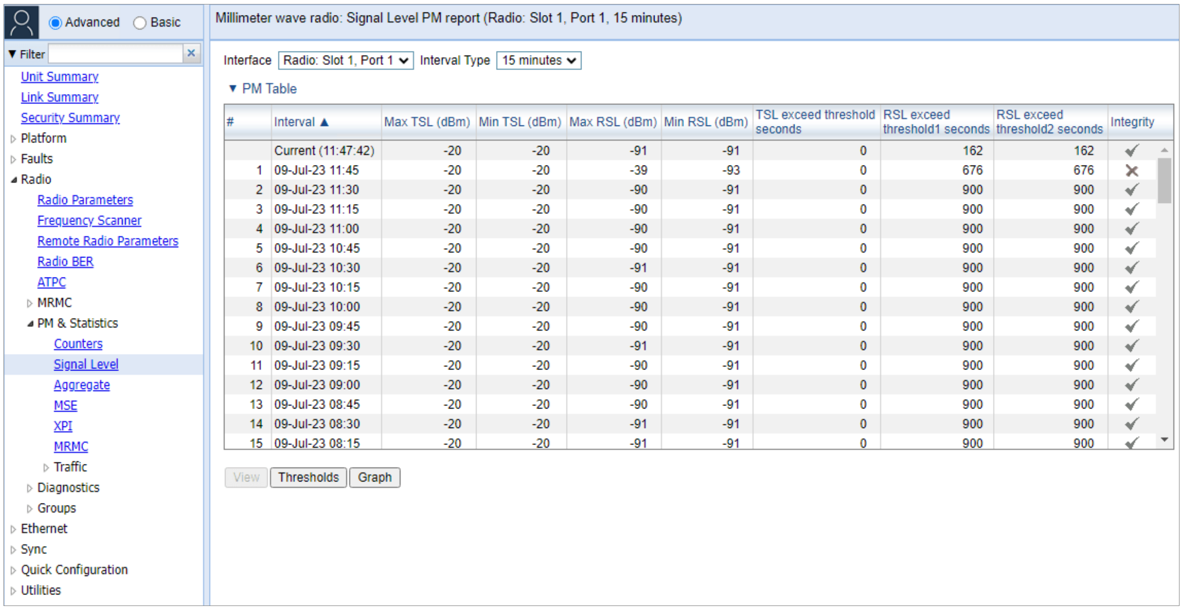
2. To clear the counters, click **Clear Counter**.

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 148 *Signal Level PM Report Page*



Millimeter wave radio: Signal Level PM report (Radio: Slot 1, Port 1, 15 minutes)

Interface: Radio: Slot 1, Port 1 — Interval Type: 15 minutes

#	Interval ▲	Max TSL (dBm)	Min TSL (dBm)	Max RSL (dBm)	Min RSL (dBm)	TSL exceed threshold seconds	RSL exceed threshold1 seconds	RSL exceed threshold2 seconds	Integrity
	Current (11:47:42)	-20	-20	-91	-91	0	162	162	✓
1	09-Jul-23 11:45	-20	-20	-39	-93	0	676	676	✗
2	09-Jul-23 11:30	-20	-20	-90	-91	0	900	900	✓
3	09-Jul-23 11:15	-20	-20	-90	-91	0	900	900	✓
4	09-Jul-23 11:00	-20	-20	-90	-91	0	900	900	✓
5	09-Jul-23 10:45	-20	-20	-90	-91	0	900	900	✓
6	09-Jul-23 10:30	-20	-20	-91	-91	0	900	900	✓
7	09-Jul-23 10:15	-20	-20	-90	-91	0	900	900	✓
8	09-Jul-23 10:00	-20	-20	-90	-91	0	900	900	✓
9	09-Jul-23 09:45	-20	-20	-90	-91	0	900	900	✓
10	09-Jul-23 09:30	-20	-20	-91	-91	0	900	900	✓
11	09-Jul-23 09:15	-20	-20	-90	-91	0	900	900	✓
12	09-Jul-23 09:00	-20	-20	-90	-91	0	900	900	✓
13	09-Jul-23 08:45	-20	-20	-90	-91	0	900	900	✓
14	09-Jul-23 08:30	-20	-20	-91	-91	0	900	900	✓
15	09-Jul-23 08:15	-20	-20	-91	-91	0	900	900	✓

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.

Signal Level PMs 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.

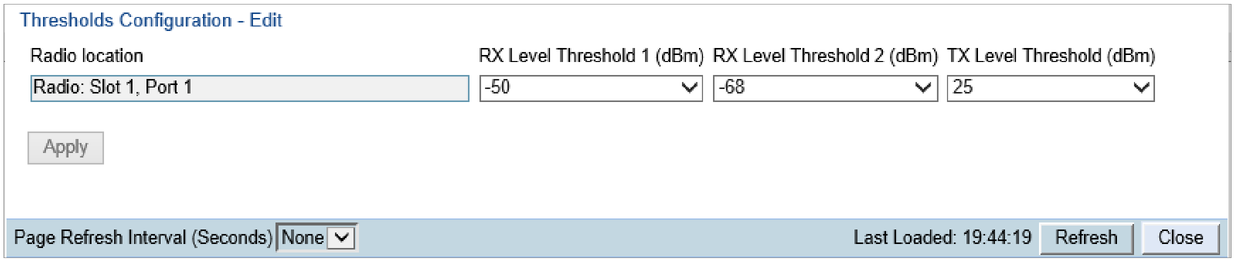
Figure 149 *Signal Level PMs*

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.
TSL exceed	The number of seconds the measured TSL exceeded the TX Level Threshold during the

Parameter	Definition
threshold seconds	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 Signal Level Thresholds, and click **Apply**.

Figure 150 *Signal Level Thresholds Configuration – Edit Page (PTP 850EX)*



Thresholds Configuration - Edit

Radio location	RX Level Threshold 1 (dBm)	RX Level Threshold 2 (dBm)	TX Level Threshold (dBm)
Radio: Slot 1, Port 1	-50	-68	25

Table 28 *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.

To display the signal level PMs report for the selected radio in graph format, click **Graph**. The Signal Level PM Report graphs page opens, offering two tabs.

- One tab displays, in graph format, the Min and Max TSL and RSL for every hour in the past day, as well as the defined TX level and RX level thresholds.
- The other tab displays, in graph format, the values of the TSL and RSL exceed threshold seconds for every hour in the past day.

In each of the graphs, you can hide the display of a parameter in the graph by clicking it in the legend. An additional click un-hides the parameter.

Figure 151 *Signal Level PM Report Graph – Min/Max TSL/RSL and TX/RX Thresholds*

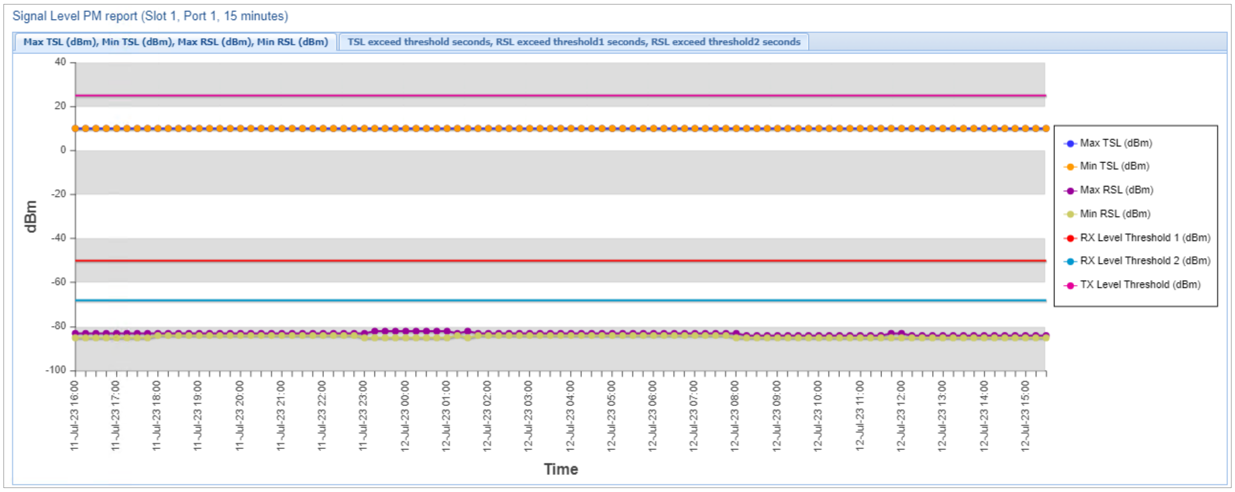
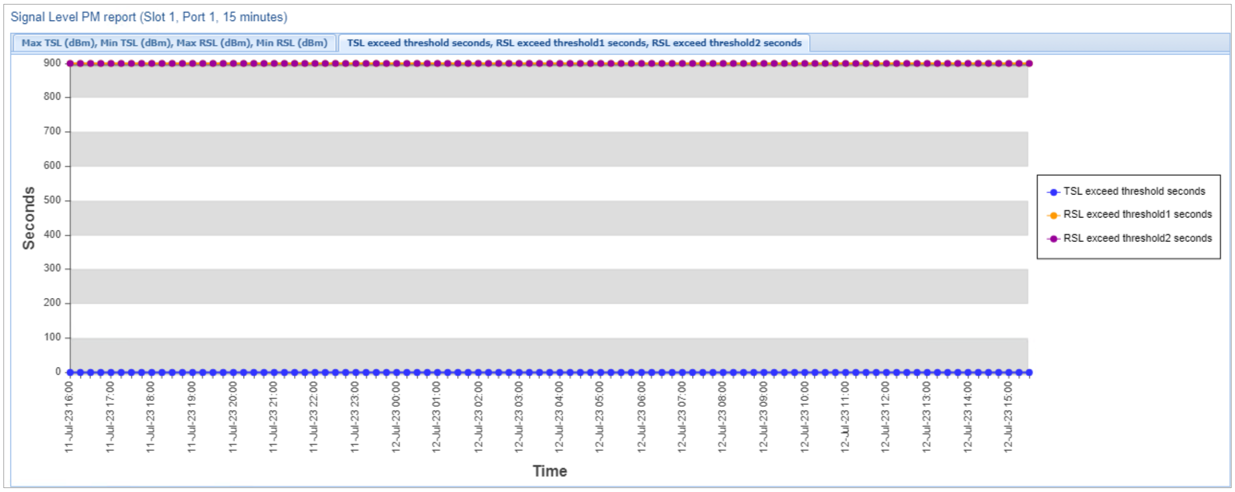


Figure 152 *Signal Level PM Report Graph – TSL/RSL Exceed Threshold Seconds*

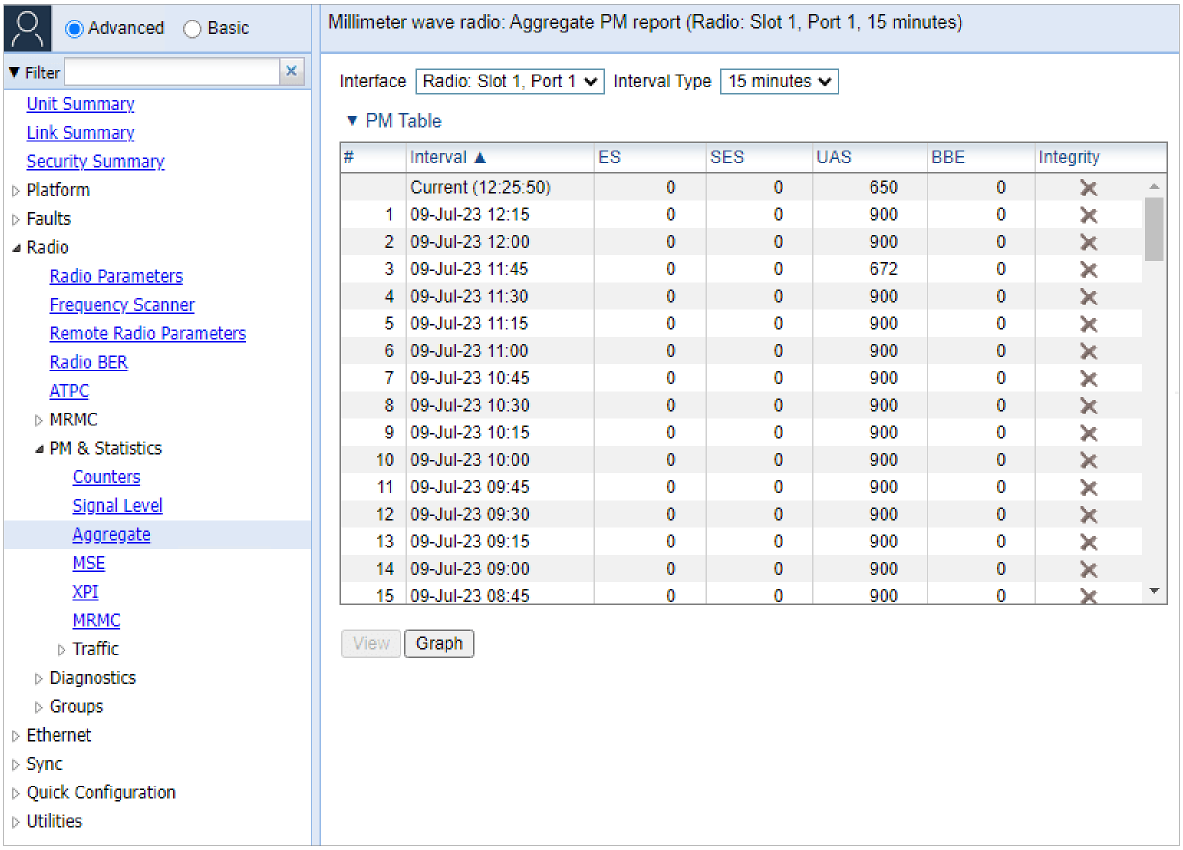


Displaying Modem BER (Aggregate) PMs

To display modem BER (Bit Error Rate) PMs per radio:

1. Select **Radio** > **PM & Statistics** > **Aggregate**. The Aggregate PM report page opens.

Figure 153 *Aggregate PM Report Page*



Millimeter wave radio: Aggregate PM report (Radio: Slot 1, Port 1, 15 minutes)

Interface: Radio: Slot 1, Port 1 | Interval Type: 15 minutes

PM Table

#	Interval ▲	ES	SES	UAS	BBE	Integrity
	Current (12:25:50)	0	0	650	0	✕
1	09-Jul-23 12:15	0	0	900	0	✕
2	09-Jul-23 12:00	0	0	900	0	✕
3	09-Jul-23 11:45	0	0	672	0	✕
4	09-Jul-23 11:30	0	0	900	0	✕
5	09-Jul-23 11:15	0	0	900	0	✕
6	09-Jul-23 11:00	0	0	900	0	✕
7	09-Jul-23 10:45	0	0	900	0	✕
8	09-Jul-23 10:30	0	0	900	0	✕
9	09-Jul-23 10:15	0	0	900	0	✕
10	09-Jul-23 10:00	0	0	900	0	✕
11	09-Jul-23 09:45	0	0	900	0	✕
12	09-Jul-23 09:30	0	0	900	0	✕
13	09-Jul-23 09:15	0	0	900	0	✕
14	09-Jul-23 09:00	0	0	900	0	✕
15	09-Jul-23 08:45	0	0	900	0	✕

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.

Modem BER (Aggregate) PMs 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 29 *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

Parameter	Definition
	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.

To display the Aggregate PM report for the selected radio in graph format, click **Graph**. The Aggregate PM Report graphs page opens, offering two tabs.

- One tab displays, in graph format, the ES, SES and UAS for every hour in the past day.
- The other tab displays, in graph format, the BBE for every hour in the past day.

In each of the graphs, you can hide the display of a parameter in the graph by clicking it in the legend. An additional click un-hides the parameter.

Figure 154 *Aggregate PM Report Graph – ES, SES and UAS*

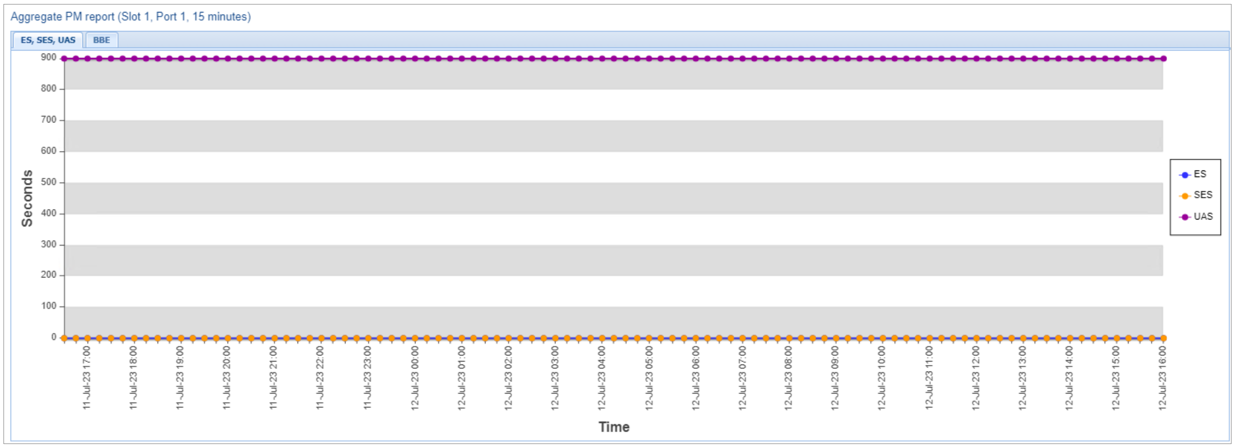
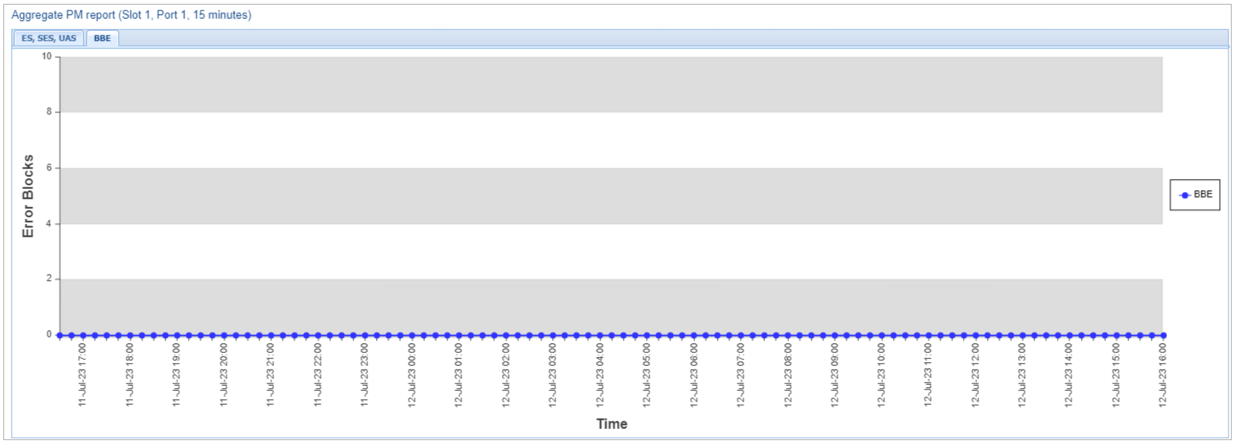


Figure 155 *Aggregate PM Report Graph – BBE*

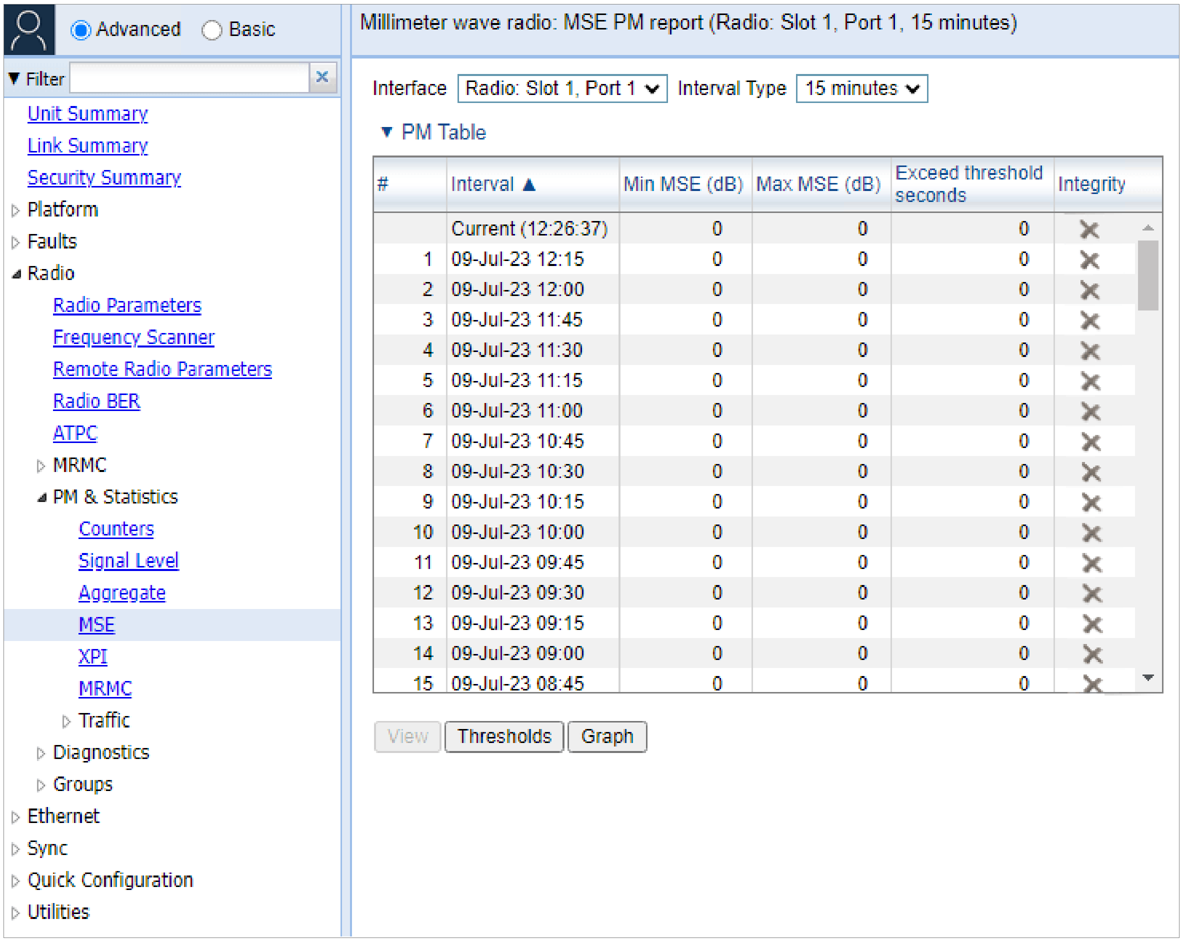


Displaying MSE PMs and Configuring MSE PM Thresholds

To display modem MSE (Minimum Square Error) PMs per radio:

1. Select **Radio** > **PM & Statistics** > **MSE**. The MSE PM report page opens.

Figure 156 *MSE PM Report Page*



Millimeter wave radio: MSE PM report (Radio: Slot 1, Port 1, 15 minutes)

Interface: Radio: Slot 1, Port 1 — Interval Type: 15 minutes

▼ PM Table

#	Interval ▲	Min MSE (dB)	Max MSE (dB)	Exceed threshold seconds	Integrity
	Current (12:26:37)	0	0	0	✕
1	09-Jul-23 12:15	0	0	0	✕
2	09-Jul-23 12:00	0	0	0	✕
3	09-Jul-23 11:45	0	0	0	✕
4	09-Jul-23 11:30	0	0	0	✕
5	09-Jul-23 11:15	0	0	0	✕
6	09-Jul-23 11:00	0	0	0	✕
7	09-Jul-23 10:45	0	0	0	✕
8	09-Jul-23 10:30	0	0	0	✕
9	09-Jul-23 10:15	0	0	0	✕
10	09-Jul-23 10:00	0	0	0	✕
11	09-Jul-23 09:45	0	0	0	✕
12	09-Jul-23 09:30	0	0	0	✕
13	09-Jul-23 09:15	0	0	0	✕
14	09-Jul-23 09:00	0	0	0	✕
15	09-Jul-23 08:45	0	0	0	✕

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.

Modem MSE PMs 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.

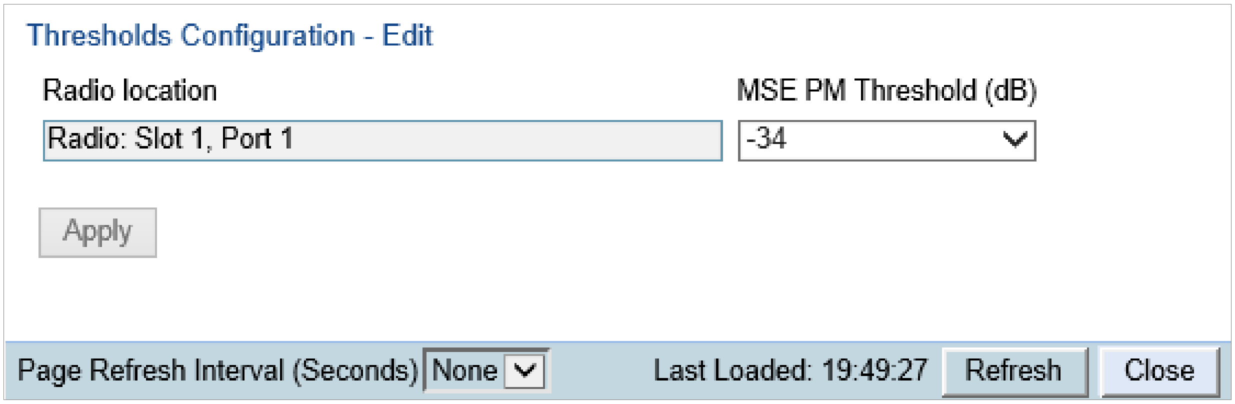
Table 30 *Modem MSE PMs*

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the

Parameter	Definition
	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.
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.
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 157 *Modem MSE Thresholds Configuration – Edit Page (PTP 850EX)*



Thresholds Configuration - Edit

Radio location	MSE PM Threshold (dB)
Radio: Slot 1, Port 1	-34

To display the MSE PM report for the selected radio in graph format, click **Graph**. The MSE PM Report graphs page opens, offering two tabs.

- One tab displays, in graph format, the Minimum and Maximum MSE for every hour in the past day, as well as the defined MSE PM threshold.
- The other tab displays, in graph format, the Exceed Threshold Seconds for every hour in the past day.

In each of the graphs, you can hide the display of a parameter in the graph by clicking it in the legend. An additional click un-hides the parameter.

Figure 158 *MSE PM Report Graph – Min/Max MSE and Threshold*

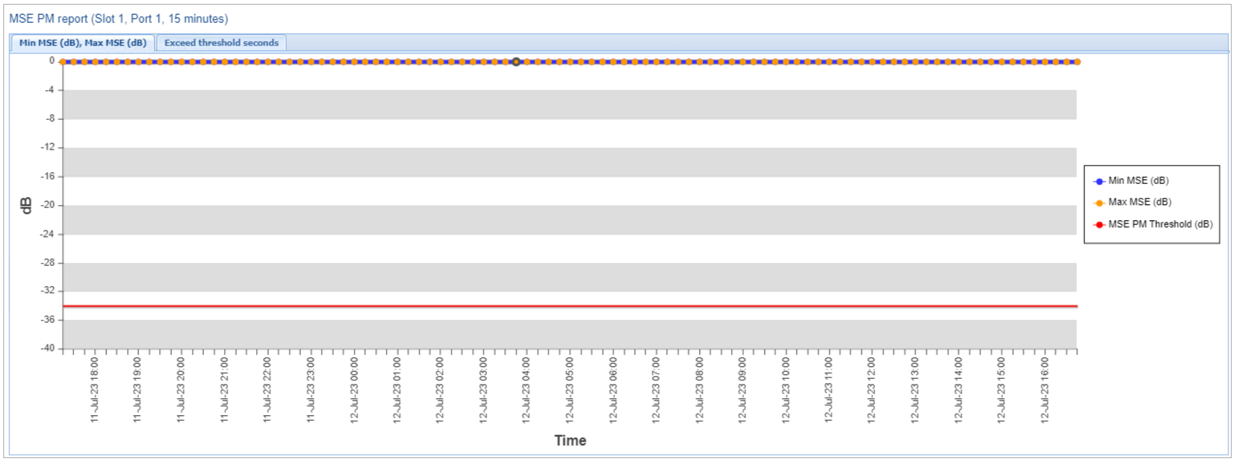
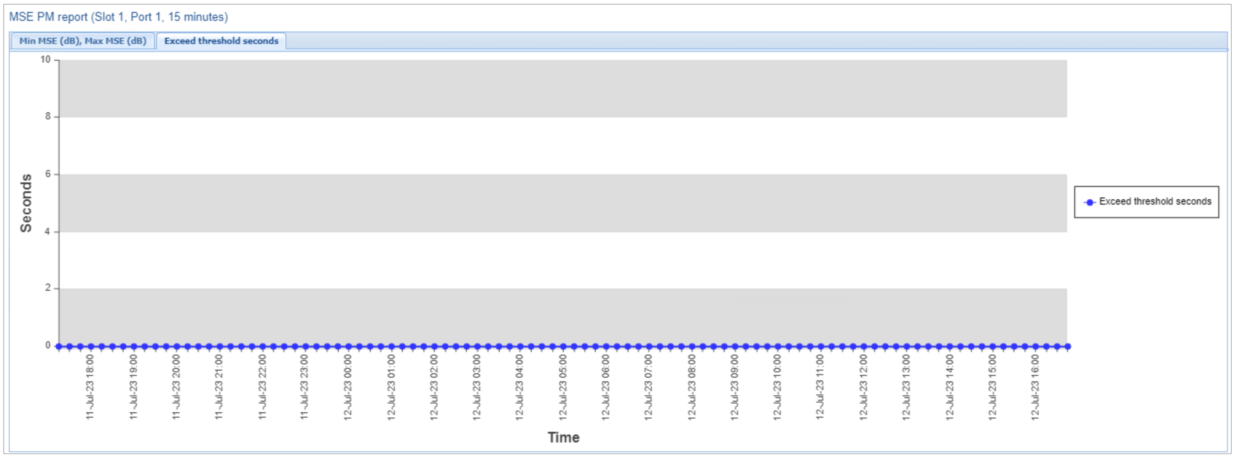


Figure 159 *MSE PM Report Graph – Exceed Threshold Seconds*



Displaying XPI PMs and Configuring XPI PM Thresholds

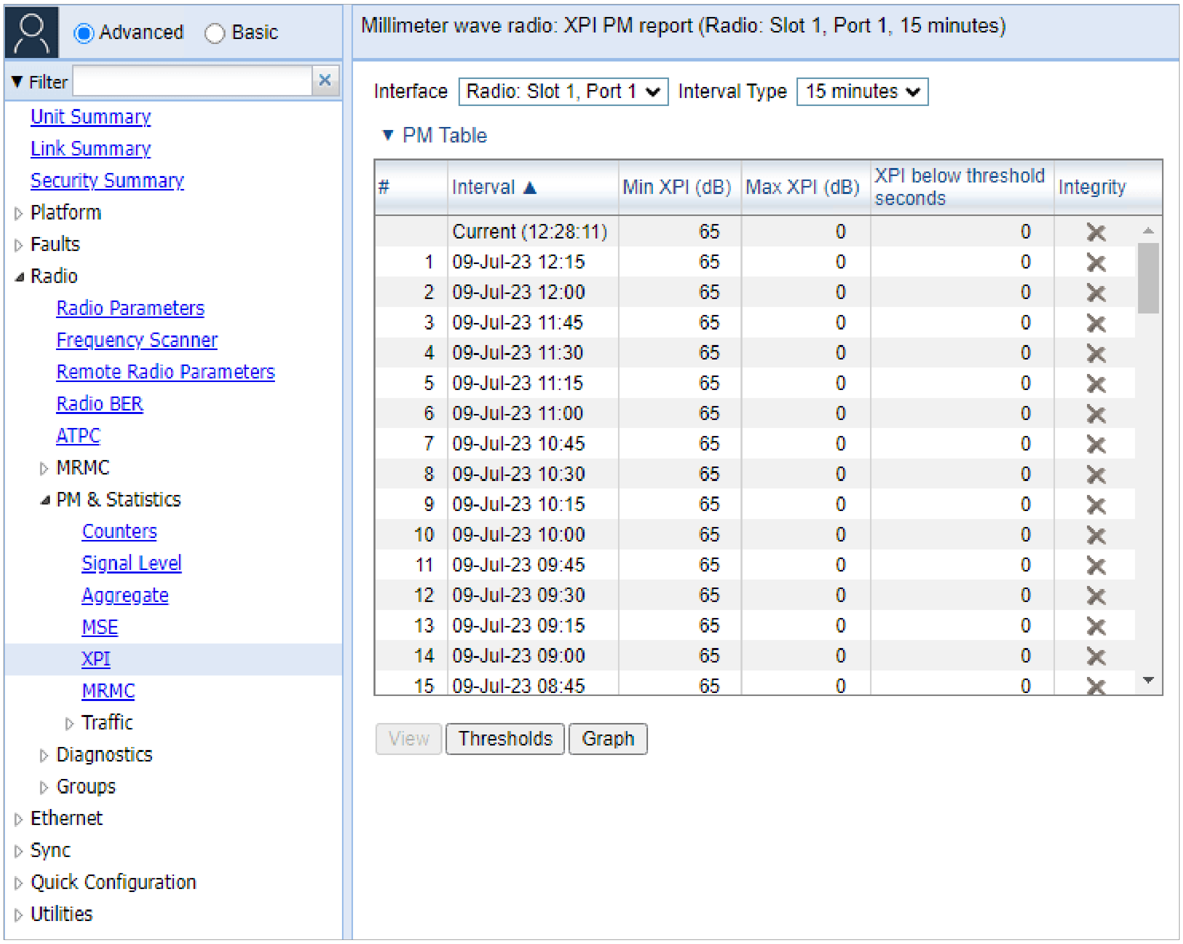
Note

For PTP 850EX, XPIC is planned for future release.

To display XPI (Cross Polarization Interface) PMs per radio:

1. Select **Radio** > **PM & Statistics** > **XPI**. The XPI PM report page opens.

Figure 160 *XPI PM Report Page*



Millimeter wave radio: XPI PM report (Radio: Slot 1, Port 1, 15 minutes)

Interface: Radio: Slot 1, Port 1 Interval Type: 15 minutes

▼ PM Table

#	Interval ▲	Min XPI (dB)	Max XPI (dB)	XPI below threshold seconds	Integrity
	Current (12:28:11)	65	0	0	✗
1	09-Jul-23 12:15	65	0	0	✗
2	09-Jul-23 12:00	65	0	0	✗
3	09-Jul-23 11:45	65	0	0	✗
4	09-Jul-23 11:30	65	0	0	✗
5	09-Jul-23 11:15	65	0	0	✗
6	09-Jul-23 11:00	65	0	0	✗
7	09-Jul-23 10:45	65	0	0	✗
8	09-Jul-23 10:30	65	0	0	✗
9	09-Jul-23 10:15	65	0	0	✗
10	09-Jul-23 10:00	65	0	0	✗
11	09-Jul-23 09:45	65	0	0	✗
12	09-Jul-23 09:30	65	0	0	✗
13	09-Jul-23 09:15	65	0	0	✗
14	09-Jul-23 09:00	65	0	0	✗
15	09-Jul-23 08:45	65	0	0	✗

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.

XPI PMs describes the XPI PMs.

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.

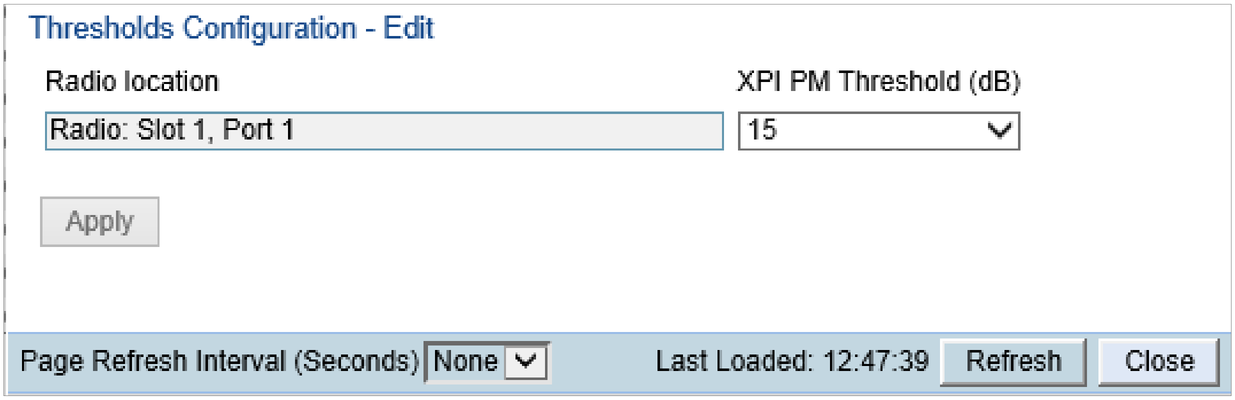
Table 31 *XPI PMs*

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.

Parameter	Definition
Max XPI (dB)	The maximum XPI level that was measured during the interval.
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 161 *XPI Thresholds Configuration – Edit Page (PTP 850EX)*



Thresholds Configuration - Edit

Radio location: Radio: Slot 1, Port 1

XPI PM Threshold (dB): 15

Page Refresh Interval (Seconds): None

Last Loaded: 12:47:39

To display the Aggregate PM report for the selected radio in graph format, click **Graph**. The Aggregate PM Report graphs page opens, offering two tabs.

- One tab displays, in graph format, the Minimum and Maximum XPI for every hour in the past day, as well as the defined XPI PM threshold.
- The other tab displays, in graph format, the XPI Below Threshold Seconds for every hour in the past day.

In each of the graphs, you can hide the display of a parameter in the graph by clicking it in the legend. An additional click un-hides the parameter.

Figure 162 *XPI PM Report Graph – Min/Max XPI and Threshold*

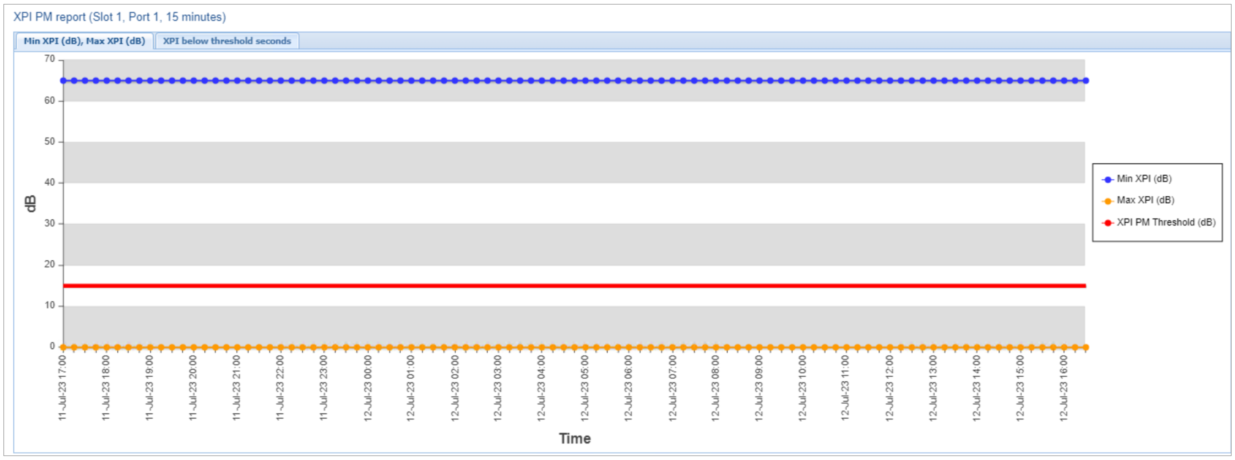
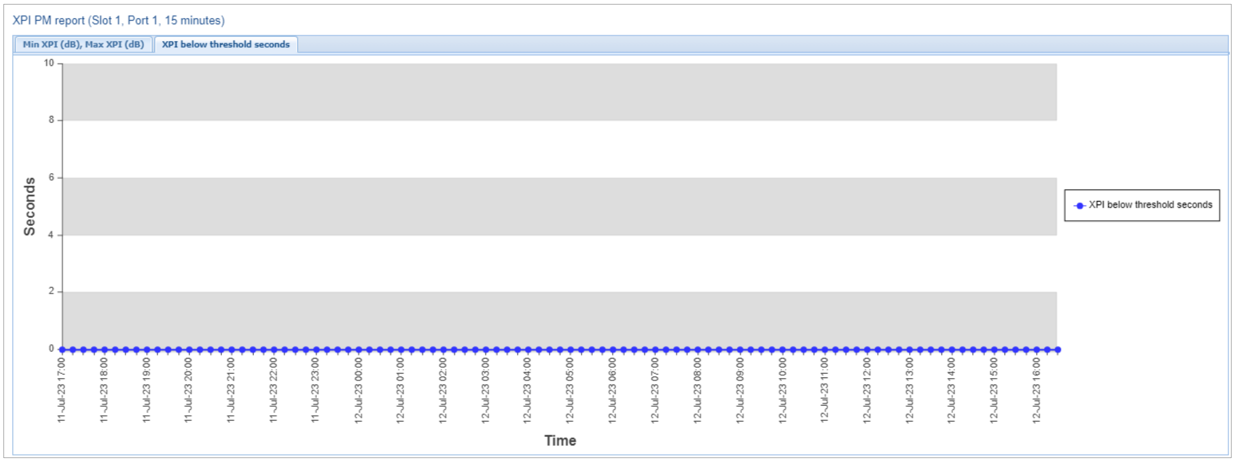


Figure 163 *XPI PM Report Graph – XPI Below Threshold Seconds*



Displaying Traffic PMs

This section includes:

- Displaying Capacity and Throughput PMs
- Displaying Utilization PMs and Configuring Utilization Thresholds

Displaying Capacity and Throughput PMs

You can display PMs for capacity and throughput for a radio, based on:

- The total Layer 1 bandwidth (payload plus overheads) sent through the radio (Mbps).
- The total effective Layer 2 traffic sent through the radio.

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.

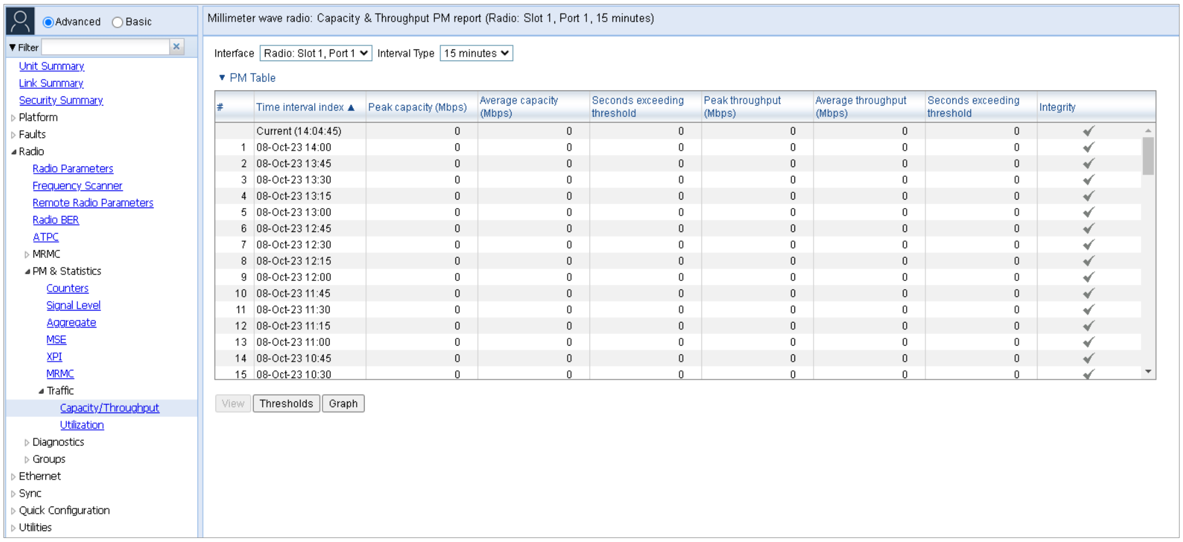
Peak counters display the maximum data rate for each interval, with a resolution of one second. This means the PM mechanism records the number of bytes sent during each second of the interval and displays the number of bytes for the highest one-second period during that interval. So, for example, when 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 radio:

1. Select **Radio** > **PM & Statistics** > **Traffic** > **Capacity/Throughput**. The Capacity PM report page opens.

   Figure 164 *Capacity PM Report Page*



Millimeter wave radio: Capacity & Throughput PM report (Radio: Slot 1, Port 1, 15 minutes)

Interface: Radio: Slot 1, Port 1 | Interval Type: 15 minutes

PM Table

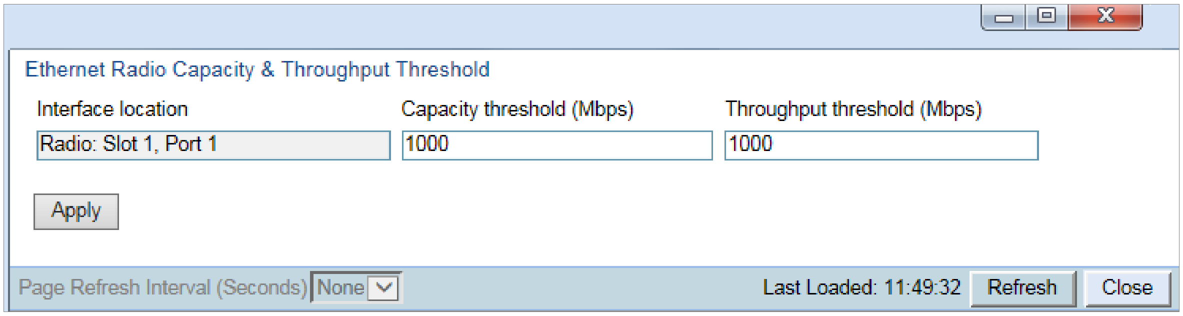
#	Time interval index ▲	Peak capacity (Mbps)	Average capacity (Mbps)	Seconds exceeding threshold	Peak throughput (Mbps)	Average throughput (Mbps)	Seconds exceeding threshold	Integrity
	Current (14:04:45)	0	0	0	0	0	0	✓
1	08-Oct-23 14:00	0	0	0	0	0	0	✓
2	08-Oct-23 13:45	0	0	0	0	0	0	✓
3	08-Oct-23 13:30	0	0	0	0	0	0	✓
4	08-Oct-23 13:15	0	0	0	0	0	0	✓
5	08-Oct-23 13:00	0	0	0	0	0	0	✓
6	08-Oct-23 12:45	0	0	0	0	0	0	✓
7	08-Oct-23 12:30	0	0	0	0	0	0	✓
8	08-Oct-23 12:15	0	0	0	0	0	0	✓
9	08-Oct-23 12:00	0	0	0	0	0	0	✓
10	08-Oct-23 11:45	0	0	0	0	0	0	✓
11	08-Oct-23 11:30	0	0	0	0	0	0	✓
12	08-Oct-23 11:15	0	0	0	0	0	0	✓
13	08-Oct-23 11:00	0	0	0	0	0	0	✓
14	08-Oct-23 10:45	0	0	0	0	0	0	✓
15	08-Oct-23 10:30	0	0	0	0	0	0	✓

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**.

To set the thresholds for capacity and throughput PMs:

1. Select **Thresholds**. The Ethernet Radio Capacity & Throughput Threshold page opens.

   Figure 165 *Ethernet Radio Capacity and Throughput Threshold Page*



Ethernet Radio Capacity & Throughput Threshold

Interface location	Capacity threshold (Mbps)	Throughput threshold (Mbps)
Radio: Slot 1, Port 1	1000	1000

Page Refresh Interval (Seconds): None

Last Loaded: 11:49:32

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**.

Capacity/Throughput PMs describes the capacity and throughput PMs.

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 32 *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 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.
Peak throughput (Mbps)	Displays the highest throughput, in Mbps, that occurred for the selected radio during the measured time interval.
Average throughput (Mbps)	Displays the average throughput, in Mbps, for the selected radio 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.
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.

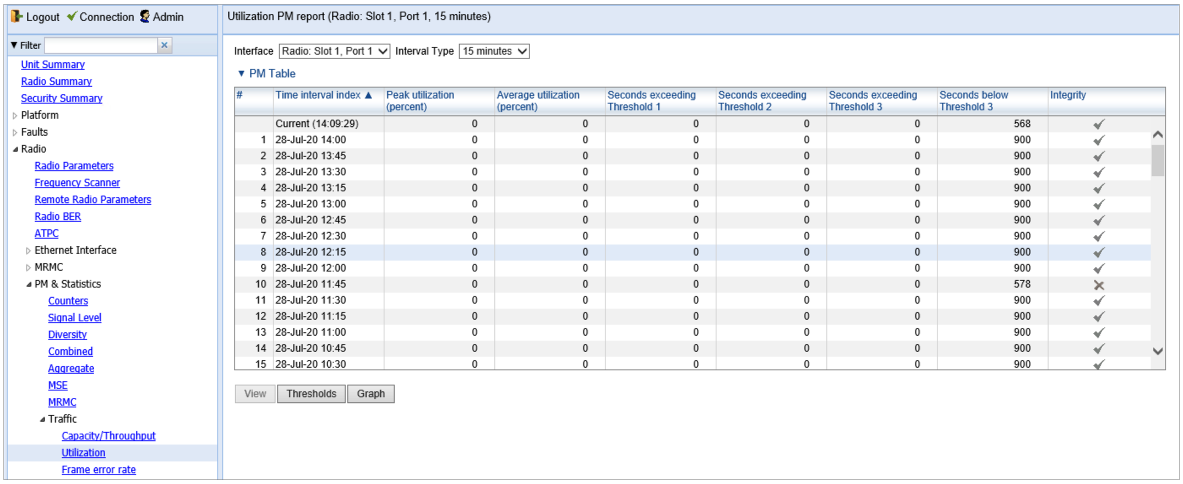
Displaying Utilization PMs and Configuring Utilization Thresholds

You can configure three radio capacity utilization thresholds, in percentage. The Utilization PM Report displays, for each radio carrier, the number of seconds in which the radio 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 166 *Utilization PM Report Page*



Utilization PM report (Radio: Slot 1, Port 1, 15 minutes)

Interface Radio: Slot 1, Port 1 Interval Type 15 minutes

▼ PM Table

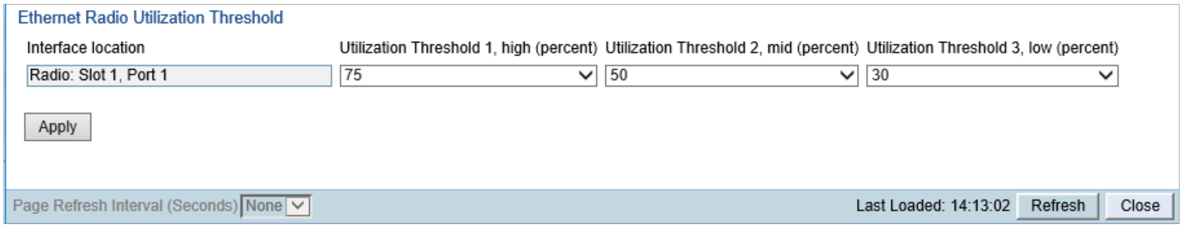
#	Time interval index ▲	Peak utilization (percent)	Average utilization (percent)	Seconds exceeding Threshold 1	Seconds exceeding Threshold 2	Seconds exceeding Threshold 3	Seconds below Threshold 3	Integrity
	Current (14:09:29)	0	0	0	0	0	568	✓
1	28-Jul-20 14:00	0	0	0	0	0	900	✓
2	28-Jul-20 13:45	0	0	0	0	0	900	✓
3	28-Jul-20 13:30	0	0	0	0	0	900	✓
4	28-Jul-20 13:15	0	0	0	0	0	900	✓
5	28-Jul-20 13:00	0	0	0	0	0	900	✓
6	28-Jul-20 12:45	0	0	0	0	0	900	✓
7	28-Jul-20 12:30	0	0	0	0	0	900	✓
8	28-Jul-20 12:15	0	0	0	0	0	900	✓
9	28-Jul-20 12:00	0	0	0	0	0	900	✓
10	28-Jul-20 11:45	0	0	0	0	0	578	✗
11	28-Jul-20 11:30	0	0	0	0	0	900	✓
12	28-Jul-20 11:15	0	0	0	0	0	900	✓
13	28-Jul-20 11:00	0	0	0	0	0	900	✓
14	28-Jul-20 10:45	0	0	0	0	0	900	✓
15	28-Jul-20 10:30	0	0	0	0	0	900	✓

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.

To set the thresholds for utilization PMs:

1. Click Thresholds. The Utilization Threshold page opens.

Figure 167 *Ethernet Radio Utilization Threshold Page*



Ethernet Radio Utilization Threshold

Interface location	Utilization Threshold 1, high (percent)	Utilization Threshold 2, mid (percent)	Utilization Threshold 3, low (percent)
Radio: Slot 1, Port 1	75	50	30

2. For each radio and Multi-Carrier ABC group, you can enter three thresholds, in % (1-100). **Utilization Threshold 1** should be the highest and **Utilization Threshold 3** should be the lowest. The default value for each threshold is 0.
3. Click **Apply**, then **Close**.

Utilization PMs describes the capacity and throughput PMs.

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 33 *Utilization 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 utilization (%)	Indicates the highest utilization of the radio capacity that occurred for the selected radio or group during the measured time interval.
Average utilization (%)	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).
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.

Ethernet Services and Interfaces

This section includes:

Related topics:

- Quality of Service (QoS)

Configuring Ethernet Service(s)

This section includes:

Ethernet Services Overview

Users can define up to 1024 Ethernet services.

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. The Service ID of the pre-defined management service is 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 service can hold two service points. A Multipoint service can hold up to 32 service points. A Management service can hold up 30 service points. The maximum number of service points that can be configured on an PTP 850EX device is 4538.

For a more detailed overview of PTP 850's service-oriented Ethernet switching engine, refer to the Technical Description for the product you are using.

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.

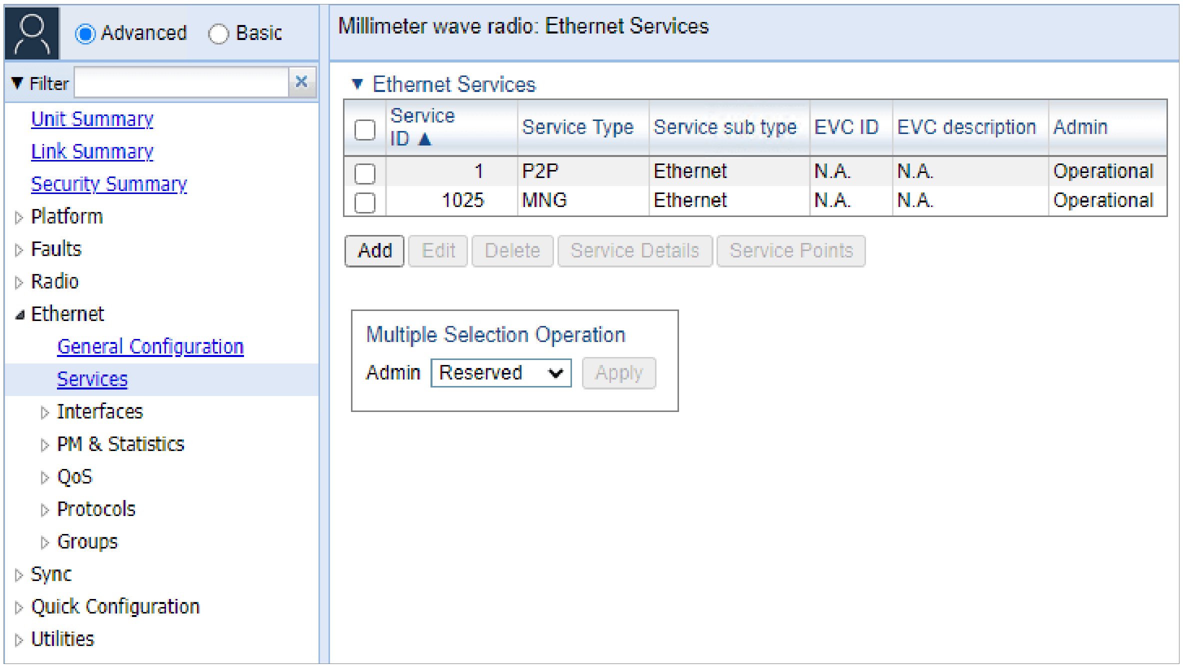
The Ethernet Services Page

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 168 *Ethernet Services Page*



Millimeter wave radio: Ethernet Services

Ethernet Services

□	Service ID ▲	Service Type	Service sub type	EVC ID	EVC description	Admin
□	1	P2P	Ethernet	N.A.	N.A.	Operational
□	1025	MNG	Ethernet	N.A.	N.A.	Operational

Multiple Selection Operation

Admin: Reserved

Ethernet Services Page Parameters describes the parameters displayed in the Ethernet Services page.

Table 34 *Ethernet Services Page Parameters*

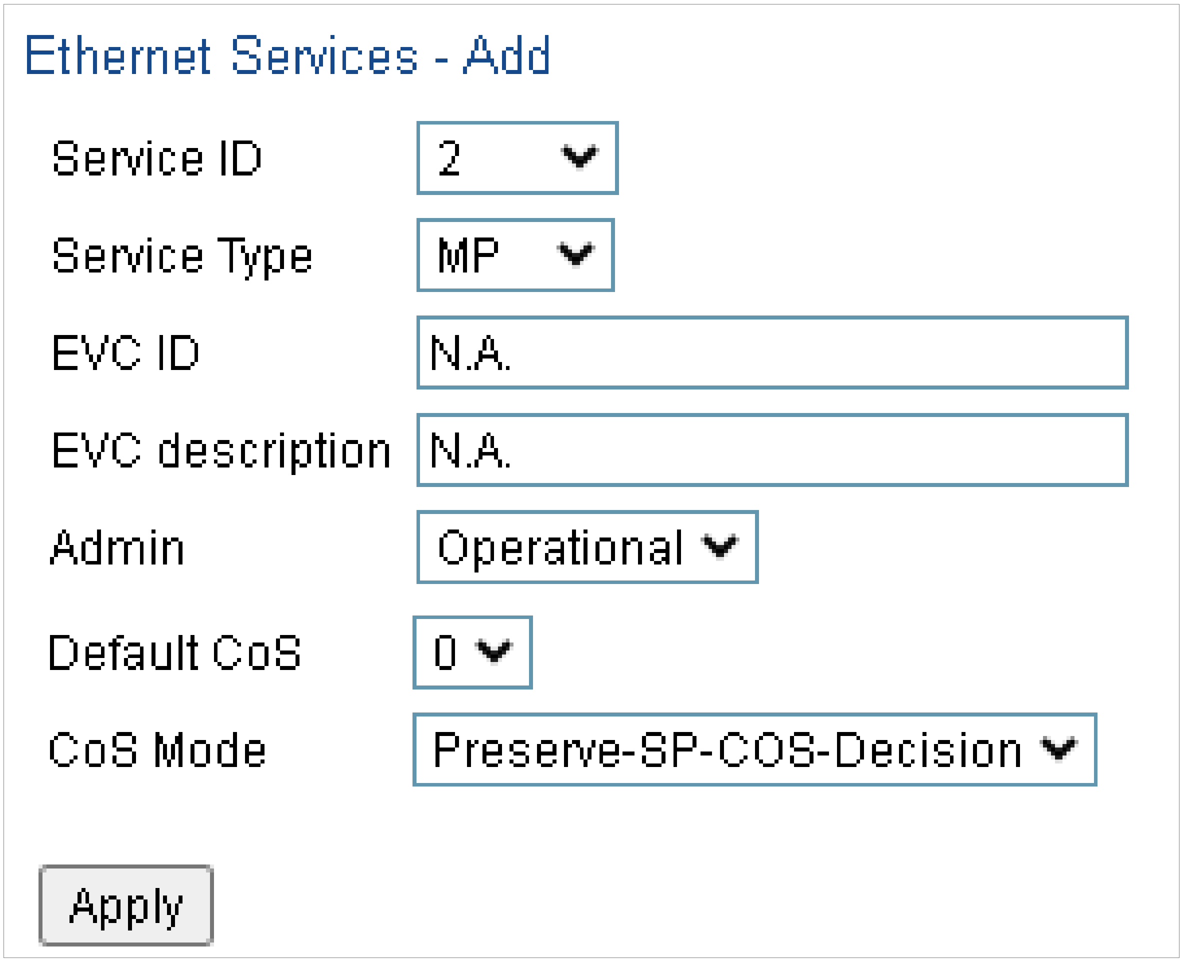
Parameter	Definition
Service ID	A unique ID for the service.
Service Type	The service type: • **MP** – Multipoint • **P2P** – Point-to-Point • **MNG** – Management
Service sub type	Indicates the type of service **(Ethernet)**.
EVC ID	The Ethernet Virtual Connection (EVC) ID. This parameter does not affect 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.

Adding an Ethernet Service

To add an Ethernet service:

1. Select **Ethernet** > **Services**. The Ethernet Services page opens (Ethernet Services Page).
2. In the Ethernet Services page, click Add. The Ethernet Services – Add page opens.

   Figure 169 *Ethernet Services - Add page*

Service ID	2
Service Type	MP
EVC ID	N.A.
EVC description	N.A.
Admin	Operational
Default CoS	0
CoS Mode	Preserve-SP-COS-Decision

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 **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.
9. 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.
10. Click **Apply**, then **Close** to close the Ethernet Services - Add page.
11. Add service points. You must add service points to the service in order for the service to carry traffic. See Configuring Service Points.

Editing a Service

To edit a service:

1. Select **Ethernet** > **Services**. The Ethernet Services page opens (Ethernet Services Page).
2. Select the service in the Service Configuration Table.
3. In the Ethernet Services page, click **Edit**. The Ethernet Services - Edit page opens.

This page is identical to the Ethernet Services - Add page (Ethernet Services - Add page). You can edit any parameter that can be configured in the Add page, except the **Service ID**.

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 (Ethernet Services Page).

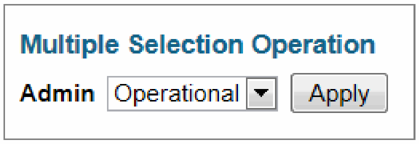
3. Select the service in the Ethernet Service Configuration Table.
4. Click **Delete.** The service is deleted.

Enabling, Disabling, or Deleting Multiple Services

To enable, disable, or delete multiple services:

1. Select **Ethernet** > **Services**. The Ethernet Services page opens (Ethernet Services Page).
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 170 *Multiple Selection Operation Section (Ethernet Services)*

Note

When setting multiple services to the Reserved state, make sure to avoid setting the management service to the Reserved state.

Viewing Service Details

To view the full service parameters:

1. Select **Ethernet** > **Services**. The Ethernet Services page opens (Ethernet Services Page).
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 (Ethernet Services - Add page). However, in the Service Details page, these fields are read-only.

Configuring Service Points

This section includes:

- Ethernet Service Points Overview
- The Ethernet Service Points Page
- Adding a Service Point
- Editing a Service Point

- Deleting a Service Point
- Attaching VLANs

Note

In very specific instances, it may be necessary to remove the outer VLAN tag on an ingress service point. See S-VLAN Ethertype 0x8100 (CISCO Mode).

Ethernet Service 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. 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 service can hold two service points. A Multipoint service can hold up to 32 service points. A management service can hold up to 30 service points. The maximum number of service points that can be configured on an PTP 850EX device is 4538.

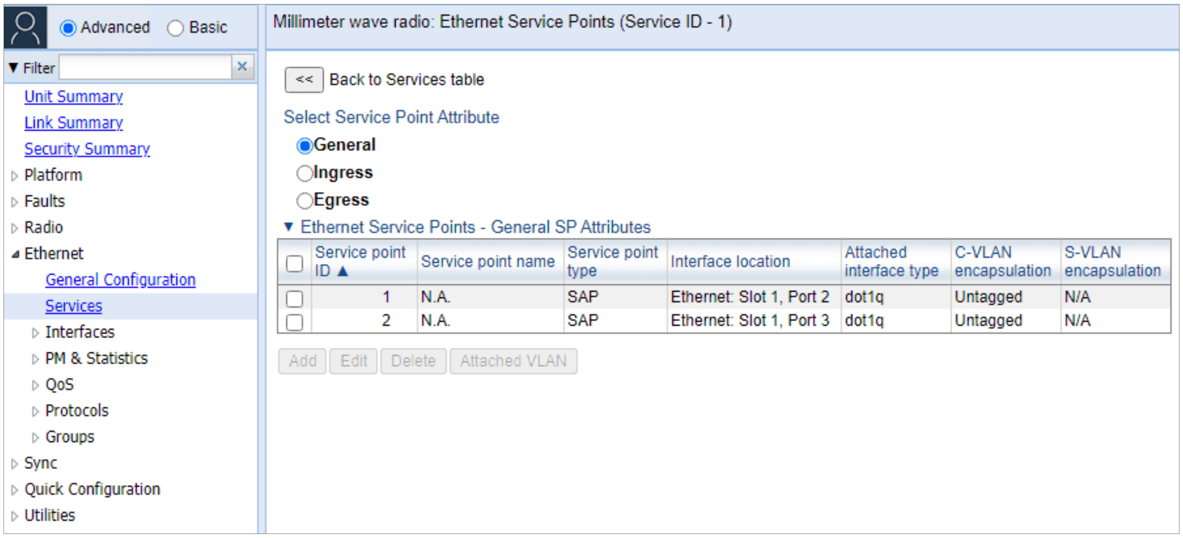
The Ethernet Service Points Page

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 (Ethernet Services Page).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens.

Figure 171 *Ethernet Service Points Page*



Millimeter wave radio: Ethernet Service Points (Service ID - 1)

<< Back to Services table

Select Service Point Attribute

● General

○ Ingress

○ Egress

▼ Ethernet Service Points - General SP Attributes

□	Service point ID ▲	Service point name	Service point type	Interface location	Attached interface type	C-VLAN encapsulation	S-VLAN encapsulation
□	1	N.A.	SAP	Ethernet: Slot 1, Port 2	dot1q	Untagged	N/A
□	2	N.A.	SAP	Ethernet: Slot 1, Port 3	dot1q	Untagged	N/A

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 Ethernet Service Points – Ingress Attributes
- Egress – See 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.

Ethernet Service Points – General SP Attributes Table

The General SP Attributes table is shown in Ethernet Service Points Page. General Service Point Attributes describes the parameters displayed in the General SP Attributes table.

Note

For PIPE service points with S-Tag classification, C-Tag traffic is classified the same as untagged traffic by the QoS classification mechanism.

Table 35 *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.
Service point	The service point type. Options are:

Parameter	Definition
type	• **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 Attached Interface Types.
C-Vlan encapsulation	The C-VLAN classified into the service point. Options are 1-4094, **Untagged**, or **N.A**. (Not Applicable). Note that N.A. can only be used with Bundle-C. 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 and **Untagged** (Not Applicable). 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.

Attached Interface Types describes the available Attached Interface Types.

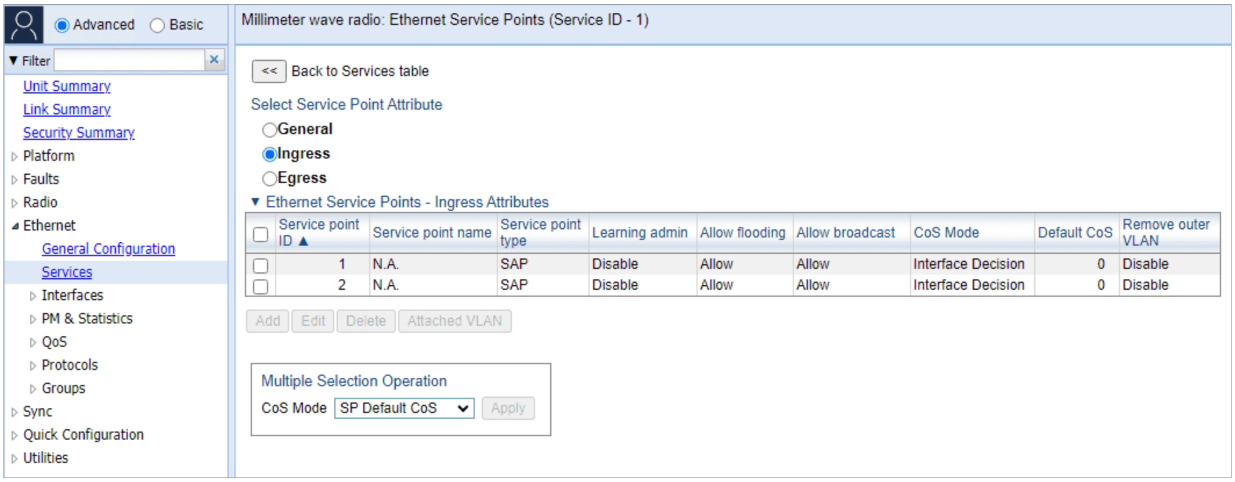
Table 36 *Attached Interface Types*

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
Q-in-Q	A single S-VLAN and C-VLAN combination is classified into the service point.	SAP and MNG

Ethernet Service Points – Ingress Attributes

Select **Ingress** in the Ethernet Service Points page to display the Ethernet Service Points – Ingress Attributes table. Service Point Ingress Attributes describes the parameters displayed in the Ingress SP Attributes table.

Figure 172 *Ethernet Service Points Page – Ingress Attributes*



Millimeter wave radio: Ethernet Service Points (Service ID - 1)

Select Service Point Attribute

○ General
● Ingress
○ Egress

▼ Ethernet Service Points - Ingress Attributes

□	Service point ID ▲	Service point name	Service point type	Learning admin	Allow flooding	Allow broadcast	CoS Mode	Default CoS	Remove outer VLAN
□	1	N.A.	SAP	Disable	Allow	Allow	Interface Decision	0	Disable
□	2	N.A.	SAP	Disable	Allow	Allow	Interface Decision	0	Disable

Multiple Selection Operation

CoS Mode: SP Default CoS

Table 37 *Service Point Ingress Attributes*

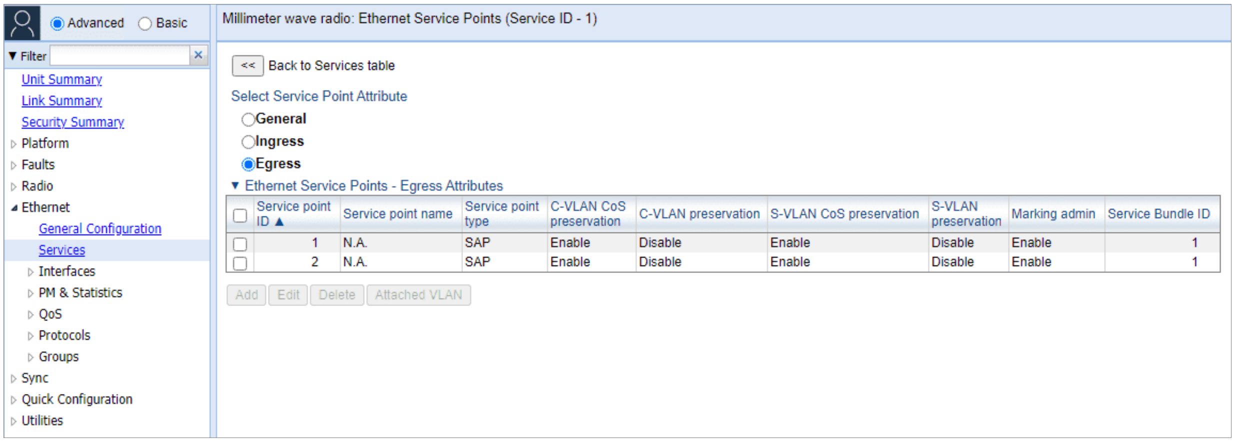
Parameter	Definition
Service point ID	This ID is unique within the service. For Point-to-Point and Multipoint services, the range of values is 1-32. For Management services, the range of values is 1-30.
Service point name	A descriptive name for the service point (optional). The Service Point Name can be up to 20 characters.
Service	The service point type. Options are:

Parameter	Definition
point type	• **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. **Note**:Additional configuration of the MAC address table can be performed via the CLI. See Configuring the MAC Address Forwarding Table (CLI).
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.
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.
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.
Remove Outer VLAN	In very specific instances, it may be necessary to remove the outer VLAN tag on an ingress service point. See S-VLAN Ethertype 0x8100 (CISCO Mode).

Ethernet Service Points – Egress Attributes

Select Egress in the Ethernet Service Points page to display the Ethernet Service Points – Egress Attributes table. Service Point Egress Attributes describes the parameters displayed in the General SP Attributes table.

Figure 173 *Ethernet Service Points Page – Egress Attributes*



Millimeter wave radio: Ethernet Service Points (Service ID - 1)

Select Service Point Attribute

○ General

○ Ingress

● Egress

Ethernet Service Points - Egress Attributes

□	Service point ID ▲	Service point name	Service point type	C-VLAN CoS preservation	C-VLAN preservation	S-VLAN CoS preservation	S-VLAN preservation	Marking admin	Service Bundle ID
□	1	N.A.	SAP	Enable	Disable	Enable	Disable	Enable	1
□	2	N.A.	SAP	Enable	Disable	Enable	Disable	Enable	1

Table 38 *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.
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 (see Marking admin, below).
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 (see Marking admin,

Parameter	Definition
	below).
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 (see Marking admin, below).
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 (see Marking admin, below).
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	1 is the only supported value.

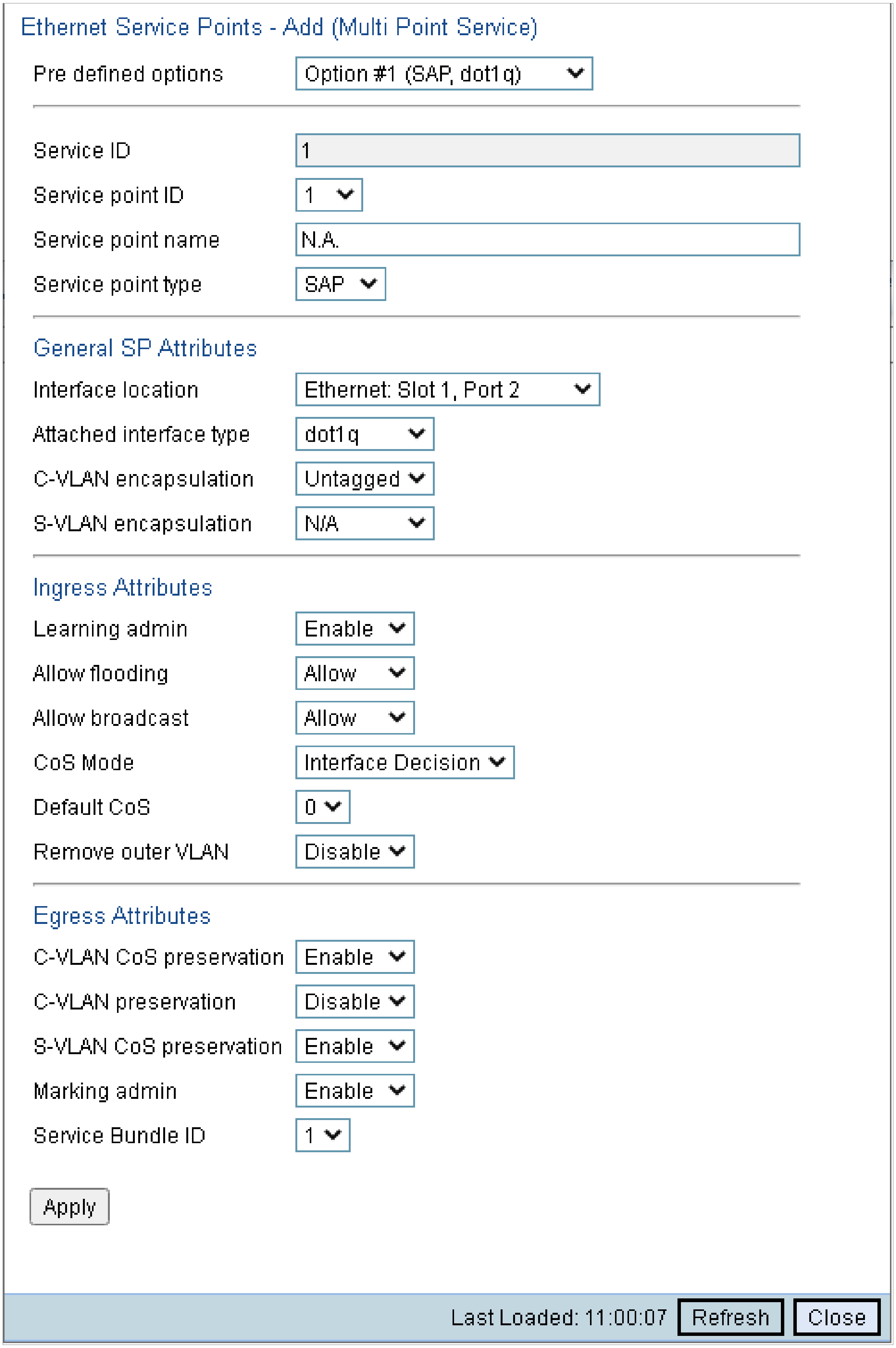
Adding a Service Point

To add a service point:

1. Select **Ethernet** > **Services**. The Ethernet Services page opens (Ethernet Services Page).
2. Select the relevant service in the Ethernet Services Configuration table.

3. Click **Service Points**. The Ethernet Service Points page opens (Ethernet Service Points Page).
4. Click **Add**. The Ethernet Service Points – Add page opens.

Figure 174 Ethernet Service Points - Add Page



Ethernet Service Points - Add (Multi Point Service)

Pre defined options	Option #1 (SAP, dot1q)
Service ID	1
Service point ID	1
Service point name	N.A.
Service point type	SAP

General SP Attributes

Interface location	Ethernet: Slot 1, Port 2
Attached interface type	dot1q
C-VLAN encapsulation	Untagged
S-VLAN encapsulation	N/A

Ingress Attributes

Learning admin	Enable
Allow flooding	Allow
Allow broadcast	Allow
CoS Mode	Interface Decision
Default CoS	0
Remove outer VLAN	Disable

Egress Attributes

C-VLAN CoS preservation	Enable
C-VLAN preservation	Disable
S-VLAN CoS preservation	Enable
Marking admin	Enable
Service Bundle ID	1

Last Loaded: 11:00:07

5. Configure the service point attributes, as described in General Service Point Attributes, Service Point Ingress Attributes, and Service Point Egress Attributes.

> **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 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.

6. Click **Apply**, then **Close**.

Editing a Service Point

To edit a service point:

1. Select **Ethernet** > **Services**. The Ethernet Services page opens (Ethernet Services Page).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens (Ethernet Service Points Page).
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 (Ethernet Service Points - Add Page). You can edit any parameter that can be configured in the Add Service Point page, except **Service ID**, **Service Point ID**, **Service Point Type**, **Interface Location**, and **Attached Interface Type**.
6. Edit the service point attributes, as described in General Service Point Attributes, Service Point Ingress Attributes, and Service Point Egress Attributes.
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 (Ethernet Services Page).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens (Ethernet Service Points Page).
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.

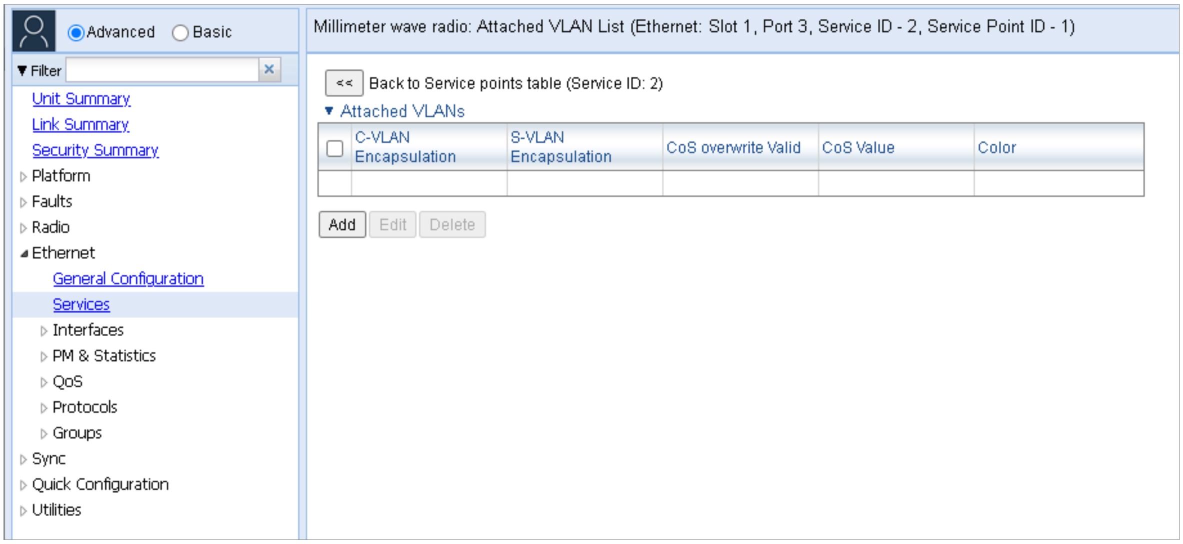
Note

A single device supports up to a maximum of 9216 VLANs (9204 VLANs in Bundle-C and 8436 VLANs in Bundle-S).

To add multiple C-VLANs:

1. Select **Ethernet** > **Services**. The Ethernet Services page opens (Ethernet Services Page).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens (Ethernet Service Points Page).
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 175 *Attached VLAN List Page*



Millimeter wave radio: Attached VLAN List (Ethernet: Slot 1, Port 3, Service ID - 2, Service Point ID - 1)

<< Back to Service points table (Service ID: 2)

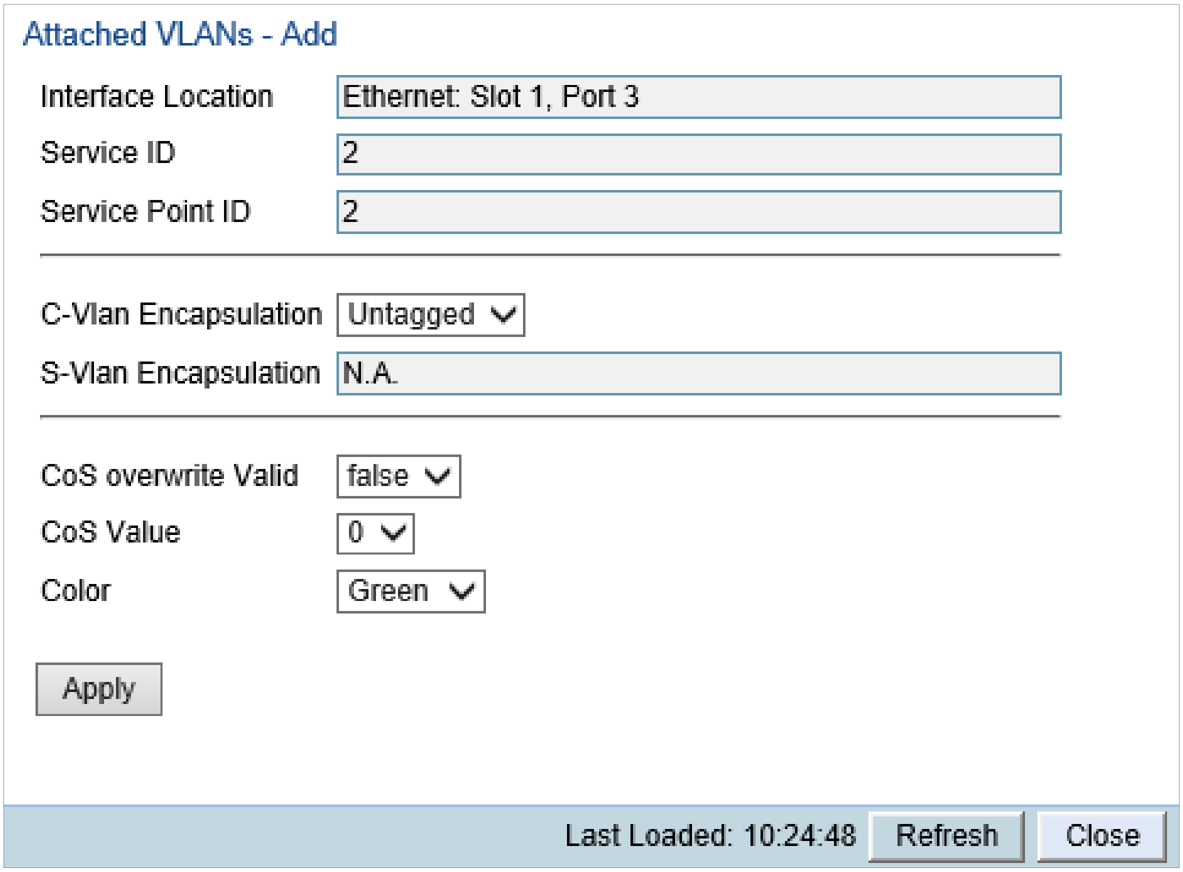
▼ Attached VLANs

□	C-VLAN Encapsulation	S-VLAN Encapsulation	CoS overwrite Valid	CoS Value	Color

Add Edit Delete

6. Click Add. The Attached VLAN List - Add page opens.

Figure 176 *Attached VLAN List - Add Page*



Attached VLANs - Add

Interface Location: Ethernet: Slot 1, Port 3

Service ID: 2

Service Point ID: 2

C-Vlan Encapsulation: Untagged

S-Vlan Encapsulation: N.A.

CoS overwrite Valid: false

CoS Value: 0

Color: Green

7. Configure the VLAN Classification parameters, described in VLAN Classification Parameters.

8. Click **Apply**, then **Close**.z

Table 39 *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.

Parameter	Definition
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.

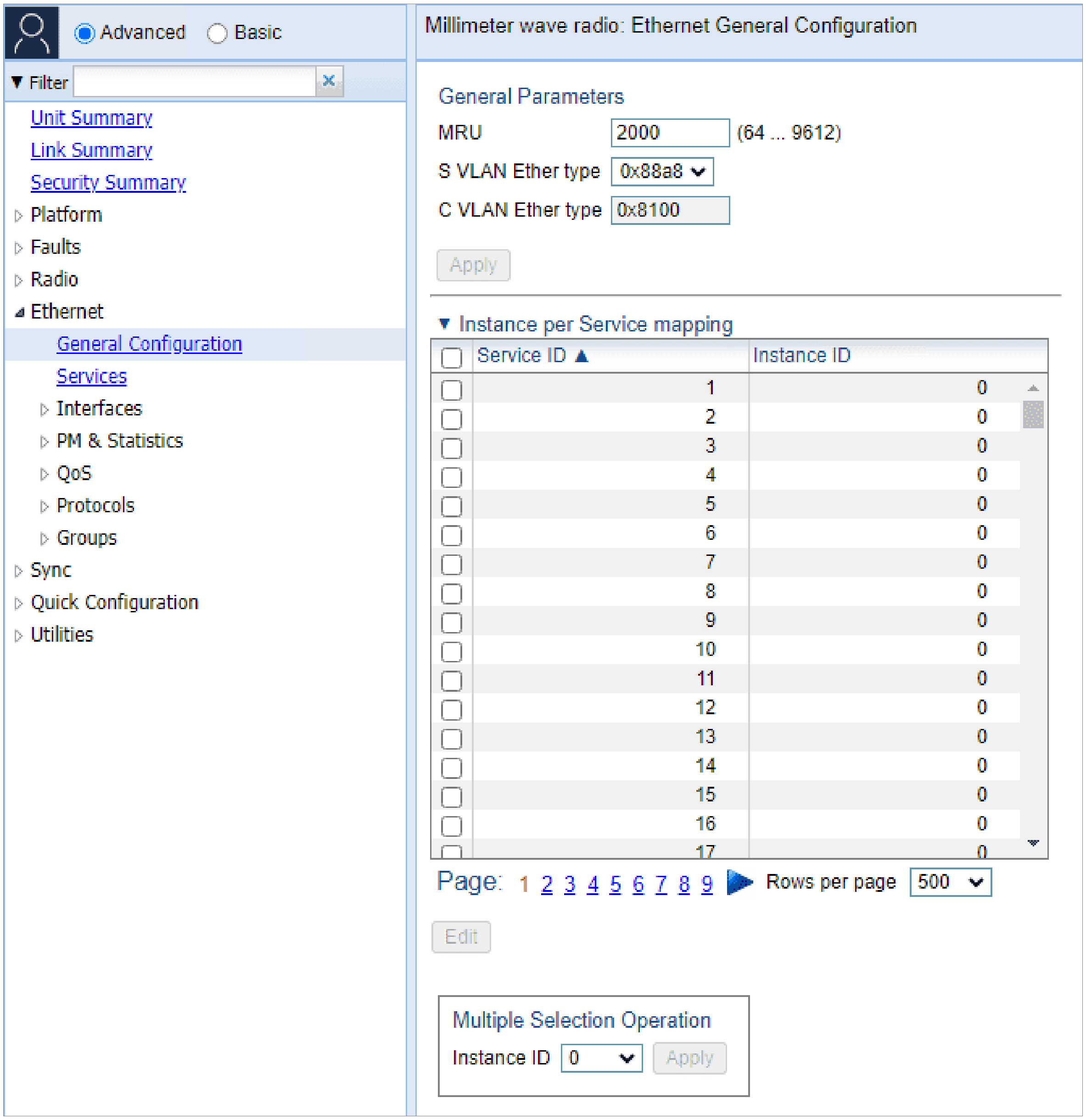
To delete a VLAN Classification table entry, select the entry in the VLAN Classification table and click **Delete**.

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 177 *Ethernet General Configuration Page*



Millimeter wave radio: Ethernet General Configuration

General Parameters

MRU	2000	(64 ... 9612)
S VLAN Ether type	0x88a8	
C VLAN Ether type	0x8100	

Apply

▼ Instance per Service mapping

□	Service ID ▲	Instance ID
□	1	0
□	2	0
□	3	0
□	4	0
□	5	0
□	6	0
□	7	0
□	8	0
□	9	0
□	10	0
□	11	0
□	12	0
□	13	0
□	14	0
□	15	0
□	16	0
□	17	0

Page: 1 2 3 4 5 6 7 8 9 ▶ Rows per page 500

Edit

Multiple Selection Operation

Instance ID 0 Apply

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.

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**.

> **Note**
>
> For information about the Instance per Service mapping table, see Mapping Ethernet Services to MSTP instances (MSTIs).

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 (Ethernet Services Page).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens (Ethernet Service Points Page).
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 (Ethernet Service Points - Add Page).
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 (Ethernet Services Page).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens (Ethernet Service Points Page).
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 (Ethernet Service Points - Add Page).
6. In the **C-VLAN preservation** field, select **Disable**.
7. Click **Apply**, then **Close**.

Configuring Ethernet Interfaces

Related Topics:

- Enabling the Interfaces (Interface Manager)
- 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.

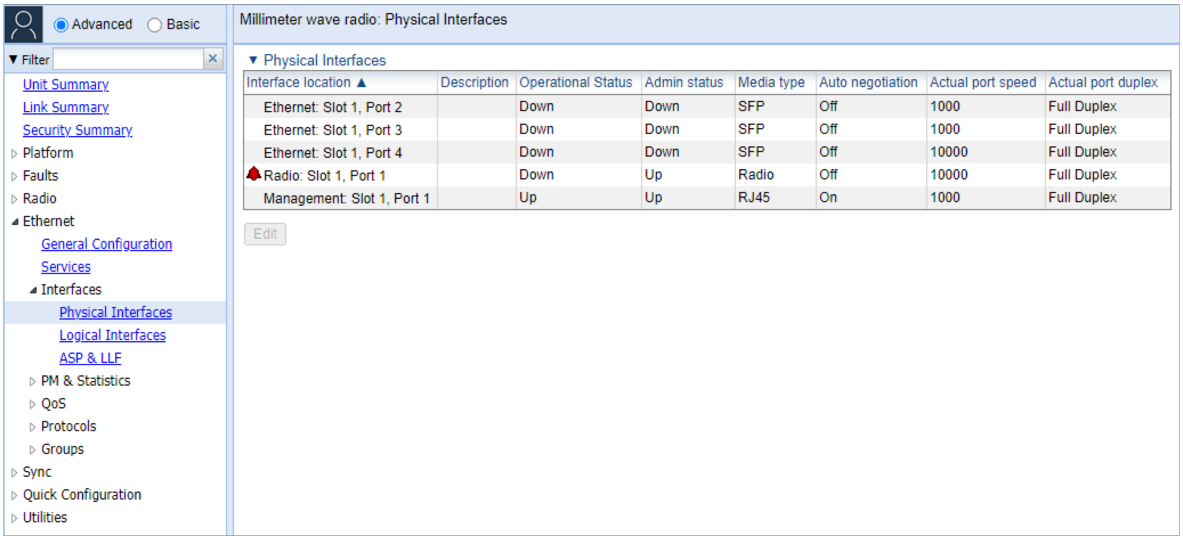
Note

When 25 Gbps ports are connected to third-party equipment:, the 25 Gbps ports on the third-party equipment must be configured to RS_FEC Clause 108. The RS_FEC Clause 108 configuration must be per the IEEE 802.3 standard for 25G SR and 25G L.

To configure the physical interface parameters:

1. Select **Ethernet** > **Interfaces** > **Physical Interfaces**. The Physical Interfaces page opens.

Figure 178 *Physical Interfaces Page (PTP 850EX)*



Millimeter wave radio: Physical Interfaces

▼ Physical Interfaces

Interface location ▲	Description	Operational Status	Admin status	Media type	Auto negotiation	Actual port speed	Actual port duplex
Ethernet: Slot 1, Port 2		Down	Down	SFP	Off	1000	Full Duplex
Ethernet: Slot 1, Port 3		Down	Down	SFP	Off	1000	Full Duplex
Ethernet: Slot 1, Port 4		Down	Down	SFP	Off	10000	Full Duplex
🔔 Radio: Slot 1, Port 1		Down	Up	Radio	Off	10000	Full Duplex
Management: Slot 1, Port 1		Up	Up	RJ45	On	1000	Full Duplex

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.

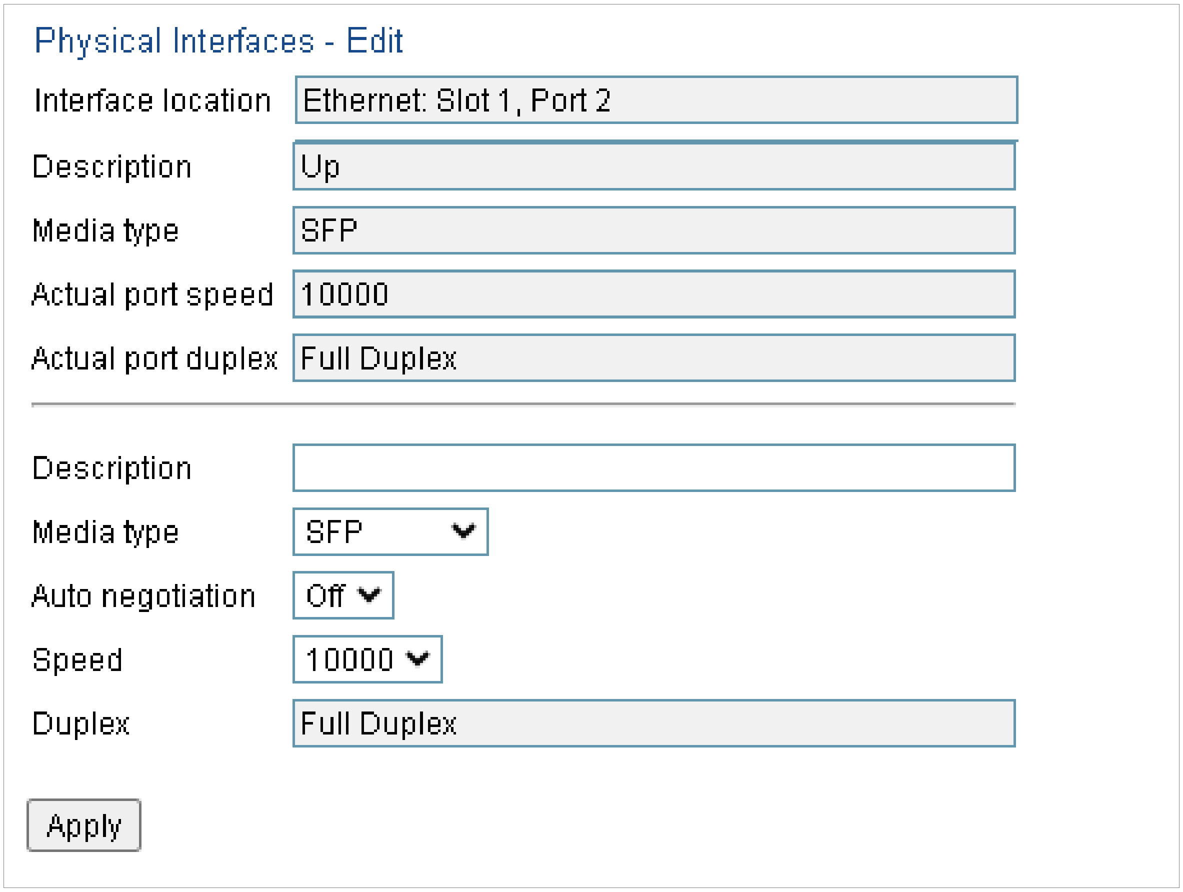
Note

For PTP 850EX, Ethernet Slot 1, Ports 2, 3, and 4 are supported. Management Slot 1 Port 1 is also supported for management.

For PTP 850EX, support for traffic with the Management port is planned for future release.

2. Select the interface you want to configure and click Edit. The Physical Interfaces - Edit page opens.

Figure 179 *Physical Interfaces - Edit Page*



Physical Interfaces - Edit

Interface location: Ethernet: Slot 1, Port 2

Description: Up

Media type: SFP

Actual port speed: 10000

Actual port duplex: Full Duplex

Description:

Media type: SFP

Auto negotiation: Off

Speed: 10000

Duplex: Full Duplex

3. Optionally, in the **Description** field, enter a description of the interface.
4. In the **Media type** field, select the physical interface layer 1 media type. Options are:
   - **Auto-Type** – NA.
   - **RJ45** – An RJ-45 interface.
   - **SFP** – An SFP, SFP+, SFP28, or QSFP Ethernet interface.
   - **Radio** – A radio interface.
5. In the **Auto negotiation** field, select On to enable or Off to disable Auto Negotiation.
   - For radio interfaces, Auto Negotiation is always **Off**.
   - For Ethernet interfaces, see Ethernet Port Speed and Auto Negotiation Options for available options per interface.
6. In the **Speed** field, select the maximum speed of the interface, in Mbps.

- For radio interfaces, the parameter is read-only and set by the system to **10000**.
- For Ethernet interfaces, see Ethernet Port Speed and Auto Negotiation Options for available options per interface.

7. In the **Duplex** field, select the interface's duplex setting (**Full Duplex** or **Half Duplex**). Only **Full-Duplex** is available in this release.
8. Click **Apply**, then **Close**.

Ethernet Port Speed and Auto Negotiation Options

The following tables summarize the Speed and Auto Negotiation options for the Ethernet traffic ports.

Table 40 *Ethernet Interface Speed and Auto Negotiation Options – PTP 850EX*

Interface	Physical Port Number	Notes	**Speed (Mbps)**	Auto Negotiation
Eth 2	P3	SFP28	1000/10000/25000	On/Off
Eth 3	P4	SFP28	1000/10000/25000	On/Off
Eth 4	P5	QSFP. Option for SFP or SFP+ (1 x 1 or 10GbE) with adaptor (1+0 configurations only)	1000/10000	On/Off
Management 1	P2	RJ-45. Management only.	100/1000	On/Off

Note

Only 1Gbps is supported with electrical SFPs.

Physical Interface Status Parameters describes the status parameters that appear in the Physical Interfaces page.

Table 41 *Physical Interface Status Parameters*

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 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	Displays the actual duplex status of the interface for the link as agreed by the two sides

Parameter	Definition
duplex	of the link after the auto negotiation process.

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 Multi-Carrier ABC group. The Controlled Interface is an Ethernet interface or LAG. An Ethernet interface can only be assigned to one Monitored interface.

Note

A radio interface that belongs to a LAG group cannot be used as a 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. See Configuring the Activation Key.

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.

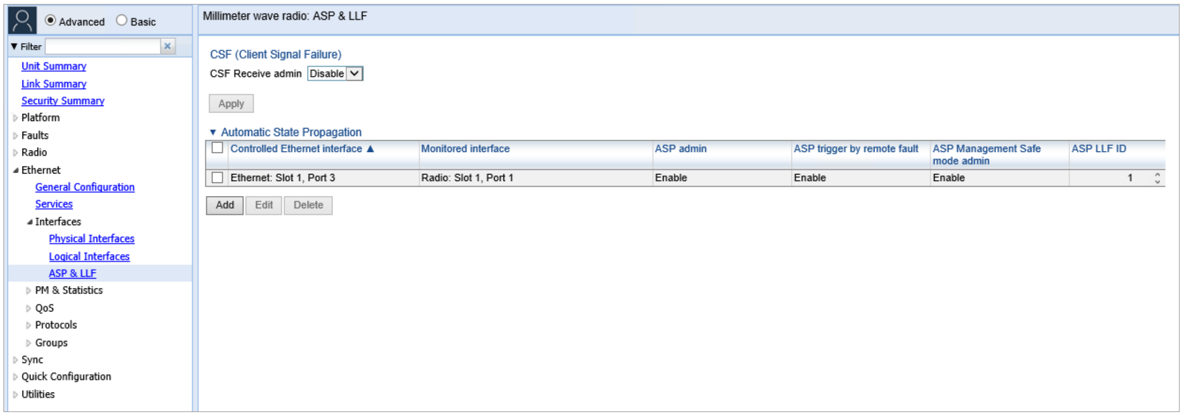
A trigger delay time can be configured, so that when a triggering event takes place, the ASP mechanism does not propagate the event until this delay time has elapsed. A trigger delay from 0 to 10,000 ms can be set per LLD ID. The delay time must be configured via CLI. See Configuring Automatic State Propagation 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** > **ASP & LLF**. The ASP & LLF page opens.

Figure 180 *ASP & LLF Page*



Millimeter wave radio: ASP & LLF

CSF (Client Signal Failure)

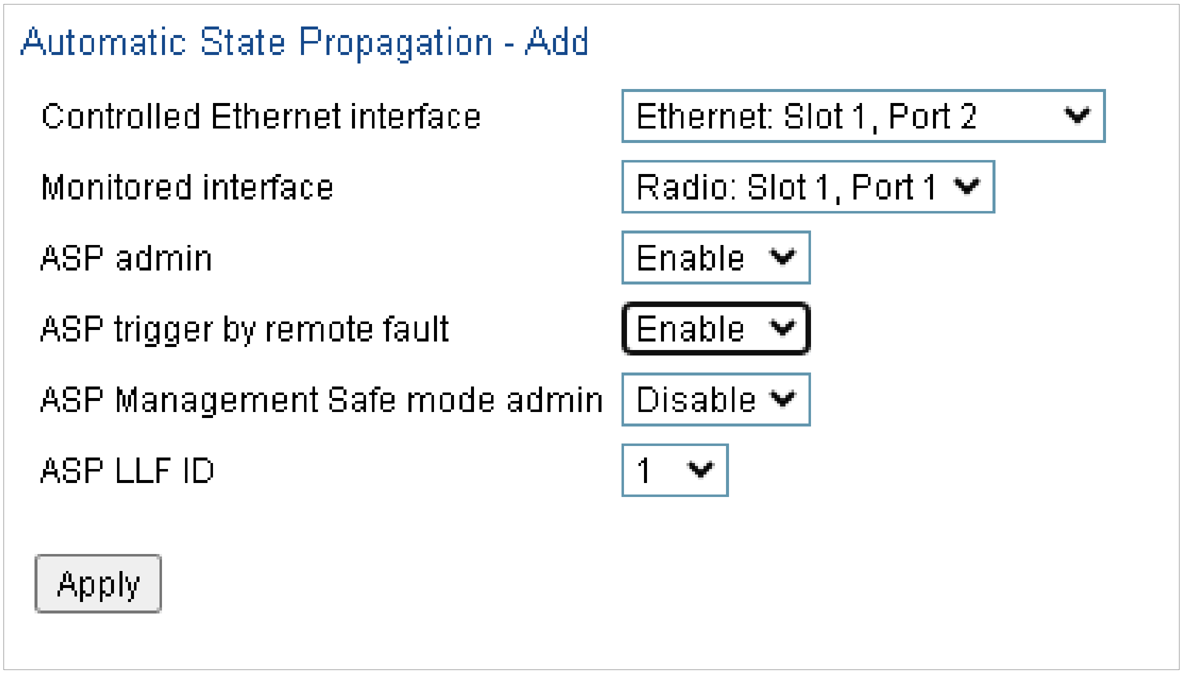
CSF Receive admin: Disable

▼ Automatic State Propagation

□	Controlled Ethernet interface ▲	Monitored interface	ASP admin	ASP trigger by remote fault	ASP Management Safe mode admin	ASP LLF ID
□	Ethernet: Slot 1, Port 3	Radio: Slot 1, Port 1	Enable	Enable	Enable	1

2. Click **Add**. The Automatic State Propagation - Add page opens.

Figure 181 *Automatic State Propagation - Add Page*



Automatic State Propagation - Add

Controlled Ethernet interface: Ethernet: Slot 1, Port 2

Monitored interface: Radio: Slot 1, Port 1

ASP admin: Enable

ASP trigger by remote fault: Enable

ASP Management Safe mode admin: Disable

ASP LLF ID: 1

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 Interface** field, select the Monitored Radio Interface or group. 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(CSF PDU). This message is used to propagate the failure indication to external equipment.

   When ASP Management Safe mode is configured, the peer unit must be configured to receive CSF PDUs. CSF receive must be enabled in order for G.8032 ERPI topology changes to be initiated upon receipt of a CSF PDU. To enable CSF receive, select **Enable** in the **CSF Receive admin** field at the top of the ASP & LLF page.

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 (Automatic State Propagation - Add Page), but the **Controlled Ethernet Interface** and **Monitored 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.

Viewing Ethernet PMs and Statistics

PTP 850 devices store and display 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

RMON Statistics

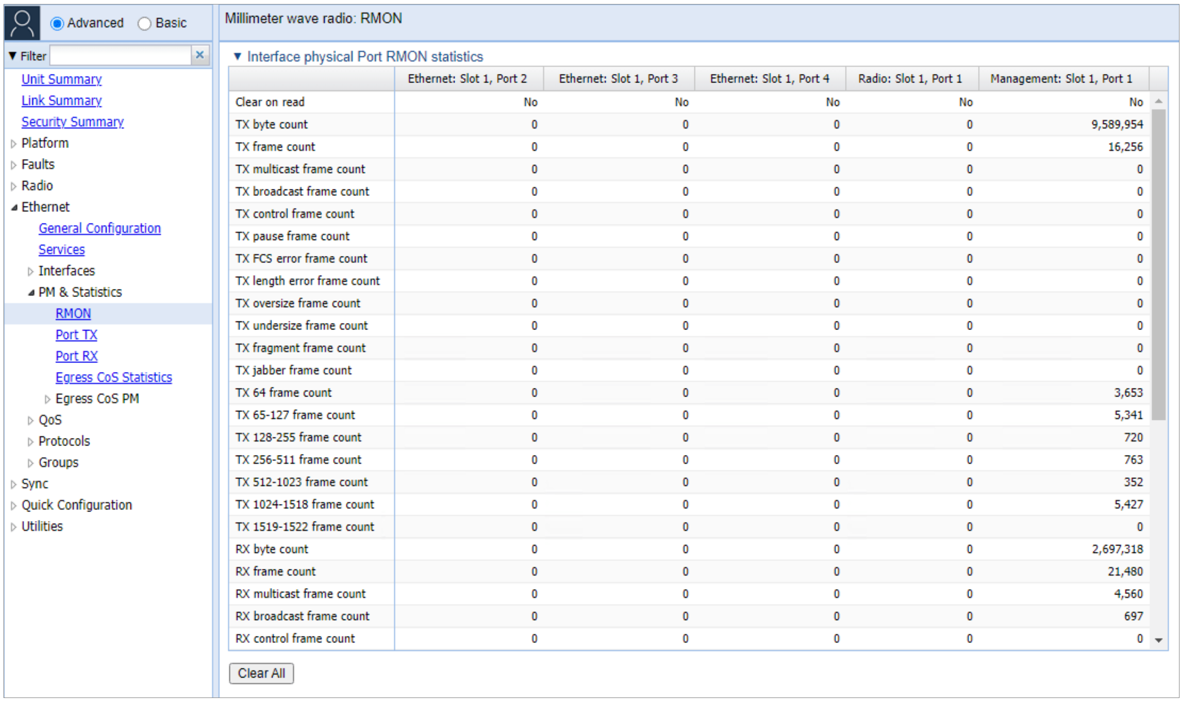
Note

RMON counters per frame size are not available for individual radio interfaces and radio groups.

To view and reset RMON statistics:

1. Select **Ethernet** > **PM & Statistics** > **RMON**. The RMON page opens.

Figure 182 *RMON Page (PTP 850EX)*



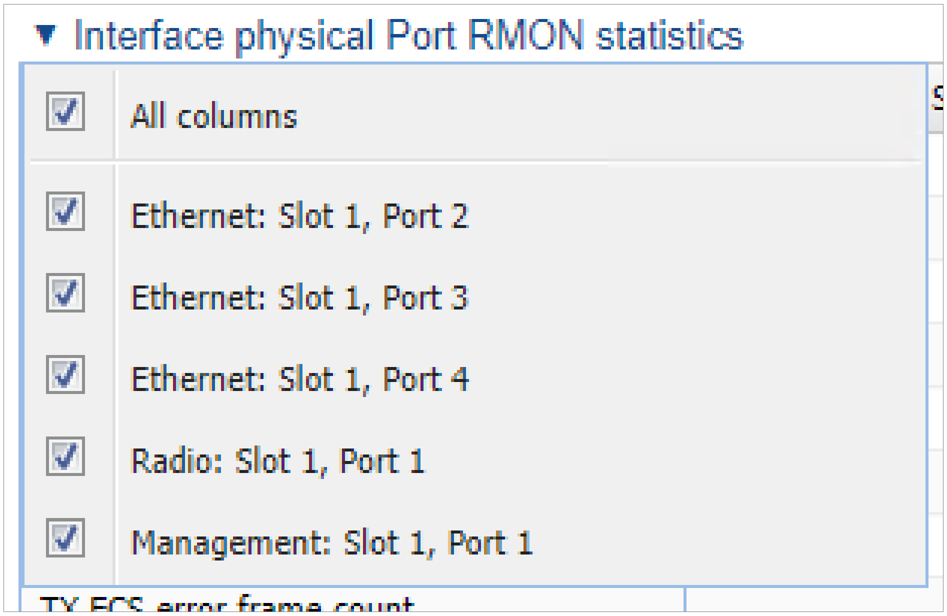
	Ethernet: Slot 1, Port 2	Ethernet: Slot 1, Port 3	Ethernet: Slot 1, Port 4	Radio: Slot 1, Port 1	Management: Slot 1, Port 1
Clear on read	No	No	No	No	No
TX byte count	0	0	0	0	9,589,954
TX frame count	0	0	0	0	16,256
TX multicast frame count	0	0	0	0	0
TX broadcast frame count	0	0	0	0	0
TX control frame count	0	0	0	0	0
TX pause frame count	0	0	0	0	0
TX FCS error frame count	0	0	0	0	0
TX length error frame count	0	0	0	0	0
TX oversize frame count	0	0	0	0	0
TX undersize frame count	0	0	0	0	0
TX fragment frame count	0	0	0	0	0
TX jabber frame count	0	0	0	0	0
TX 64 frame count	0	0	0	0	3,653
TX 65-127 frame count	0	0	0	0	5,341
TX 128-255 frame count	0	0	0	0	720
TX 256-511 frame count	0	0	0	0	763
TX 512-1023 frame count	0	0	0	0	352
TX 1024-1518 frame count	0	0	0	0	5,427
TX 1519-1522 frame count	0	0	0	0	0
RX byte count	0	0	0	0	2,697,318
RX frame count	0	0	0	0	21,480
RX multicast frame count	0	0	0	0	4,560
RX broadcast frame count	0	0	0	0	697
RX control frame count	0	0	0	0	0

- 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 183 *RMON Page – Hiding and Displaying Columns*



▼ Interface physical Port RMON statistics

☑ All columns

☑ Ethernet: Slot 1, Port 2

☑ Ethernet: Slot 1, Port 3

☑ Ethernet: Slot 1, Port 4

☑ Radio: Slot 1, Port 1

☑ Management: Slot 1, Port 1

TX FCS error frame count

Note

If you click the table title itself, all columns are hidden. To un-hide the columns, click the table title again.

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

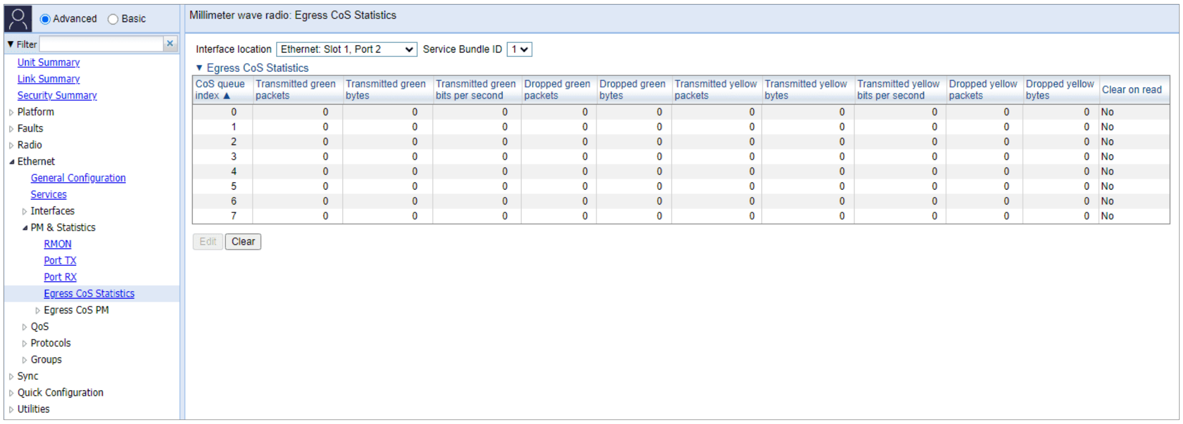
Note

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 184 *Egress CoS Statistics Page*



Millimeter wave radio: Egress CoS Statistics

Interface location: Ethernet: Slot 1, Port 2
Service Bundle ID: 1

▼ Egress CoS Statistics

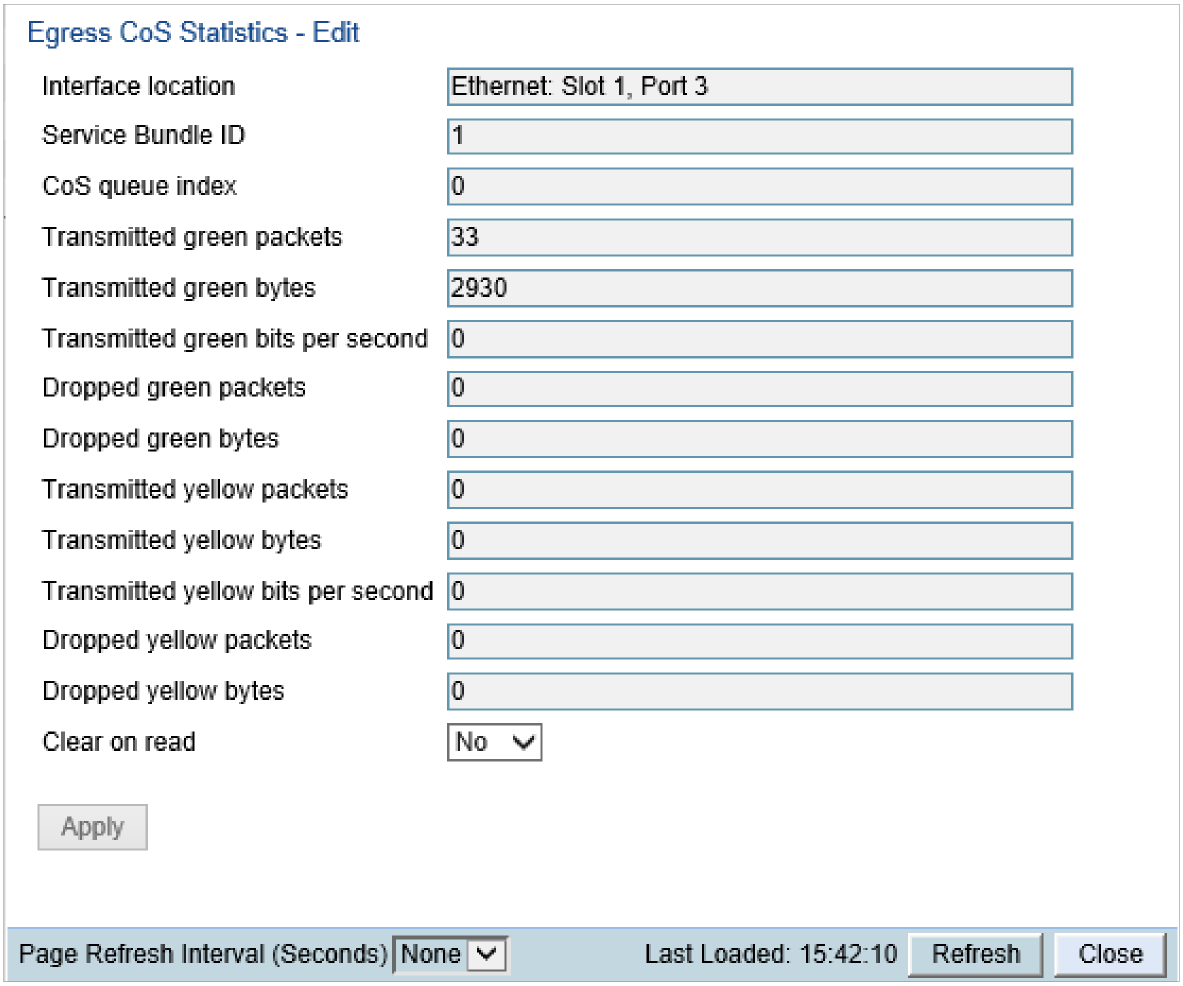
CoS queue index ▲	Transmitted green packets	Transmitted green bytes	Transmitted green bits per second	Dropped green packets	Dropped green bytes	Transmitted yellow packets	Transmitted yellow bytes	Transmitted yellow bits per second	Dropped yellow packets	Dropped yellow bytes	Clear on read
0	0	0	0	0	0	0	0	0	0	0	No
1	0	0	0	0	0	0	0	0	0	0	No
2	0	0	0	0	0	0	0	0	0	0	No
3	0	0	0	0	0	0	0	0	0	0	No
4	0	0	0	0	0	0	0	0	0	0	No
5	0	0	0	0	0	0	0	0	0	0	No
6	0	0	0	0	0	0	0	0	0	0	No
7	0	0	0	0	0	0	0	0	0	0	No

2. In the **Service bundle ID** field, select 1

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**. You can also clear the entire table by clicking **Clear** underneath the table.

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 185 *Egress CoS Statistics – Edit Page*



Egress CoS Statistics - Edit

Interface location	Ethernet: Slot 1, Port 3
Service Bundle ID	1
CoS queue index	0
Transmitted green packets	33
Transmitted green bytes	2930
Transmitted green bits per second	0
Dropped green packets	0
Dropped green bytes	0
Transmitted yellow packets	0
Transmitted yellow bytes	0
Transmitted yellow bits per second	0
Dropped yellow packets	0
Dropped yellow bytes	0
Clear on read	No

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**.

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), in bytes and in packets, layer1 and layer2, broadcast and multicast 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:

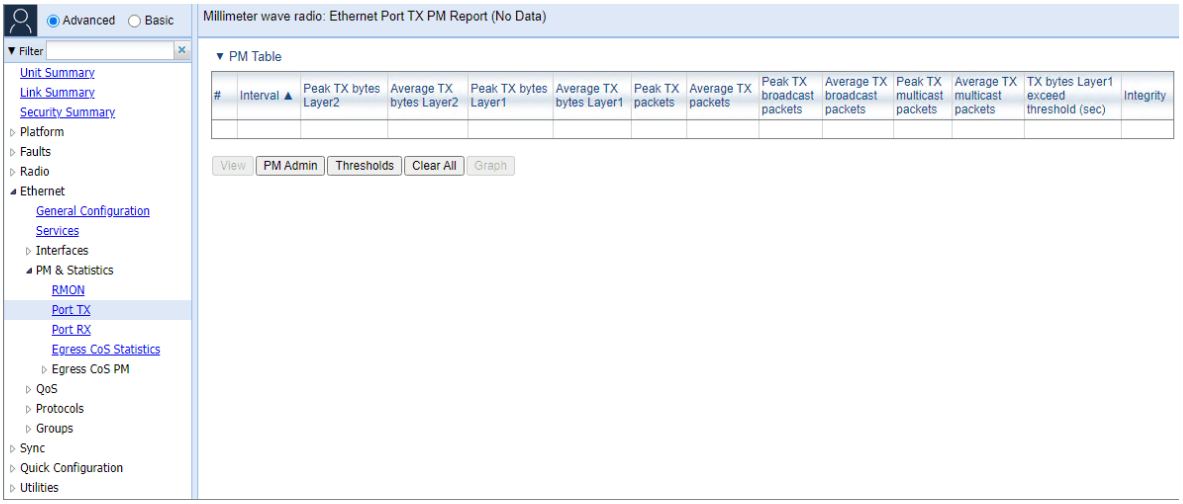
- Displaying Ethernet Port TX PMs
- Enabling or Disabling Gathering of Port TX PM Statistics per Interface
- Setting the Ethernet Port TX Threshold

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 186 *Ethernet Port TX PM Report Page*



Millimeter wave radio: Ethernet Port TX PM Report (No Data)

▼ PM Table

#	Interval ▲	Peak TX bytes Layer2	Average TX bytes Layer2	Peak TX bytes Layer1	Average TX bytes Layer1	Peak TX packets	Average TX packets	Peak TX broadcast packets	Average TX broadcast packets	Peak TX multicast packets	Average TX multicast packets	TX bytes Layer1 exceed threshold (sec)	Integrity

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.

Ethernet TX Port PMs describes the Ethernet TX port PMs.

Table 42 *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... TX bytes... TX Packets... Layer1... Layer2...	Various peak transmission rates (per second) and average transmission rates (per second), both in bytes and in packets, In layer1 and in layer2, for each measured time interval.
Peak... Average... TX packets	Peak transmission rates (per second) and average transmission rates (per second), in packets, for each measured time interval.
Peak... Average... TX broadcast...TX multicast... packets	Various peak transmission rates (per second) and average transmission rates (per second), in broadcast and multicast 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.

Parameter	Definition
	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).

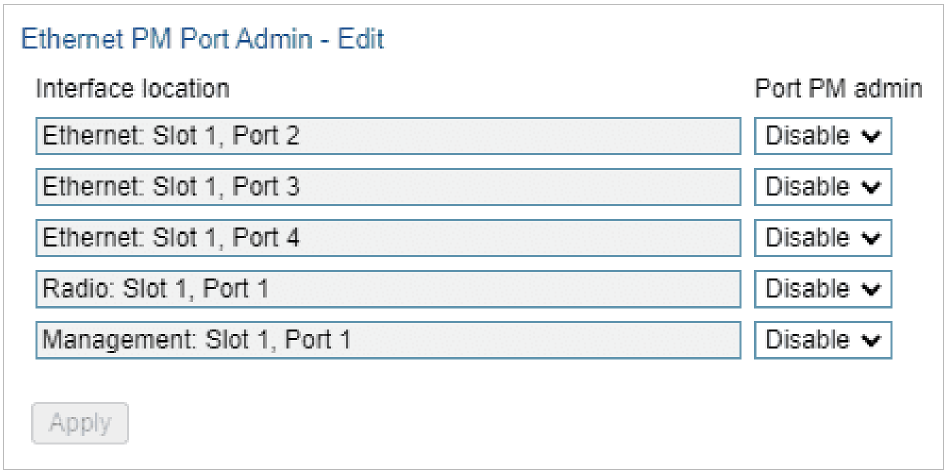
To clear the PMs, click **Clear All**.

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 187 *Ethernet PM Port Admin Page*



Ethernet PM Port Admin - Edit

Interface location	Port PM admin
Ethernet: Slot 1, Port 2	Disable
Ethernet: Slot 1, Port 3	Disable
Ethernet: Slot 1, Port 4	Disable
Radio: Slot 1, Port 1	Disable
Management: Slot 1, Port 1	Disable

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 **Apply**.

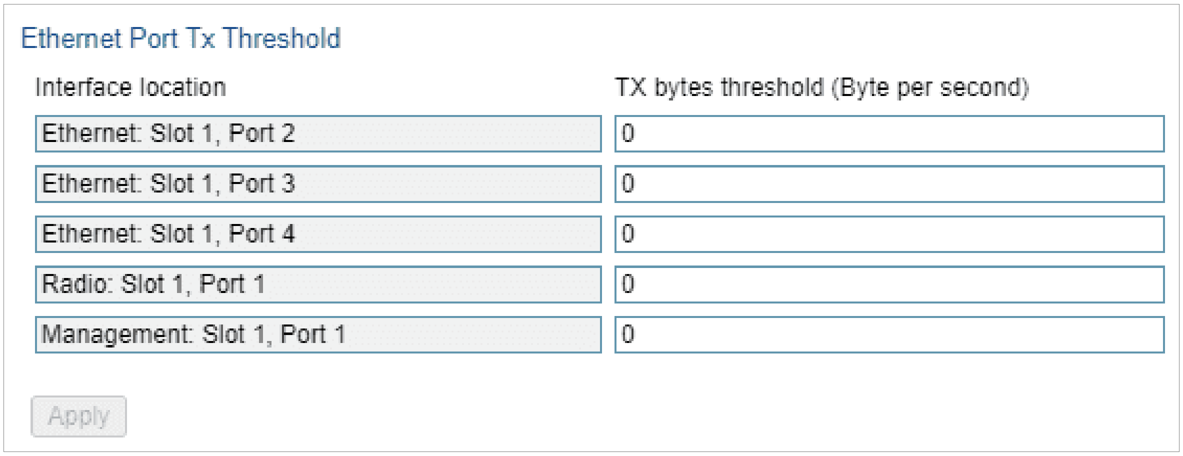
Setting the Ethernet Port TX Threshold

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 **Thresholds**. The Ethernet Port Tx Threshold page opens.

Figure 188 *Ethernet Port Tx Threshold Page (PTP 850EX)*



Ethernet Port Tx Threshold

Interface location	TX bytes threshold (Byte per second)
Ethernet: Slot 1, Port 2	0
Ethernet: Slot 1, Port 3	0
Ethernet: Slot 1, Port 4	0
Radio: Slot 1, Port 1	0
Management: Slot 1, Port 1	0

2. For each interface, you can enter a threshold, in bytes per second, between 0 and 4294967295.
3. Click **Apply**, then **Close**.

Port RX Statistics

The Ethernet Port RX PM report page displays PMs that measure various peak RX rates (per second) and average RX rates (per second), in bytes and in packets, layer1 and layer2, broadcast and multicast, 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:

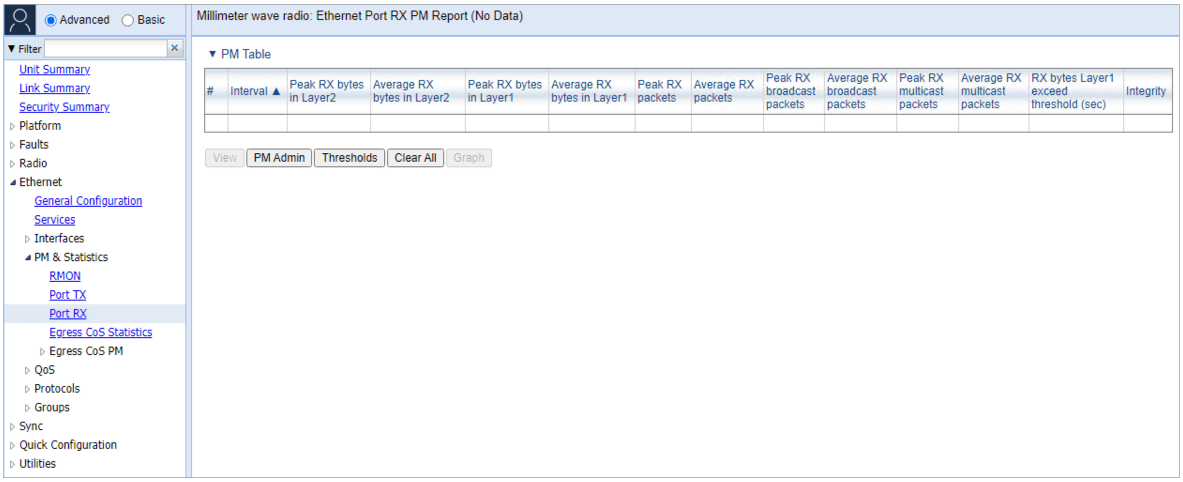
- Displaying Ethernet Port RX PMs
- Enabling or Disabling Gathering of Port RX PM Statistics per Interface
- Setting the Ethernet Port RX Threshold

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 189 *Ethernet Port RX PM Report Page*



Millimeter wave radio: Ethernet Port RX PM Report (No Data)

▼ PM Table

#	Interval ▲	Peak RX bytes in Layer2	Average RX bytes in Layer2	Peak RX bytes in Layer1	Average RX bytes in Layer1	Peak RX packets	Average RX packets	Peak RX broadcast packets	Average RX broadcast packets	Peak RX multicast packets	Average RX multicast packets	RX bytes Layer1 exceed threshold (sec)	Integrity

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**.

Ethernet RX Port PMs describes the Ethernet RX port PMs.

Table 43 *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... RX bytes... RX Packets... Layer1... Layer2...	Various peak RX rates (per second) and average RX rates (per second), both in bytes and in packets, in layer1 and in layer2, for each measured time interval.
Peak... Average... RX packets	Peak RX rates (per second) and average RX rates (per second), in packets, for each measured time interval.
Peak... Average... RX broadcast...RX multicast...packets	Various peak RX rates (per second) and average RX rates (per second), in broadcast and multicast 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.
Integrity	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).

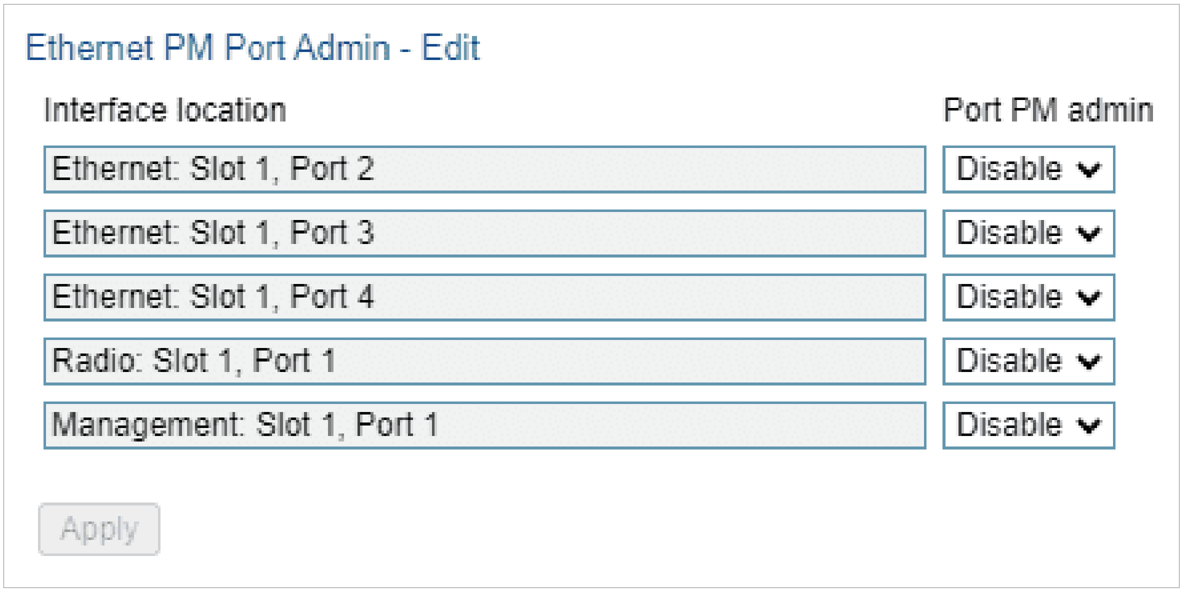
To clear the PMs, click **Clear All**.

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 190 *Ethernet PM Port Admin Page (PTP 850EX)*



Ethernet PM Port Admin - Edit

Interface location	Port PM admin
Ethernet: Slot 1, Port 2	Disable
Ethernet: Slot 1, Port 3	Disable
Ethernet: Slot 1, Port 4	Disable
Radio: Slot 1, Port 1	Disable
Management: Slot 1, Port 1	Disable

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**.

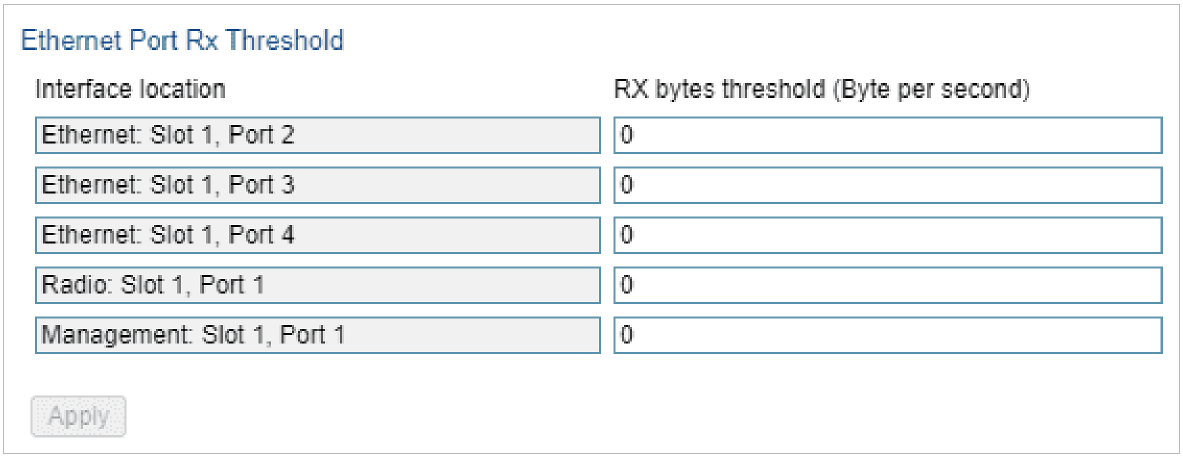
Setting the Ethernet Port RX Threshold

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 **Thresholds**. The Ethernet Port Rx Threshold page opens.

Figure 191 *Ethernet Port Rx Threshold Page (PTP 850EX)*



Ethernet Port Rx Threshold

Interface location	RX bytes threshold (Byte per second)
Ethernet: Slot 1, Port 2	0
Ethernet: Slot 1, Port 3	0
Ethernet: Slot 1, Port 4	0
Radio: Slot 1, Port 1	0
Management: Slot 1, Port 1	0

2. For each interface, you can enter a threshold, in bytes per second, between 0 and 4294967295.
3. Click **Apply**, then **Close**.

Quality of Service (QoS)

This section includes:

- QoS Overview
- Configuring Classification
- Configuring Policers (Rate Metering)
- Configuring Marking
- Configuring WRED
- Configuring Egress Shaping
- Configuring Scheduling
- Configuring the Egress Byte Compensation
- Configuring and Displaying Queue-Level PMs

Note

You can display additional QoS egress PMs and statistics via CLI. For information, see Displaying Egress PMs and Statistics (CLI).

QoS Overview

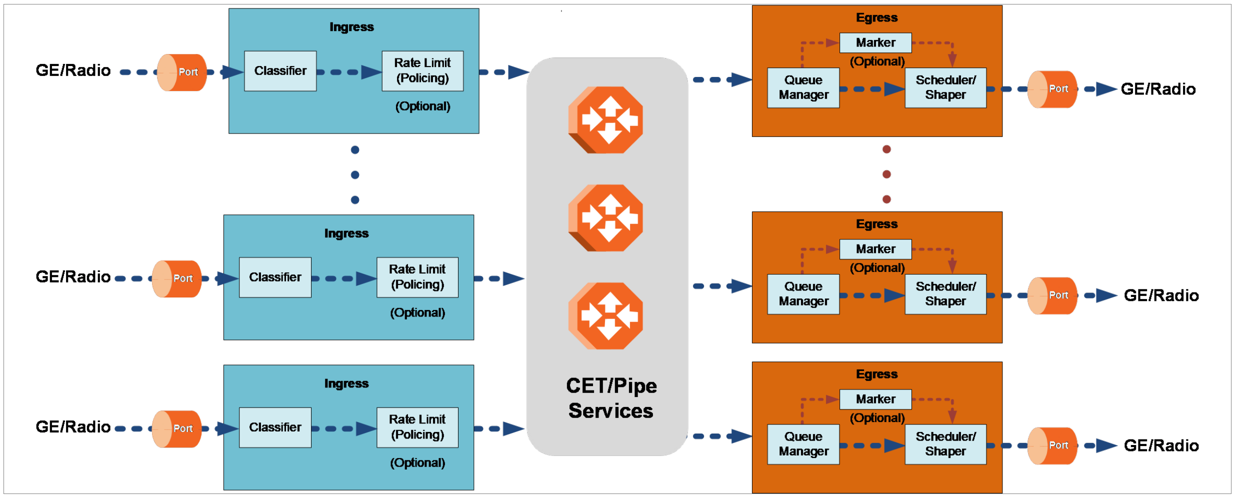
Quality of Service (QoS) deals with the way frames are handled within the switching fabric. QoS is required in order to deal with many different network scenarios, such as traffic congestion, packet availability, and delay restrictions.

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.

QoS Block Diagram 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 192 *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 the interface and service point levels. 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.

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 and per port).
- **Marker** – This mechanism provides the ability to modify priority bits in frames based on the calculated CoS and Color.

Eight transmission queues are provided per port.

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 Ethernet Service Points – Ingress Attributes.
- For instructions how to configure classification at the service level, see Adding an Ethernet Service.

This section includes:

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).

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. Classification priorities depend on the product type.

Classification is performed according to the following priorities:

- Service
- Service Point
- VLAN ID (CLI-only – see Configuring VLAN Classification and Override (CLI))
- 802.1p bits
- MPLS EXP field
- DSCP bits (only considered if MPLS is not present, regardless of trust setting)
- Default interface 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 the required classification is based on 802.1p bits or DSCP 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.

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.

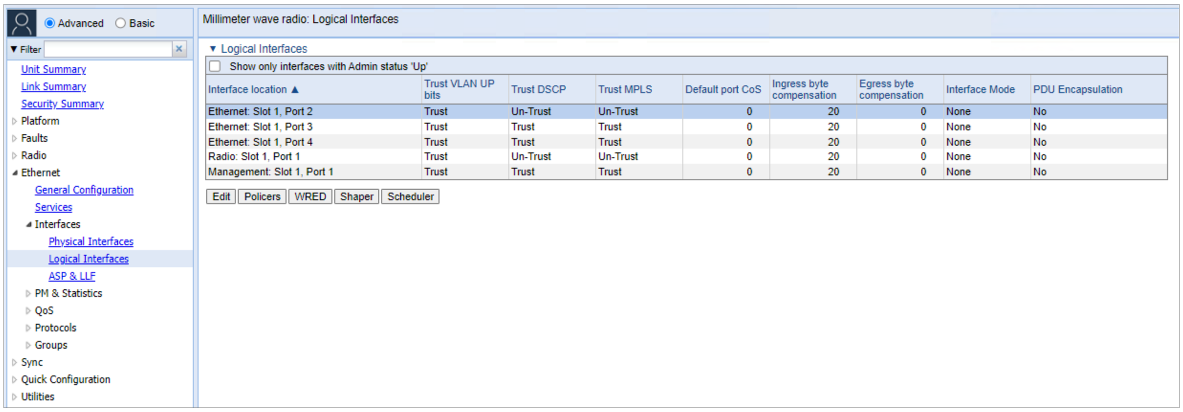
Configuring Ingress Path Classification on a Logical Interface

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 193 *Logical Interfaces Page*



Millimeter wave radio: Logical Interfaces

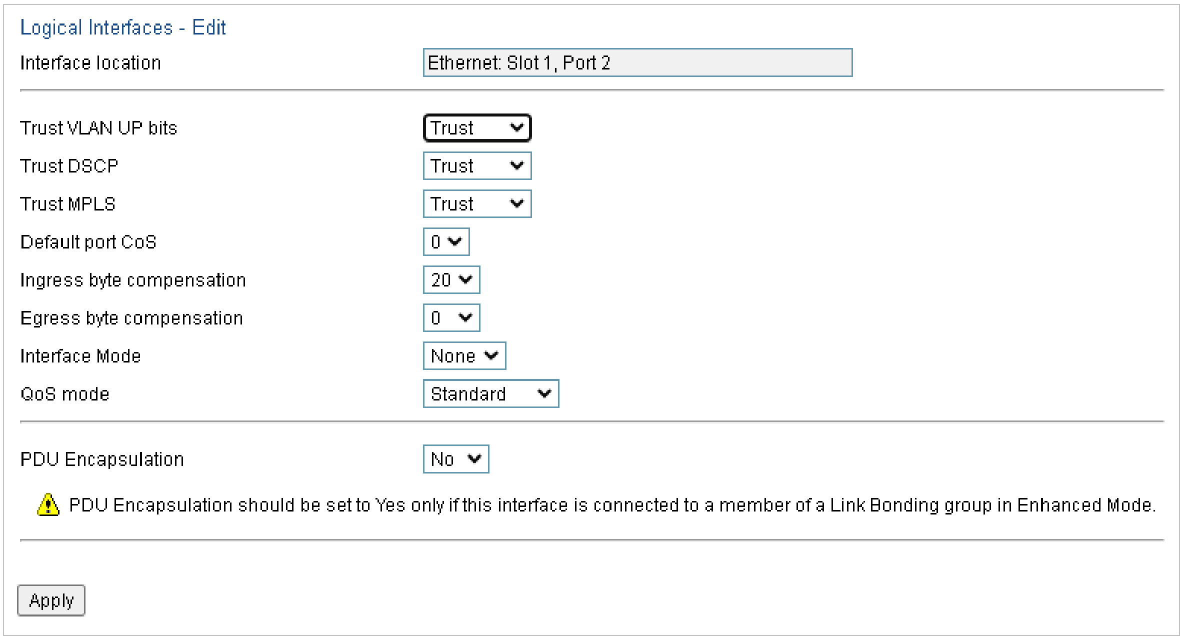
▼ Logical Interfaces

□ Show only interfaces with Admin status 'Up'

Interface location ▲	Trust VLAN UP bits	Trust DSCP	Trust MPLS	Default port CoS	Ingress byte compensation	Egress byte compensation	Interface Mode	PDU Encapsulation
Ethernet: Slot 1, Port 2	Trust	Un-Trust	Un-Trust	0	20	0	None	No
Ethernet: Slot 1, Port 3	Trust	Trust	Trust	0	20	0	None	No
Ethernet: Slot 1, Port 4	Trust	Trust	Trust	0	20	0	None	No
Radio: Slot 1, Port 1	Trust	Un-Trust	Un-Trust	0	20	0	None	No
Management: Slot 1, Port 1	Trust	Trust	Trust	0	20	0	None	No

2. Select the interface you want to configure and click **Edit**. The Logical Interfaces - Edit page opens.\

Figure 194 *Logical Interfaces - Edit Page*



Logical Interfaces - Edit

Interface location: Ethernet: Slot 1, Port 2

Trust VLAN UP bits: Trust

Trust DSCP: Trust

Trust MPLS: Trust

Default port CoS: 0

Ingress byte compensation: 20

Egress byte compensation: 0

Interface Mode: None

QoS mode: Standard

PDU Encapsulation: No

⚠ PDU Encapsulation should be set to Yes only if this interface is connected to a member of a Link Bonding group in Enhanced Mode.

3. Configure the parameters described in Logical Interface Classification Parameters.
4. Click **Apply**, then **Close**.

Note

The **Ingress byte compensation** field is not applicable to PTP 850EX. The **Egress byte compensation** field is described in Configuring the Egress Byte Compensation.

Table 44 *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 have priority over 802.1p Trust Mode, 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.
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. If MPLS EXP priority bits are present, DSCP is not considered regardless of the Trust mode setting and regardless of whether an MPLS match was found. • **Un-Trust** – The interface does not consider DSCP during classification.

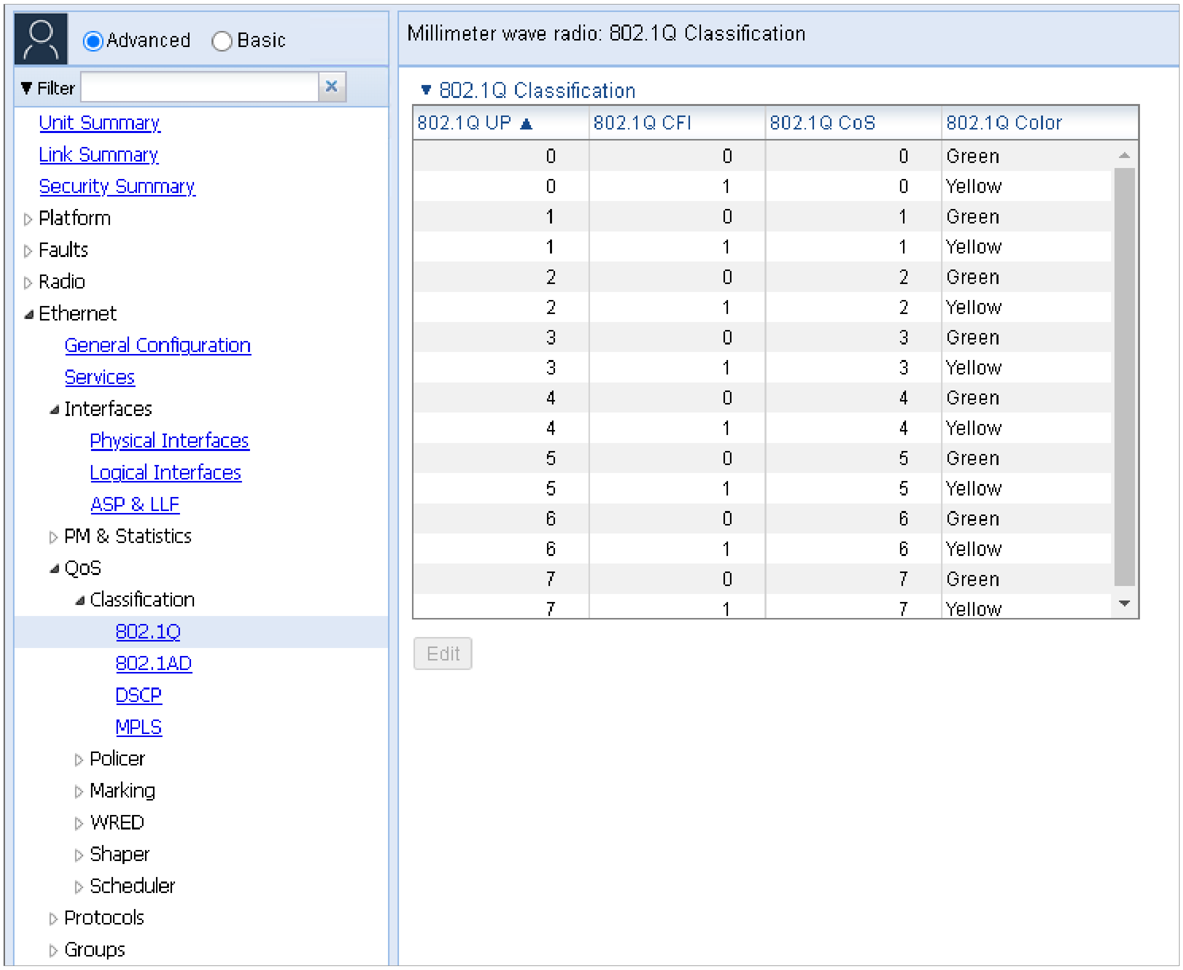
Parameter	Definition
Trust MPLS	Select the interface's trust mode for MPLS bits: • **Trust** – The interface performs QoS and color classification according to a user-configurable table for MPLS EXP to CoS and color classification. • **Un-Trust** – The interface does not consider MPLS bits during classification.
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	Not applicable to PTP 850EX.
Egress Byte Compensation	See Configuring the Egress Byte Compensation.
Interface Mode	Reserved for future use.
QoS Mode	Only **Standard** is supported.
PDU Encapsulation	Should be set to **No**.

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 195 *802.1Q Classification Page*



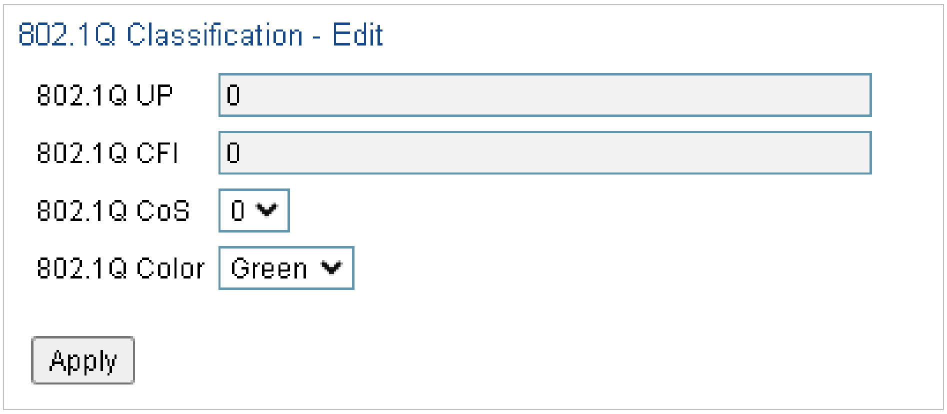
Millimeter wave radio: 802.1Q Classification

802.1Q Classification

802.1Q UP ▲	802.1Q CFI	802.1Q CoS	802.1Q Color
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

2. Select the row you want to modify and click **Edit**. The 802.1Q Classification – Edit page opens.

Figure 196 *802.1Q Classification - Edit Page*



802.1Q Classification - Edit

802.1Q UP	0
802.1Q CFI	0
802.1Q CoS	0
802.1Q Color	Green

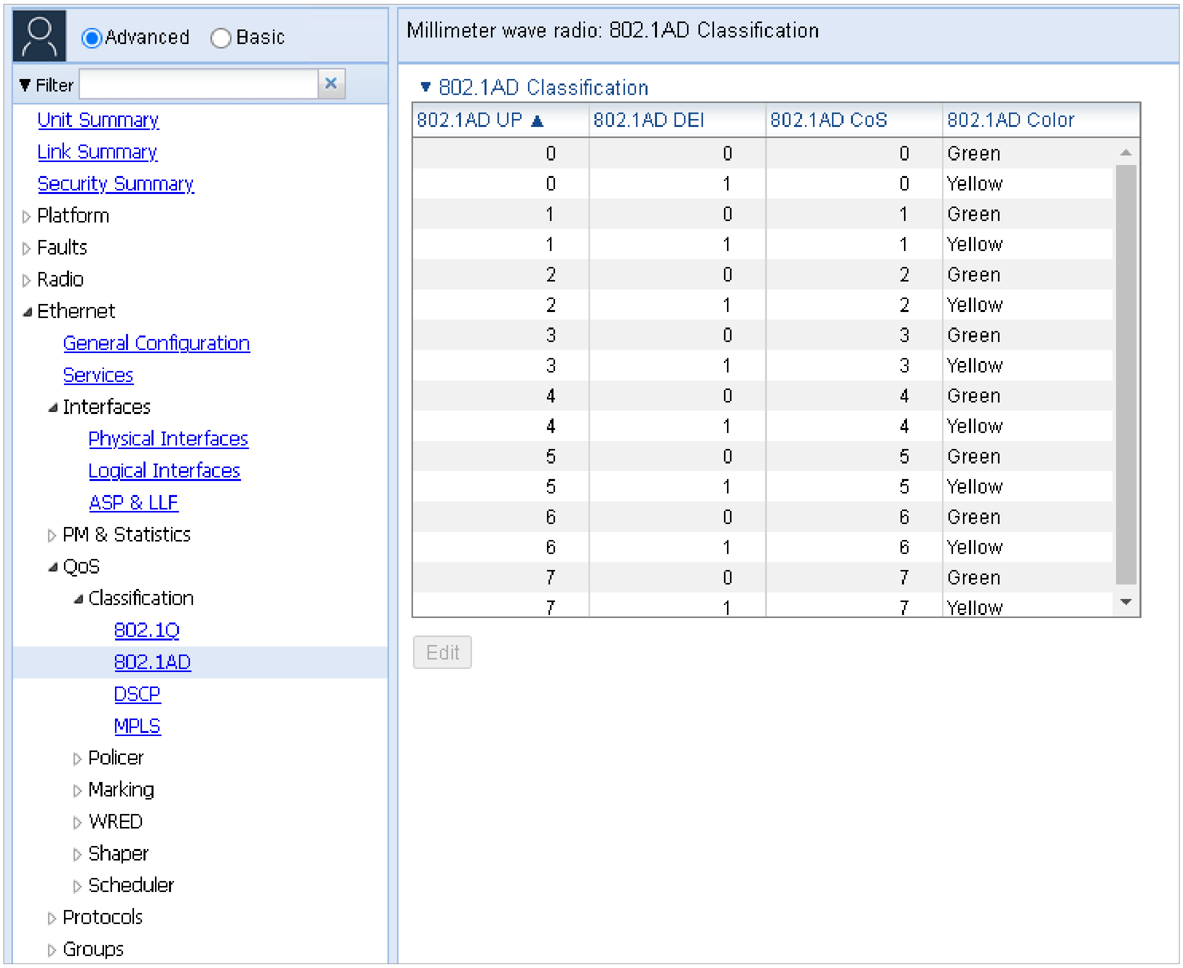
3. Modify the parameters you want to change:
    - **802.1Q UP** – Read-only. The User Priority (UP) bit to be mapped.
    - **802.1Q CFI** – Read-only. The CFI bit to be mapped.
    - **802.1Q CoS** – The CoS assigned to frames with the designated UP and CFI.
    - **802.1Q Color** – The Color assigned to frames with the designated UP and CFI.
4. Click **Apply**, then **Close**.

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 197 *802.1AD Classification Page*



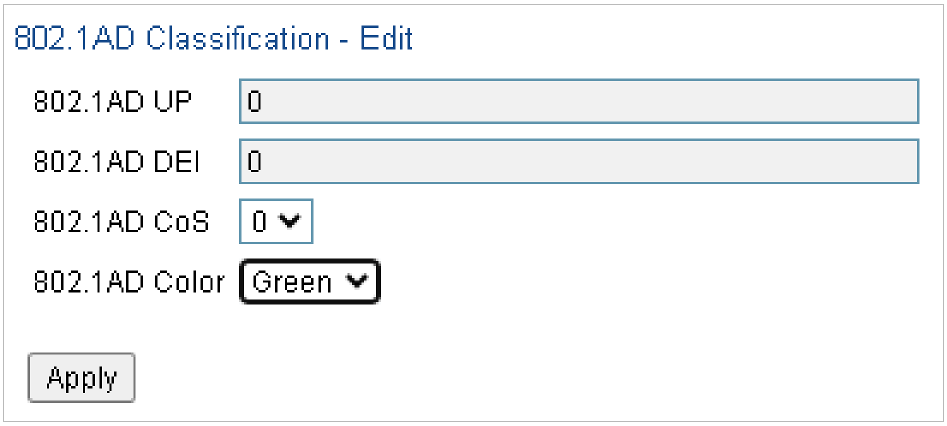
Millimeter wave radio: 802.1AD Classification

802.1AD Classification

802.1AD UP ▲	802.1AD DEI	802.1AD CoS	802.1AD Color
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

2. Select the row you want to modify and click **Edit**. The 802.1AD Classification - Edit page opens.

Figure 198 *802.1AD Classification - Edit Page*



802.1AD Classification - Edit

802.1AD UP: 0

802.1AD DEI: 0

802.1AD CoS: 0

802.1AD Color: Green

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**.

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:

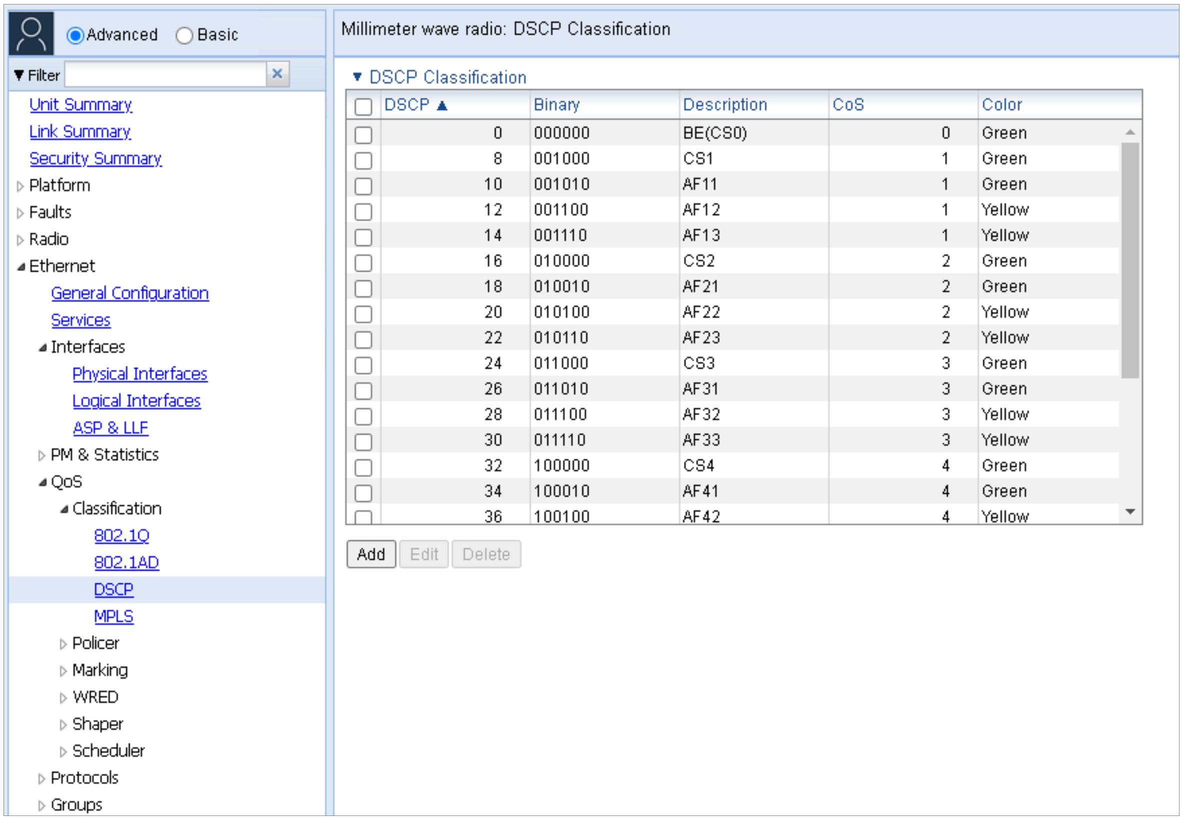
- **DSCP** – The DSCP value to be mapped.
- **Binary** – The binary representation of the DSCP value.
- **Description** – A description of the DSCP value.
- **CoS** – The CoS assigned to frames with the designated DSCP value.
- **Color** – The Color assigned to frames with the designated DSCP value.

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 64.

To modify the classification criteria for DSCPs:

1. Select **Ethernet** > **QoS** > **Classification** > **DSCP**. The DSCP Classification page opens.

Figure 199 *DSCP Classification Page*



● Advanced ○ Basic

Filter

- Unit Summary
- Link Summary
- Security Summary
- Platform
- Faults
- Radio
- Ethernet
  - General Configuration
  - Services
  - Interfaces
    - Physical Interfaces
    - Logical Interfaces
    - ASP & LLF
  - PM & Statistics
  - QoS
    - Classification
      - 802.1Q
      - 802.1AD
      - DSCP
      - MPLS
    - Policer
    - Marking
    - WRED
    - Shaper
    - Scheduler
  - Protocols
  - Groups

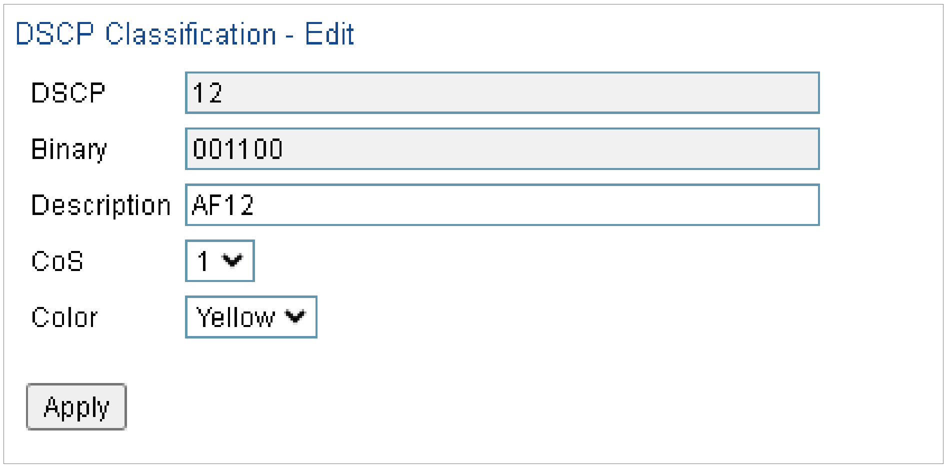
Millimeter wave radio: DSCP Classification

DSCP Classification

□	DSCP ▲	Binary	Description	CoS	Color
□	0	000000	BE(CS0)	0	Green
□	8	001000	CS1	1	Green
□	10	001010	AF11	1	Green
□	12	001100	AF12	1	Yellow
□	14	001110	AF13	1	Yellow
□	16	010000	CS2	2	Green
□	18	010010	AF21	2	Green
□	20	010100	AF22	2	Yellow
□	22	010110	AF23	2	Yellow
□	24	011000	CS3	3	Green
□	26	011010	AF31	3	Green
□	28	011100	AF32	3	Yellow
□	30	011110	AF33	3	Yellow
□	32	100000	CS4	4	Green
□	34	100010	AF41	4	Green
□	36	100100	AF42	4	Yellow

2. Select the row you want to modify and click **Edit**. The DSCP Classification - Edit page opens.

Figure 200 *DSCP Classification - Edit Page*



DSCP Classification - Edit

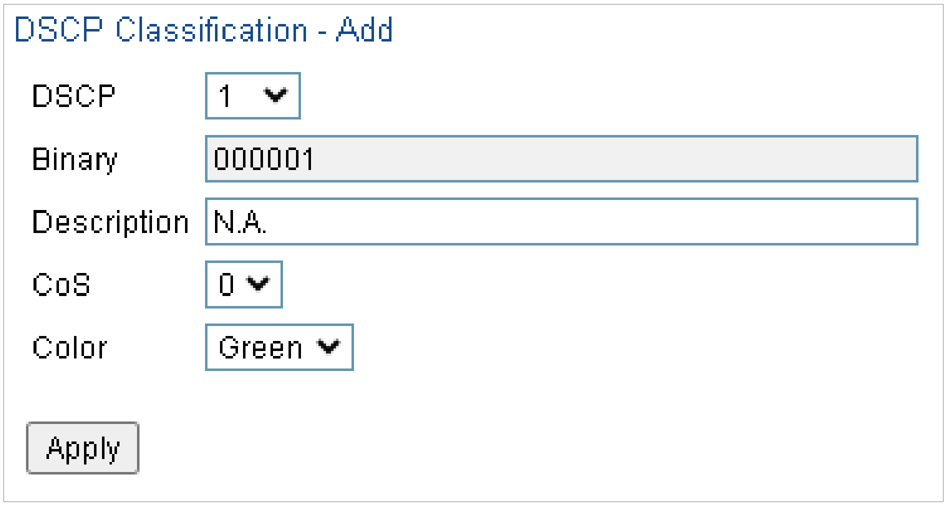
DSCP	12
Binary	001100
Description	AF12
CoS	1
Color	Yellow

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** –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 (DSCP Classification Page).
2. Click **Add**. The DSCP Classification - Add page opens.

Figure 201 *DSCP Classification - Add Page*



DSCP Classification - Add

DSCP	1
Binary	000001
Description	N.A.
CoS	0
Color	Green

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 (DSCP Classification Page).
2. Select the row you want to modify and click **Delete**. A confirmation window opens.
3. Click **OK**. The entry is deleted.

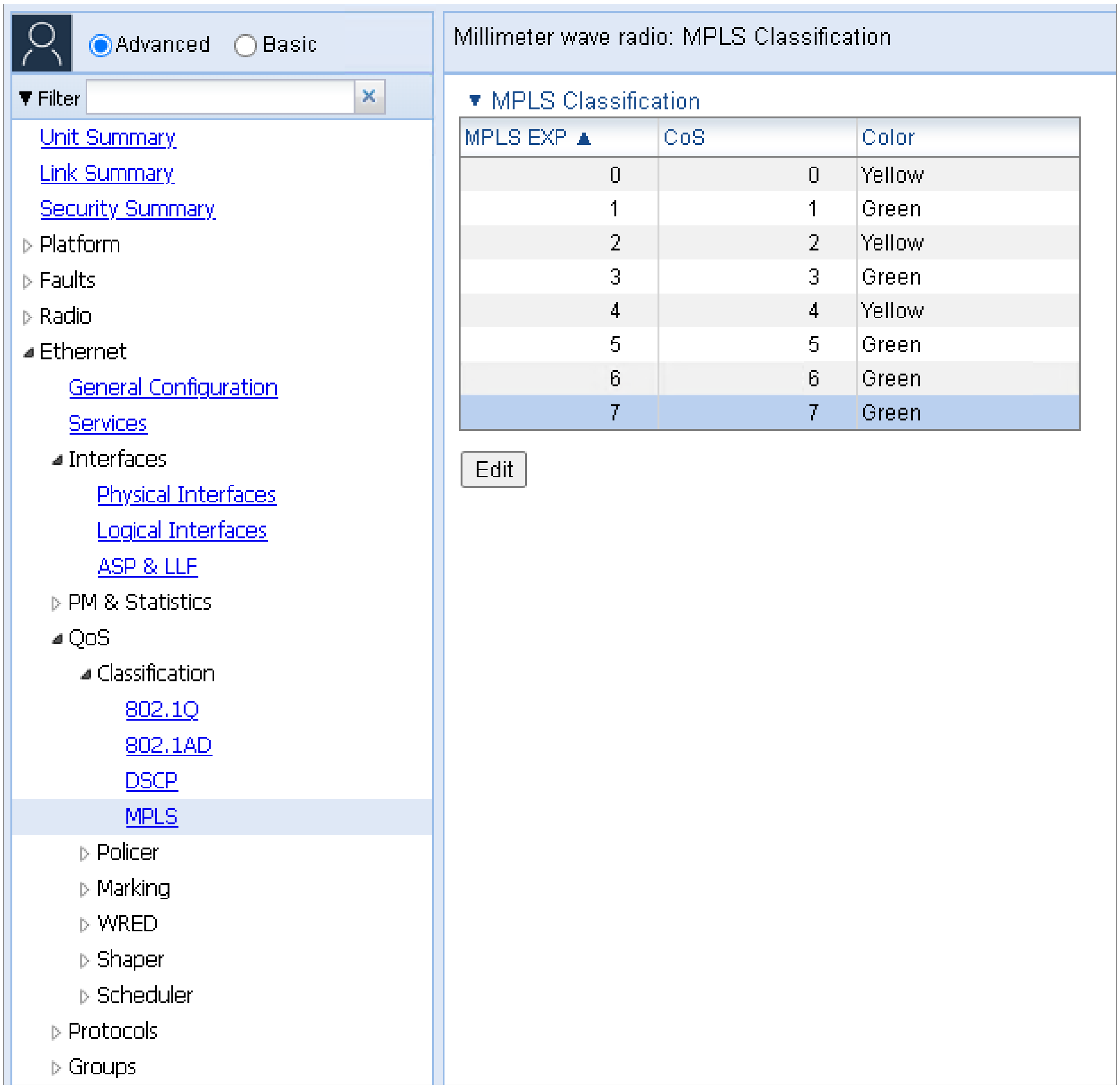
Modifying the MPLS EXP Bit Classification Table

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 202 *MPLS Classification Page*



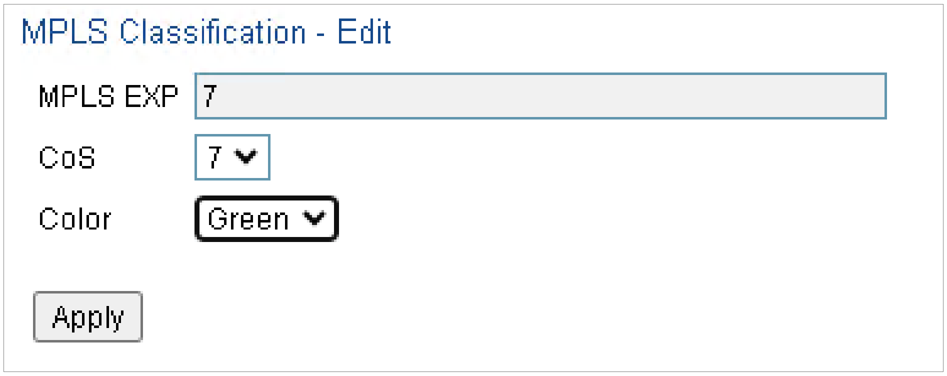
Millimeter wave radio: MPLS Classification

MPLS Classification

MPLS EXP ▲	CoS	Color
0	0	Yellow
1	1	Green
2	2	Yellow
3	3	Green
4	4	Yellow
5	5	Green
6	6	Green
7	7	Green

2. Select the row you want to modify and click **Edit**. The MPLS Classification - Edit page opens.

Figure 203 *MPLS Classification - Edit Page*



MPLS Classification - Edit

MPLS EXP: 7

CoS: 7

Color: Green

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**.

Configuring Policers (Rate Metering)

This section includes:

- Policer (Rate Metering) Overview
- Configuring Policer Profiles
- Assigning Policers to Interfaces

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 must be configured via CLI. See Configuring Policers (Rate Metering) (CLI).

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.

Configuring Policer Profiles

This section includes:

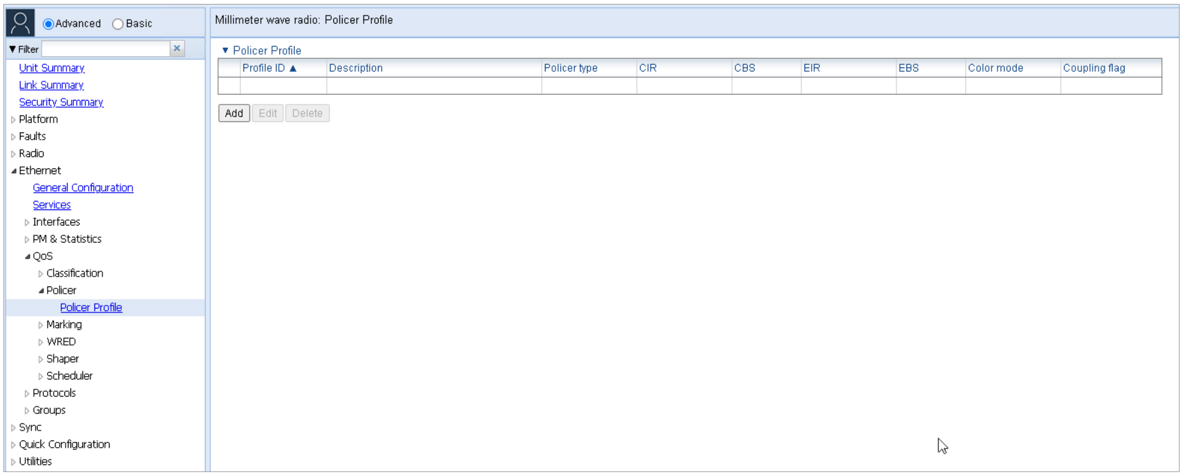
- Adding a Policer Profile
- Editing a Policer Profile
- Deleting a Policer Profile

Adding a Policer Profile

To add a policer profile:

1. Select **Ethernet** > **QoS** > **Policer** > **Policer Profile**. The Policer Profile page opens.

   Figure 204 *Policer Profile Page*



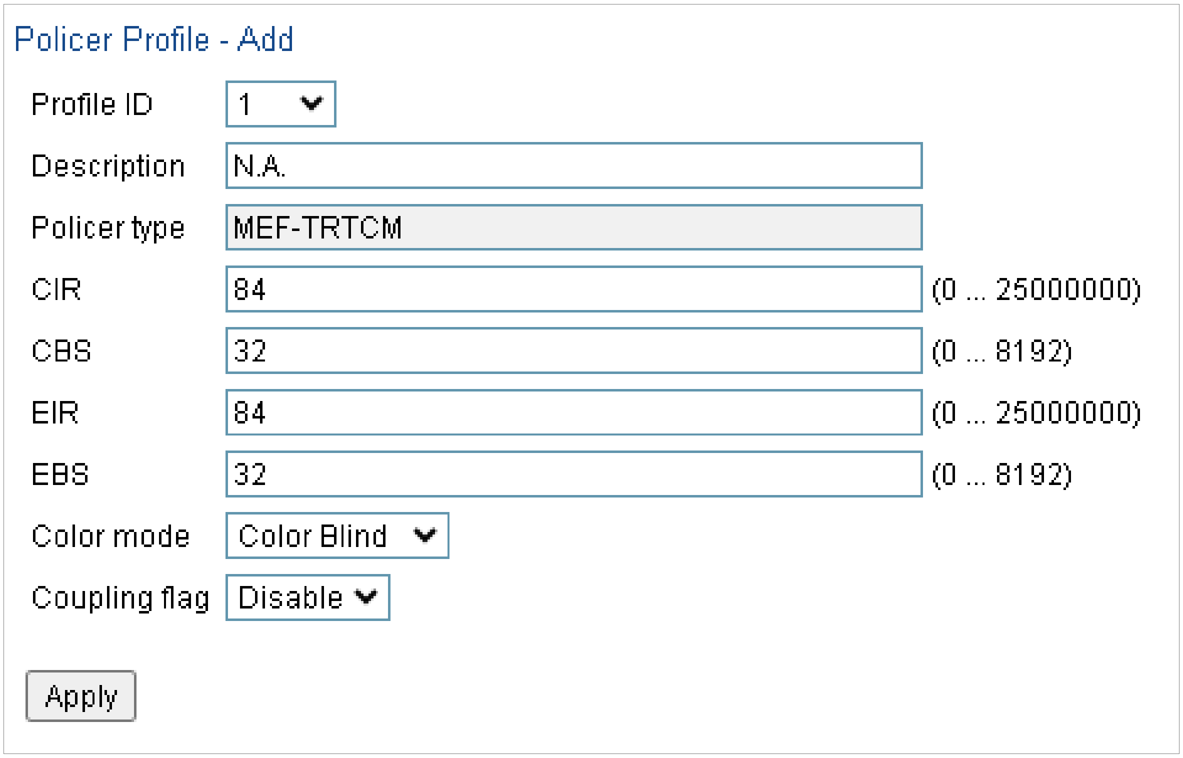
Millimeter wave radio: Policer Profile

▼ Policer Profile

	Profile ID ▲	Description	Policer type	CIR	CBS	EIR	EBS	Color mode	Coupling flag

2. Click Add. The Policer Profile - Add page opens.

Figure 205 *Policer Profile - Add Page*



Policer Profile - Add

Profile ID	1	
Description	N.A.	
Policer type	MEF-TRTCM	
CIR	84	(0 ... 25000000)
CBS	32	(0 ... 8192)
EIR	84	(0 ... 25000000)
EBS	32	(0 ... 8192)
Color mode	Color Blind	
Coupling flag	Disable	

3. Configure the profile’s parameters. See Policer Profile Parameters for a description of the policer profile parameters.

4. Click **Apply**, then **Close**.

Table 45 *Policer Profile Parameters*

Parameter	Definition
Profile ID	A unique ID for the policer profile. You can choose any unused value from 1 to 250. 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 kbps. Permitted values are 0 through 25,000,000 kbps. If the value is 0, all incoming CIR traffic is dropped. The default value is 84.
CBS	Enter the Committed Burst Rate (CBR) for the policer, in Kbytes. Permitted values are 0 through 8192 Kbytes. The default value is 32.
EIR	Enter the Excess Information Rate (EIR) for the policer, in kbps. Permitted values are 0 through 25,000,000. If the value is 0, all incoming EIR traffic is dropped. The default value is 84.

Parameter	Definition
EBS	Enter the Excess Burst Rate (EBR) for the policer, in Kbytes. Permitted values are 0 through 8192 Kbytes. The default value is 32.
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 (Policer Profile - Add Page). 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:

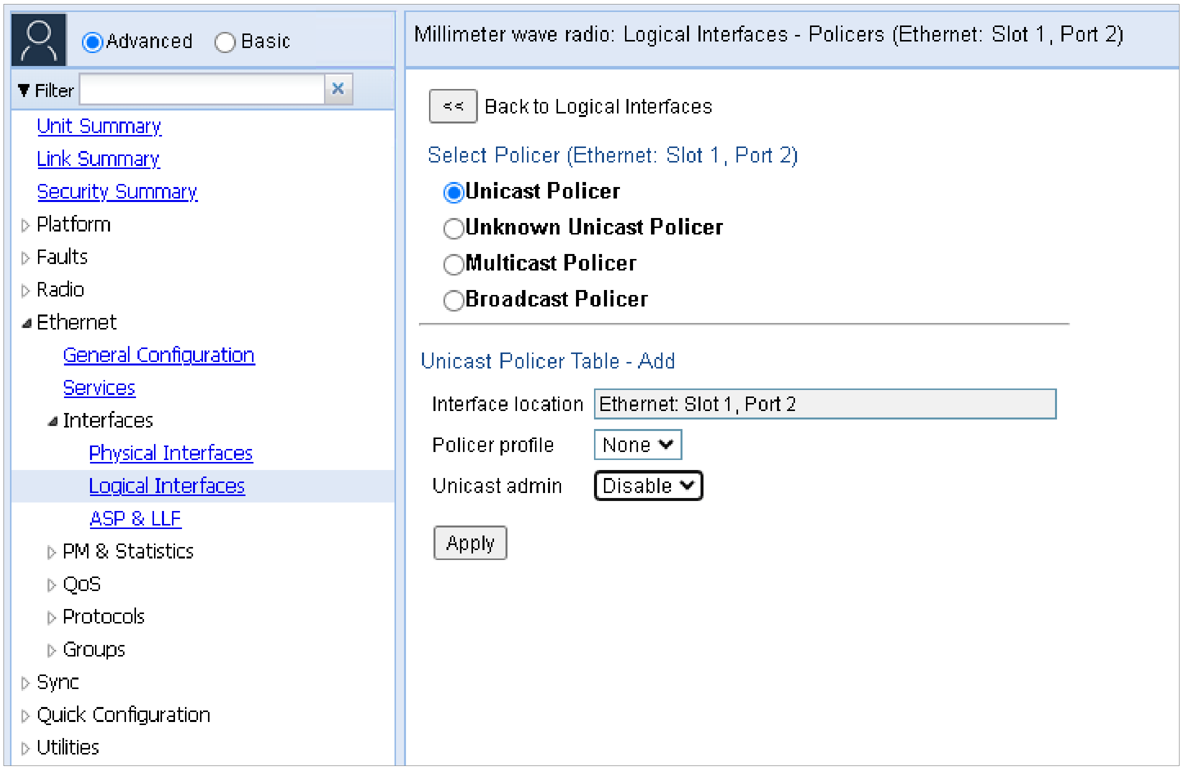
1. Select the profiles in the Policer Profile table or select all the profiles by selecting the check box in the top row.
2. Click **Delete**. The profiles are deleted.

Assigning Policers to Interfaces

To assign policers to a logical interface:

1. Select Ethernet > Interfaces > Logical Interfaces. The Logical Interfaces page opens (Logical Interfaces Page).
2. Select the interface in the Ethernet Logical Port Configuration table and click Policers. The Policers page opens.

Figure 206 *Logical Interfaces – Policers Page – Unicast Policer (Default)*



Millimeter wave radio: Logical Interfaces - Policers (Ethernet: Slot 1, Port 2)

Select Policer (Ethernet: Slot 1, Port 2)

● **Unicast Policer**
○ **Unknown Unicast Policer**
○ **Multicast Policer**
○ **Broadcast Policer**

Unicast Policer Table - Add

Interface location	Ethernet: Slot 1, Port 2
Policer profile	None
Unicast admin	Disable

For a logical interface, you can assign policers to the following traffic flows:

- Unicast Policer
- Unknown Unicast Policer
- Multicast Policer
- Broadcast Policer

Assigning Unicast Policers

To assign a policer for unicast traffic to a logical interface:

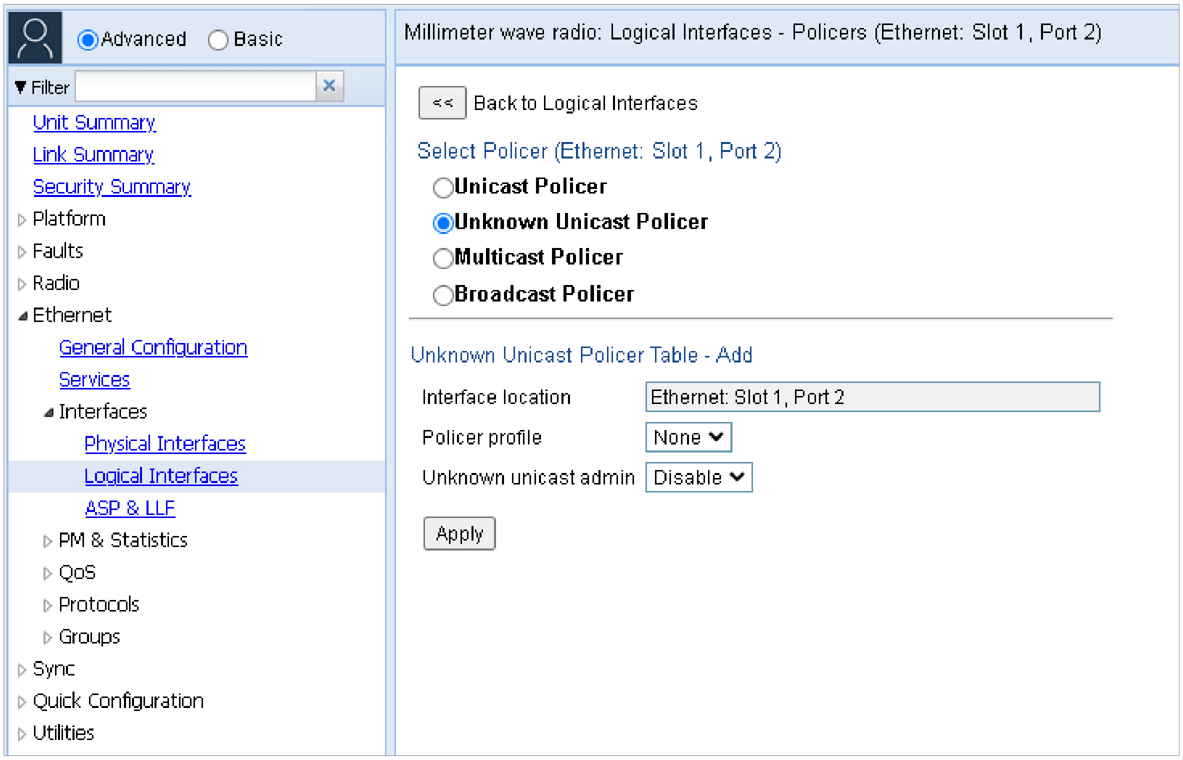
1. Select **Ethernet** > **Interfaces** > **Logical Interfaces**. The Logical Interfaces page opens (Logical Interfaces Page).
2. Select the interface in the Ethernet Logical Port Configuration Table and click **Policers**. The Policers page opens. By default, the Policers page opens to the Unicast Policer table (Logical Interfaces – Policers Page – Unicast Policer (Default)).
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 (Logical Interfaces Page).
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 (Logical Interfaces – Policers Page – Unicast Policer (Default)).
3. Select **Unknown Unicast Policer**. The Unknown Unicast Policer table appears.

Figure 207 *Logical Interfaces – Policers Page – Unknown Unicast Policer*



Millimeter wave radio: Logical Interfaces - Policers (Ethernet: Slot 1, Port 2)

<< Back to Logical Interfaces

Select Policer (Ethernet: Slot 1, Port 2)

○ Unicast Policer
● Unknown Unicast Policer
○ Multicast Policer
○ Broadcast Policer

Unknown Unicast Policer Table - Add

Interface location	Ethernet: Slot 1, Port 2
Policer profile	None
Unknown unicast admin	Disable

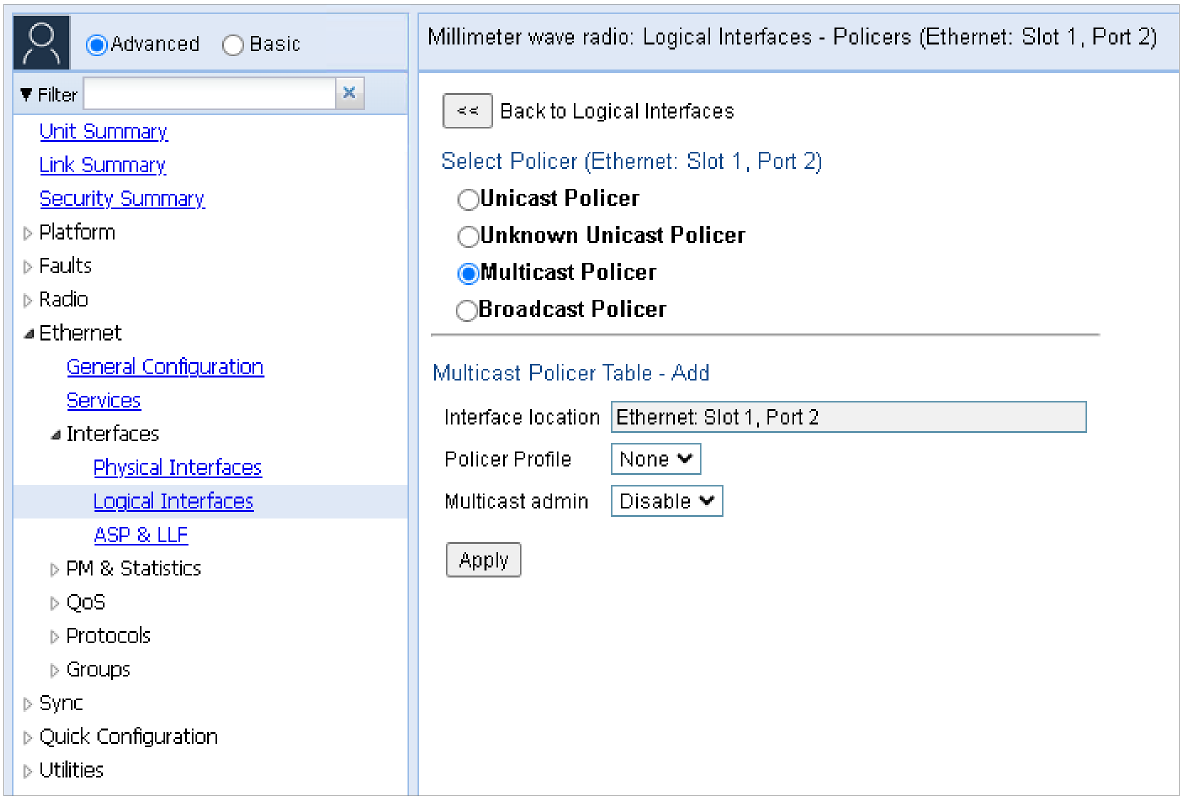
4. In the **Policer profile** field, select a profile from the policer profiles defined in the system. The **Policer profile** drop-down list includes the ID and description of all defined profiles.
5. In the **Unknown unicast admin** field, select **Enable** to enable policing on unknown unicast traffic flows from the logical interface, or **Disable** to disable policing on unknown unicast traffic flows from the logical interface.
6. Click **Apply**.

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 (Logical Interfaces Page).
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 (Logical Interfaces – Policers Page – Unicast Policer (Default)).
3. Select **Multicast Policer**. The Multicast Policer table appears.

Figure 208 *Logical Interfaces – Policers Page – Multicast Policer*



Millimeter wave radio: Logical Interfaces - Policers (Ethernet: Slot 1, Port 2)

Select Policer (Ethernet: Slot 1, Port 2)

○ **Unicast Policer**
○ **Unknown Unicast Policer**
● **Multicast Policer**
○ **Broadcast Policer**

Multicast Policer Table - Add

Interface location	Ethernet: Slot 1, Port 2
Policer Profile	None
Multicast admin	Disable

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**.

Assigning Broadcast Policers

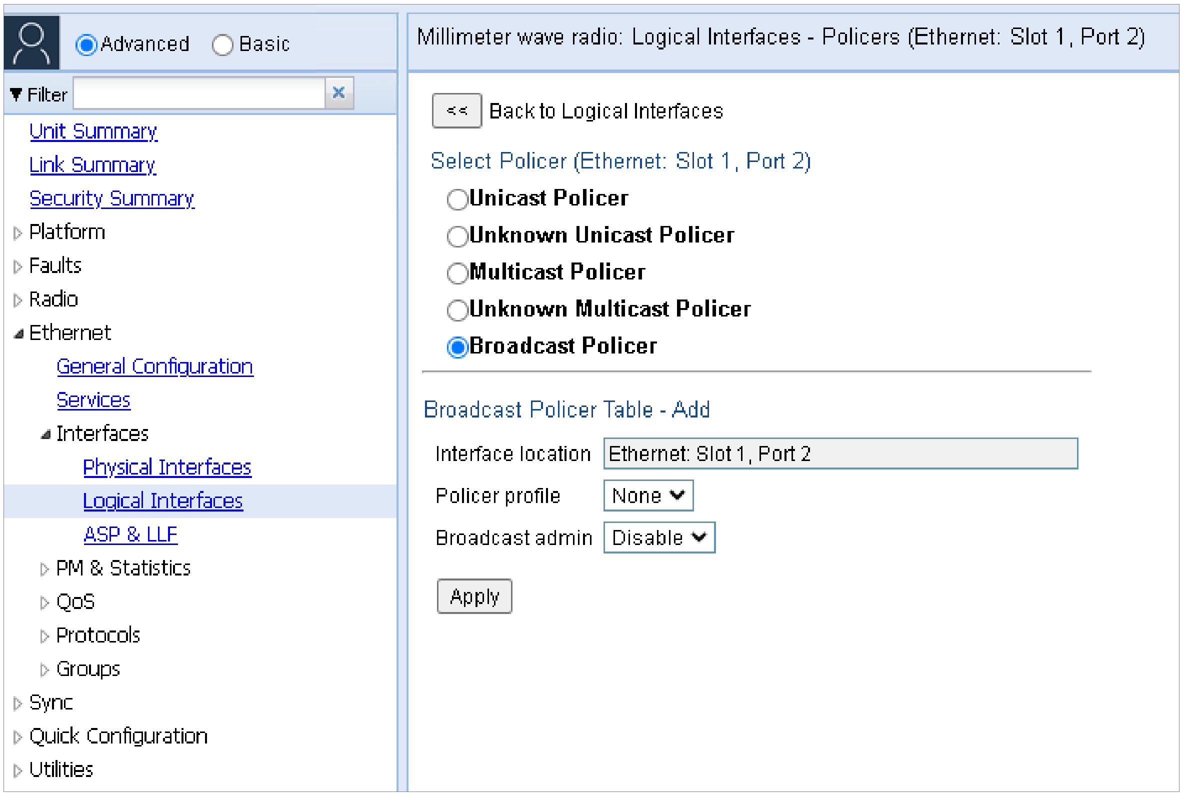
To assign a policer for broadcast traffic to a logical interface:

1. Select **Ethernet** > **Interfaces** > **Logical Interfaces**. The Logical Interfaces page opens (Logical Interfaces Page).
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 (Logical Interfaces –

Policers Page – Unicast Policer (Default)).

3. Select **Broadcast Policer**. The Broadcast Policer table appears.

Figure 209 *Logical Interfaces – Policers Page – Broadcast Policer*



Millimeter wave radio: Logical Interfaces - Policers (Ethernet: Slot 1, Port 2)

Select Policer (Ethernet: Slot 1, Port 2)

○ Unicast Policer
○ Unknown Unicast Policer
○ Multicast Policer
○ Unknown Multicast Policer
● Broadcast Policer

Broadcast Policer Table - Add

Interface location	Ethernet: Slot 1, Port 2
Policer profile	None
Broadcast admin	Disable

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**.

Configuring Marking

This section includes:

- Marking Overview
- Enabling Marking
- Modifying the Marking Table

Marking Overview

Marking refers to the ability to overwrite the outgoing priority bits and Color of the outer VLAN of the egress frame. Marking mode is only applied if the outer frame is S-VLAN and S-VLAN CoS preservation is disabled, or if the outer frame is C-VLAN and C-VLAN CoS preservation is disabled. If outer VLAN preservation is enabled for the relevant outer VLAN, the egress CoS and Color are the same as the CoS and Color of the frame when it ingressed into the switching fabric.

Marking is performed according to a global table that maps CoS and Color values to the 802.1Q UP and 802.1AD UP bits and maps Color values to the DEI or CFI bits. If Marking is enabled on a service point, the CoS and Color of frames egressing the service via that service point are overwritten according to this global mapping table.

If marking and CoS preservation for the relevant outer VLAN are both disabled, marking is applied according to the Green frame values in the global marking table.

If CoS preservation is enabled, an added VLAN always has UP and DEI set to 0.

Enabling Marking

Marking is enabled and disabled on the service point level. See Ethernet Service Points – Egress Attributes.

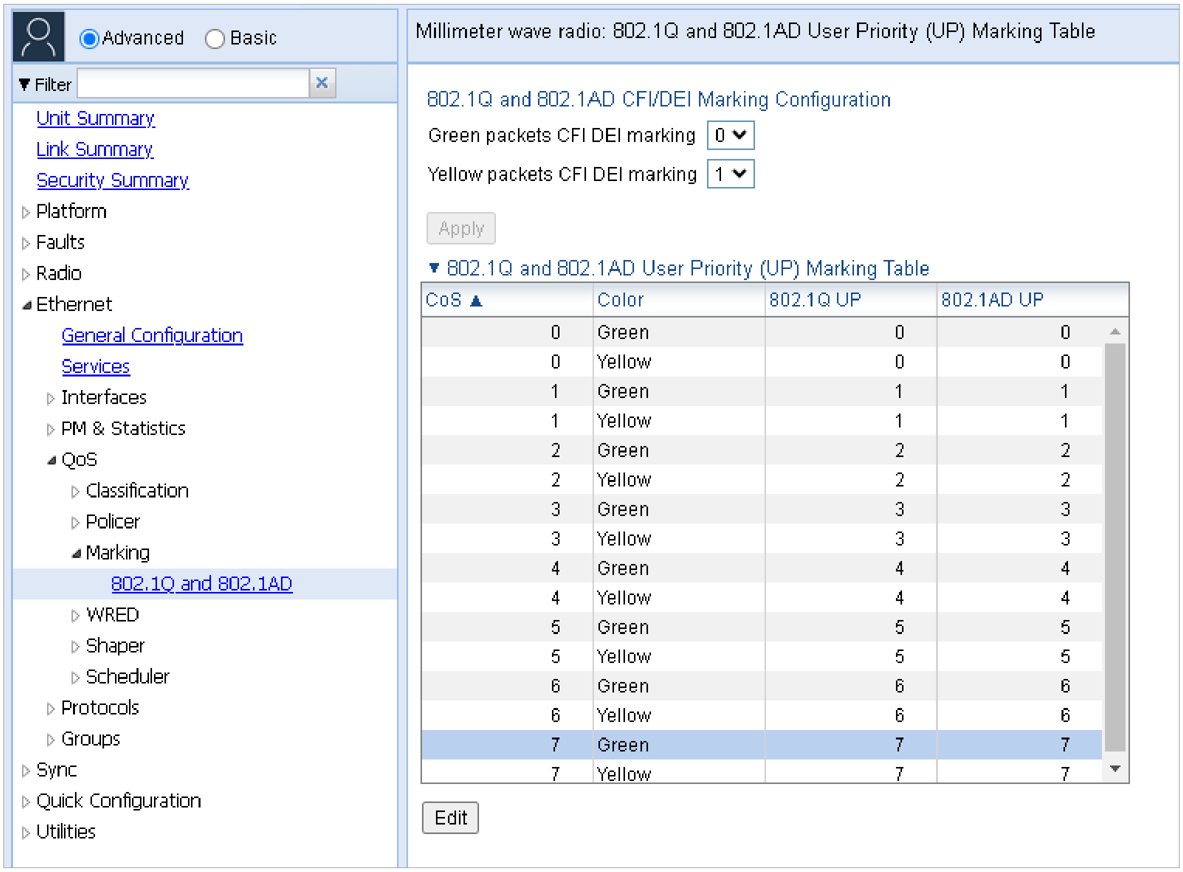
Modifying the Marking Table

The 802.1Q and 802.1AD User Priority (UP) Marking table enables you to modify the mapping of CoS and Color to UP bits and the mapping of Color to CFI/DEI bits. The mapping is implemented when Marking is enabled.

To modify CFI/DEI Marking:

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 210 *802.1Q Marking Page*



Millimeter wave radio: 802.1Q and 802.1AD User Priority (UP) Marking Table

802.1Q and 802.1AD CFI/DEI Marking Configuration

Green packets CFI DEI marking: 0

Yellow packets CFI DEI marking: 1

▼ 802.1Q and 802.1AD User Priority (UP) Marking Table

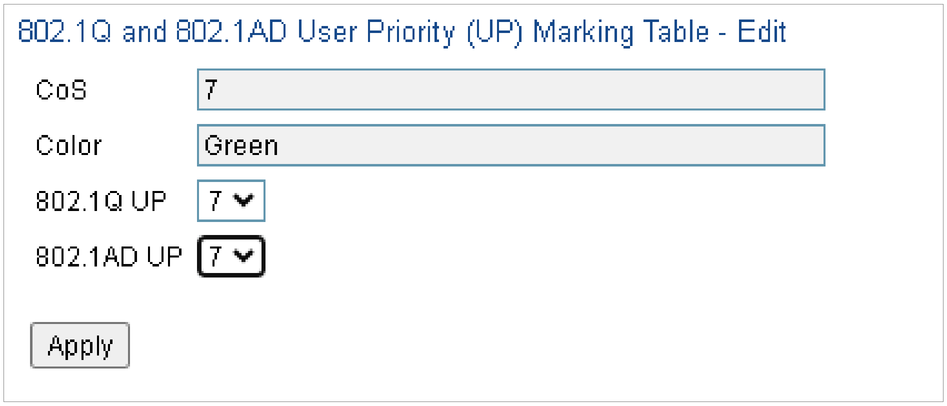
CoS ▲	Color	802.1Q UP	802.1AD UP
0	Green	0	0
0	Yellow	0	0
1	Green	1	1
1	Yellow	1	1
2	Green	2	2
2	Yellow	2	2
3	Green	3	3
3	Yellow	3	3
4	Green	4	4
4	Yellow	4	4
5	Green	5	5
5	Yellow	5	5
6	Green	6	6
6	Yellow	6	6
7	Green	7	7
7	Yellow	7	7

2. In the **Green packets CFI/DEI marking** field, select 0 or 1.
3. In the **Yellow packets CFI/DEI marking** field, select 0 or 1.
4. Click **Apply**.

To modify the 802.1Q and 802.1AD User Priority (UP) Marking table:

1. 802.1Q Marking page, select the row you want to modify and click **Edit**. The 802.1Q Marking - Edit page opens.

Figure 211 *802.1Q Marking - Edit Page*



802.1Q and 802.1AD User Priority (UP) Marking Table - Edit

CoS: 7

Color: Green

802.1Q UP: 7

802.1AD UP: 7

2. Enter the new 802.1Q UP and 802.1Q CFI values.
3. Click **Apply**, then **Close**.

Configuring WRED

This section includes:

- WRED Overview
- Configuring WRED Profiles
- Assigning WRED Profiles to Queues

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.
- 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.

TBD12.8.5For Ethernet ports:

- All memory is shared among all the queues
- There is no guaranteed minimum queue size
- The default maximum queue size is 128 KB (set by the default WRED profile)
- The maximum queue size can be 1.25 MB (regardless of the WRED setting)
- The maximum queue size is not guaranteed and depends on the traffic load

For radio ports, queue size can be configured up to a maximum of 8 MB.

TBD12.8With respect to queue size, note the following:

- All memory is shared among all the queues
- There is no guaranteed minimum queue size
- The default maximum queue size is 128 KB (set by the default WRED profile)
- The maximum queue size can be 1.25 MB (regardless of the WRED setting)
- The maximum queue size is not guaranteed and depends on the traffic load

Configuring WRED Profiles

This section includes:

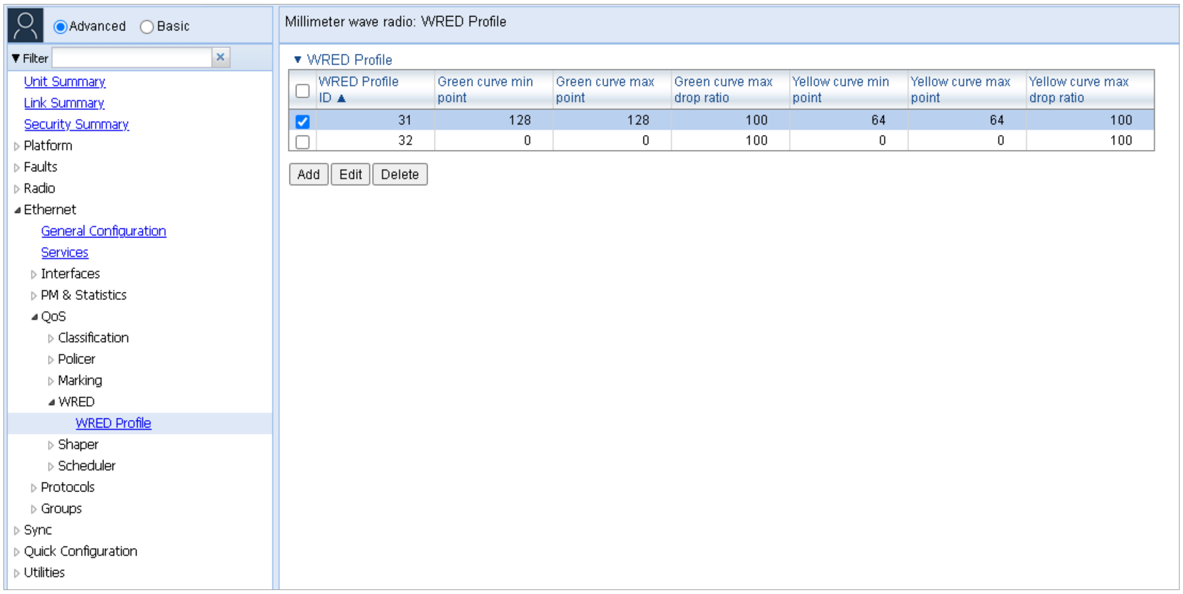
- Adding a WRED Profile
- Editing a WRED Profile
- Deleting a WRED Profile

Adding a WRED Profile

To add a WRED profile:

1. Select **Ethernet** > **QoS** > **WRED** > **WRED Profile**. The WRED Profile page opens.

Figure 212 *WRED Profile Page*



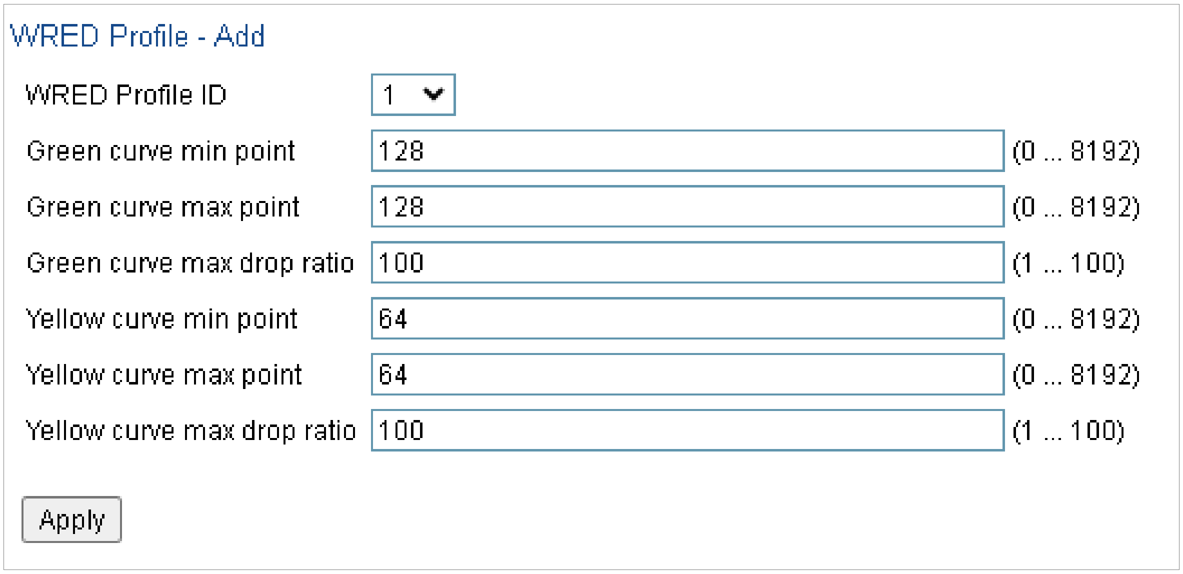
Millimeter wave radio: WRED Profile

WRED Profile

□	WRED Profile ID ▲	Green curve min point	Green curve max point	Green curve max drop ratio	Yellow curve min point	Yellow curve max point	Yellow curve max drop ratio
☑	31	128	128	100	64	64	100
□	32	0	0	100	0	0	100

2. Click **ADD**. The WRED Profile - Add page opens, with default values displayed.

Figure 213 *WRED Profile - Add Page*



WRED Profile - Add

WRED Profile ID	1	
Green curve min point	128	(0 ... 8192)
Green curve max point	128	(0 ... 8192)
Green curve max drop ratio	100	(1 ... 100)
Yellow curve min point	64	(0 ... 8192)
Yellow curve max point	64	(0 ... 8192)
Yellow curve max drop ratio	100	(1 ... 100)

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 throughput 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 throughput 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 throughput 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 percentage (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 (WRED Profile Page).
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 (WRED Profile - Add Page). 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 (WRED Profile Page) and click **Delete**. The profile is deleted.

To delete multiple WRED profiles:

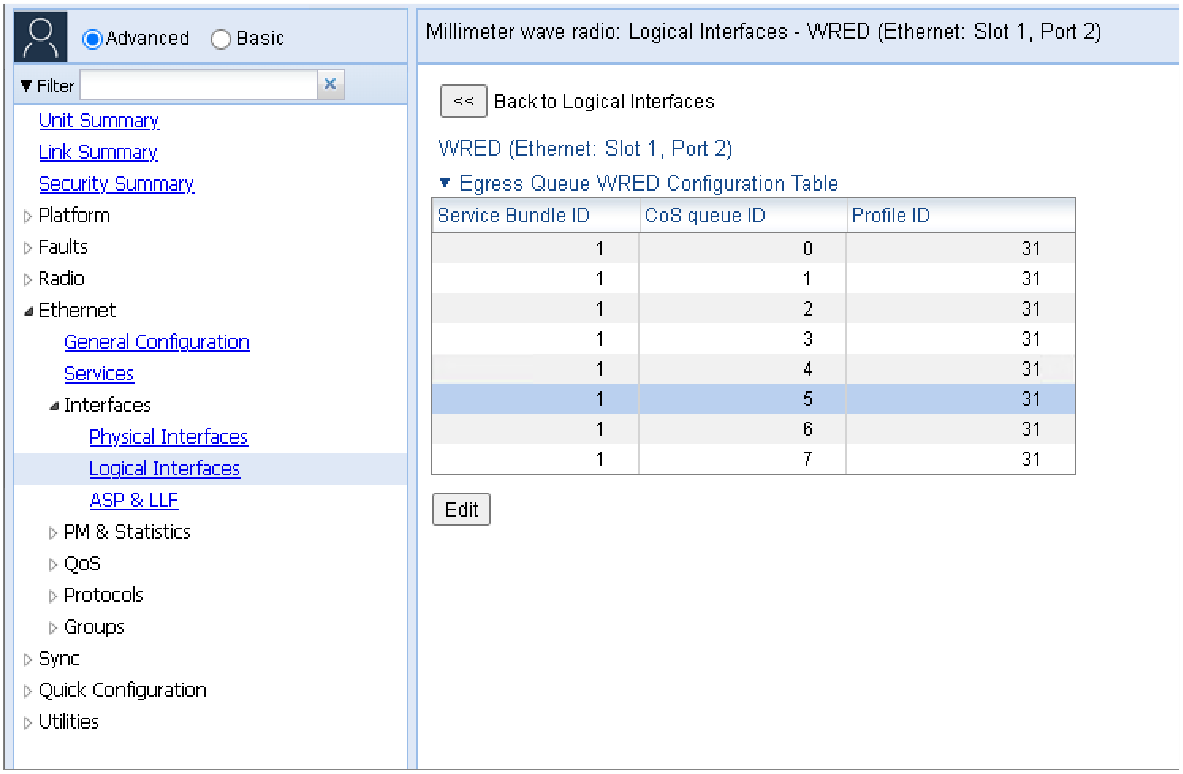
1. Select the profiles in the WRED Profile Configuration table or select all the profiles by selecting the check box in the top row.
2. Click **Delete**. The profiles are deleted.

Assigning WRED Profiles to Queues

To assign a WRED profile to a queue:

1. Select **Ethernet** > **Interfaces** > **Logical Interfaces**. The Logical Interfaces page opens (Logical Interfaces Page).
2. Select an interface in the Ethernet Logical Port Configuration table and click **WRED**. The WRED page opens.

Figure 214 *Logical Interfaces – WRED Page*



Millimeter wave radio: Logical Interfaces - WRED (Ethernet: Slot 1, Port 2)

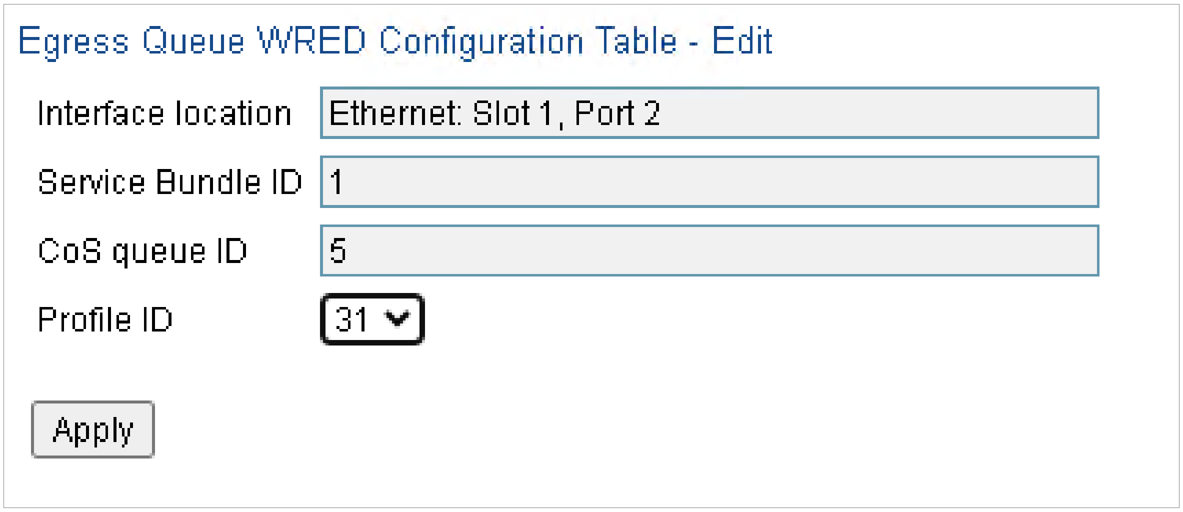
WRED (Ethernet: Slot 1, Port 2)

▼ Egress Queue WRED Configuration Table

Service Bundle ID	CoS queue ID	Profile ID
1	0	31
1	1	31
1	2	31
1	3	31
1	4	31
1	5	31
1	6	31
1	7	31

3. Select a CoS Queue ID and click **Edit**. The Logical Interfaces – WRED – Edit page opens.

Figure 215 *Logical Interfaces – WRED - Edit Page*



Egress Queue WRED Configuration Table - Edit

Interface location	Ethernet: Slot 1, Port 2
Service Bundle ID	1
CoS queue ID	5
Profile ID	31

4. In the **Profile ID** field, select the WRED profile you want to assign to the selected queue.

Note

The Service Bundle ID is always 1.

5. Click **Apply**, then **Close**.

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 an Interface and Service Bundle

Egress Shaping Overview

Egress shaping determines the traffic profile for each queue. PTP 850 can perform queue shaping on the queue level, using single 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

Queue shapers cannot be assigned to radio interfaces. This ability is planned for future release.

PTP 850 can also perform service bundle-level shaping. On the service bundle level, you can configure up to 256 single leaky bucket shaper profiles and assign them to interfaces. If no profile is attached to the interface, no egress shaping is performed on that interface. Only Service Bundle 1 is supported with PTP 850EX.

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.

Configuring Queue Shaper Profiles

This section includes:

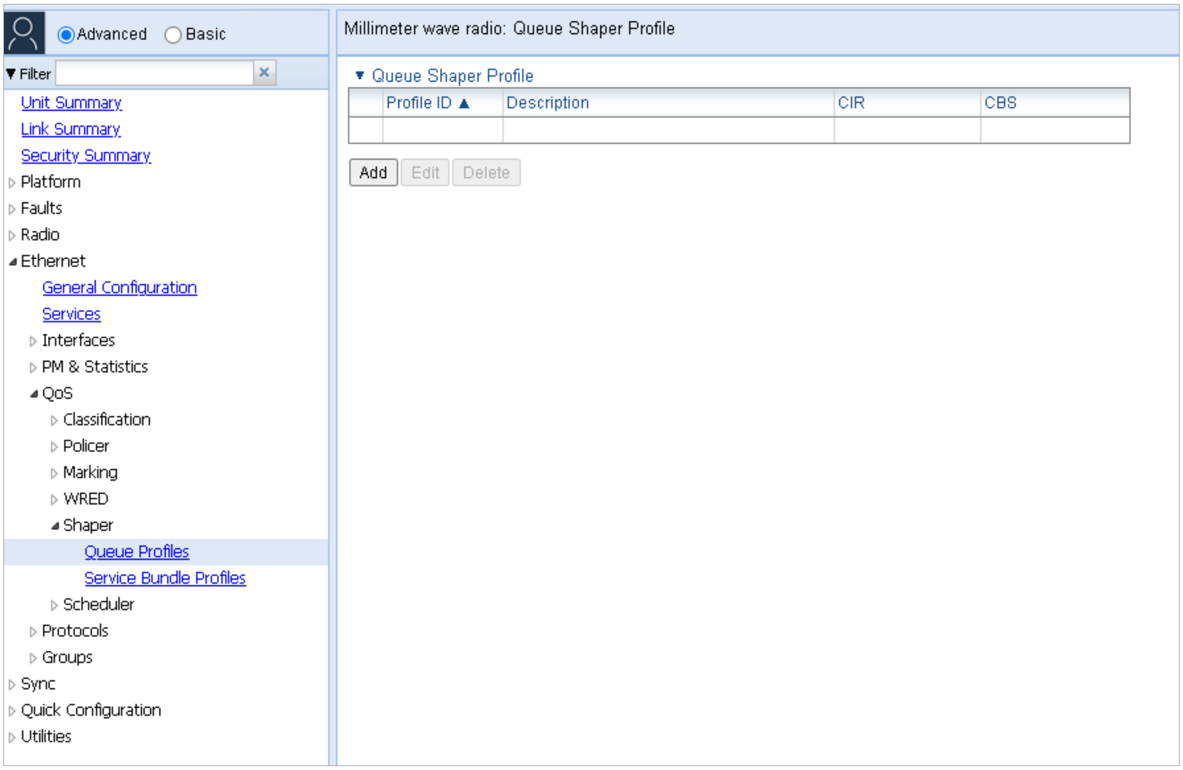
- Adding a Queue Shaper Profile
- Editing a Queue Shaper Profile
- Deleting a Queue Shaper Profile

Adding a Queue Shaper Profile

To add a queue shaper profile:

1. Select **Ethernet** > **QoS** > **Shaper** > **Queue Profiles**. The Queue Shaper Profile page opens.

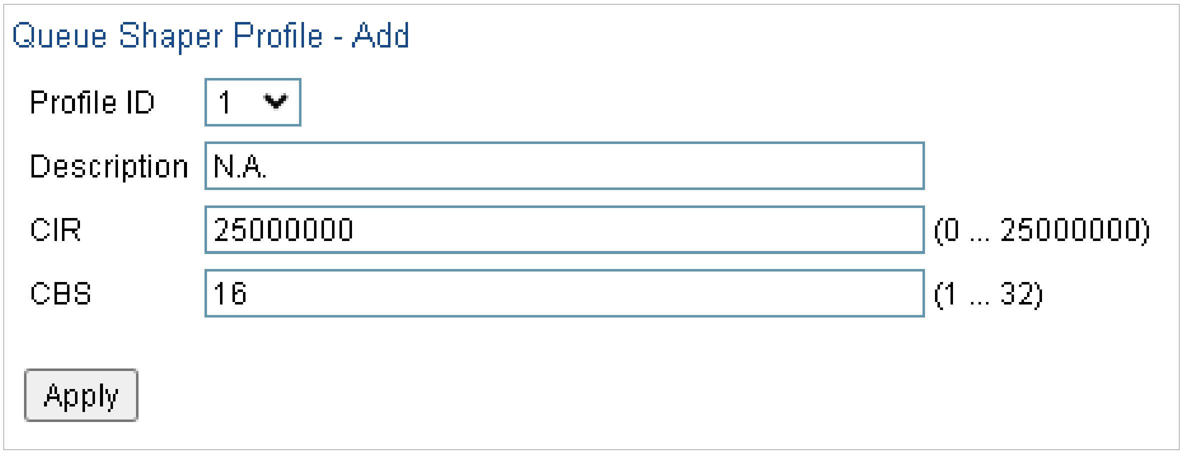
Figure 216 *Queue Shaper Profile Page*



	Profile ID ▲	Description	CIR	CBS

2. Click **Add**. The Queue Shaper – Add page opens, with default values displayed.

Figure 217 *Queue Shaper Profile – Add Page*



Queue Shaper Profile - Add

Profile ID	1	
Description	N.A.	
CIR	25000000	(0 ... 25000000)
CBS	16	(1 ... 32)

3. Configure the profile's parameters. See Queue Shaper Profile Parameters for a description of the queue shaper profile parameters.

4. Click **Apply**, then **Close**.

Table 46 *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.
Description	A description of the queue shaper profile.
CIR	Enter the Committed Information Rate (CIR) for the shaper, in kbps. Permitted values are 0-25000000 kbps (25 Gbps). If the value is 0, all incoming CIR traffic is dropped. The default value is 25000000 kbps.
CBS	Enter the Committed Burst Rate (CBR) for the shaper, in KB. 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 (Queue Shaper Profile Page).
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 (Queue Shaper Profile – Add Page). 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 (Queue Shaper Profile Page) 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

This section includes:

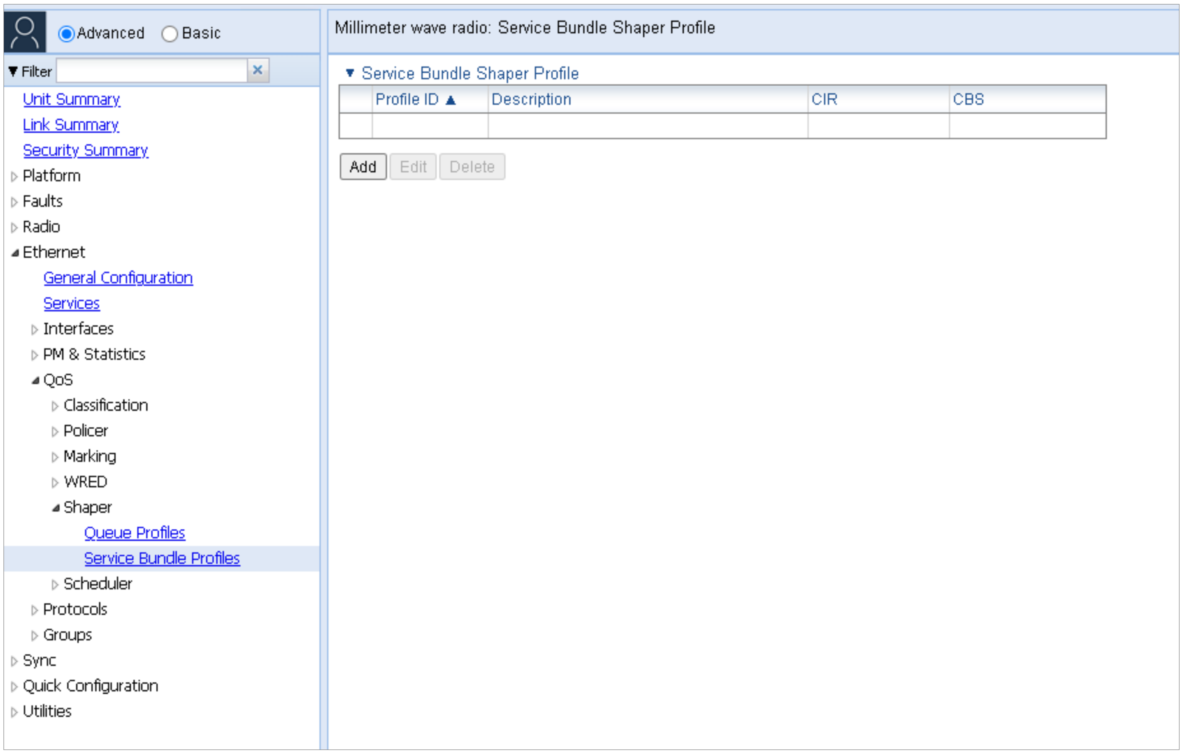
- Adding a Service Bundle Shaper Profile
- Editing a Service Bundle Shaper Profile
- Deleting a Service Bundle Shaper Profile

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 218 *Service Bundle Shaper Profile Page*



● Advanced ○ Basic

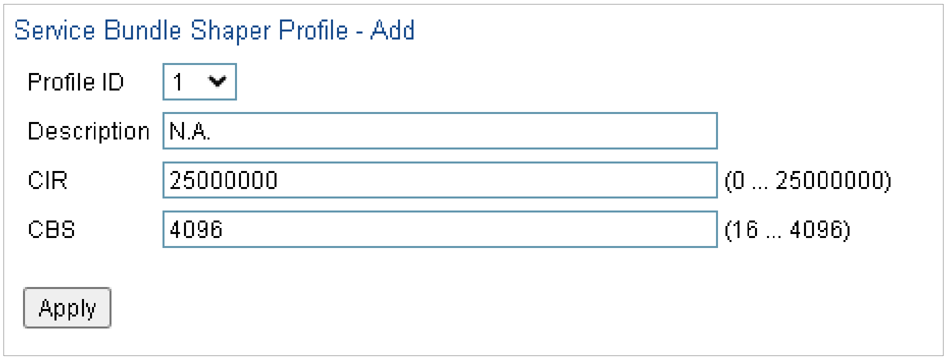
Millimeter wave radio: Service Bundle Shaper Profile

▼ Service Bundle Shaper Profile

	Profile ID ▲	Description	CIR	CBS

2. Click **Add**. The Service Bundle Shaper Profile – Add page opens, with default values displayed.

Figure 219 *Service Bundle Shaper Profile – Add Page*



Service Bundle Shaper Profile - Add

Profile ID	1	
Description	N.A.	
CIR	25000000	(0 ... 25000000)
CBS	4096	(16 ... 4096)

3. In the **Profile ID** field, select a unique ID to identify the profile. Permitted values are 2-32.

Note

Profile 1 is pre-defined and read-only.

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 kbps. Permitted values are 0 – 25,000,000 kbps.
6. In the **CBS** field, enter the Committed Burst Size (CBS) for the shaper, in KBytes. Permitted values are 1-4096 KBytes. The default value is 4096 KBytes.
7. Click **Apply**, then **Close**.

Editing a Service Bundle Shaper Profile

To edit a service bundle shaper profile:

1. Select **Ethernet** > **QoS** > **Shaper** > **Service Bundle Profiles**. The Service Bundle Shaper Profile page opens (Service Bundle Shaper Profile Page).
2. Select the profile you want to edit and click **Edit**. The Service Bundle Shaper Profile – Edit page opens. This page is similar to the Service Bundle Shaper Profile – Add page (Service Bundle Shaper Profile – Add Page). You can edit any parameter except the Profile ID.
3. Modify the profile.
4. Click **Apply**, then **Close**.

Deleting a Service Bundle Shaper Profile

You cannot delete a service bundle shaper profile that is assigned to an interface. You must first remove the profile from the interface, then delete the profile.

To delete a service bundle shaper profile, select the profile in the Service Bundle Shaper Profiles Configuration table (Service Bundle Shaper Profile Page) and click **Delete**. The profile is deleted.

To delete multiple service bundle shaper profiles:

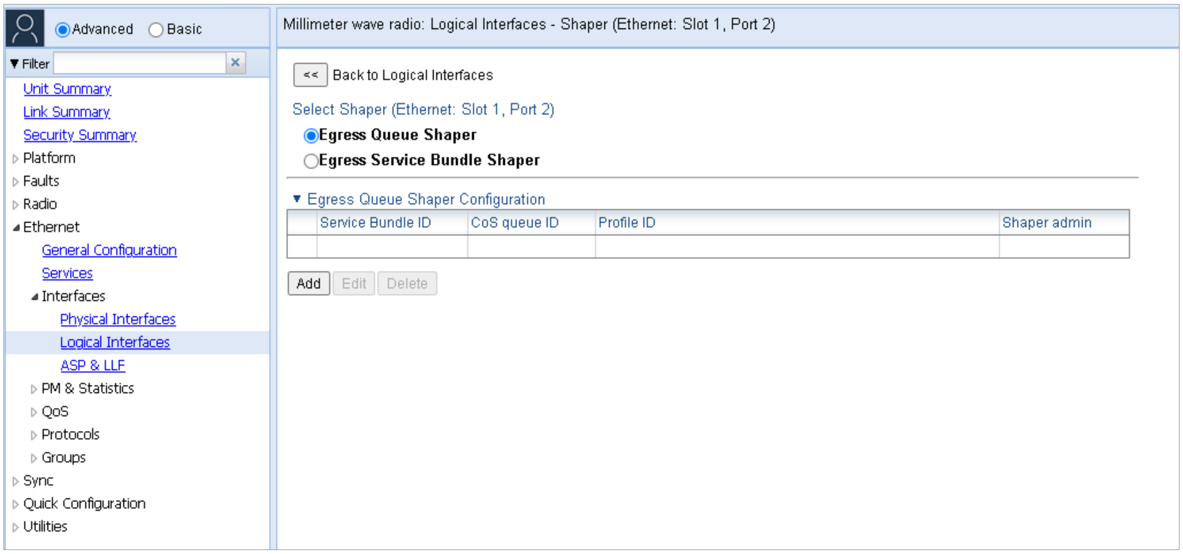
1. Select the profiles in the Service Bundle Shaper Profiles Configuration table or select all the profiles by selecting the check box in the top row.
2. Click **Delete**. The profiles are deleted.

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 (Logical Interfaces Page).
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 220 *Logical Interfaces – Shaper – Egress Queue Shaper*



Millimeter wave radio: Logical Interfaces - Shaper (Ethernet: Slot 1, Port 2)

Select Shaper (Ethernet: Slot 1, Port 2)

● Egress Queue Shaper

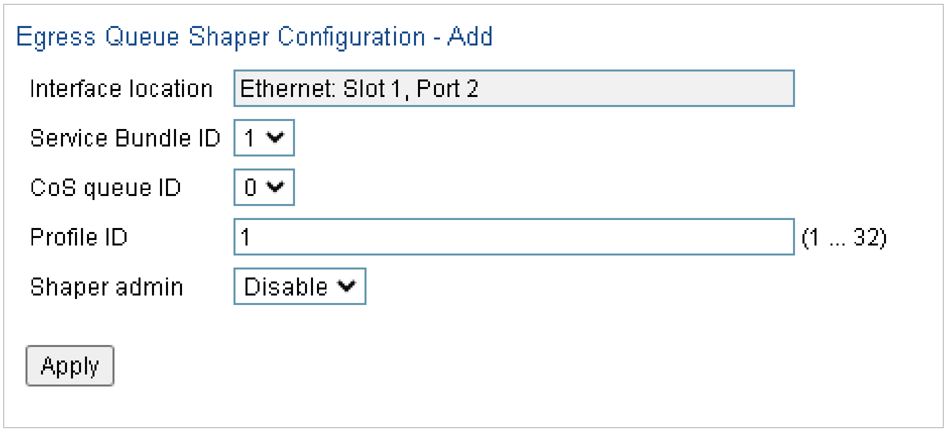
○ Egress Service Bundle Shaper

▼ Egress Queue Shaper Configuration

	Service Bundle ID	CoS queue ID	Profile ID	Shaper admin

3. Click **Add**. The Egress Queue Shaper Configuration – Add page opens.

Figure 221 *Logical Interfaces – Egress Queue Shaper Configuration – Add Page*



Egress Queue Shaper Configuration - Add

Interface location	Ethernet: Slot 1, Port 2
Service Bundle ID	1
CoS queue ID	0
Profile ID	1 (1 ... 32)
Shaper admin	Disable

4. In the **Service Bundle ID** field, select 1.
5. 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.
6. In the **Profile ID** field, select from a list of configured queue shaper profiles. See Configuring Queue Shaper Profiles.
7. 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.
8. Click **Apply**, then **Close**.

To assign a different queue shaper profile to a queue:

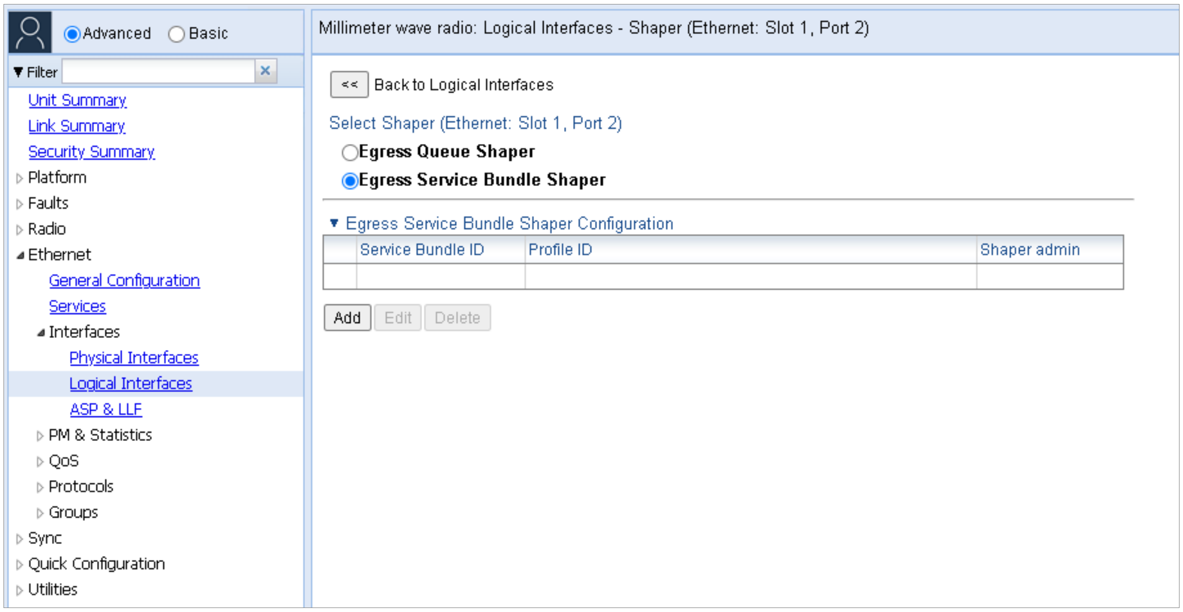
1. Select **Ethernet** > **Interfaces** > **Logical Interfaces**. The Logical Interfaces page opens (Logical Interfaces Page).
2. Select an interface in the Ethernet Logical Port Configuration table and click **Shaper**. The Logical Interfaces – Shaper page opens, with the Egress Queue Shaper Configuration table open by default (Logical Interfaces – Shaper – Egress Queue Shaper).
3. 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 (Logical Interfaces – Egress Queue Shaper Configuration – Add Page).
4. To assign a different egress queue shaper profile, select the profile in the **Profile ID** field.
5. 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.
6. Click **Apply**, then **Close**.

Assigning a Service Bundle Shaper Profile to an Interface and Service Bundle

To assign a service bundle shaper profile to an interface and service bundle:

1. Select **Ethernet** > **Interfaces** > **Logical Interfaces**. The Logical Interfaces page opens (Logical Interfaces Page).
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 (Logical Interfaces – Shaper – Egress Queue Shaper).
3. Select **Egress Service Bundle Shaper**. The Egress Service Bundle Shaper Configuration table appears. All service bundle shaper profiles defined in the system are listed in the table.

Figure 222 *Logical Interfaces – Shaper – Egress Service Bundle Shaper*



Millimeter wave radio: Logical Interfaces - Shaper (Ethernet: Slot 1, Port 2)

● Advanced ○ Basic

Select Shaper (Ethernet: Slot 1, Port 2)

○ Egress Queue Shaper

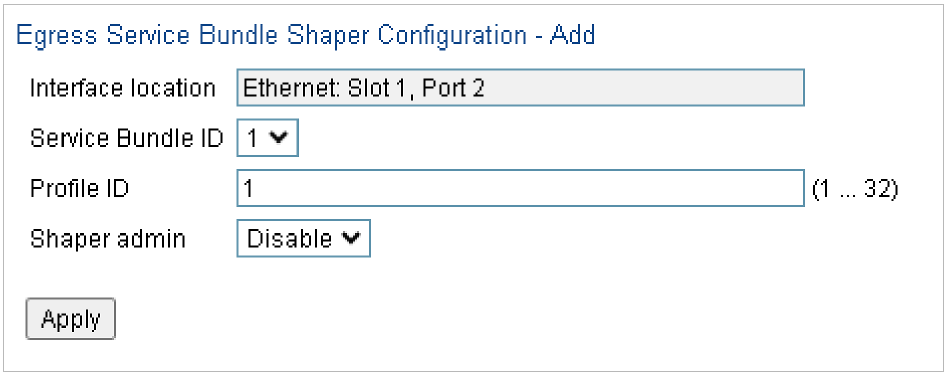
● Egress Service Bundle Shaper

▾ Egress Service Bundle Shaper Configuration

	Service Bundle ID	Profile ID	Shaper admin

4. Click **Add**. The Egress Service Bundle Shaper Configuration – Add page opens.

Figure 223 *Logical Interfaces – Egress Service Bundle Shaper Configuration – Add Page*



Egress Service Bundle Shaper Configuration - Add

Interface location	Ethernet: Slot 1, Port 2
Service Bundle ID	1
Profile ID	1 (1 ... 32)
Shaper admin	Disable

Note

Only one service bundle (Service Bundle ID 1) is supported.

5. In the **Service Bundle ID** field, select a Service Bundle to which to assign the service bundle shaper profile.
6. In the **Profile ID** field, select from a list of configured service bundle shaper profiles. See Configuring Service Bundle Shaper Profiles.
7. In the **Shaper Admin** field, select **Enable** to enable egress service bundle shaping, or **Disable** to disable egress service bundle shaping.
8. Click **Apply**, then **Close**.

To assign a different service bundle shaper profile:

1. Select **Ethernet** > **Interfaces** > **Logical Interfaces**. The Logical Interfaces page opens (Logical Interfaces Page).
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 (Logical Interfaces – Shaper – Egress Queue Shaper).
3. Select **Egress Service Bundle Shaper**. The Egress Service Bundle Shaper Configuration table appears (Logical Interfaces – Shaper – Egress Service Bundle Shaper). All service bundle shaper profiles defined in the system are listed in the table.
4. Select the row you want to edit and click **Edit**. The Egress Service Bundle Shaper Configuration – Edit page opens. This page is similar to the Egress Service Bundle Shaper Configuration – Add page (Logical Interfaces – Egress Service Bundle Shaper Configuration – Add Page).
5. To assign a different egress queue shaper profile, select the profile in the **Profile ID** field.
6. To enable or disable egress service bundle shaping, select **Enable** or **Disable**.
7. Click **Apply**, then **Close**.

Configuring Scheduling

This section includes:

- Scheduling Overview
- Configuring Priority Profiles
- Configuring Queue WFQ Profiles
- Assigning a Priority Profile to an Interface
- Assigning a Queue WFQ Profile to an Interface

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.

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:

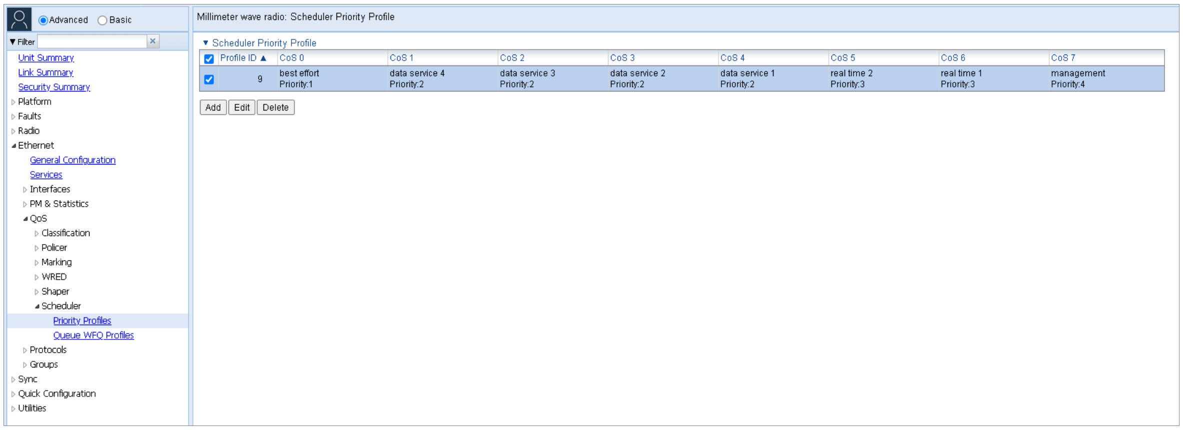
- Adding a Scheduler Priority Profile
- Editing a Service Scheduler Priority Profile
- Deleting a Scheduler Priority Profile

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 224 *Scheduler Priority Profile Page*



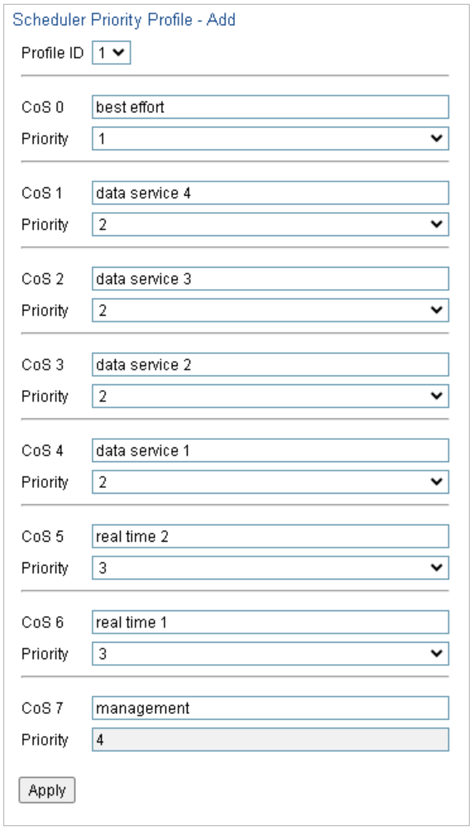
Millimeter wave radio: Scheduler Priority Profile

▼ Scheduler Priority Profile

☑	Profile ID ▲	CoS 0	CoS 1	CoS 2	CoS 3	CoS 4	CoS 5	CoS 6	CoS 7
☑	9	best effort Priority:1	data service 4 Priority:2	data service 3 Priority:2	data service 2 Priority:2	data service 1 Priority:2	real time 2 Priority:3	real time 1 Priority:3	management Priority:4

2. Click **Add**. The Scheduler Priority Profile – Add page opens, with default values displayed.

   Figure 225 *Scheduler Priority Profile – Add Page*



Scheduler Priority Profile - Add

Profile ID	1
CoS 0	best effort
Priority	1
CoS 1	data service 4
Priority	2
CoS 2	data service 3
Priority	2
CoS 3	data service 2
Priority	2
CoS 4	data service 1
Priority	2
CoS 5	real time 2
Priority	3
CoS 6	real time 1
Priority	3
CoS 7	management
Priority	4

3. In the **Profile ID** field, select a unique Profile ID between 1 and 8.

4. For each CoS value, enter the priority, from 4 (highest) to 1 (lowest) (1-4). This priority is applied to 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**.

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 (Scheduler Priority Profile Page).
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 (Scheduler Priority Profile – Add Page). 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 (Scheduler Priority Profile Page) 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.

Configuring Queue WFQ Profiles

This section includes:

- WFQ Overview
- Adding a Queue WFQ Profile
- Editing a Queue WFQ Priority Profile
- Deleting a Queue WFQ Profile

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.

The system supports up to six queue 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 queue WFQ profile.

Table 47 *Queue WFQ Profile Example*

Profile ID (1-7) CoS	Queue Weight
0	15
1	15
2	15
3	15
4	15
5	15
6	15
7	20

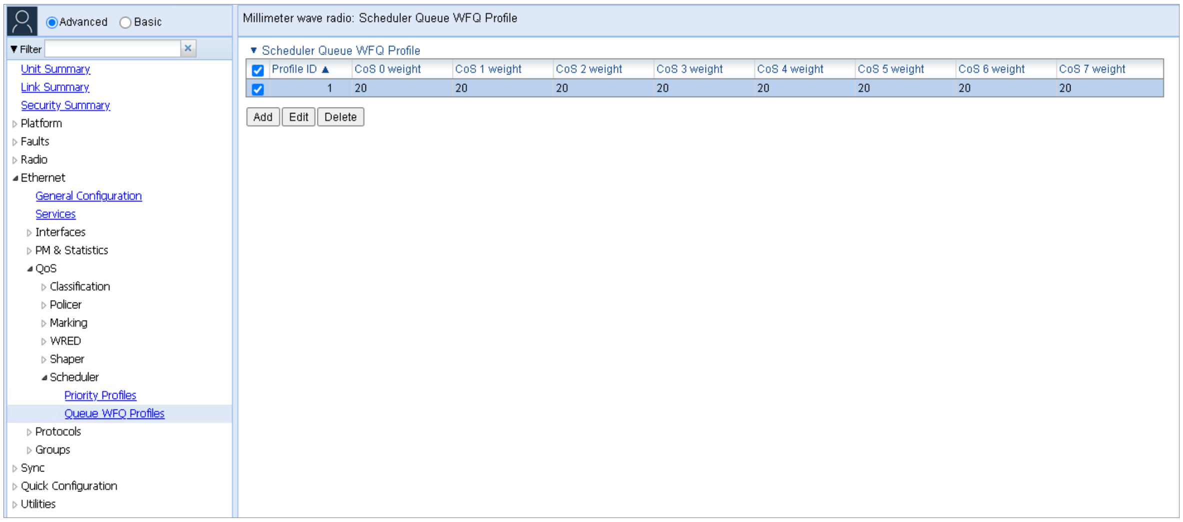
You can attach one of the configured queue WFQ profiles to each interface. By default, the interface is assigned Profile ID 1, the pre-defined system profile. Profile ID 1 assigns 20 to each CoS.

Adding a Queue WFQ Profile

To add a queue WFQ profile:

1. Select **Ethernet** > **QoS** > **Scheduler** > **Queue WFQ Profiles**. The Scheduler Queue WFQ Profile page opens.

Figure 226 *Scheduler Queue WFQ Profile Page*



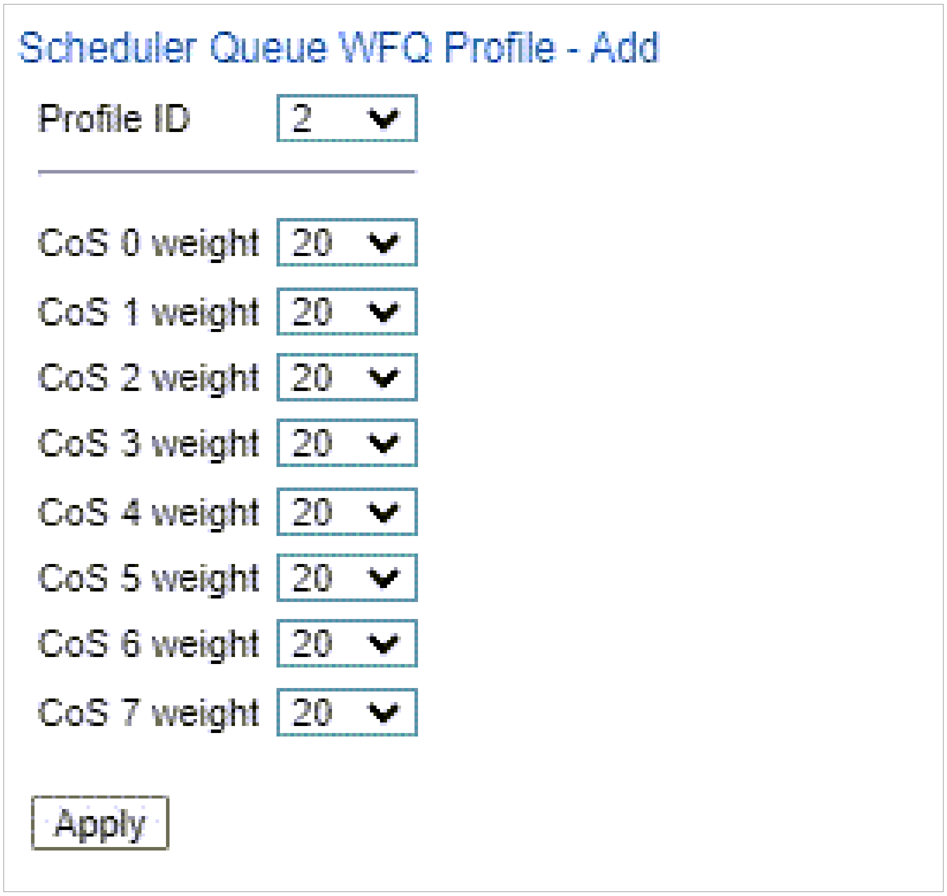
Millimeter wave radio: Scheduler Queue WFQ Profile

▼ Scheduler Queue WFQ Profile

☑	Profile ID ▲	CoS 0 weight	CoS 1 weight	CoS 2 weight	CoS 3 weight	CoS 4 weight	CoS 5 weight	CoS 6 weight	CoS 7 weight
☑	1	20	20	20	20	20	20	20	20

2. Click **Add**. The Scheduler Queue WFQ Profile – Add page opens, with default values displayed.

Figure 227 *Scheduler Queue WFQ Profile – Add Page*



Scheduler Queue WFQ Profile - Add

Profile ID 2

CoS 0 weight 20

CoS 1 weight 20

CoS 2 weight 20

CoS 3 weight 20

CoS 4 weight 20

CoS 5 weight 20

CoS 6 weight 20

CoS 7 weight 20

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 weight for that CoS, from 1 to 20.
5. Click **Apply**, then **Close**.

Editing a Queue WFQ Priority Profile

To edit a scheduler queue WFQ profile:

1. Select **Ethernet** > **QoS** > **Scheduler** > **Queue WFQ Profiles**. The Scheduler Queue WFQ Profile page opens (Scheduler Queue WFQ Profile Page).
2. Select the profile you want to edit and click **Edit**. The Scheduler Queue WFQ Profile – Edit page opens. This page is similar to the Scheduler Queue WFQ Profile – Add page (Scheduler Queue WFQ Profile – Add Page). You can edit any parameter except the **Profile ID**.
3. Modify the profile.
4. Click **Apply**, then **Close**.

Deleting a Queue WFQ Profile

To delete a scheduler WFQ profile, select the profile in the Scheduler WFQ Profiles page (Scheduler Queue WFQ Profile 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.

Assigning a Priority Profile to an Interface

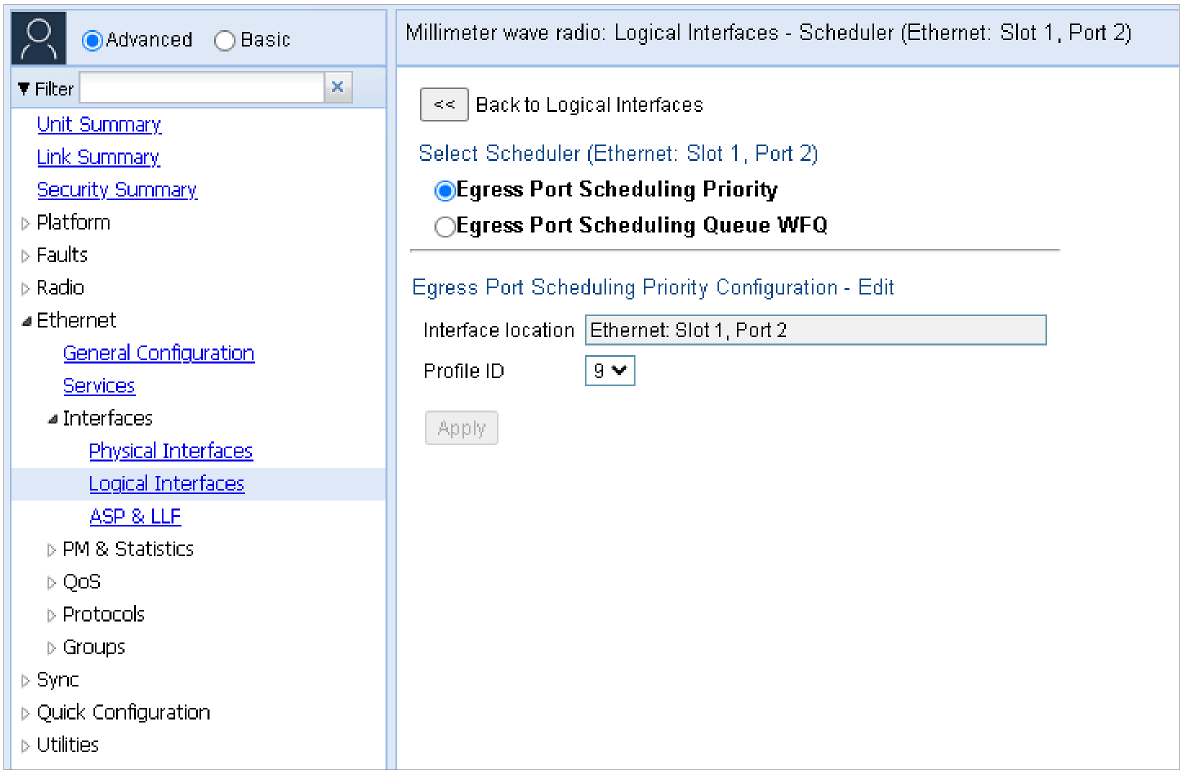
Note

When a profile is assigned to an interface or when a profile that is already assigned to an interface is modified, the device must be reset before the change is applied. Until the device is reset, an alarm is raised. This alarm has Alarm ID 105, *System reset is required after priority profile has been changed*. This alarm is also raised if the default profile (Profile 9) is modified, even if the profile is not assigned to an interface.

To assign a priority profile to an interface:

1. Select **Ethernet** > **Interfaces** > **Logical Interfaces**. The Logical Interfaces page opens (Logical Interfaces Page).
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 228 *Logical Interfaces – Scheduler – Egress Port Scheduling Priority*



Millimeter wave radio: Logical Interfaces - Scheduler (Ethernet: Slot 1, Port 2)

Back to Logical Interfaces

Select Scheduler (Ethernet: Slot 1, Port 2)

● Egress Port Scheduling Priority
○ Egress Port Scheduling Queue WFQ

Egress Port Scheduling Priority Configuration - Edit

Interface location: Ethernet: Slot 1, Port 2

Profile ID: 9

3. In the **Profile ID** field, select from a list of configured scheduling priority profiles. See Configuring Priority Profiles.

4. Click **Apply**, then **Close**.

Assigning a Queue WFQ Profile to an Interface

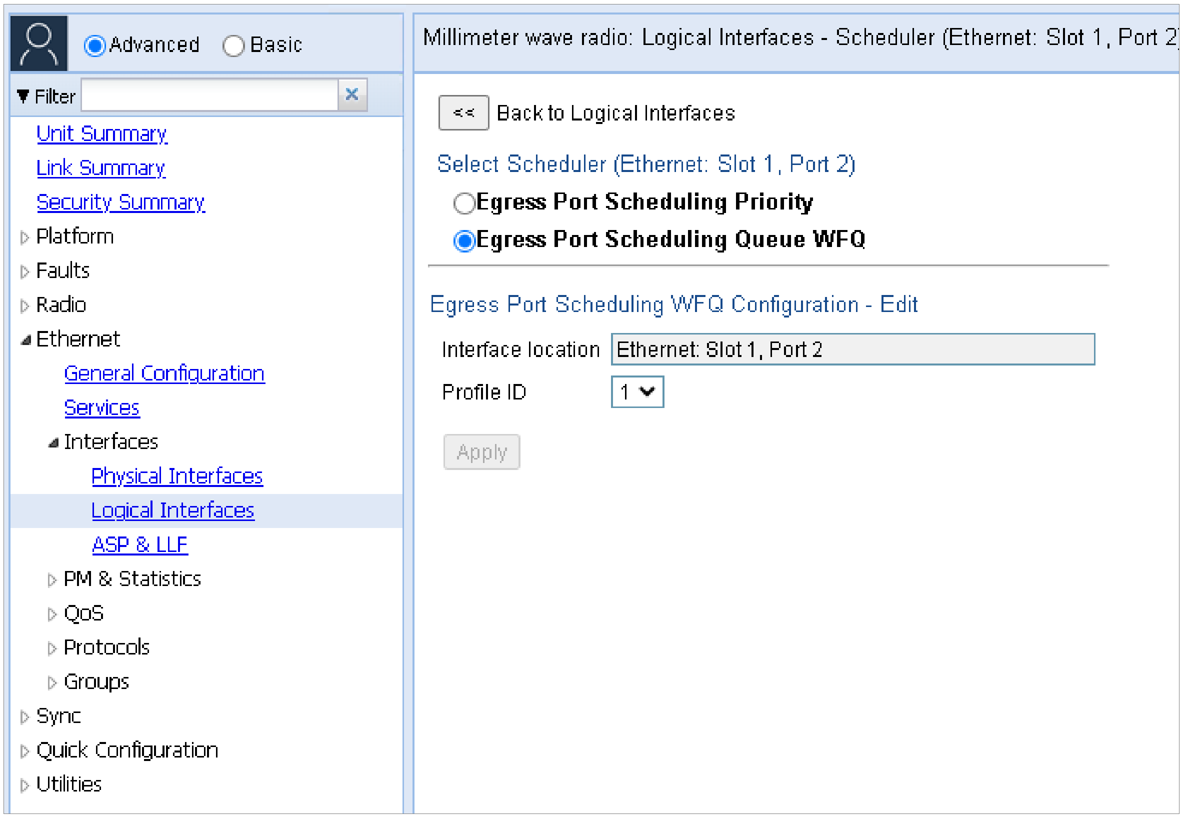
To assign a queue WFQ profile to an interface:

1. Select **Ethernet** > **Interfaces** > **Logical Interfaces**. The Logical Interfaces page opens (Logical Interfaces Page).

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 (Logical Interfaces – Scheduler – Egress Port Scheduling Priority).

3. Select **Egress Port Scheduling Queue WFQ**. The Egress Port Scheduling Queue WFQ Configuration – Edit page opens.

Figure 229 *Logical Interfaces – Scheduler – Egress Port Scheduling Queue WFQ*



Millimeter wave radio: Logical Interfaces - Scheduler (Ethernet: Slot 1, Port 2

Back to Logical Interfaces

Select Scheduler (Ethernet: Slot 1, Port 2)

○ **Egress Port Scheduling Priority**

● **Egress Port Scheduling Queue WFQ**

Egress Port Scheduling WFQ Configuration - Edit

Interface location: Ethernet: Slot 1, Port 2

Profile ID: 1

4. In the **Profile ID** field, select from a list of configured scheduling priority profiles. See Configuring Queue WFQ Profiles.
5. Click **Apply**, then **Close**.

Configuring the Egress Byte Compensation

You can define the 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 egress byte compensation value for a logical interface:

1. Select **Ethernet** > **Interfaces** > **Logical Interfaces**. The Logical Interfaces page opens (Logical Interfaces Page).
2. Select the interface you want to configure and click **Edit**. The Logical Interfaces - Edit page opens (Logical Interfaces - Edit Page).
3. 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.
4. Click **Apply**, then **Close**.

Note

The **Ingress byte compensation** field is not applicable to PTP 850EX and should not be adjusted.

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.

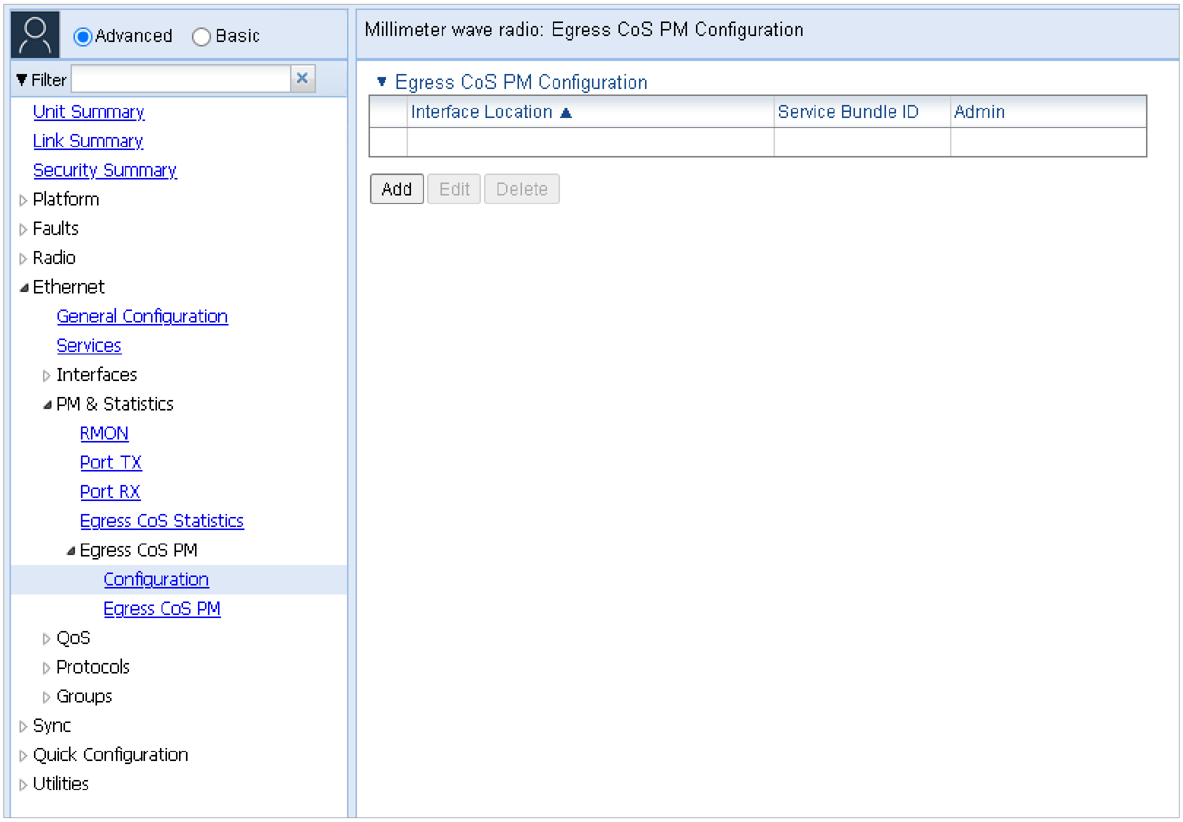
One collection rule is available per interface.

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 230 *Egress CoS PM Configuration Page*



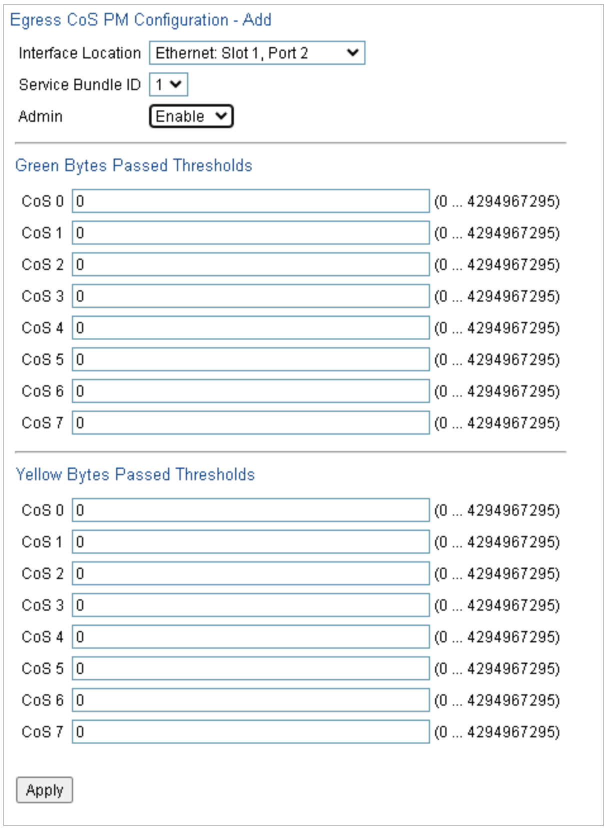
Millimeter wave radio: Egress CoS PM Configuration

▼ Egress CoS PM Configuration

	Interface Location ▲	Service Bundle ID	Admin

2. Click Add. The Egress CoS PM Configuration – Add page opens.

Figure 231 *Egress CoS PM Configuration – Add Page*



Egress CoS PM Configuration - Add

Interface Location	Ethernet: Slot 1, Port 2
Service Bundle ID	1
Admin	Enable

Green Bytes Passed Thresholds

CoS 0	0	(0 ... 4294967295)
CoS 1	0	(0 ... 4294967295)
CoS 2	0	(0 ... 4294967295)
CoS 3	0	(0 ... 4294967295)
CoS 4	0	(0 ... 4294967295)
CoS 5	0	(0 ... 4294967295)
CoS 6	0	(0 ... 4294967295)
CoS 7	0	(0 ... 4294967295)

Yellow Bytes Passed Thresholds

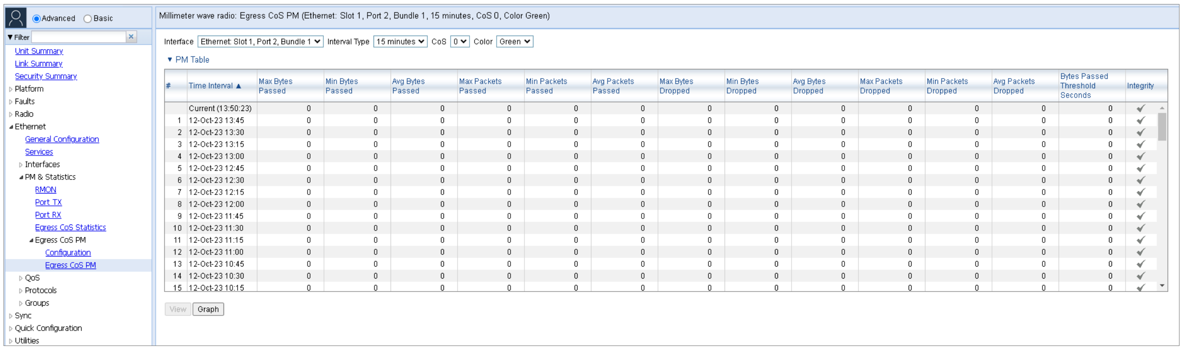
CoS 0	0	(0 ... 4294967295)
CoS 1	0	(0 ... 4294967295)
CoS 2	0	(0 ... 4294967295)
CoS 3	0	(0 ... 4294967295)
CoS 4	0	(0 ... 4294967295)
CoS 5	0	(0 ... 4294967295)
CoS 6	0	(0 ... 4294967295)
CoS 7	0	(0 ... 4294967295)

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 (1-7).
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 232 *Egress CoS PM Page*



Millimeter wave radio: Egress CoS PM (Ethernet: Slot 1, Port 2, Bundle 1, 15 minutes, CoS 0, Color Green)

Interface: Ethernet: Slot 1, Port 2, Bundle 1 Interval Type: 15 minutes CoS: 0 Color: Green

▼ PM Table

#	Time Interval ▲	Max Bytes Passed	Min Bytes Passed	Avg Bytes Passed	Max Packets Passed	Min Packets Passed	Avg Packets Passed	Max Bytes Dropped	Min Bytes Dropped	Avg Bytes Dropped	Max Packets Dropped	Min Packets Dropped	Avg Packets Dropped	Bytes Passed Threshold Seconds	Integrity
	Current (13:50:23)	0	0	0	0	0	0	0	0	0	0	0	0	0	✓
1	12-Oct-23 13:45	0	0	0	0	0	0	0	0	0	0	0	0	0	✓
2	12-Oct-23 13:30	0	0	0	0	0	0	0	0	0	0	0	0	0	✓
3	12-Oct-23 13:15	0	0	0	0	0	0	0	0	0	0	0	0	0	✓
4	12-Oct-23 13:00	0	0	0	0	0	0	0	0	0	0	0	0	0	✓
5	12-Oct-23 12:45	0	0	0	0	0	0	0	0	0	0	0	0	0	✓
6	12-Oct-23 12:30	0	0	0	0	0	0	0	0	0	0	0	0	0	✓
7	12-Oct-23 12:15	0	0	0	0	0	0	0	0	0	0	0	0	0	✓
8	12-Oct-23 12:00	0	0	0	0	0	0	0	0	0	0	0	0	0	✓
9	12-Oct-23 11:45	0	0	0	0	0	0	0	0	0	0	0	0	0	✓
10	12-Oct-23 11:30	0	0	0	0	0	0	0	0	0	0	0	0	0	✓
11	12-Oct-23 11:15	0	0	0	0	0	0	0	0	0	0	0	0	0	✓
12	12-Oct-23 11:00	0	0	0	0	0	0	0	0	0	0	0	0	0	✓
13	12-Oct-23 10:45	0	0	0	0	0	0	0	0	0	0	0	0	0	✓
14	12-Oct-23 10:30	0	0	0	0	0	0	0	0	0	0	0	0	0	✓
15	12-Oct-23 10:15	0	0	0	0	0	0	0	0	0	0	0	0	0	✓

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 module, muting of a radio interface, and an operational status of **Down**.

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)

Configuring G.8032

This section includes:

- G.8032 Overview
- Configuring the Destination MAC Address
- Adding ERPIs
- 0Configuring 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.

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.

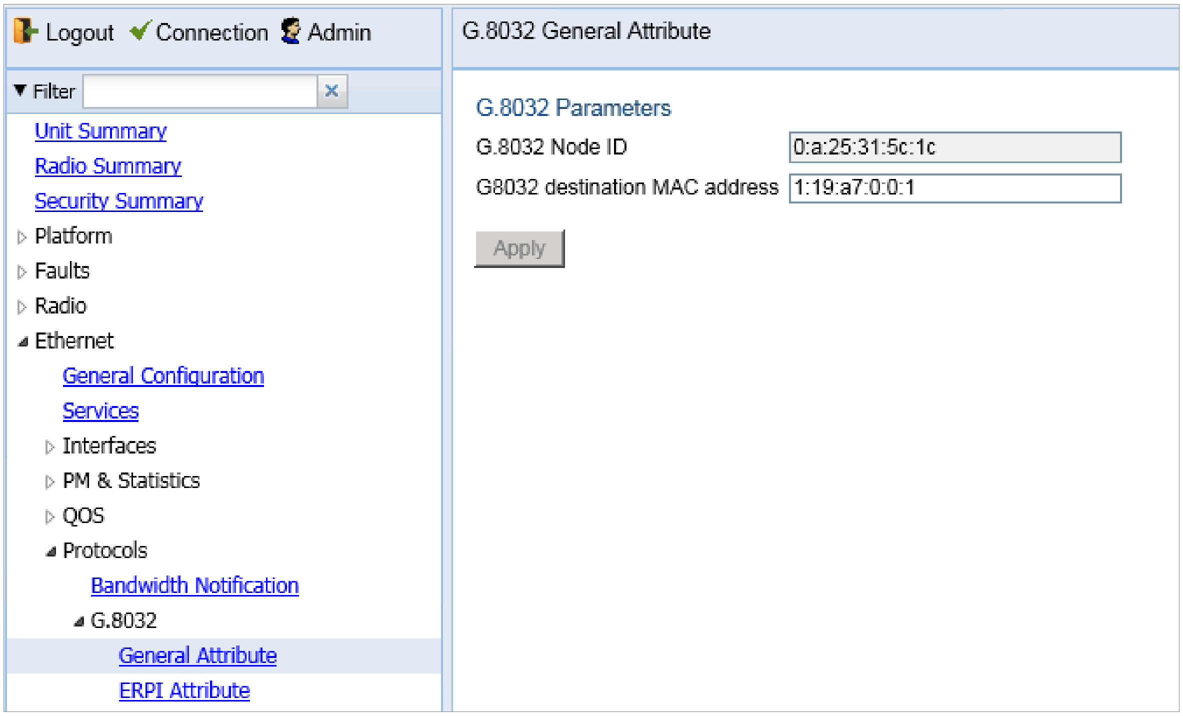
For a more detailed description of G.8032, refer to the Technical Description for the product you are using.

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 233 *G.8032 General Attribute Page*



G.8032 General Attribute

G.8032 Parameters

G.8032 Node ID: 0:a:25:31:5c:1c

G8032 destination MAC address: 1:19:a7:0:0:1

2. In the **G8032 destination MAC address field**, enter the destination MAC address for PDUs generated by the node.
3. Click **Apply**.

Note

The G.8032 Node ID field displays the base MAC address for the node. This field is read-only.

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.

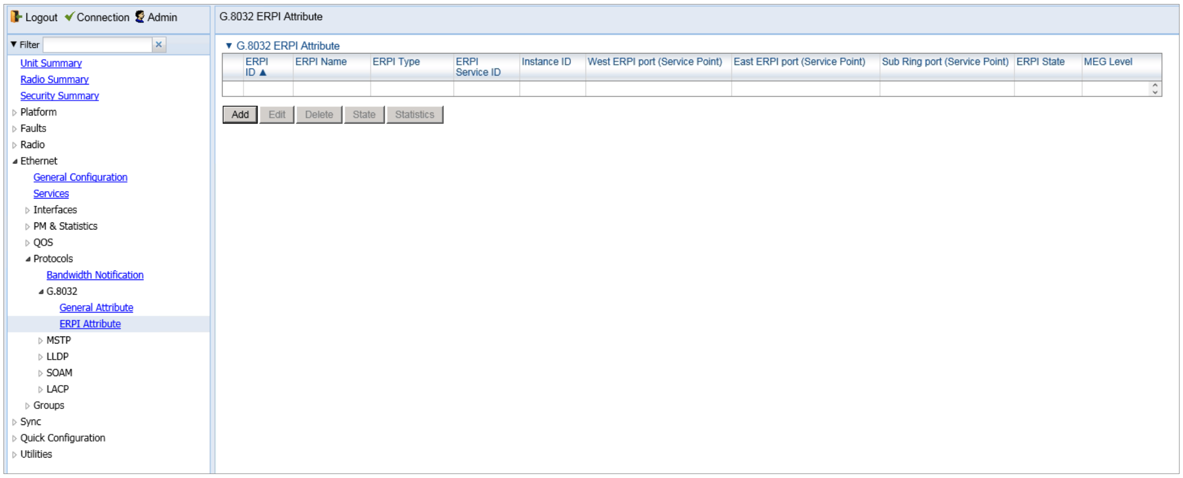
Note

Before adding an ERPI to an Ethernet service, the service must be mapped to an MSTP instance. See Mapping Ethernet Services to MSTP instances (MSTIs).

To add an ERPI:

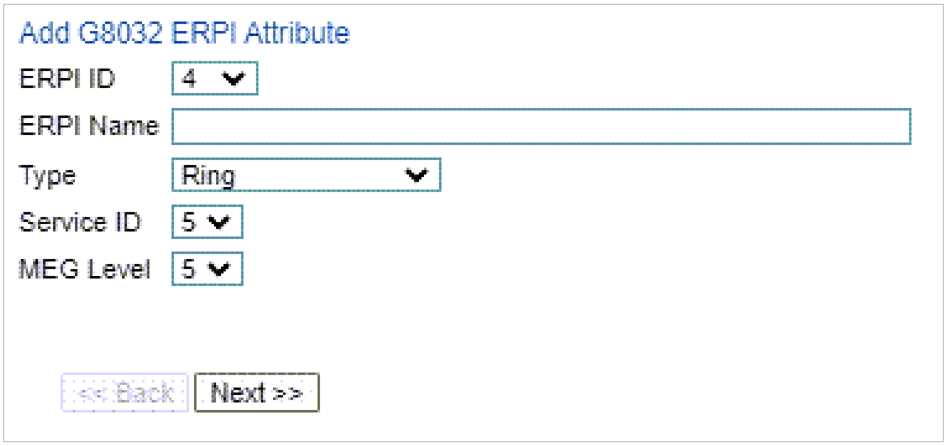
1. Select **Ethernet** > **Protocols** > **G.8032** > **ERPI Attribute**. The G.8032 ERPI Attribute page opens.

Figure 234 *G.8032 ERPI Attribute Page*



2. Click **Add**. The Add G8032 ERPI Attribute wizard opens.

Figure 235 *G.8032 ERPI Attribute Wizard – Page 1*



Add G8032 ERPI Attribute

ERPI ID: 4

ERPI Name:

Type: Ring

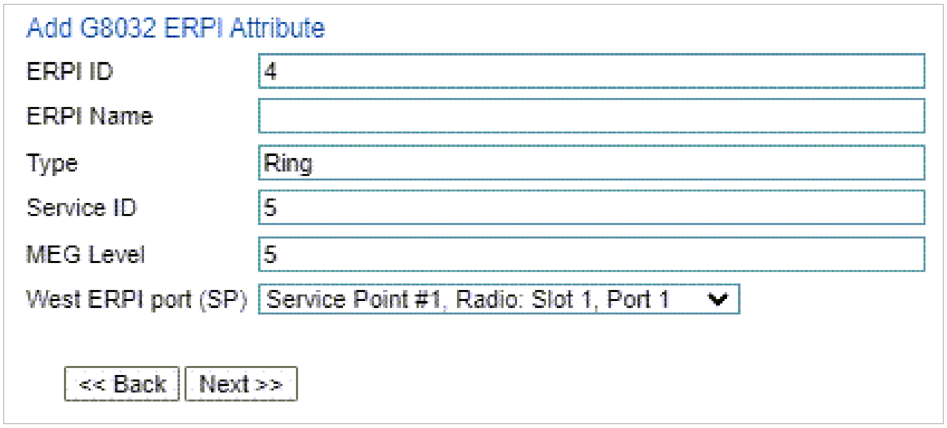
Service ID: 5

MEG Level: 5

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 236 *G.8032 ERPI Attribute Wizard – Page 2*



Add G8032 ERPI Attribute

ERPI ID	4
ERPI Name	
Type	Ring
Service ID	5
MEG Level	5
West ERPI port (SP)	Service Point #1, Radio: Slot 1, Port 1

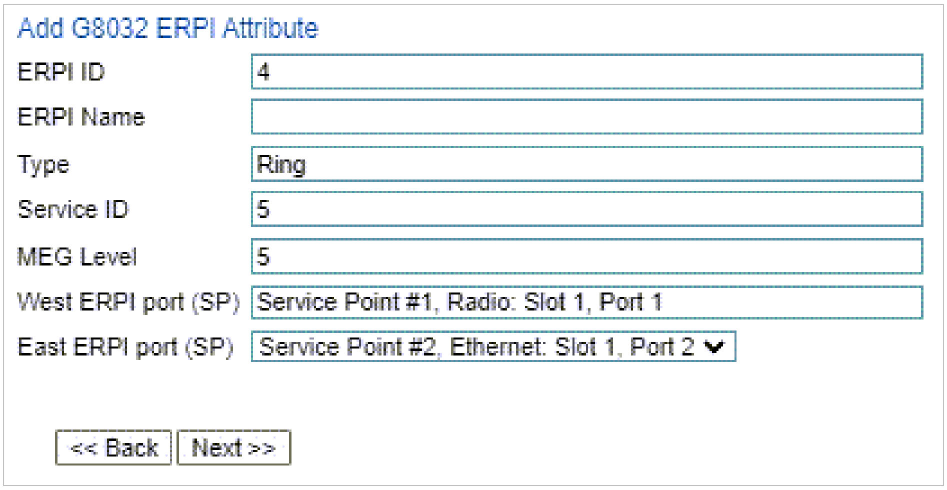
9. In the **West ERPI port (SP)** field, select the first endpoint for the ERPI. This can be any service point that has been configured for the service.

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 237 *G.8032 ERPI Attribute Wizard – Page 3*



Add G8032 ERPI Attribute

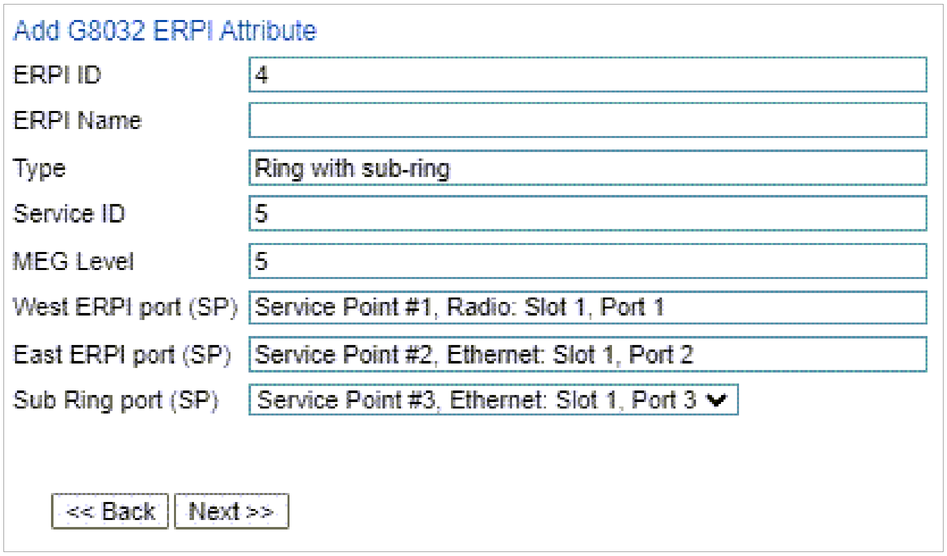
ERPI ID	4
ERPI Name	
Type	Ring
Service ID	5
MEG Level	5
West ERPI port (SP)	Service Point #1, Radio: Slot 1, Port 1
East ERPI port (SP)	Service Point #2, Ethernet: Slot 1, Port 2

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 Verify that the parameters of the ERPI are correct and click Submit..
    - If the Type is Ring with sub-ring, the fourth page of the Add G.8032 ERPI Attribute wizard opens.

Figure 238 *G.8032 ERPI Attribute Wizard – Page 4*



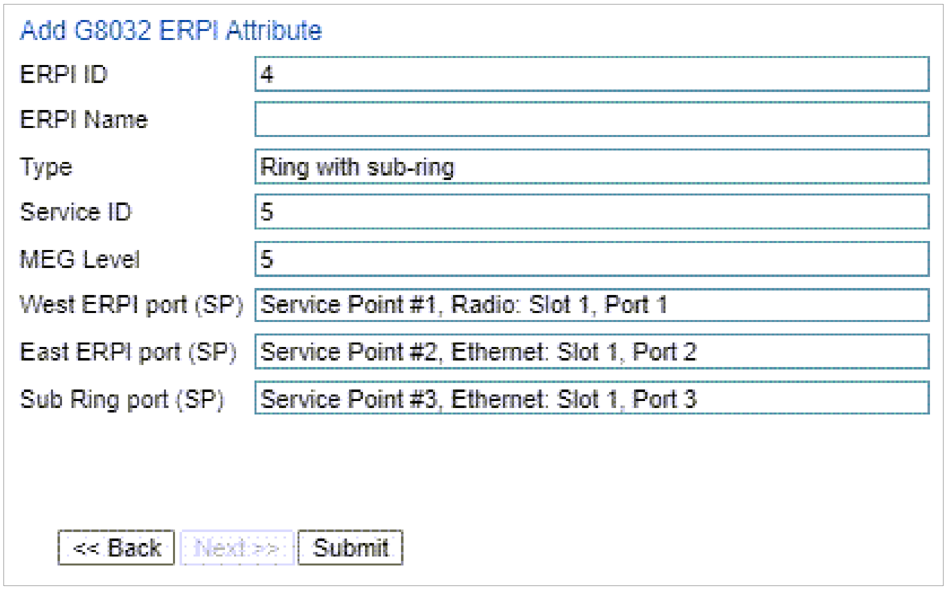
Add G8032 ERPI Attribute

ERPI ID	4
ERPI Name	
Type	Ring with sub-ring
Service ID	5
MEG Level	5
West ERPI port (SP)	Service Point #1, Radio: Slot 1, Port 1
East ERPI port (SP)	Service Point #2, Ethernet: Slot 1, Port 2
Sub Ring port (SP)	Service Point #3, Ethernet: Slot 1, Port 3

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 239 *G.8032 ERPI Attribute Wizard – Submit*



Add G8032 ERPI Attribute

ERPI ID	4
ERPI Name	
Type	Ring with sub-ring
Service ID	5
MEG Level	5
West ERPI port (SP)	Service Point #1, Radio: Slot 1, Port 1
East ERPI port (SP)	Service Point #2, Ethernet: Slot 1, Port 2
Sub Ring port (SP)	Service Point #3, Ethernet: Slot 1, Port 3

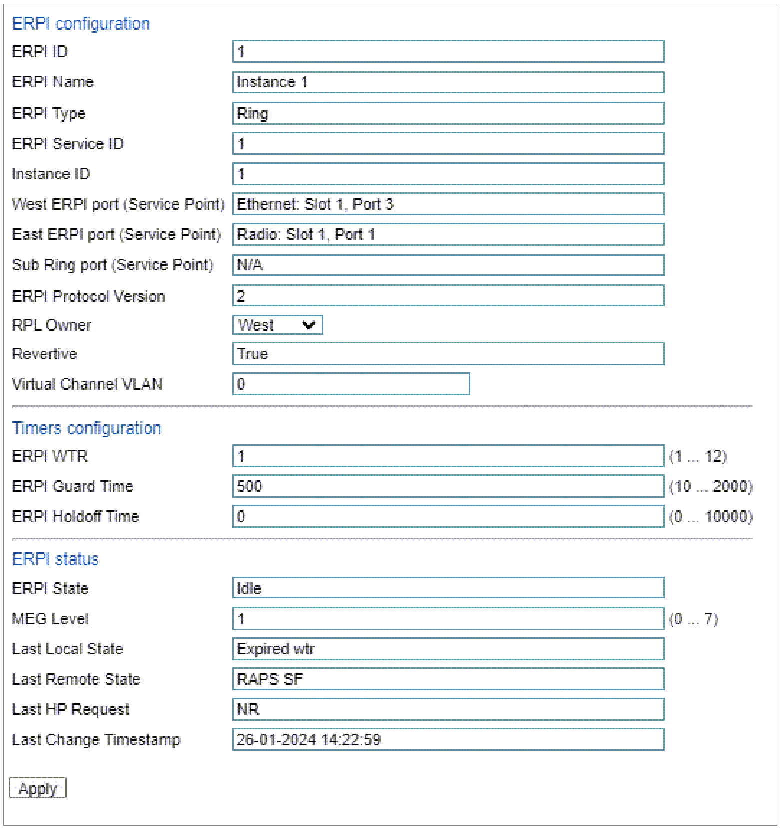
15. Verify that the parameters of the ERPI are correct and click **Submit**.

0Configuring 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 (G.8032 ERPI Attribute Page).
2. Select the ERPI and click **Edit**. The ERPI Attribute – Edit page opens.

Figure 240 *G.8032 ERPI Attribute – Edit Page*



ERPI configuration

ERPI ID	1	
ERPI Name	Instance 1	
ERPI Type	Ring	
ERPI Service ID	1	
Instance ID	1	
West ERPI port (Service Point)	Ethernet: Slot 1, Port 3	
East ERPI port (Service Point)	Radio: Slot 1, Port 1	
Sub Ring port (Service Point)	N/A	
ERPI Protocol Version	2	
RPL Owner	West	
Revertive	True	
Virtual Channel VLAN	0	

Timers configuration

ERPI WTR	1	(1 ... 12)
ERPI Guard Time	500	(10 ... 2000)
ERPI Holdoff Time	0	(0 ... 10000)

ERPI status

ERPI State	Idle	
MEG Level	1	(0 ... 7)
Last Local State	Expired wtr	
Last Remote State	RAPS SF	
Last HP Request	NR	
Last Change Timestamp	26-01-2024 14:22:59	

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.

> **Note**
>
> The Guard Time is used to prevent Ethernet ring nodes from acting upon outdated R-APS messages and prevents the possibility of forming a closed loop.

- **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 (G.8032 ERPI Attribute Page).
2. Select the ERPI and click **Edit**. The ERPI Attribute – Edit page opens (G.8032 ERPI Attribute – Edit Page).
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**.

Viewing the ERPI Configuration and Status Parameters

The G.8032 ERPI Attribute page (G.8032 ERPI Attribute Page) 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 (G.8032 ERPI Attribute Page).
2. Select the ERPI and click **Edit**. The ERPI Attribute – Edit page opens (G.8032 ERPI Attribute – Edit Page).
   - ERPI Configuration Parameters lists and describes the parameters in the ERPI configuration section of the ERPI Attribute – Edit page.
   - ERPI Status Parameters lists and describes the parameters in the ERPI status section of the ERPI Attribute – Edit page.

Table 48 *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.

Parameter	Definition
Instance ID	Read-only. The MSTI to which the Ethernet service is mapped. See Mapping Ethernet Services to MSTP instances (MSTIs).
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 0Configuring 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 49 *ERPI Status Parameters*

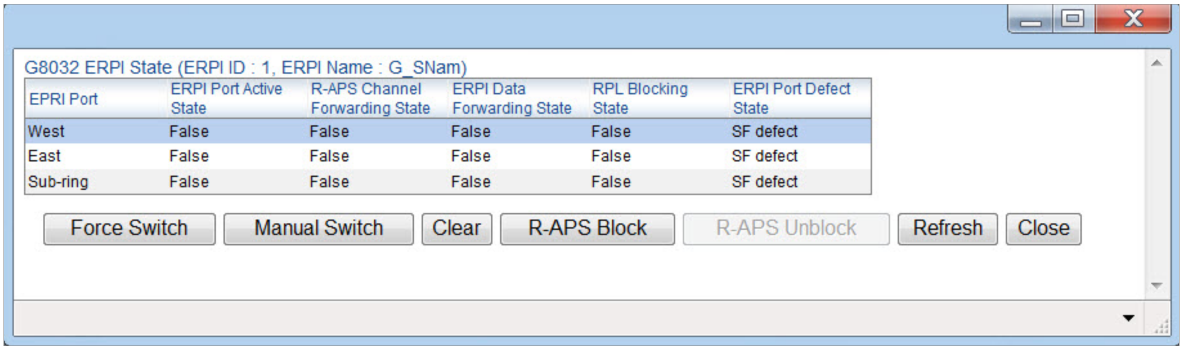
Parameter	Definition
ERPI State	Indicates the current ERPI state. Possible values are: • Initializing • Idle • Pending • Protecting • FS (Forced Switch) • MS (Manual Switch)
MEG Level	The Maintenance Entity Group (MEG) level used for R-APS messages sent in the ERPI.
Last Local State	Describes the current 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 Timestamp	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 (G.8032 ERPI Attribute Page).
2. Select the ERPI and click **State**. The ERPI Attribute – State page opens.

Figure 241 *G.8032 ERPI Attribute – State Page*



G8032 ERPI State (ERPI ID : 1, ERPI Name : G_SNam)

EPRI Port	ERPI Port Active State	R-APS Channel Forwarding State	ERPI Data Forwarding State	RPL Blocking State	ERPI Port Defect State
West	False	False	False	False	SF defect
East	False	False	False	False	SF defect
Sub-ring	False	False	False	False	SF defect

ERPI State Parameters lists and describes the parameters in the ERPI Attribute – State page.

Table 50 *ERPI State Parameters*

Parameter	Definition
ERPI Port	Identifies whether the row is for the West endpoint, the East endpoint, or a Sub-Ring connection point.
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 service point is in blocked state.
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 (G.8032 ERPI Attribute Page).
2. Select the ERPI and click **State**. The ERPI Attribute – State page opens (G.8032 ERPI Attribute – State Page).
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 (G.8032 ERPI Attribute Page).
2. Select the ERPI and click State. The ERPI Attribute – State page opens (G.8032 ERPI Attribute – State Page).
3. Select the service point on which you want to perform the operation.

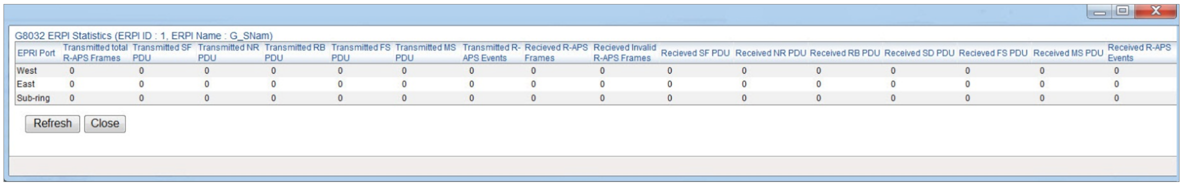
- To block R-APS message transmission on the service point, click R-APS Block.
- To enable R-APS message transmission on the service point, click R-APS Unblock.

Viewing ERPI Statistics

To view statistics about an ERPI:

1. Select **Ethernet** > **Protocols** > **G.8032** > **ERPI Attribute**. The G.8032 ERPI Attribute page opens (G.8032 ERPI Attribute Page).
2. Select the ERPI and click **Statistics**. The ERPI Attribute – Statistics page opens.

Figure 242 *G.8032 ERPI Attribute – Statistics Page*



G8032 ERPI Statistics (ERPI ID : 1, ERPI Name : G_SNam)

EPRI Port	Transmitted total R-APS Frames	Transmitted SF PDU	Transmitted NR PDU	Transmitted RB PDU	Transmitted FS PDU	Transmitted MS PDU	Transmitted R-APS Events	Recieved R-APS Frames	Recieved Invalid R-APS Frames	Recieved SF PDU	Received NR PDU	Received RB PDU	Received SD PDU	Recieved FS PDU	Received MS PDU	Received R-APS Events
West	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
East	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sub-ring	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

ERPI Statistics lists and describes the statistics shown in the ERPI Attribute – Statistics page.

Table 51 *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.

Parameter	Definition
Frames	
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 Events	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 Frames	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 Events	Reserved for future use.

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.

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).

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.

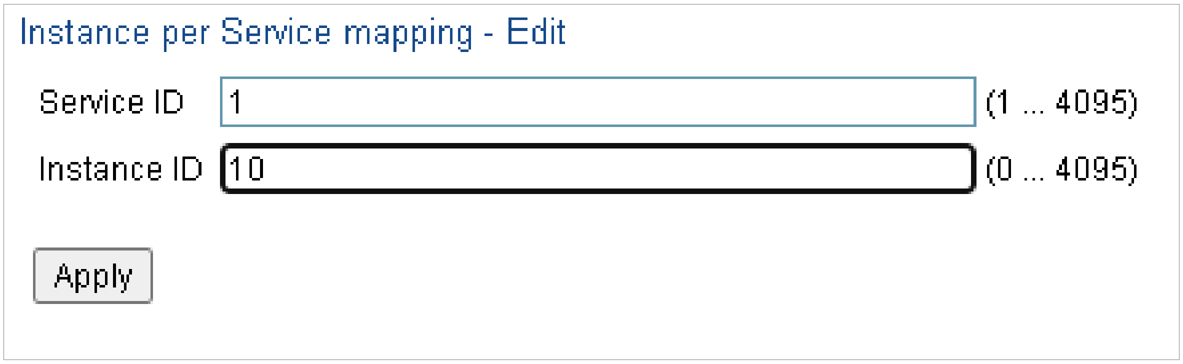
Note

Ethernet service-to-MSTI mapping is also a prerequisite to configuring G.8032. See Configuring G.8032.

To map Ethernet services to MSTP instances (MSTIs):

1. Select **Ethernet** > **General Configuration**. The Ethernet General Configuration page opens (Ethernet General Configuration Page).
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 243 *Instance Per Service Mapping – Edit Page*



Instance per Service mapping - Edit

Service ID: 1 (1 ... 4095)

Instance ID: 10 (0 ... 4095)

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:

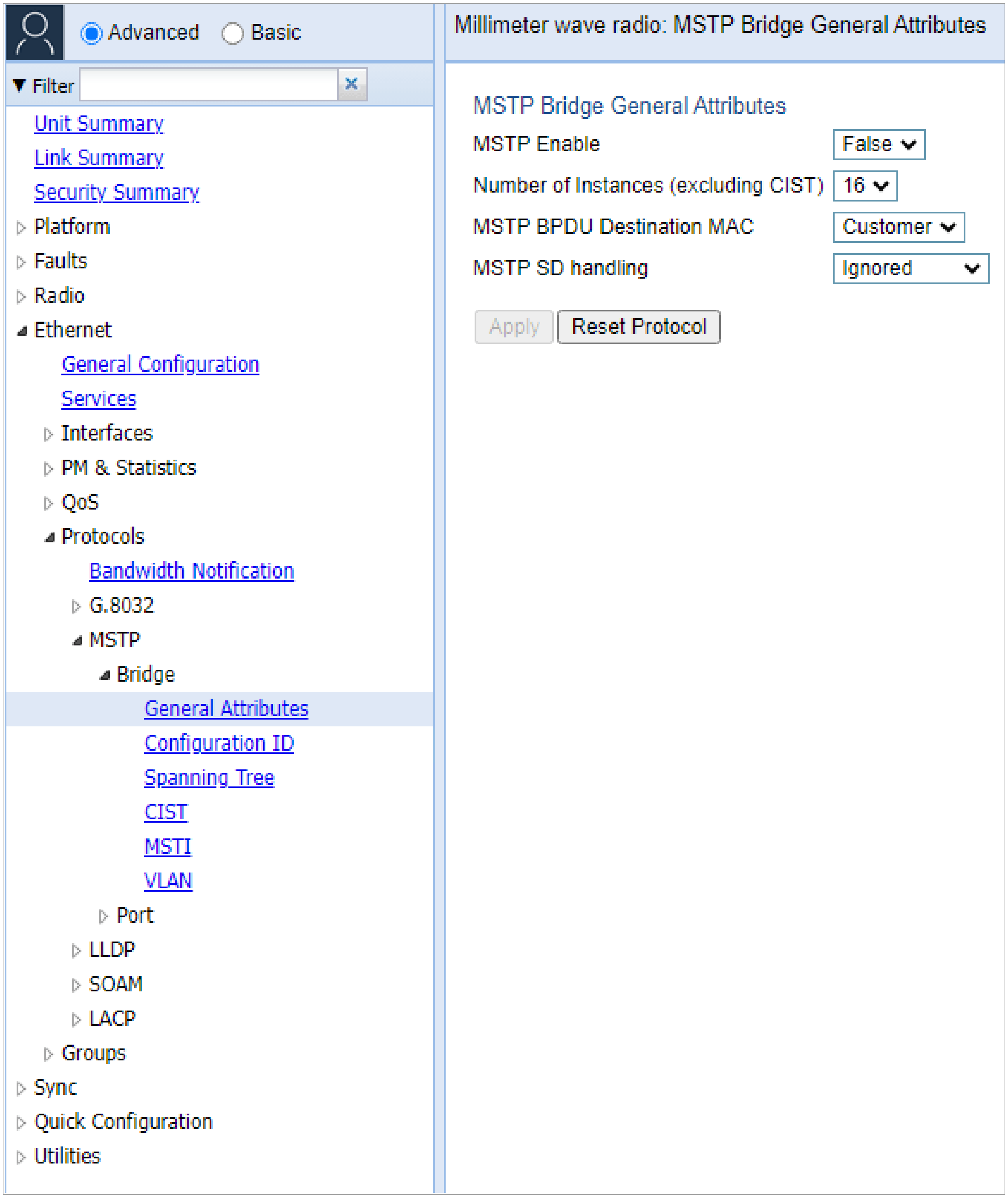
- Enabling MSTP and Configuring the MSTP Bridge General Attributes
- Viewing and Configuring the MSTP Bridge Configuration ID
- Viewing and Configuring the MSTP Bridge Spanning Tree
- Viewing and Configuring the MSTP Bridge CIST Parameters
- Viewing and Configuring the MSTP Bridge MSTI Parameters
- Viewing 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 244 *MSTP Bridge General Attributes Page*



Millimeter wave radio: MSTP Bridge General Attributes

MSTP Bridge General Attributes

MSTP Enable	False
Number of Instances (excluding CIST)	16
MSTP BPDU Destination MAC	Customer
MSTP SD handling	Ignored

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).

   Note

   Changing the Number of Instances causes the MSTP stack to reset.

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.

   Note

   SD handling is planned for future release.

6. Click **Apply**.

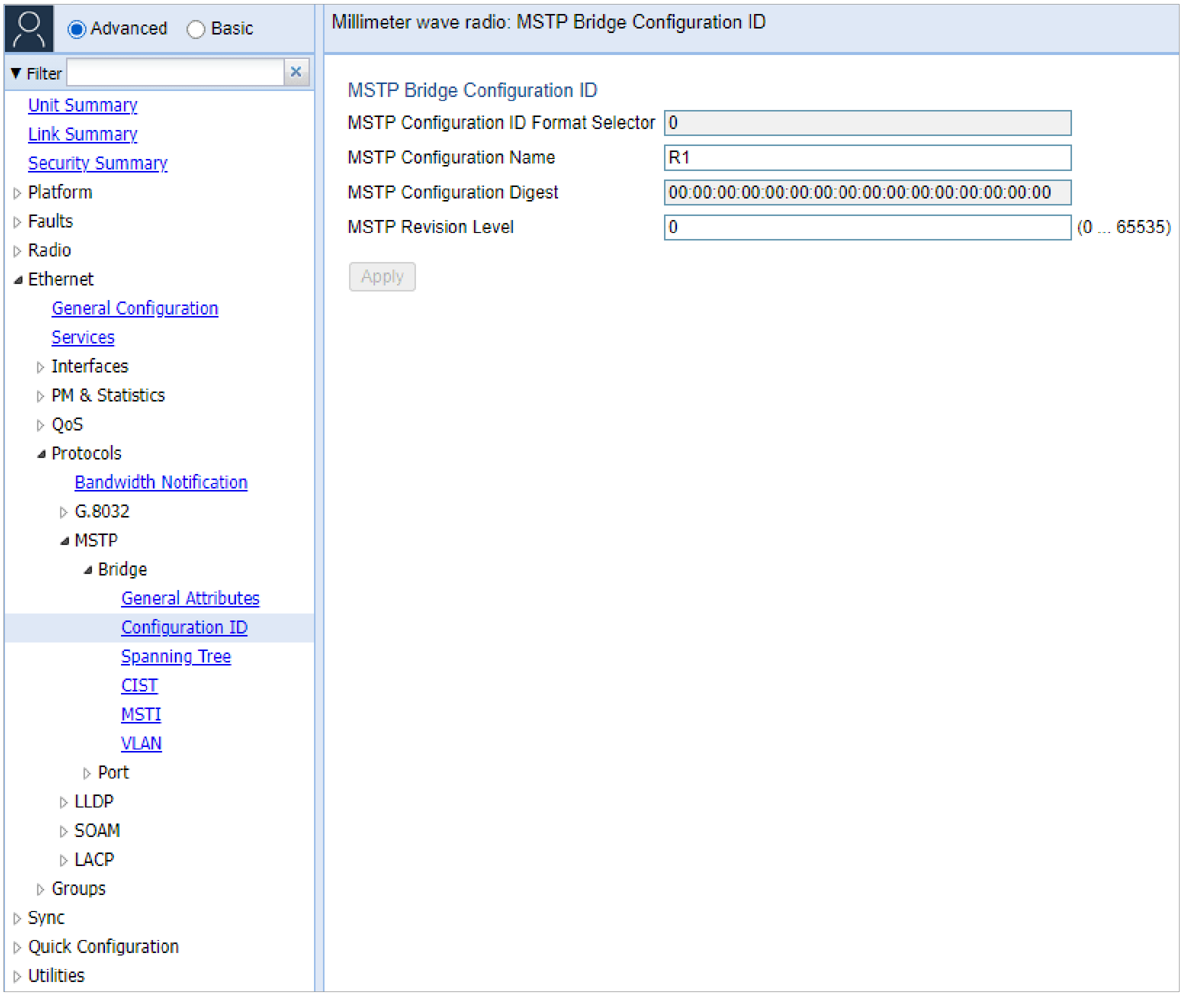
To reset the MSTP stack, click **Reset Protocol**.

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 245 *MSTP Bridge Configuration ID Page*



Millimeter wave radio: MSTP Bridge Configuration ID

MSTP Bridge Configuration ID

MSTP Configuration ID Format Selector: 0

MSTP Configuration Name: R1

MSTP Configuration Digest: 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

MSTP Revision Level: 0 (0 ... 65535)

2. Modify the configurable parameters.
3. Click **Apply**.

MSTP Bridge Configuration ID Parameters lists and describes the parameters in the MSTP Bridge Configuration ID page.

Table 52 *MSTP Bridge Configuration ID Parameters*

Parameter	Definition
MSTP Configuration ID Format Selector	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 Digest	Read-only. Displays the MSTP Configuration Digest.
MSTP Revision Level	Enter a valid MSTP revision level.

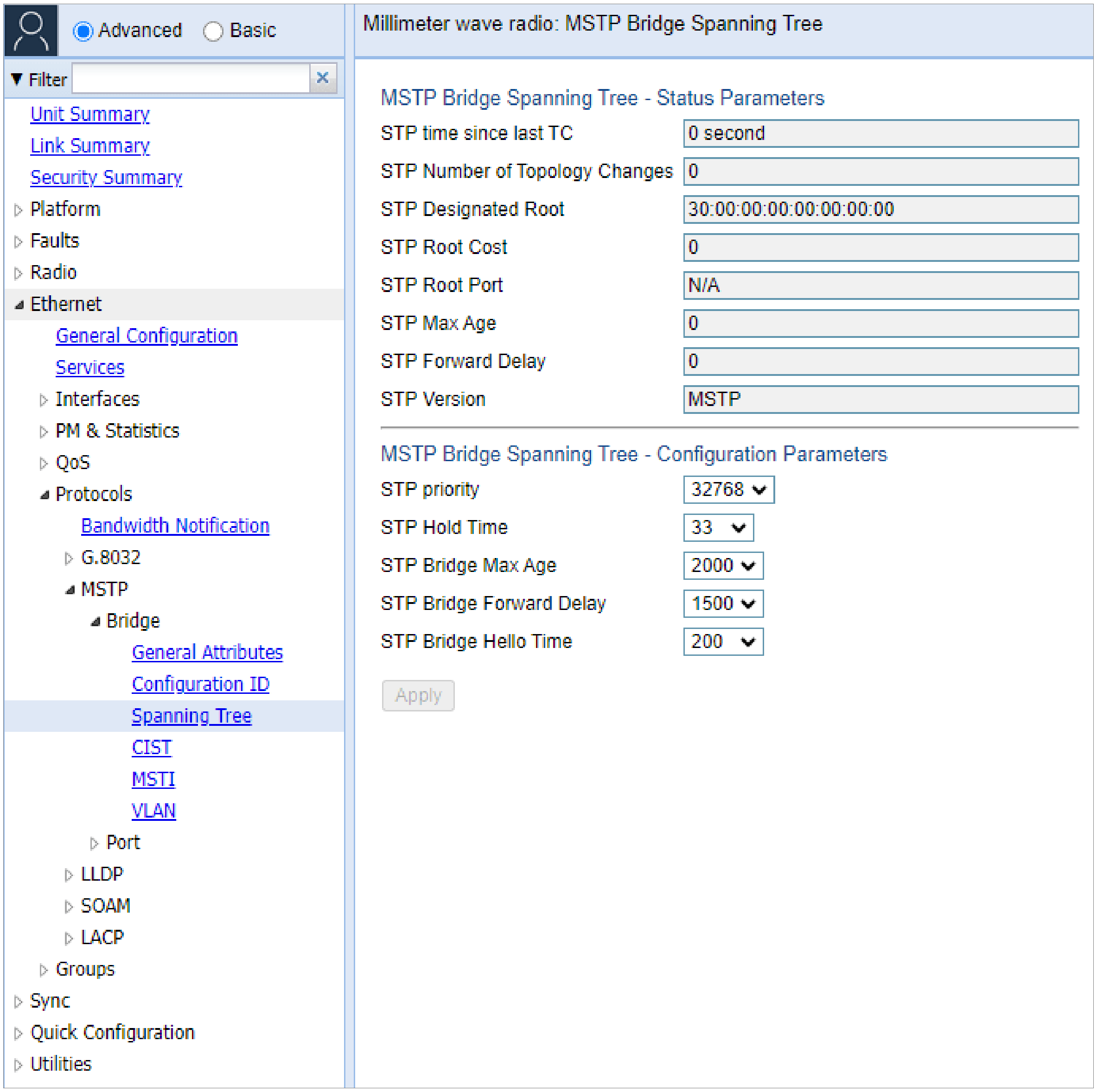
Parameter	Definition
	Note: Changing the Revision Level when MSTP is enabled causes the MSTP stack to reset.

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 246 *MSTP Bridge Spanning Tree Page*



Millimeter wave radio: MSTP Bridge Spanning Tree

MSTP Bridge Spanning Tree - Status Parameters

STP time since last TC	0 second
STP Number of Topology Changes	0
STP Designated Root	30:00:00:00:00:00:00:00
STP Root Cost	0
STP Root Port	N/A
STP Max Age	0
STP Forward Delay	0
STP Version	MSTP

MSTP Bridge Spanning Tree - Configuration Parameters

STP priority	32768
STP Hold Time	33
STP Bridge Max Age	2000
STP Bridge Forward Delay	1500
STP Bridge Hello Time	200

2. Modify the configurable parameters, described in MSTP Bridge Spanning Tree Configuration Parameters.
3. Click **Apply**.

MSTP Bridge Spanning Tree Status Parameters lists and describes the status parameters in the MSTP Bridge Spanning Tree page.

Table 53 *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 bridges use if and when this bridge becomes the root.
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 becomes the root.
STP Version	The STP version the bridge is currently running (MSTP).

Table 54 *MSTP Bridge Spanning Tree Configuration Parameters*

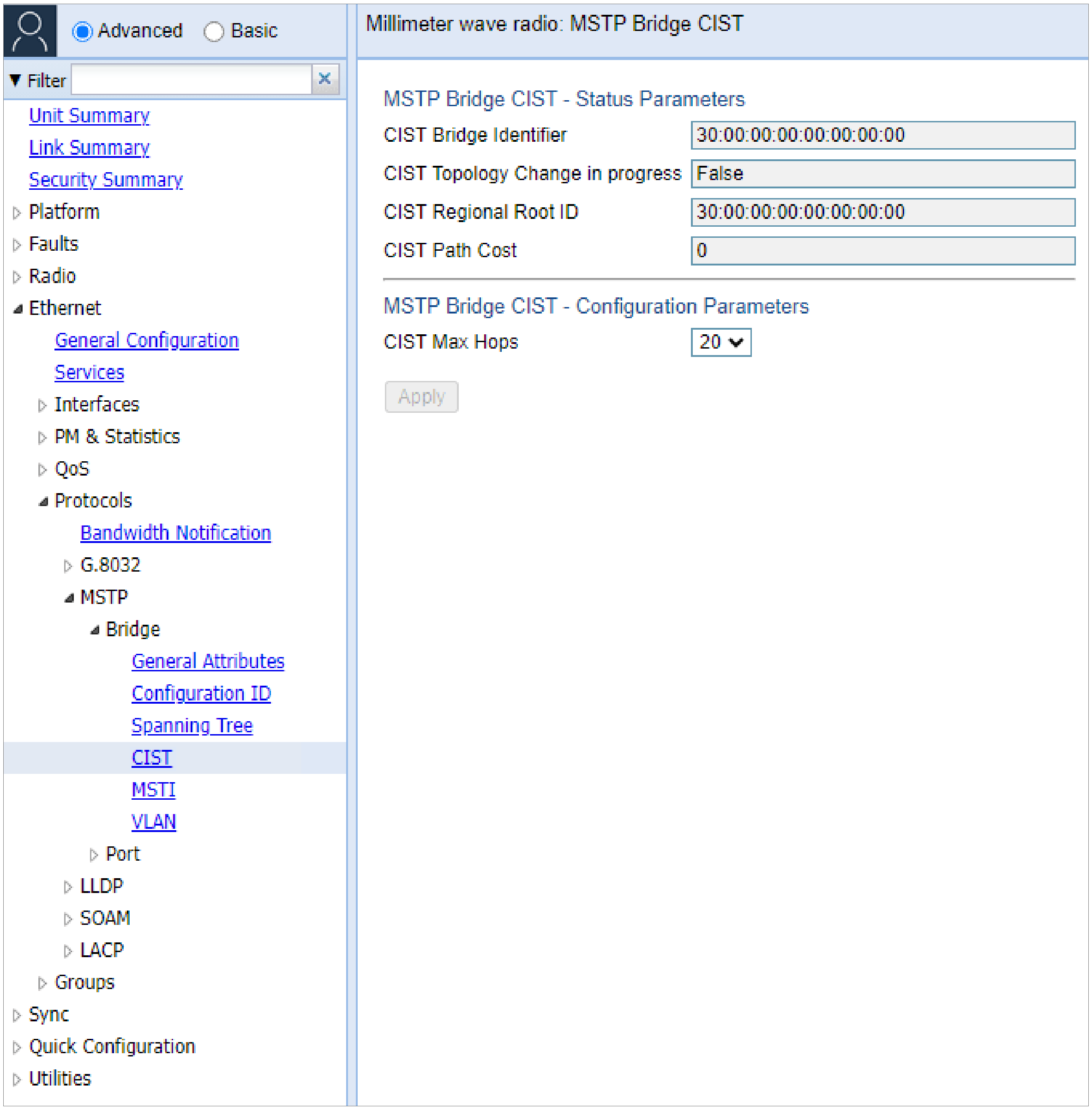
Parameter	Definition
STP Priority	Select a value as the writeable portion of the Bridge ID. This value constitutes the first two octets of the Bridge ID. Possible values are 0-61440, in steps of 4096
STP Hold Time	Select a value (in cs) as the interval length during which no more than two configuration 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. Options are 600-4000 cs.
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 247 *MSTP Bridge CIST Page*



Millimeter wave radio: MSTP Bridge CIST

MSTP Bridge CIST - Status Parameters

CIST Bridge Identifier	30:00:00:00:00:00:00:00
CIST Topology Change in progress	False
CIST Regional Root ID	30:00:00:00:00:00:00:00
CIST Path Cost	0

MSTP Bridge CIST - Configuration Parameters

CIST Max Hops: 20

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**.

MSTP Bridge CIST Status Parameters lists and describes the status parameters in the MSTP Bridge CIST page.

Table 55 *MSTP Bridge CIST Status Parameters*

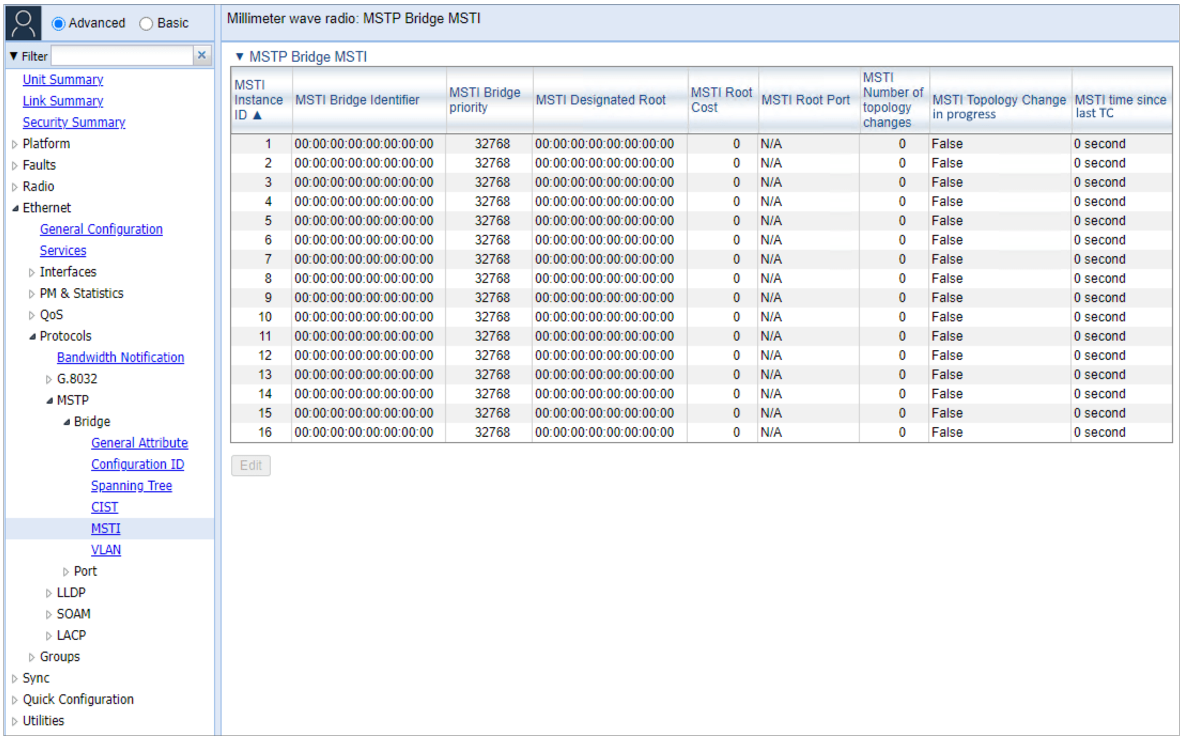
Parameter	Definition
CIST Bridge Identifier	The Bridge ID of the CIST.
CIST Topology Change in Progress	Indicates whether a topology change is currently in progress for any port that is part of the CIST.
CIST Regional Root ID	The Bridge ID of the current CIST regional root.
CIST Path Cost	The CIST path 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 248 *MSTP Bridge MSTI Page*



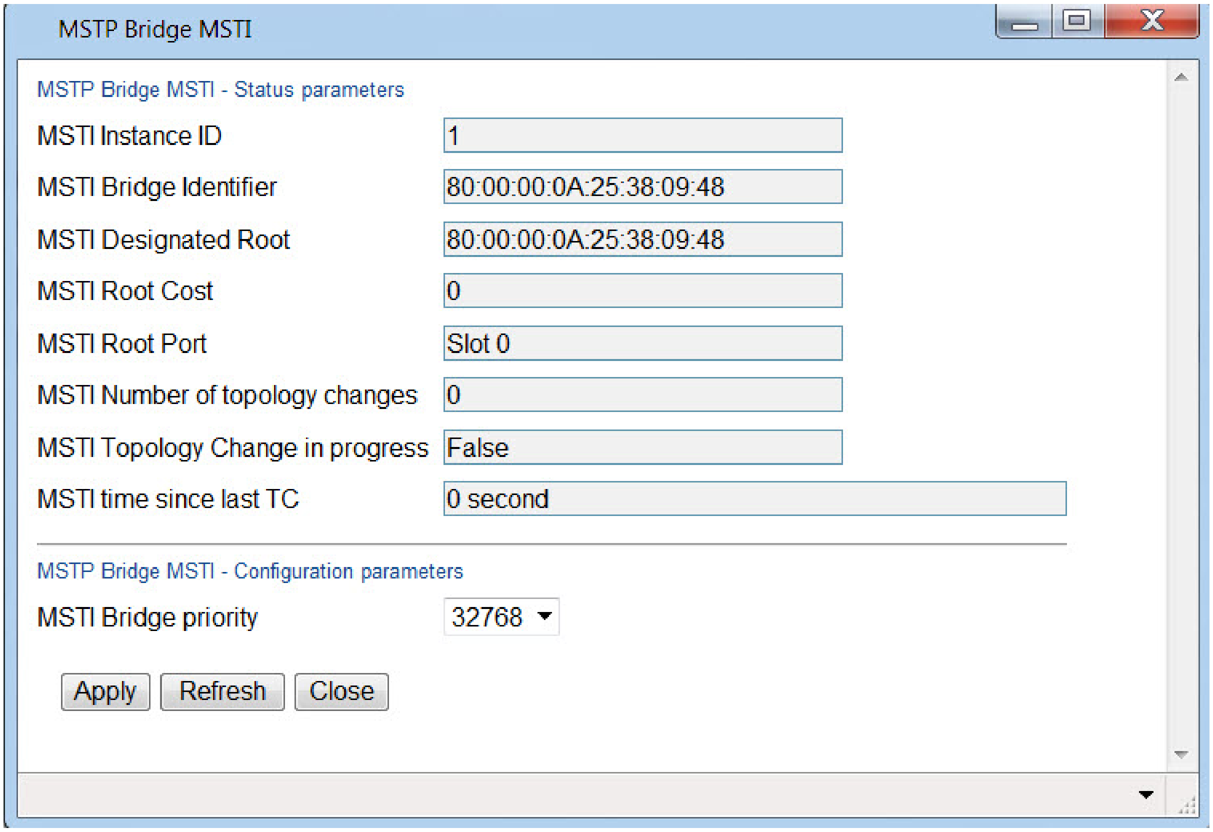
Millimeter wave radio: MSTP Bridge MSTI

▼ MSTP Bridge MSTI

MSTI Instance ID ▲	MSTI Bridge Identifier	MSTI Bridge priority	MSTI Designated Root	MSTI Root Cost	MSTI Root Port	MSTI Number of topology changes	MSTI Topology Change in progress	MSTI time since last TC
1	00:00:00:00:00:00:00:00	32768	00:00:00:00:00:00:00:00	0	N/A	0	False	0 second
2	00:00:00:00:00:00:00:00	32768	00:00:00:00:00:00:00:00	0	N/A	0	False	0 second
3	00:00:00:00:00:00:00:00	32768	00:00:00:00:00:00:00:00	0	N/A	0	False	0 second
4	00:00:00:00:00:00:00:00	32768	00:00:00:00:00:00:00:00	0	N/A	0	False	0 second
5	00:00:00:00:00:00:00:00	32768	00:00:00:00:00:00:00:00	0	N/A	0	False	0 second
6	00:00:00:00:00:00:00:00	32768	00:00:00:00:00:00:00:00	0	N/A	0	False	0 second
7	00:00:00:00:00:00:00:00	32768	00:00:00:00:00:00:00:00	0	N/A	0	False	0 second
8	00:00:00:00:00:00:00:00	32768	00:00:00:00:00:00:00:00	0	N/A	0	False	0 second
9	00:00:00:00:00:00:00:00	32768	00:00:00:00:00:00:00:00	0	N/A	0	False	0 second
10	00:00:00:00:00:00:00:00	32768	00:00:00:00:00:00:00:00	0	N/A	0	False	0 second
11	00:00:00:00:00:00:00:00	32768	00:00:00:00:00:00:00:00	0	N/A	0	False	0 second
12	00:00:00:00:00:00:00:00	32768	00:00:00:00:00:00:00:00	0	N/A	0	False	0 second
13	00:00:00:00:00:00:00:00	32768	00:00:00:00:00:00:00:00	0	N/A	0	False	0 second
14	00:00:00:00:00:00:00:00	32768	00:00:00:00:00:00:00:00	0	N/A	0	False	0 second
15	00:00:00:00:00:00:00:00	32768	00:00:00:00:00:00:00:00	0	N/A	0	False	0 second
16	00:00:00:00:00:00:00:00	32768	00:00:00:00:00:00:00:00	0	N/A	0	False	0 second

2. To view all the bridge parameters of an MSTI and/or configure its bridge priority, select the MSTI and click Edit.

Figure 249 *MSTP Bridge MSTI – Edit Page*



MSTP Bridge MSTI

MSTP Bridge MSTI - Status parameters

MSTI Instance ID: 1

MSTI Bridge Identifier: 80:00:00:0A:25:38:09:48

MSTI Designated Root: 80:00:00:0A:25:38:09:48

MSTI Root Cost: 0

MSTI Root Port: Slot 0

MSTI Number of topology changes: 0

MSTI Topology Change in progress: False

MSTI time since last TC: 0 second

MSTP Bridge MSTI - Configuration parameters

MSTI Bridge priority: 32768

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**.

MSTP Bridge MSTI Status Parameters lists and describes the status parameters in the MSTP Bridge MSTI page.

Figure 250 *MSTP Bridge MSTI Status Parameters*

Parameter	Definition
MSTI Instance ID	The MSTI ID.
MSTI Bridge Identifier	The Bridge ID for the MSTI.
MSTI Designated Root	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.

Parameter	Definition
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 Progress	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 port in the MSTI.

Viewing the MSTP VLAN Parameters

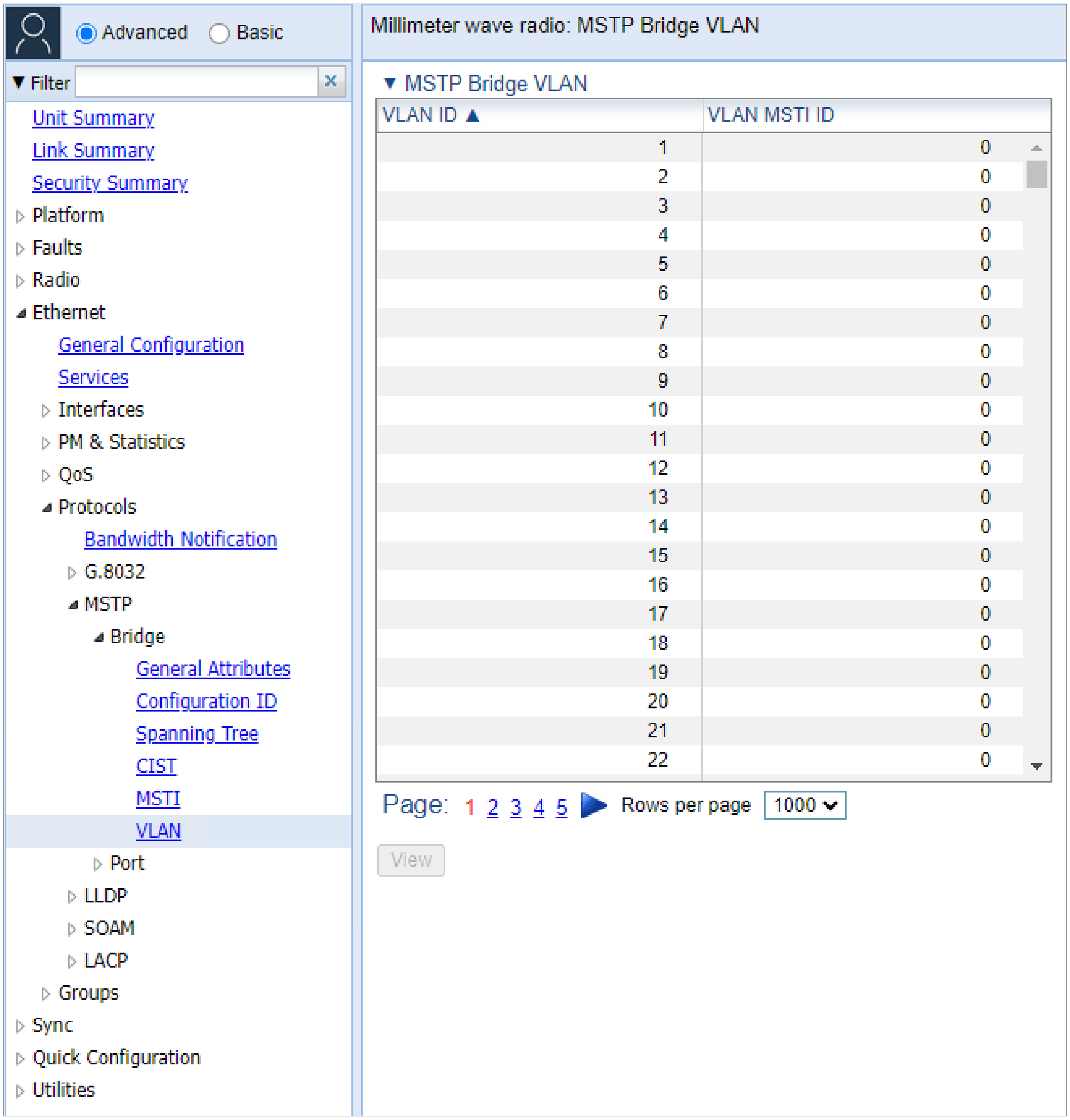
Each Ethernet service is mapped to an MSTI. By default, all services (VLAN ID) are assigned to MSTI 0 (CIST). See Mapping Ethernet Services to MSTP instances (MSTIs).

> **Note**
>
> A service mapped to MSTI 4095 is never blocked by any protocol.

To view the VLAN ID to MSTI mapping table:

1. Select **Ethernet** > **Protocols** > **MSTP** > **Bridge** > **VLAN**. The MSTP Bridge VLAN page opens.

Figure 251 *MSTP Bridge VLAN Page*



Millimeter wave radio: MSTP Bridge VLAN

MSTP Bridge VLAN

VLAN ID ▲	VLAN MSTI ID
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0
22	0

Page: 1 2 3 4 5 ▶ Rows per page 1000

Configuring the MSTP Port Parameters

This section includes:

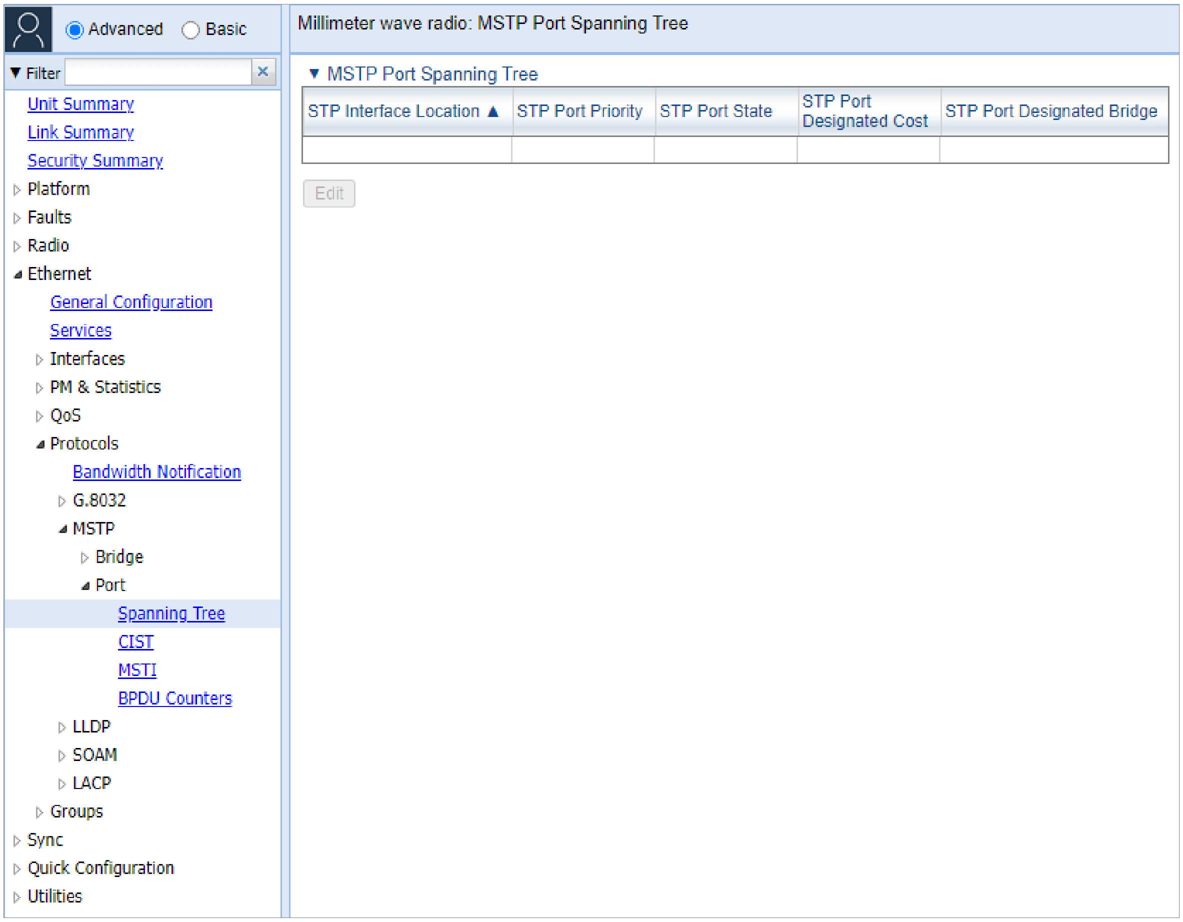
- Viewing and Configuring the MSTP Port Spanning Tree
- Viewing and Configuring the MSTP Port CIST Parameters
- Viewing and Configuring the MSTP Port MSTI Parameters
- Viewing and Resetting the BPDU Counters

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 252 *MSTP Port Spanning Tree Page*



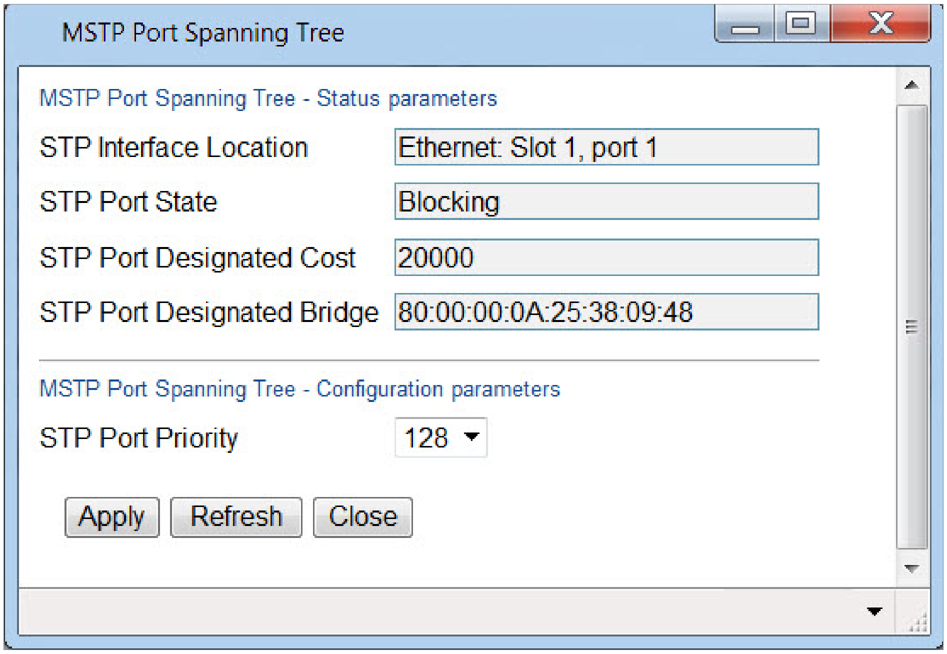
Millimeter wave radio: MSTP Port Spanning Tree

▼ MSTP Port Spanning Tree

STP Interface Location ▲	STP Port Priority	STP Port State	STP Port Designated Cost	STP Port Designated Bridge

2. Select an interface and click **Edit**. The MSTP Port Spanning Tree – Edit page opens.

Figure 253 *MSTP Port Spanning Tree – Edit Page*



MSTP Port Spanning Tree

MSTP Port Spanning Tree - Status parameters

STP Interface Location: Ethernet: Slot 1, port 1

STP Port State: Blocking

STP Port Designated Cost: 20000

STP Port Designated Bridge: 80:00:00:0A:25:38:09:48

MSTP Port Spanning Tree - Configuration parameters

STP Port Priority: 128

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**.

MSTP Port Spanning Tree Status Parameters lists and describes the status parameters in the MSTP Port Spanning Tree page.

Table 56 *MSTP Port Spanning Tree Status Parameters*

Parameter	Definition
STP Interface Location	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 MAC addresses of incoming frames. • **Disabled** – The port is disabled (not by MSTP).
STP Port	The CIST Path Cost of the segment connected to this port. This value is compared to

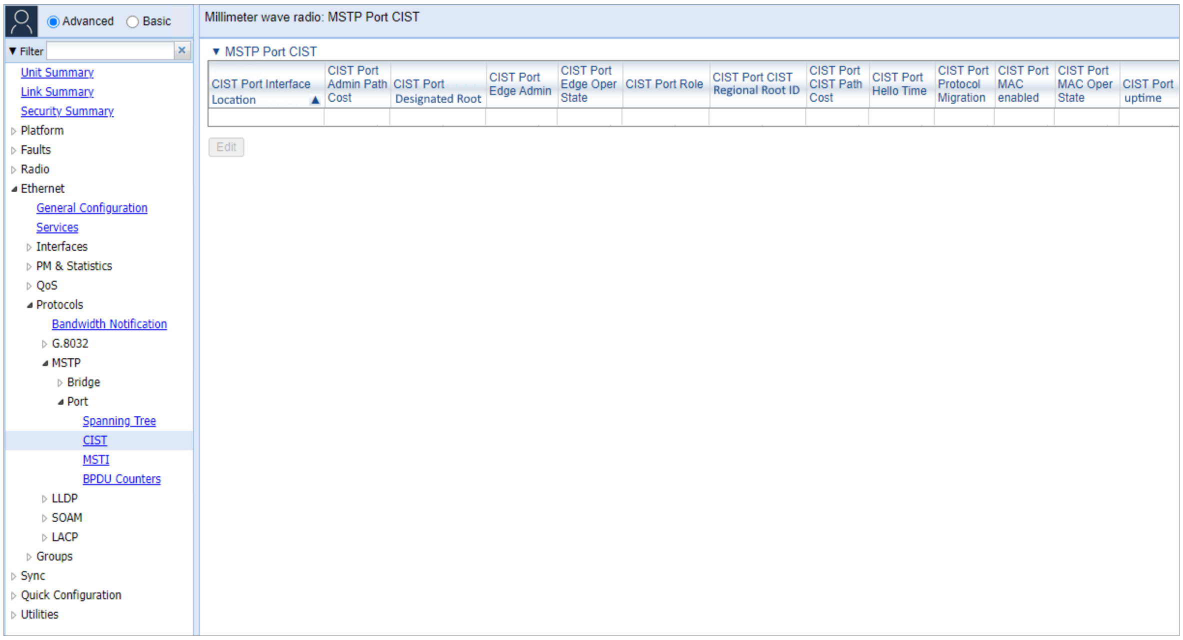
Parameter	Definition
Designated Cost	the root path cost in received BPDUs.
STP Port Designated Bridge	The CIST Bridge ID of the bridge that this port considers to be the designated bridge for this port's segment.

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 254 *MSTP Port CIST Page*



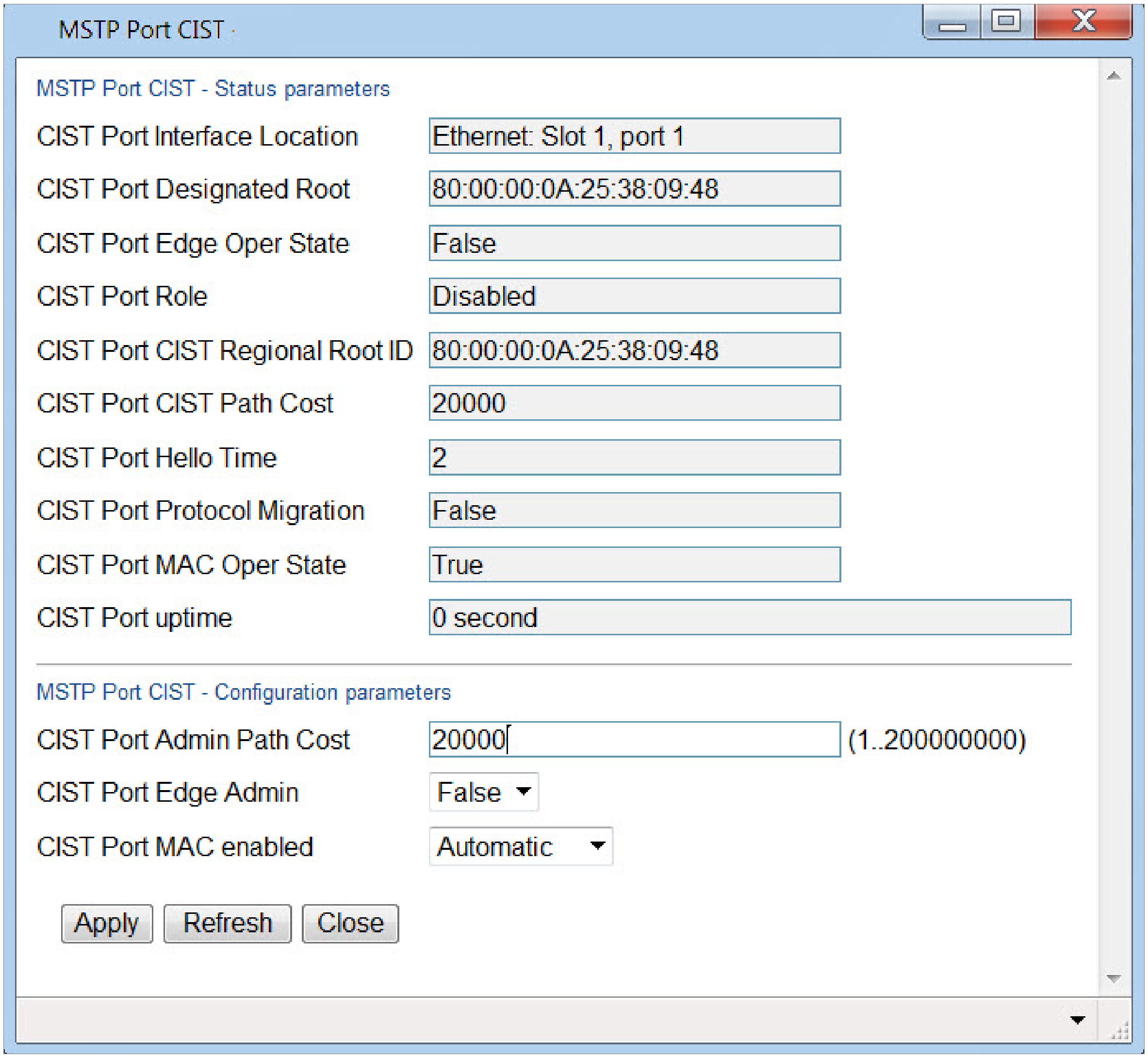
Millimeter wave radio: MSTP Port CIST

▼ MSTP Port CIST

CIST Port Interface Location ▲	CIST Port Admin Path Cost	CIST Port Designated Root	CIST Port Edge Admin	CIST Port Edge Oper State	CIST Port Role	CIST Port CIST Regional Root ID	CIST Port CIST Path Cost	CIST Port Hello Time	CIST Port Protocol Migration	CIST Port MAC enabled	CIST Port MAC Oper State	CIST Port uptime

2. Select an interface and click **Edit**. The MSTP Port CIST – Edit page opens.

Figure 255 *MSTP Port CIST – Edit Page*



MSTP Port CIST

MSTP Port CIST - Status parameters

CIST Port Interface Location	Ethernet: Slot 1, port 1
CIST Port Designated Root	80:00:00:0A:25:38:09:48
CIST Port Edge Oper State	False
CIST Port Role	Disabled
CIST Port CIST Regional Root ID	80:00:00:0A:25:38:09:48
CIST Port CIST Path Cost	20000
CIST Port Hello Time	2
CIST Port Protocol Migration	False
CIST Port MAC Oper State	True
CIST Port uptime	0 second

MSTP Port CIST - Configuration parameters

CIST Port Admin Path Cost	20000 (1..200000000)
CIST Port Edge Admin	False
CIST Port MAC enabled	Automatic

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.

> **Note**
>
> Changing the value of this parameter is considered to be a topology change by the MSTP mechanism.

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**.

MSTP Port CIST Status Parameters lists and describes the status parameters in the MSTP Port Spanning Tree page.

Table 57 *MSTP Port CIST Status Parameters*

Parameter	Definition
CIST Port Interface Location	The slot number and port number of the port.
CIST Port Designated Root	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 automatically determines its operational Edge port state.
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 bridge. • **Alternate** – The port is not forwarding traffic (blocked) but can become a Designated port after MSTP calculation.

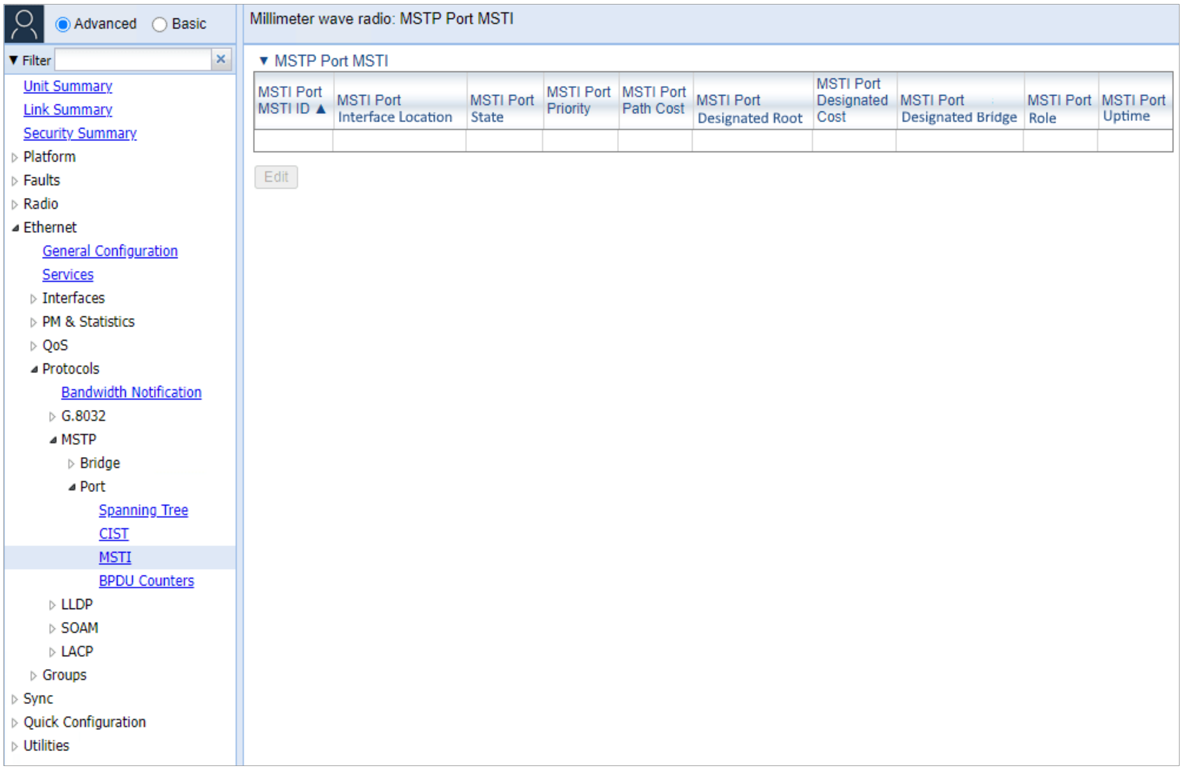
Parameter	Definition
CIST Port CIST Regional Route ID	The Bridge ID of the current CIST Regional Root.
CIST Port CIST Path Cost	The CIST path cost from the transmitting bridge to the CIST regional root. If the transmitting bridge is the CIST regional root, the value of this parameter will be 0.
CIST Port Hello Time	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. **Note**: Migration support is planned for future release.
CIST Port MAC Oper State	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 256 *MSTP Port MSTI Page*



● Advanced ○ Basic

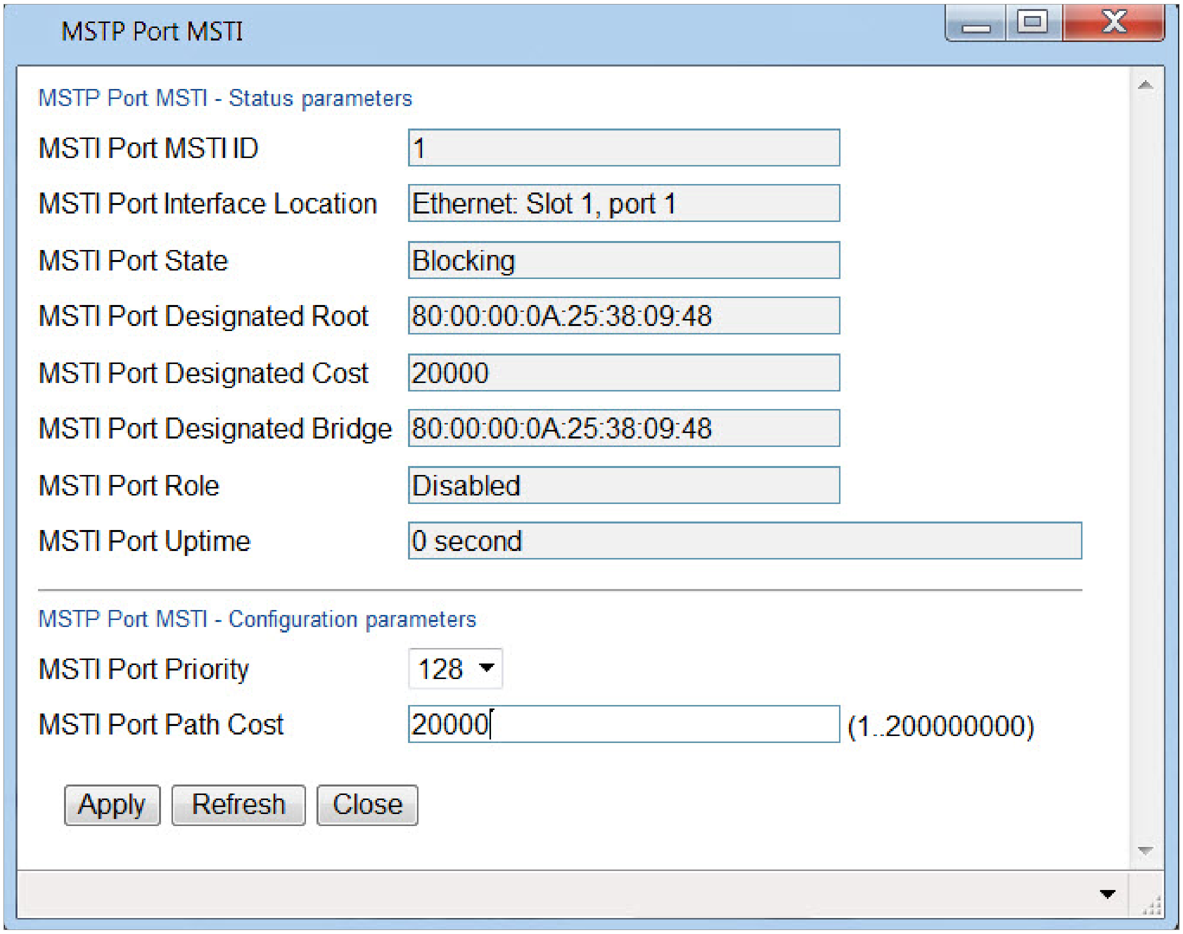
Millimeter wave radio: MSTP Port MSTI

▼ MSTP Port MSTI

MSTI Port MSTI ID ▲	MSTI Port Interface Location	MSTI Port State	MSTI Port Priority	MSTI Port Path Cost	MSTI Port Designated Root	MSTI Port Designated Cost	MSTI Port Designated Bridge	MSTI Port Role	MSTI Port Uptime

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 257 *MSTP Port MSTI – Edit Page*



MSTP Port MSTI

MSTP Port MSTI - Status parameters

MSTI Port MSTI ID: 1

MSTI Port Interface Location: Ethernet: Slot 1, port 1

MSTI Port State: Blocking

MSTI Port Designated Root: 80:00:00:0A:25:38:09:48

MSTI Port Designated Cost: 20000

MSTI Port Designated Bridge: 80:00:00:0A:25:38:09:48

MSTI Port Role: Disabled

MSTI Port Uptime: 0 second

MSTP Port MSTI - Configuration parameters

MSTI Port Priority: 128

MSTI Port Path Cost: 20000 (1..200000000)

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.

> **Note**
>
> Changing the value of this parameter is considered to be a topology change by the MSTP mechanism.

4. In the **MSTI Port Path Cost** field, select the port's Path Cost parameter value 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 is affected.

5. Click **Apply**, then **Close**.

MSTP Port MSTI Status Parameters lists and describes the status parameters in the MSTP MSTI Tree page.

Table 58 *MSTP Port MSTI Status Parameters*

Parameter	Definition
MSTI Port MSTI	The MSTI ID.

Parameter	Definition
ID	
MSTI Port Interface Location	The slot number and port number of the port.
MSTI Port State	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 Root	The Regional Root ID component of the port's Port Priority vector for the MSTI.
MSTI Port Designated Cost	The Internal Root Path Cost component of the port's MSTI port priority vector, for the MSTI.
MSTI Port Designated Bridge	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. • **Alternat**e – 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.

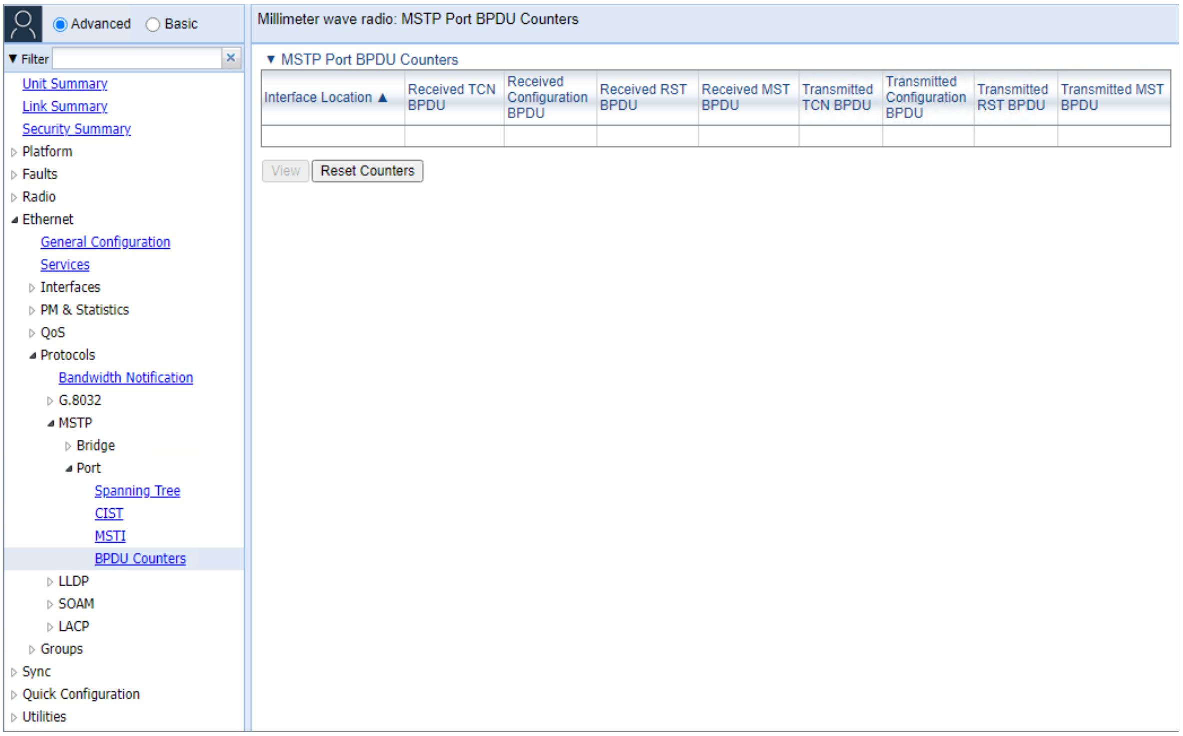
Parameter	Definition
MSTI Port Uptime	The port's uptime parameter value for the MSTI. This is the number of seconds that have elapsed since the port was last reset or initialized.

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 258 *MSTP Port BPDU Counters Page*



Millimeter wave radio: MSTP Port BPDU Counters

▼ MSTP Port BPDU Counters

Interface Location ▲	Received TCN BPDU	Received Configuration BPDU	Received RST BPDU	Received MST BPDU	Transmitted TCN BPDU	Transmitted Configuration BPDU	Transmitted RST BPDU	Transmitted MST BPDU

- 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.

MSTP BPDU Counters describes the available MSTP BPDU counters.

Table 59 *MSTP BPDU Counters*

Parameter	Definition
Interface Location	The location of the port.
Received TCN BPDU	The number of Topology Change Notifications (TCN) BPDUs received since the last counter reset.
Received Configuration BPDU	The number of configuration BPDUs received since the last counter reset.

Parameter	Definition
Received RST BPDU	The number of Rapid Spanning Tree (RST) BPDUs received since the last counter reset.
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 BPDU	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.

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

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.

The Monitored Interface can be a single radio interface, a Multi-Carrier ABC group, a Multiband group, or a radio LAG. To be used as a Monitored Interface, the LAG must consist of radio interfaces only.

Note

The Control Interface can be a single Ethernet interface or an Ethernet LAG. To be used as a Control Interface, the LAG must consist of Ethernet interfaces only. When the Control

Interface is a LAG, EBN messages are only sent to the first active member of the LAG.

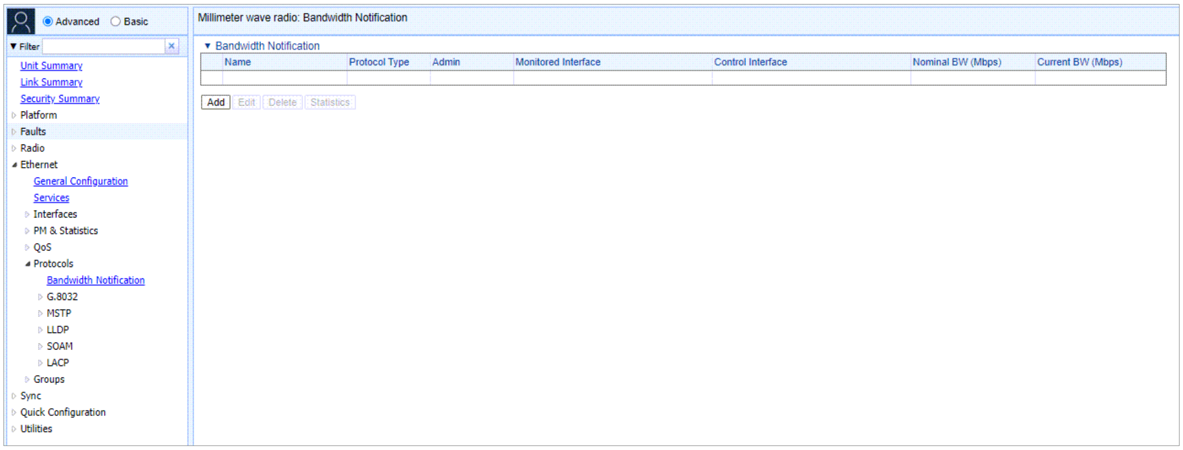
The same radio interface can be configured as a Monitored Interface for multiple EBN instances. However, an Ethernet interface can only be configured as a Control Interface for a single EBN instance.

Adding an ETH-BN Entity

To add an ETH-BN entity:

1. Select Ethernet > Protocols > Bandwidth Notification. The Bandwidth Notification page opens.

Figure 259 *Bandwidth Notification Page*



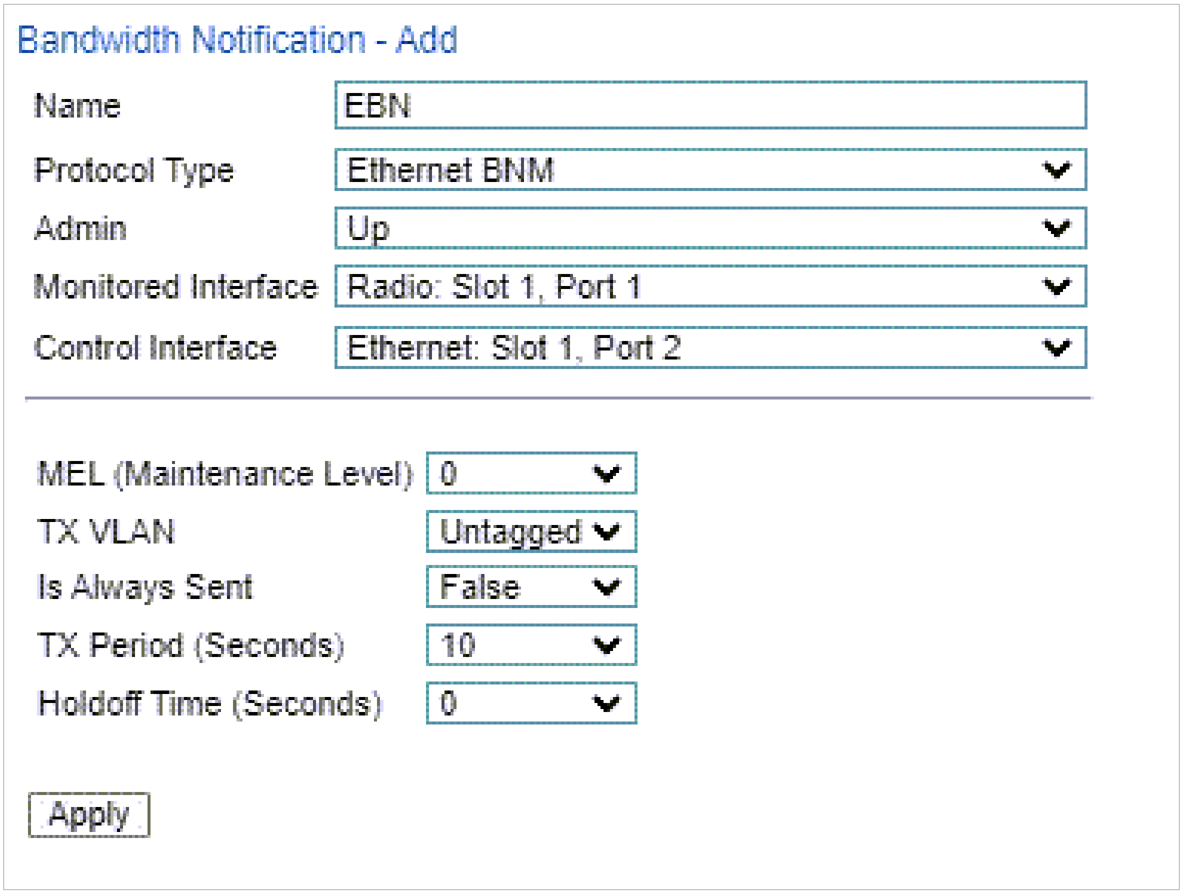
Millimeter wave radio: Bandwidth Notification

▼ Bandwidth Notification

Name	Protocol Type	Admin	Monitored Interface	Control Interface	Nominal BW (Mbps)	Current BW (Mbps)

2. Click **Add**. The Bandwidth Notification - Add page opens.

Figure 260 *Bandwidth Notification – Add Page*



Bandwidth Notification - Add

Name	EBN
Protocol Type	Ethernet BNM
Admin	Up
Monitored Interface	Radio: Slot 1, Port 1
Control Interface	Ethernet: Slot 1, Port 2
MEL (Maintenance Level)	0
TX VLAN	Untagged
Is Always Sent	False
TX Period (Seconds)	10
Holdoff Time (Seconds)	0

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. It can be an individual Ethernet interface or a LAG group.
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. For Link Bonding configurations, it is recommended to leave the default value of 0 so that BNM frames will be sent immediately to the Link Bonding group on the main unit.

> **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**.

ETH-BN Status Parameters describes the status (read-only) fields in the Bandwidth Notification table.

Table 60 *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.

Editing an ETH-BN Entity

To edit an ETH-BN entity:

1. Select **Ethernet** > **Protocols** > **Bandwidth Notification**. The Bandwidth Notification page opens (Bandwidth Notification Page).
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 (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**.

Deleting an ETH-BN Entity

To delete an ETH-BN entity:

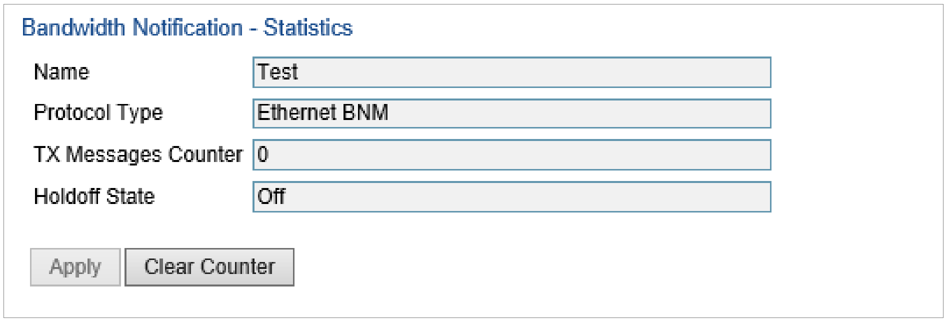
1. Select **Ethernet** > **Protocols** > **Bandwidth Notification**. The Bandwidth Notification page opens (Bandwidth Notification Page).
2. Select the ETH-BN entity in the Bandwidth Notification page.
3. Click **Delete**. The ETH-BN entity is removed.

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 (Bandwidth Notification Page).
2. Select the ETH-BN entity in the Bandwidth Notification page.
3. Click Statistics. The Bandwidth Notification - Statistics page opens.

Figure 261 *Bandwidth Notification - Statistics Page (ETH-BN)*



Bandwidth Notification - Statistics

Name	Test
Protocol Type	Ethernet BNM
TX Messages Counter	0
Holdoff State	Off

ETH-BN Entity Statistics Parameters describes the ETH-BN entity statistics.

Table 61 *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.

Configuring LLDP

This section includes:

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 – 2009 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.

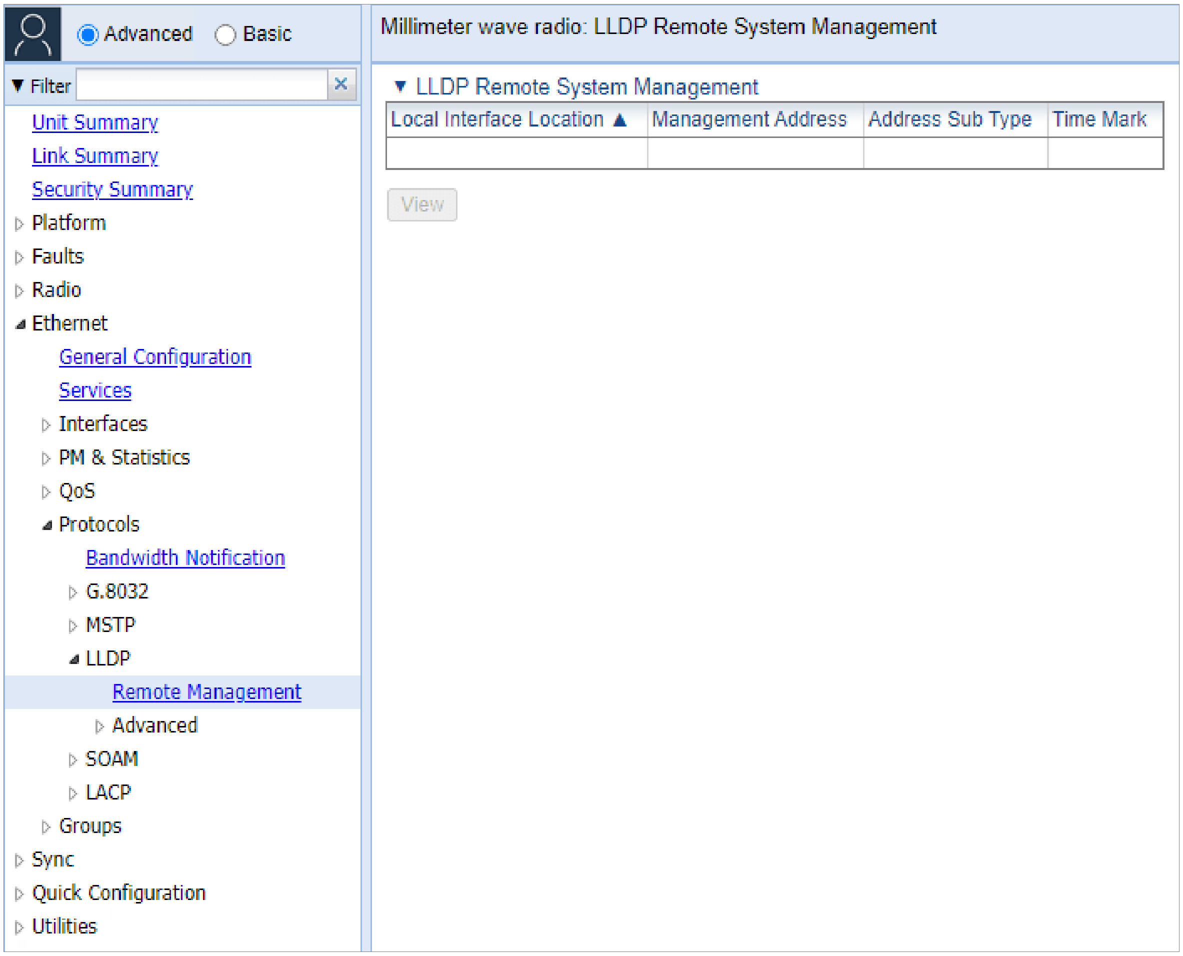
LLDP is used to send notifications to the NMS, based on data of the local unit and data gathered from peer systems. These notifications enable the NMS to build an accurate network topology.

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 262 *LLDP Remote System Management Page*



Millimeter wave radio: LLDP Remote System Management

▼ LLDP Remote System Management

Local Interface Location ▲	Management Address	Address Sub Type	Time Mark

LLDP Remote System Management Parameters describes the LLDP remote system management parameters. These parameters are read-only.

Table 62 *LLDP Remote System Management Parameters*

Parameter	Definition
Local Interface Location	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.
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.

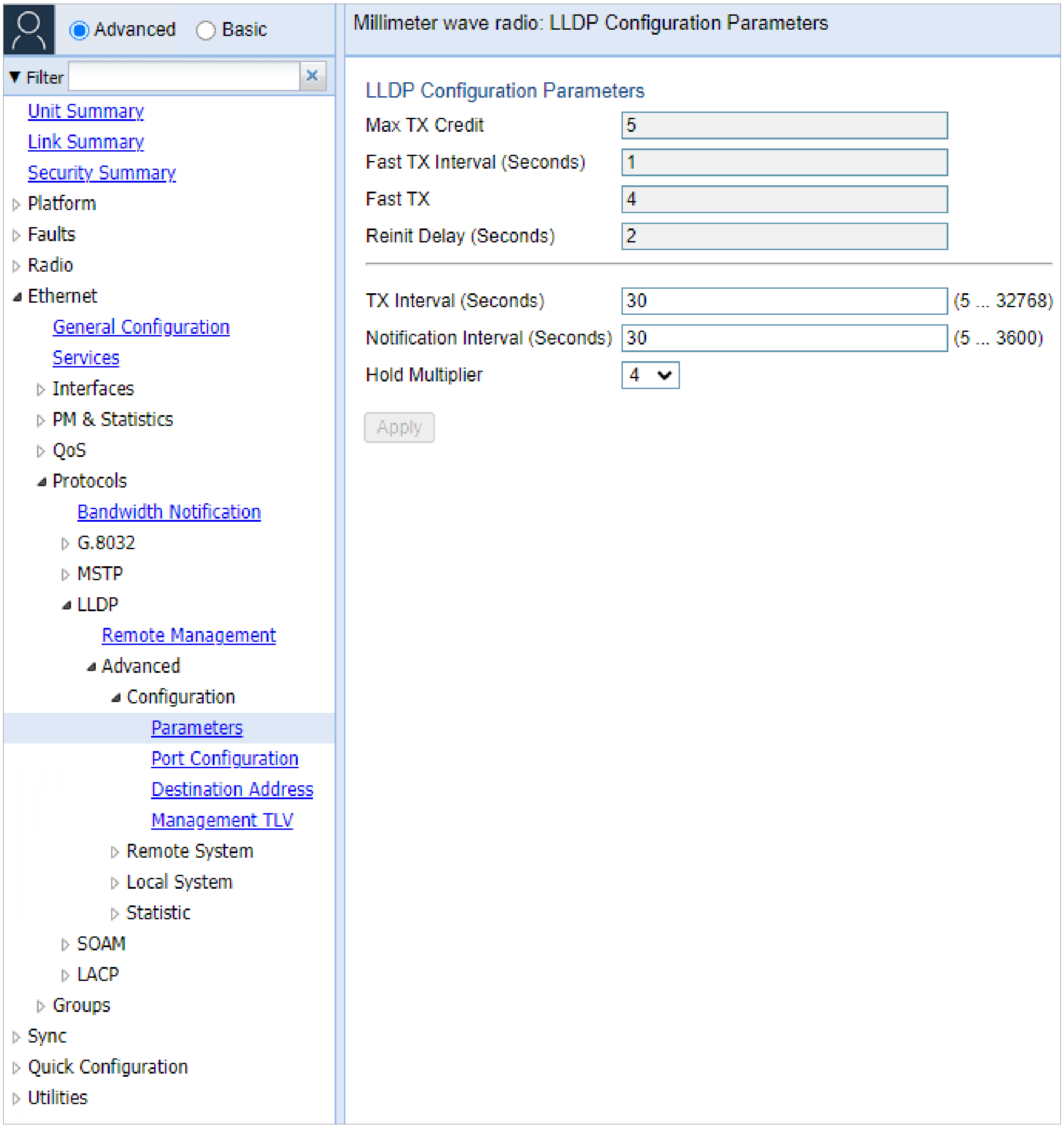
Note

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 263 *LLDP Configuration Parameters Page*



Millimeter wave radio: LLDP Configuration Parameters

LLDP Configuration Parameters

Max TX Credit	5	
Fast TX Interval (Seconds)	1	
Fast TX	4	
Reinit Delay (Seconds)	2	
TX Interval (Seconds)	30	(5 ... 32768)
Notification Interval (Seconds)	30	(5 ... 3600)
Hold Multiplier	4	

2. Modify the configurable parameters, described in LLDP Configurable Configuration Parameters.

3. Click **Apply**.

LLDP Read-Only Configuration Parameters lists and describes the status parameters in the LLDP Configuration Parameters page.

Table 63 *LLDP Read-Only Configuration Parameters*

Parameter	Definition
Max TX	Displays the maximum number of consecutive LLDPDUs that can be transmitted at any

Parameter	Definition
Credit	one time. In this release, the Max TX Credit is set at 5.
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.

Table 64 *LLDP Configurable Configuration Parameters*

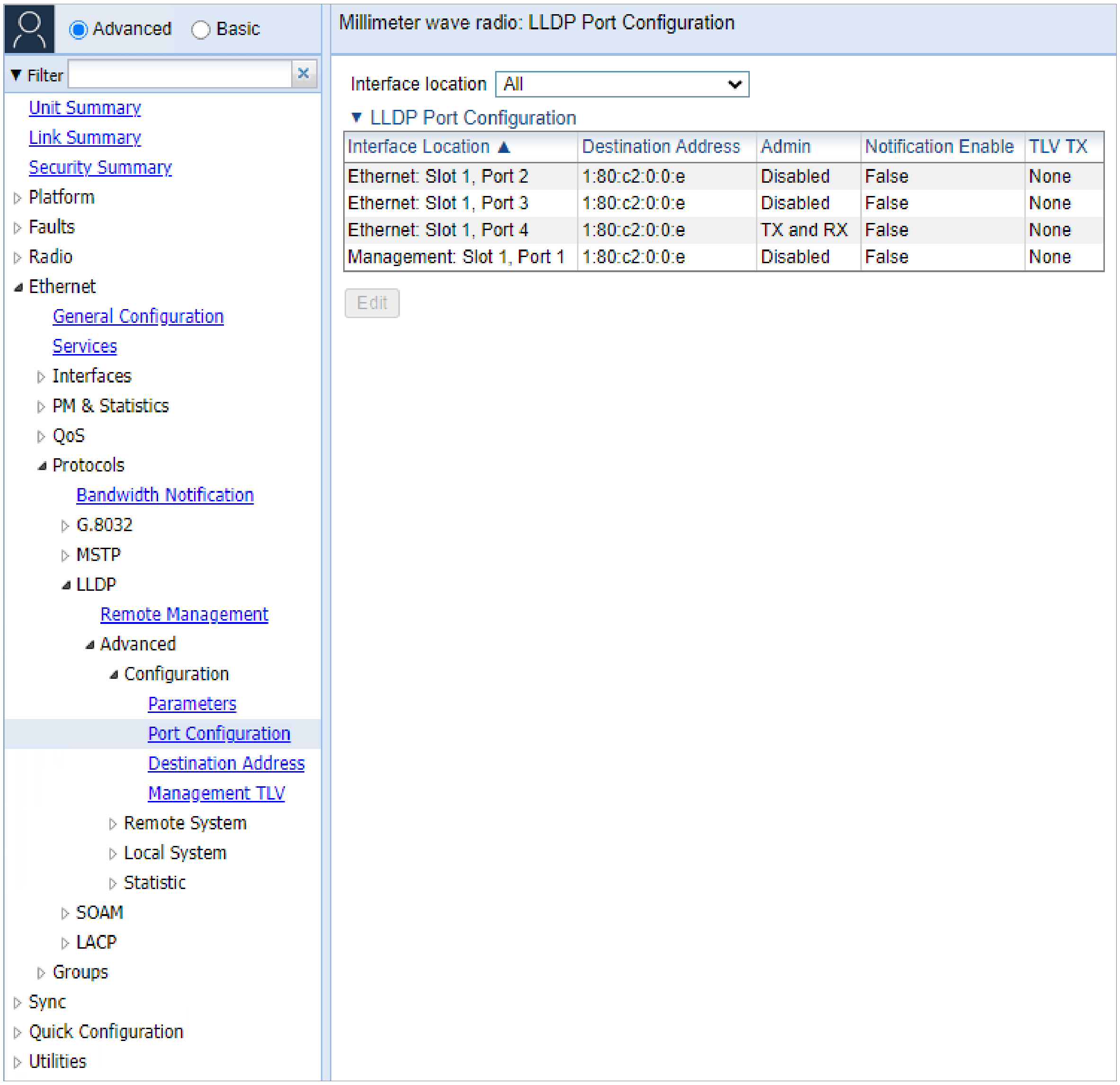
Parameter	Definition
TX Interval (Seconds)	Defines the interval, in seconds, at which LLDP frames are transmitted. You can select a value from 5 to 32768. The default value is 30.
Notification Interval (Seconds)	Defines the interval, in seconds, between transmission of LLDP notifications during normal 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 264 *LLDP Port Configuration Page (PTP 850EX)*



Millimeter wave radio: LLDP Port Configuration

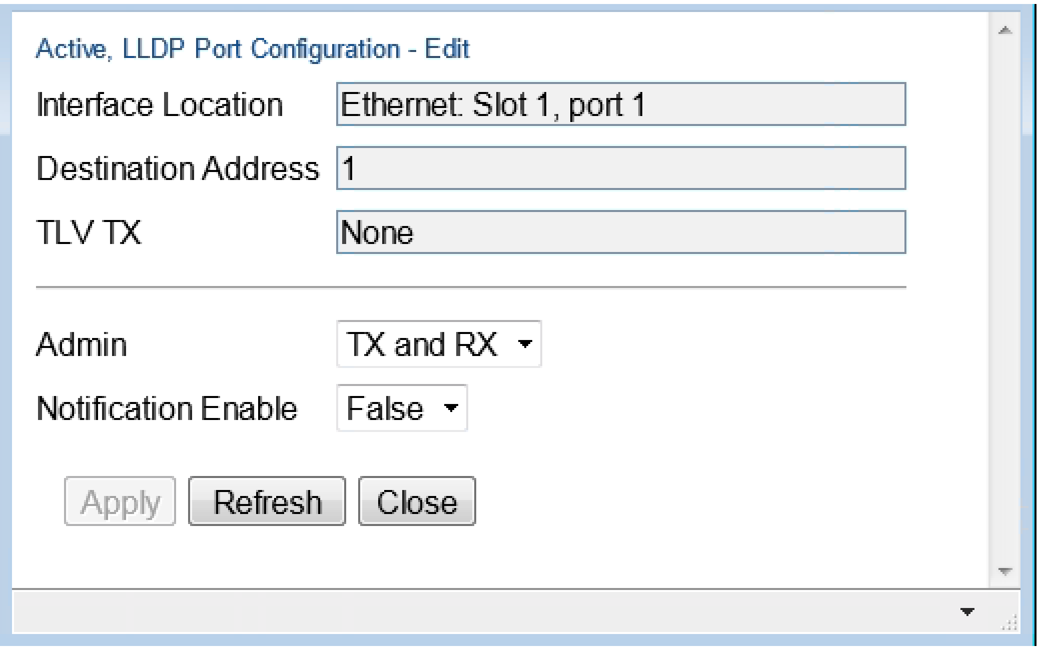
Interface location: All

▼ LLDP Port Configuration

Interface Location ▲	Destination Address	Admin	Notification Enable	TLV TX
Ethernet: Slot 1, Port 2	1:80:c2:0:0:e	Disabled	False	None
Ethernet: Slot 1, Port 3	1:80:c2:0:0:e	Disabled	False	None
Ethernet: Slot 1, Port 4	1:80:c2:0:0:e	TX and RX	False	None
Management: Slot 1, Port 1	1:80:c2:0:0:e	Disabled	False	None

2. Select an interface and click **Edit**. The LLDP Port Configuration - Edit page opens.

Figure 265 *LLDP Port Configuration - Edit Page*



Active, LLDP Port Configuration - Edit

Interface Location: Ethernet: Slot 1, port 1

Destination Address: 1

TLV TX: None

Admin: TX and RX

Notification Enable: False

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**.

LLDP Port Configuration Status Parameters lists and describes the status parameters in the LLDP Port Configuration page.

Table 65 *LLDP Port Configuration Status Parameters*

Parameter	Definition
Interface Location	Identifies the port.
Destination	The destination address of the LLDP agent associated with this port.

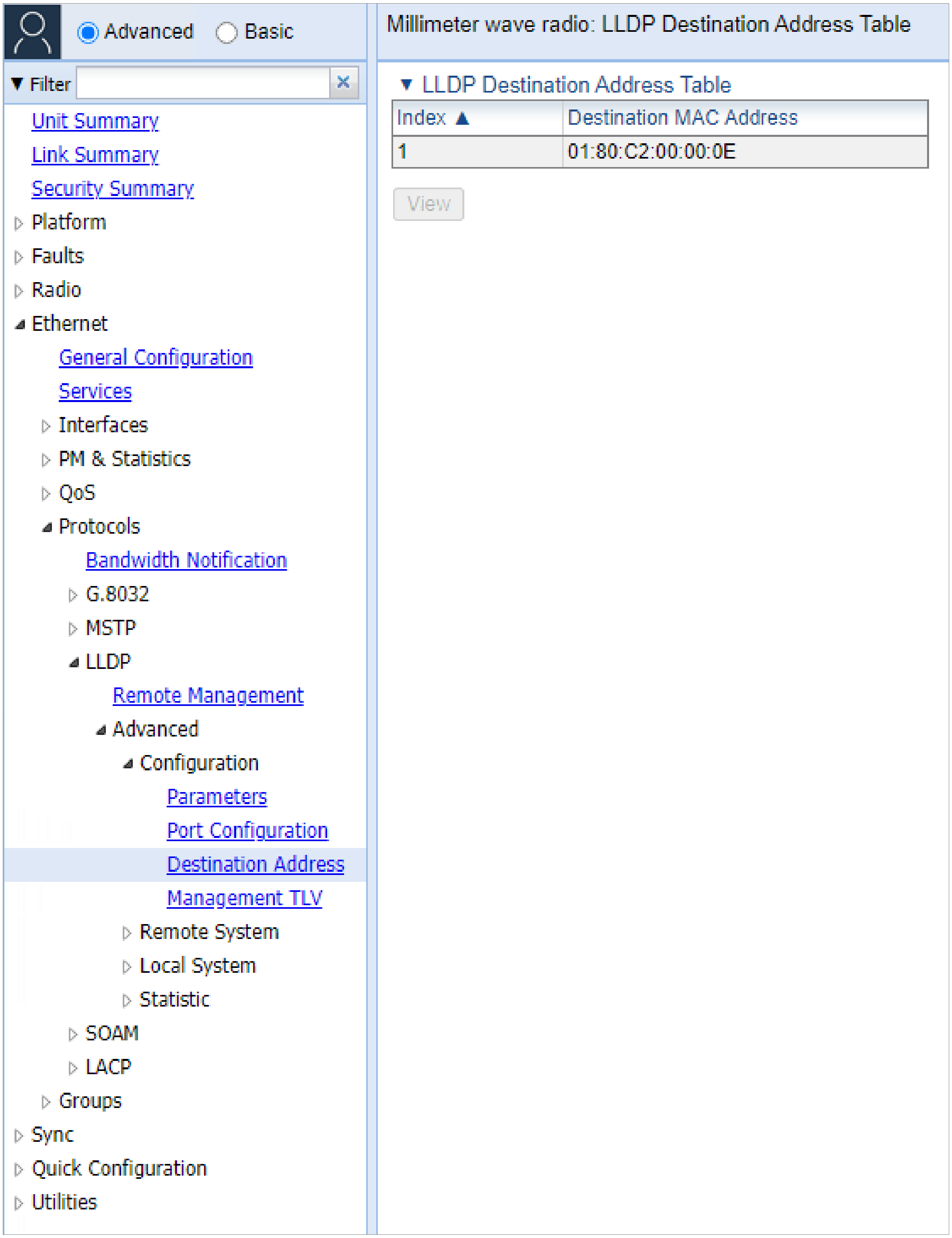
Parameter	Definition
Address	
TLV TX	Indicates which of the unit's capabilities is transmitted by the LLDP agent for the port: • **PortDesc** – The LLDP agent transmits Port Description TLVs. • **SysName** – The LLDP agent transmits System Name TLVs. • **SysDesc** – The LLDP agent transmits System Description 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 266 *LLDP Destination Address Table Page*



Millimeter wave radio: LLDP Destination Address Table

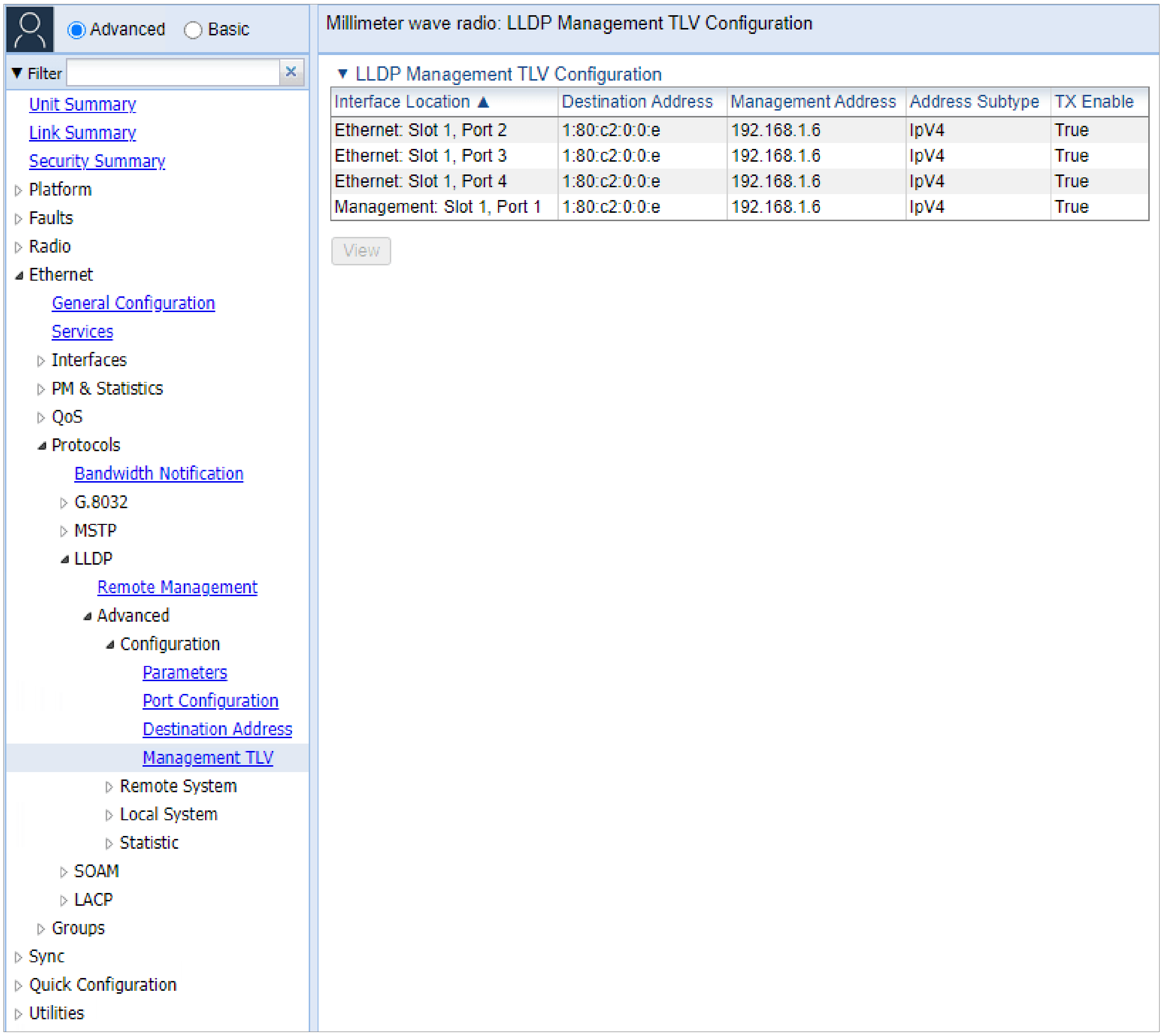
LLDP Destination Address Table

Index ▲	Destination MAC Address
1	01:80:C2:00:00:0E

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 267 *LLDP Management TLV Configuration Page (PTP 850EX)*



Millimeter wave radio: LLDP Management TLV Configuration

▼ LLDP Management TLV Configuration

Interface Location ▲	Destination Address	Management Address	Address Subtype	TX Enable
Ethernet: Slot 1, Port 2	1:80:c2:0:0:e	192.168.1.6	IpV4	True
Ethernet: Slot 1, Port 3	1:80:c2:0:0:e	192.168.1.6	IpV4	True
Ethernet: Slot 1, Port 4	1:80:c2:0:0:e	192.168.1.6	IpV4	True
Management: Slot 1, Port 1	1:80:c2:0:0:e	192.168.1.6	IpV4	True

LLDP Management TLV Parameters lists and describes the status parameters in the LLDP Management TLV Configuration page.

Table 66 *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 Address	The unit's IP address.

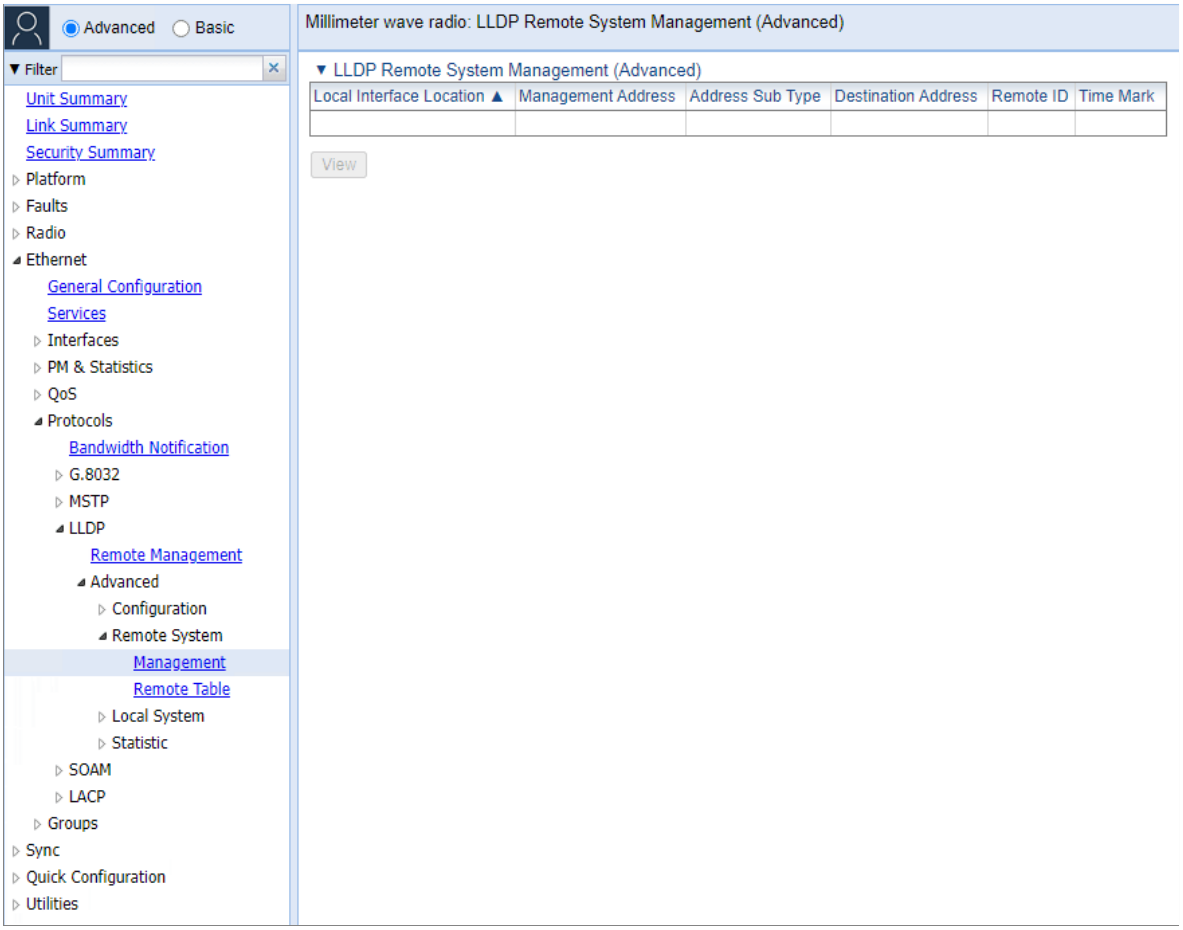
Parameter	Definition
Address Subtype	Defines the type of the management address identifier encoding used for the Management Address.
Tx Enable	Indicates whether the unit's Management Address is transmitted with LLDPDUs. In this release, the Management Address is always sent.

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 268 *LLDP Remote System Management (Advanced) Page*



Millimeter wave radio: LLDP Remote System Management (Advanced)

▼ LLDP Remote System Management (Advanced)

Local Interface Location ▲	Management Address	Address Sub Type	Destination Address	Remote ID	Time Mark

LLDP Remote System Management Parameters describes the LLDP remote system management parameters. These parameters are read-only.

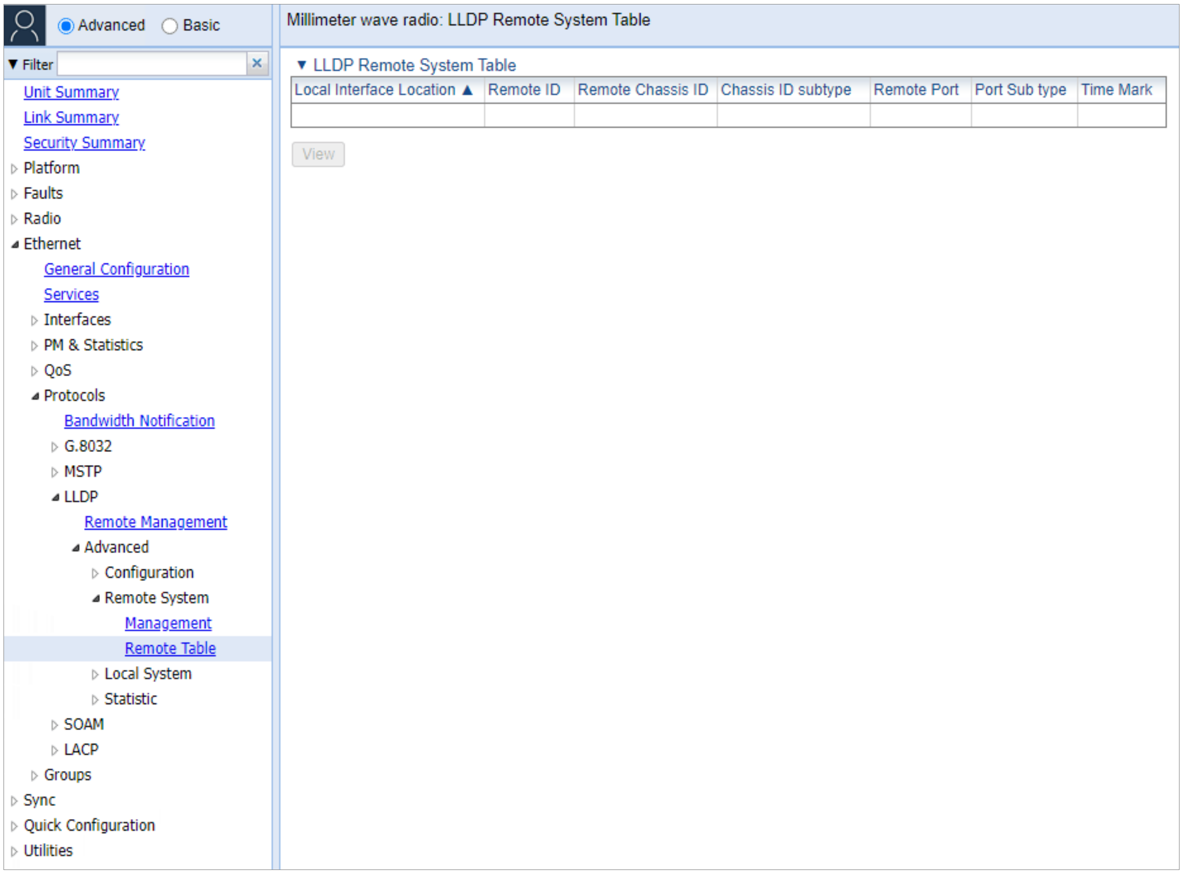
Table 67 *LLDP Remote System Management Parameters*

Parameter	Definition
Local Interface Location	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 Address	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 269 *LLDP Remote System Table Page*



Millimeter wave radio: LLDP Remote System Table

▼ LLDP Remote System Table

Local Interface Location ▲	Remote ID	Remote Chassis ID	Chassis ID subtype	Remote Port	Port Sub type	Time Mark

LLDP Remote System Table Parameters describes the parameters in the LLDP Remote System Table page. These parameters are read-only.

Table 68 *LLDP Remote System Table Parameters*

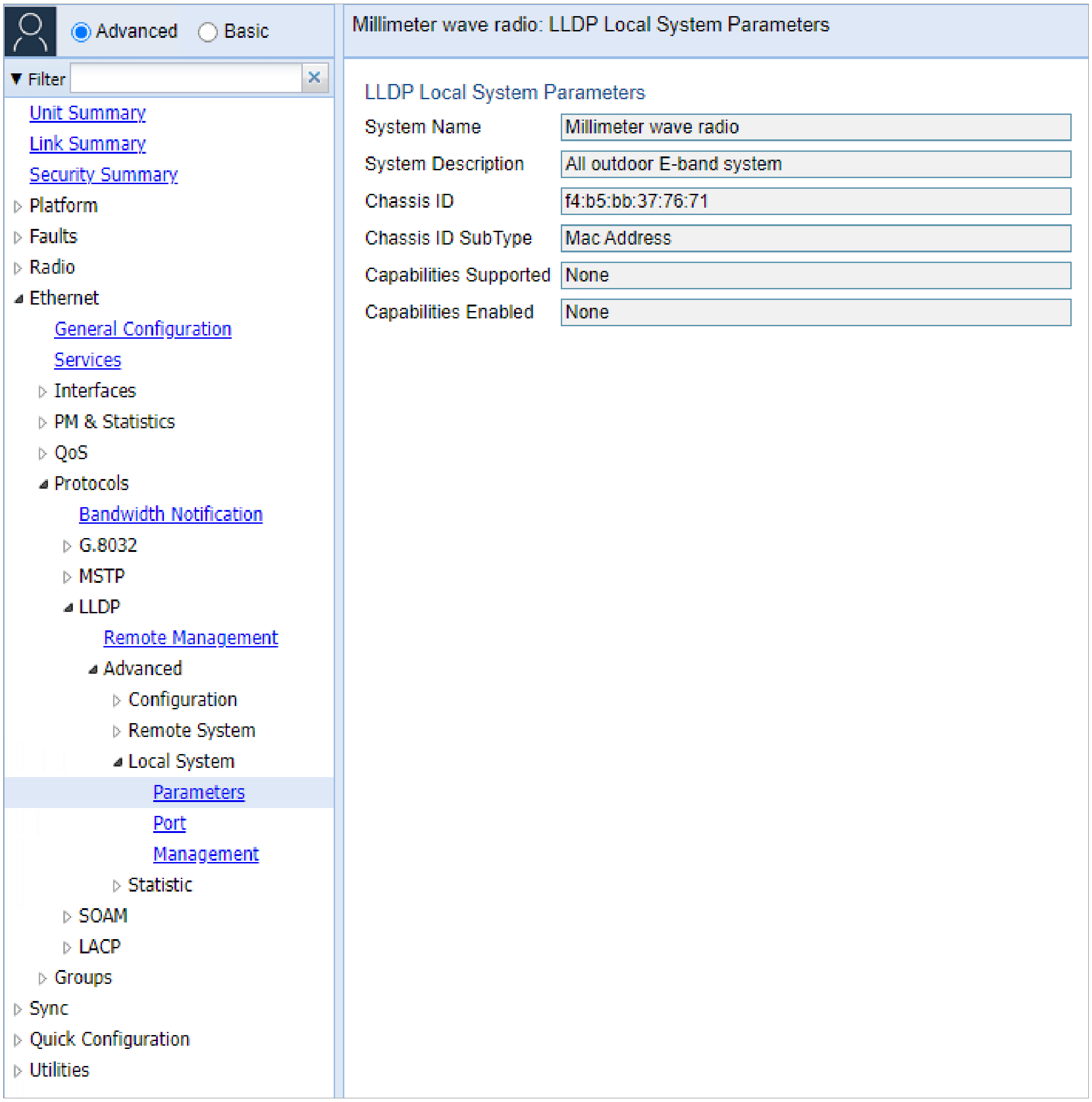
Parameter	Definition
Local Interface Location	The location of the local interface.
Remote ID	An arbitrary local integer value used by this agent to identify a particular connection instance, unique only for the indicated peer.
Remote Chassis ID	An octet string used to identify the peer's hardware unit.
Chassis ID Subtype	The type of encoding used to identify the peer's hardware unit.
Remote Port	An octet string used to identify the port component associated with the remote system.
Port Sub type	The type of port identifier encoding used in the peer's Port ID.
Time Mark	The time the entry was created.

Displaying the Local Unit's Parameters

To display the unit parameters, as transmitted by the LLDP agents:

1. Select **Ethernet** > **Protocols** > **LLDP** > **Advanced** > **Local System** > **Parameters**. The LLDP Local System Parameters page opens.

Figure 270 *LLDP Local System Parameters Page (PTP 850EX)*



Millimeter wave radio: LLDP Local System Parameters

LLDP Local System Parameters

System Name	Millimeter wave radio
System Description	All outdoor E-band system
Chassis ID	f4:b5:bb:37:76:71
Chassis ID SubType	Mac Address
Capabilities Supported	None
Capabilities Enabled	None

LLDP Local System Parameters describes the parameters in the LLDP Local System Parameters page. These parameters are read-only.

Table 69 *LLDP Local System Parameters*

Parameter	Definition
System	The system name included in TLVs transmitted by the LLDP agent, as defined in the

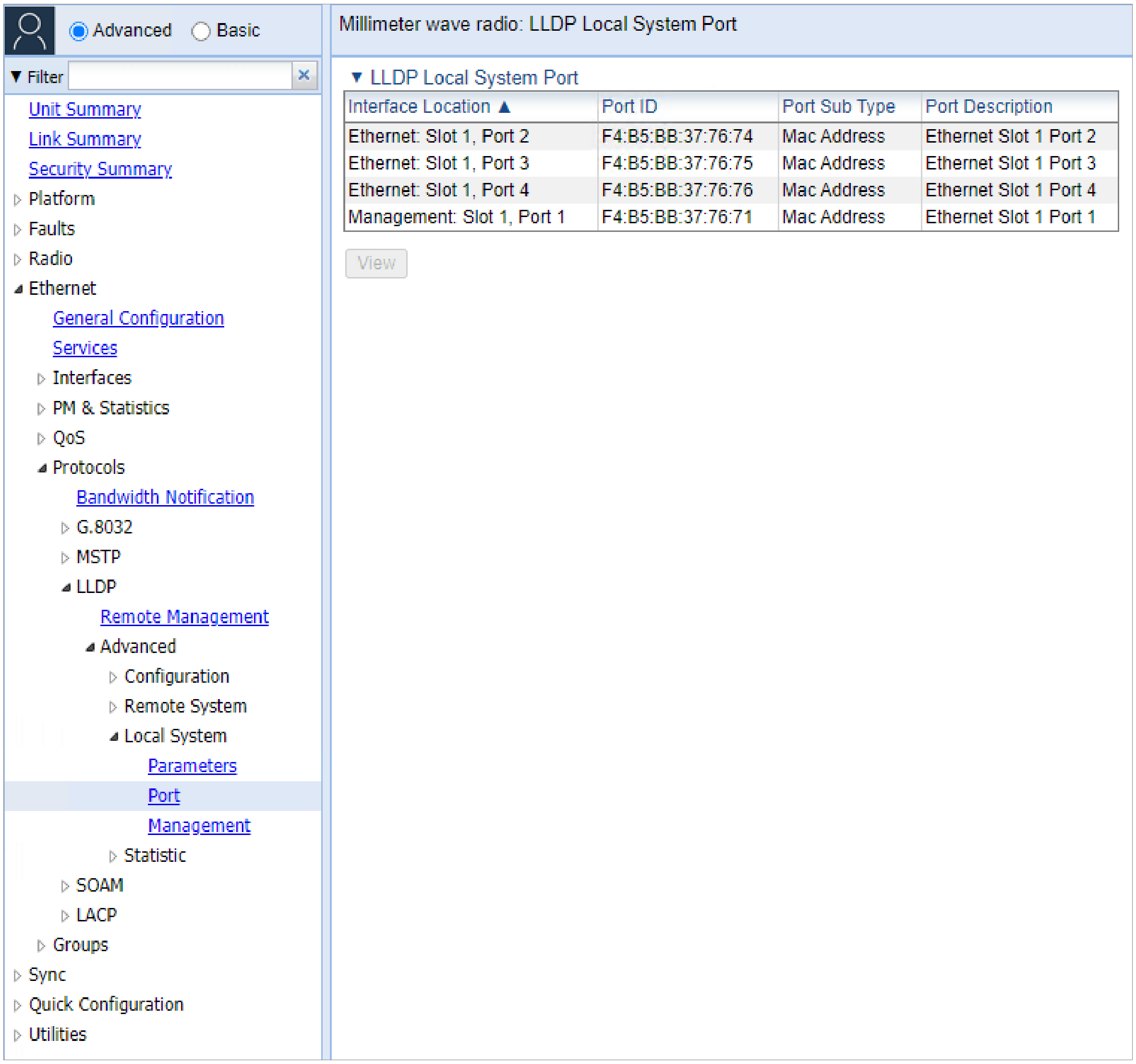
Parameter	Definition
Name	**Name** field of the Unit Parameters page. See Configuring Unit Parameters.
System Description	The system description included in TLVs transmitted by the LLDP agent, as defined in the **Description** field of the Unit Parameters page. See Configuring Unit Parameters.
Chassis 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 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
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

Parameter	Definition
	10 – twoPortMACRelay

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 271 *LLDP Local System Port Page (PTP 850EX)*



Millimeter wave radio: LLDP Local System Port

LLDP Local System Port

Interface Location ▲	Port ID	Port Sub Type	Port Description
Ethernet: Slot 1, Port 2	F4:B5:BB:37:76:74	Mac Address	Ethernet Slot 1 Port 2
Ethernet: Slot 1, Port 3	F4:B5:BB:37:76:75	Mac Address	Ethernet Slot 1 Port 3
Ethernet: Slot 1, Port 4	F4:B5:BB:37:76:76	Mac Address	Ethernet Slot 1 Port 4
Management: Slot 1, Port 1	F4:B5:BB:37:76:71	Mac Address	Ethernet Slot 1 Port 1

LLDP Local System Port Parameters describes the parameters in the LLDP Local System Port page. These parameters are read-only.

Table 70 *LLDP Local System Port Parameters*

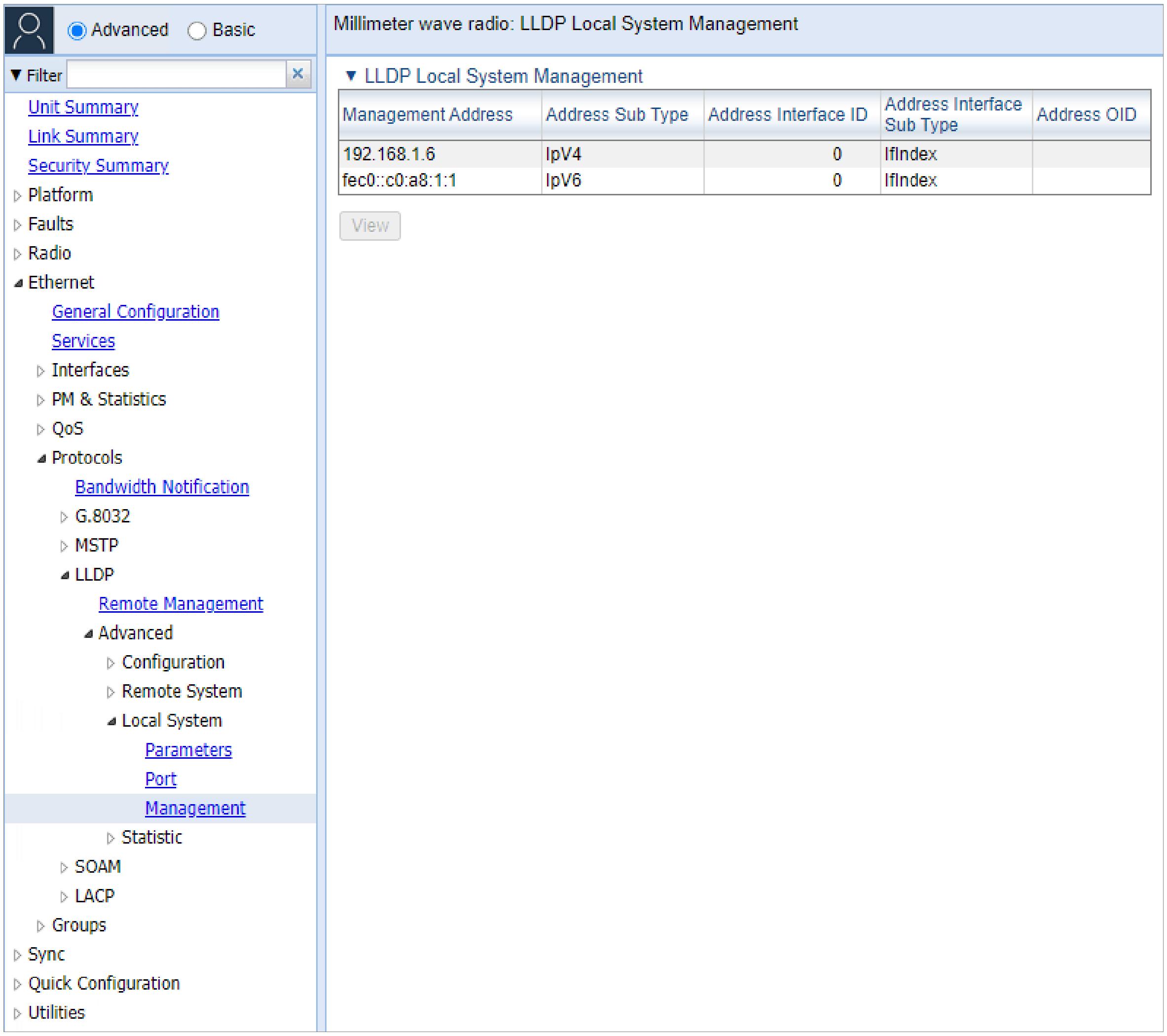
Parameter	Definition
Interface	Identifies the port.

Parameter	Definition
Location	
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 Description	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 272 *LLDP Local System Management Page*



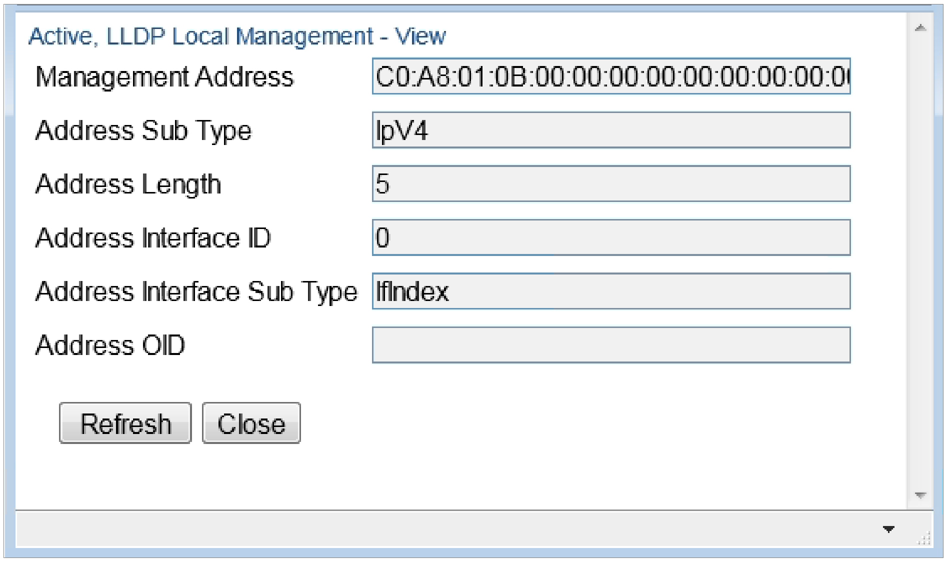
Millimeter wave radio: LLDP Local System Management

▼ LLDP Local System Management

Management Address	Address Sub Type	Address Interface ID	Address Interface Sub Type	Address OID
192.168.1.6	IpV4	0	IfIndex	
fec0::c0:a8:1:1	IpV6	0	IfIndex	

2. To display all the parameters, select a row and click View.

Figure 273 *LLDP Local System Management – View Page*



Active, LLDP Local Management - View

Management Address	C0:A8:01:0B:00:00:00:00:00:00:00:00:0(
Address Sub Type	IpV4
Address Length	5
Address Interface ID	0
Address Interface Sub Type	IfIndex
Address OID	

LLDP Local System Management Parameters describes the parameters in the LLDP Local System Management page. These parameters are read-only.

Table 71 *LLDP Local System Management Parameters*

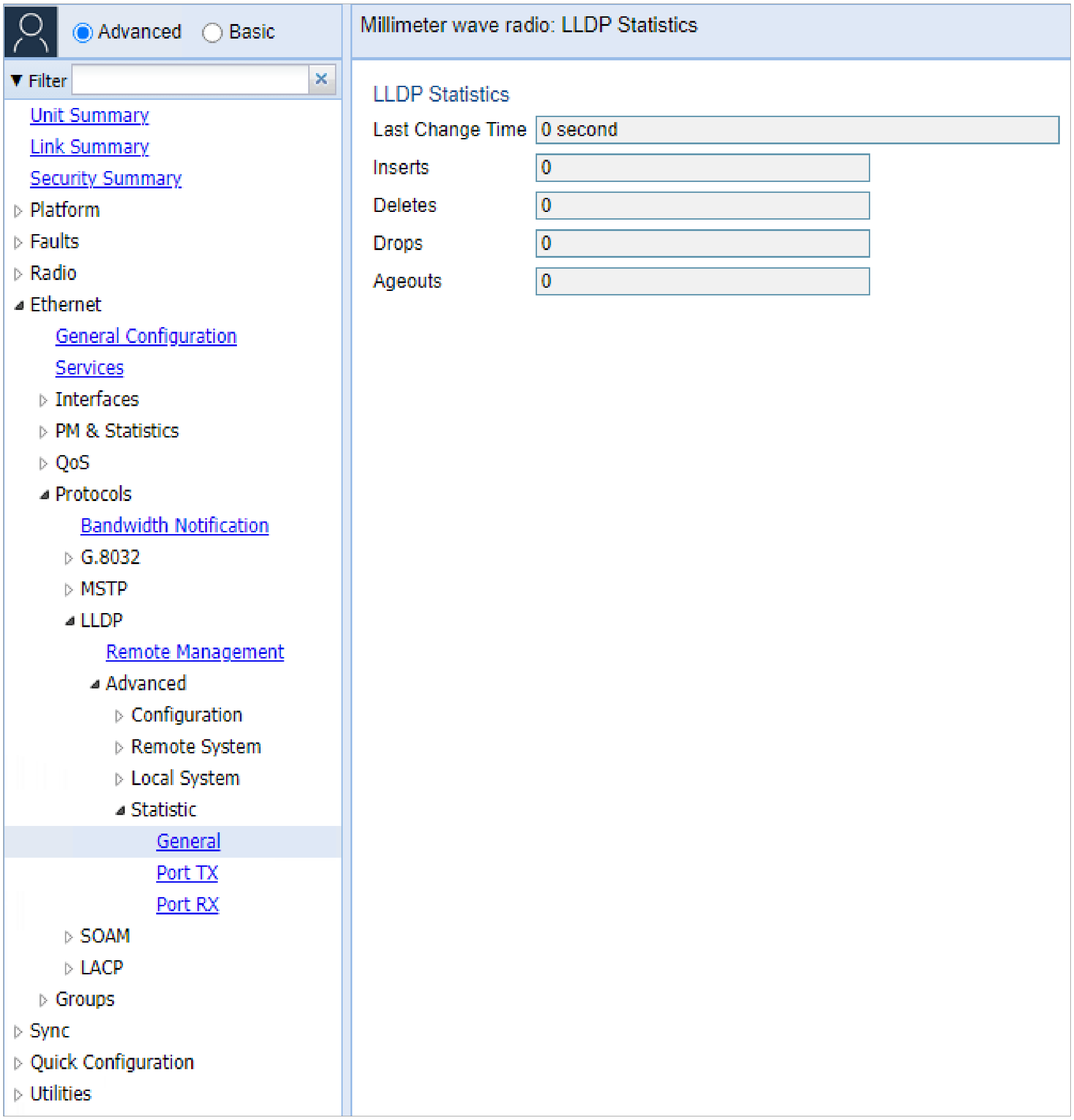
Parameter	Definition
Management Address	The local unit's IP address.
Address Sub Type	The format of the local unit's IP Address.
Address Length	Reserved for future use.
Address Interface ID	Reserved for future use.
Address Interface Sub Type	Reserved for future use.
Address OID	Reserved for future use.

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 Statistics page opens.

Figure 274 *LLDP Statistics Page*



Millimeter wave radio: LLDP Statistics

LLDP Statistics

Last Change Time: 0 second

Inserts: 0

Deletes: 0

Drops: 0

Ageouts: 0

LLDP Statistics describes the statistics in the LLDP Statistics page.

Table 72 *LLDP Statistics*

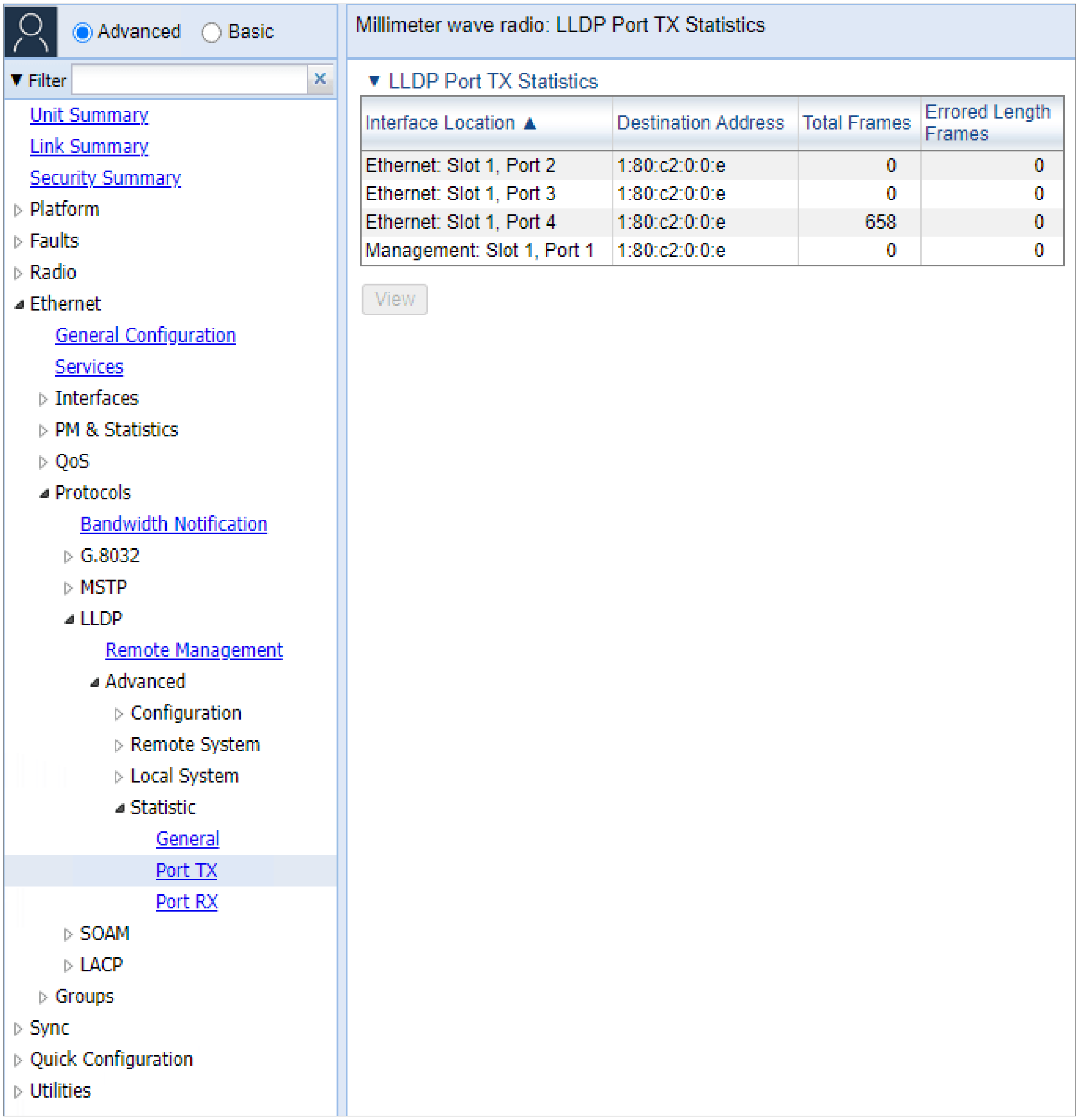
Parameter	Definition
Last Change Time	The time of the most recent change in the remote unit, as reported via LLDP.
Inserts	The number of times the information from the remote system has changed.

Parameter	Definition
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 Statistics page opens.

Figure 275 *LLDP Port TX Statistics Page (PTP 850EX)*



Millimeter wave radio: LLDP Port TX Statistics

▼ LLDP Port TX Statistics

Interface Location ▲	Destination Address	Total Frames	Errored Length Frames
Ethernet: Slot 1, Port 2	1:80:c2:0:0:e	0	0
Ethernet: Slot 1, Port 3	1:80:c2:0:0:e	0	0
Ethernet: Slot 1, Port 4	1:80:c2:0:0:e	658	0
Management: Slot 1, Port 1	1:80:c2:0:0:e	0	0

LLDP Port TX Statistics describes the statistics in the LLDP Port TX Statistics page.

Table 73 *LLDP Port TX Statistics*

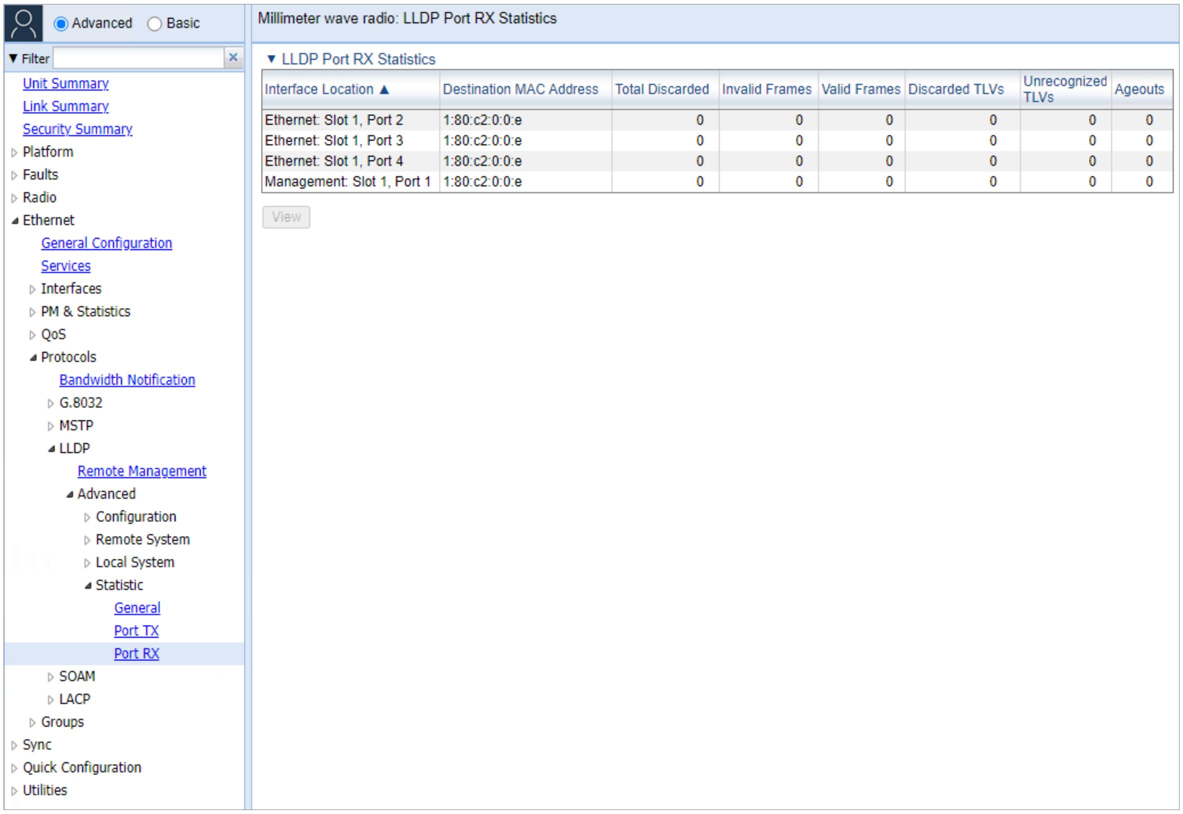
Parameter	Definition
Interface Location	The index value used to identify the port in LLDP transmissions.
Destination Address	The LLDP MAC address associated with this entry.
Total Frames	The number of LLDP frames transmitted by the LLDP agent on this port to the destination

Parameter	Definition
	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 Statistics page opens.

Figure 276 *LLDP Port RX Statistics Page (PTP 850EX)*



Millimeter wave radio: LLDP Port RX Statistics

▼ LLDP Port RX Statistics

Interface Location ▲	Destination MAC Address	Total Discarded	Invalid Frames	Valid Frames	Discarded TLVs	Unrecognized TLVs	Ageouts
Ethernet: Slot 1, Port 2	1:80:c2:0:0:e	0	0	0	0	0	0
Ethernet: Slot 1, Port 3	1:80:c2:0:0:e	0	0	0	0	0	0
Ethernet: Slot 1, Port 4	1:80:c2:0:0:e	0	0	0	0	0	0
Management: Slot 1, Port 1	1:80:c2:0:0:e	0	0	0	0	0	0

LLDP Port RX Statistics describes the statistics in the LLDP Port TX Statistics page.

Table 74 *LLDP Port RX Statistics*

Parameter	Definition
Interface Location	The index value used to identify the port in LLDP transmissions.

Parameter	Definition
Destination MAC Address	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 port.
Unrecognized TLVs	The number of LLDP TLVs received on the given port that are not recognized by LLDP agent.
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 allowed.

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

Configuring the Sync Source

Note

To configure a sync source on which the sync source Quality parameter is set according to ANSI specifications, you must change the ETSI/ANSI mode to ANSI before configuring the sync source. See Changing the ETSI/ANSI Mode (CLI).

An interface with an electrical SFP module cannot be used as a Sync source.

The 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
```

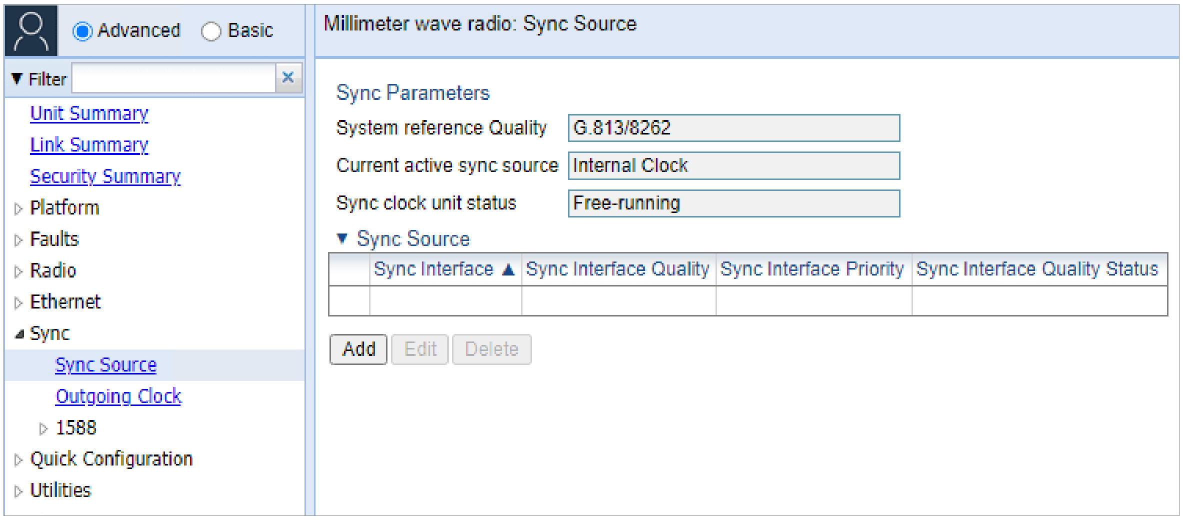
When configuring an Ethernet interface as a Sync source, the Media Type of the interface must be SFP, *not* Auto-Type. To view and configure the Media Type of an Ethernet interface, see Configuring Ethernet Interfaces.

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 277 *Sync Source Page*



Millimeter wave radio: Sync Source

Sync Parameters

System reference Quality: G.813/8262

Current active sync source: Internal Clock

Sync clock unit status: Free-running

▼ Sync Source

	Sync Interface ▲	Sync Interface Quality	Sync Interface Priority	Sync Interface Quality Status

Sync Source Parameters lists and defines the sync source status parameters.

Table 75 *Sync Source Parameters*

Parameter	Definition
System Reference Quality	The quality of the current synchronization source interface.
Current Active Sync Source	The currently active system synchronization source interface.
Sync Clock Unit Status	The status of the unit's Sync E mechanism.

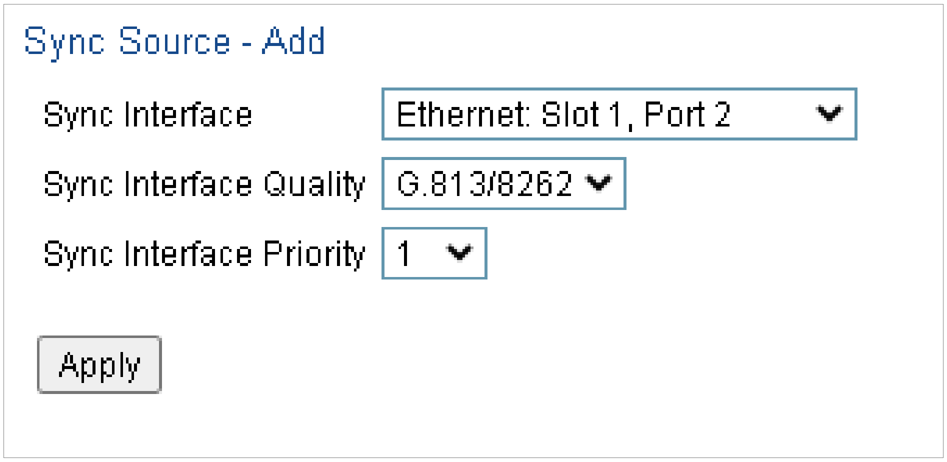
Parameter	Definition
Sync Interface	Displays the interface that is configured as a synchronization source.
Sync Interface Quality	Displays the quality level assigned to this synchronization source. This enables the system to select the source with the highest quality as the current synchronization source. 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.

Adding a Sync Source

To add a synchronization source:

1. In the Sync Source page (Sync Source Page), click **Add**. The Sync Source – Add page opens.

Figure 278 *Sync Source – Add Page*



Sync Source - Add

Sync Interface	Ethernet: Slot 1, Port 2
Sync Interface Quality	G.813/8262
Sync Interface Priority	1

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**.

Editing a Sync Source

To edit a synchronization source:

1. In the Sync Source page (Sync Source Page), 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**.

Deleting a Sync Source

To delete a synchronization source:

1. Select the synchronization source in the Sync Source page (Sync Source Page).
2. Click **Delete**. The synchronization source is deleted.

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 850EX implement the passing of SSM messages over the radio interfaces. SSM timing in PTP 850EX 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:

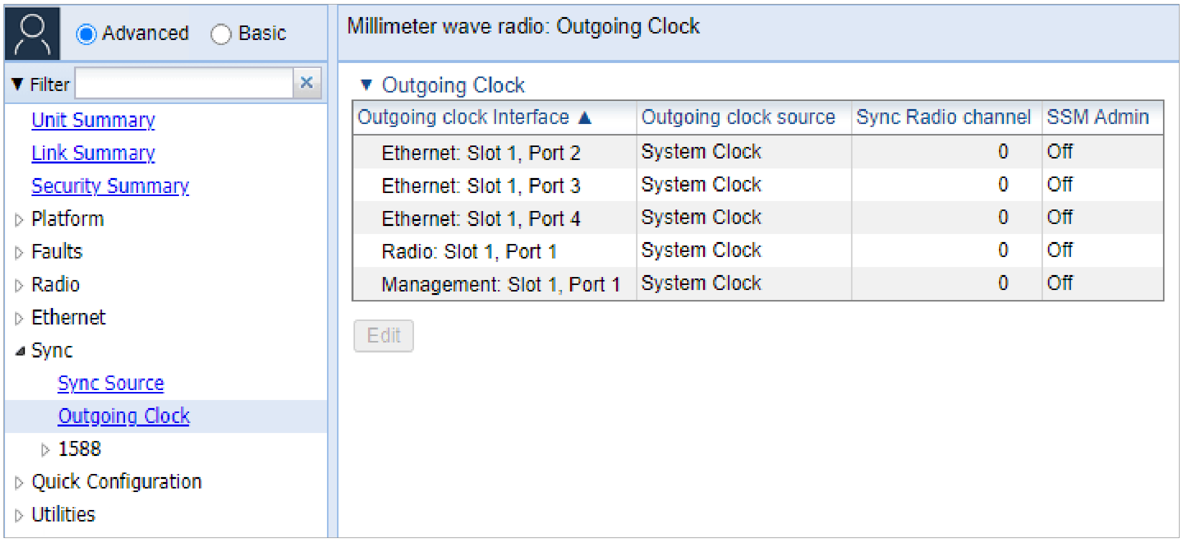
```
root> platform sync mode set automatic
```

To configure the outgoing clock on an Ethernet interface, the Media Type of the interface must be 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 279 *Outgoing Clock Page (PTP 850EX)*



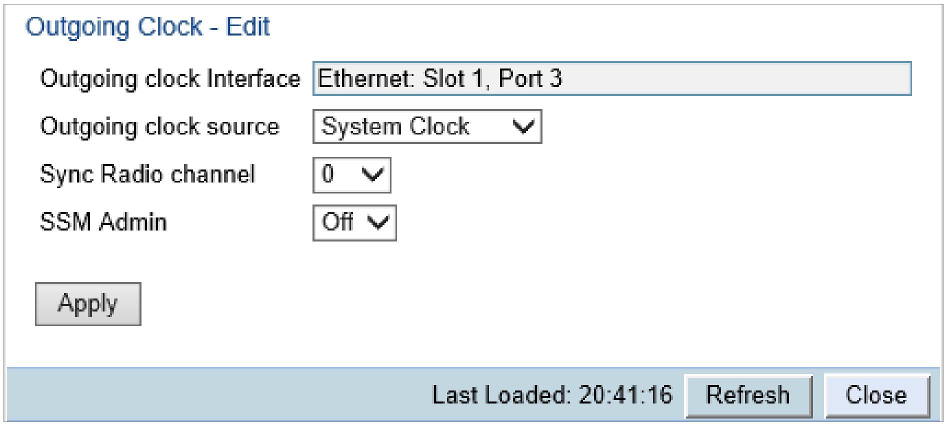
Millimeter wave radio: Outgoing Clock

Outgoing Clock

Outgoing clock Interface ▲	Outgoing clock source	Sync Radio channel	SSM Admin
Ethernet: Slot 1, Port 2	System Clock	0	Off
Ethernet: Slot 1, Port 3	System Clock	0	Off
Ethernet: Slot 1, Port 4	System Clock	0	Off
Radio: Slot 1, Port 1	System Clock	0	Off
Management: Slot 1, Port 1	System Clock	0	Off

2. Select the interface you want to configure and click **Edit**. The Outgoing Clock – Edit page opens.

Figure 280 *Outgoing Clock – Edit Page*



Outgoing Clock - Edit

Outgoing clock Interface	Ethernet: Slot 1, Port 3
Outgoing clock source	System Clock
Sync Radio channel	0
SSM Admin	Off

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.

Configuring 1588 Transparent Clock

PTP 850 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

1588 TC is not supported when Master-Slave communication is using the IPv6 transport layer.

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.

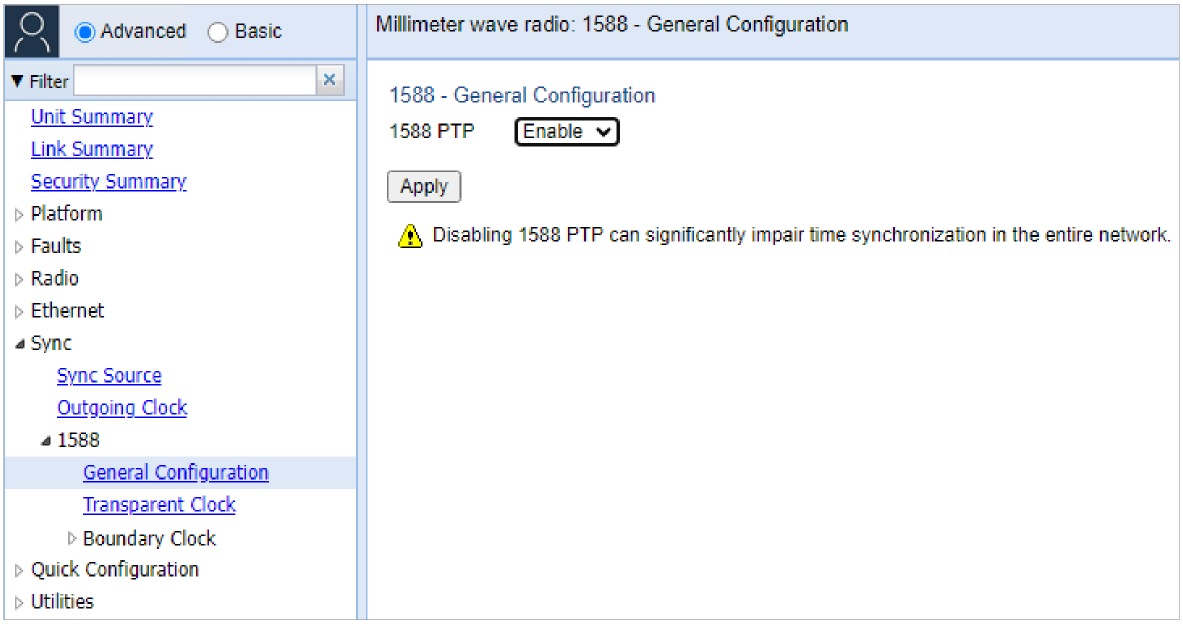
Make sure to enable Transparent Clock on the remote side of the link before enabling it on the local side.

PTP phase alignment relies on symmetric delay between the timestamping units. Therefore, to ensure the best results, it is recommended to use the same port speed (e.g., 10 Gbps), media type (e.g., RJ-45 or SFP) and equipment type (e.g., PTP 850EX) on both sides of the link.

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 281 *1588 General Configuration Page*



Millimeter wave radio: 1588 - General Configuration

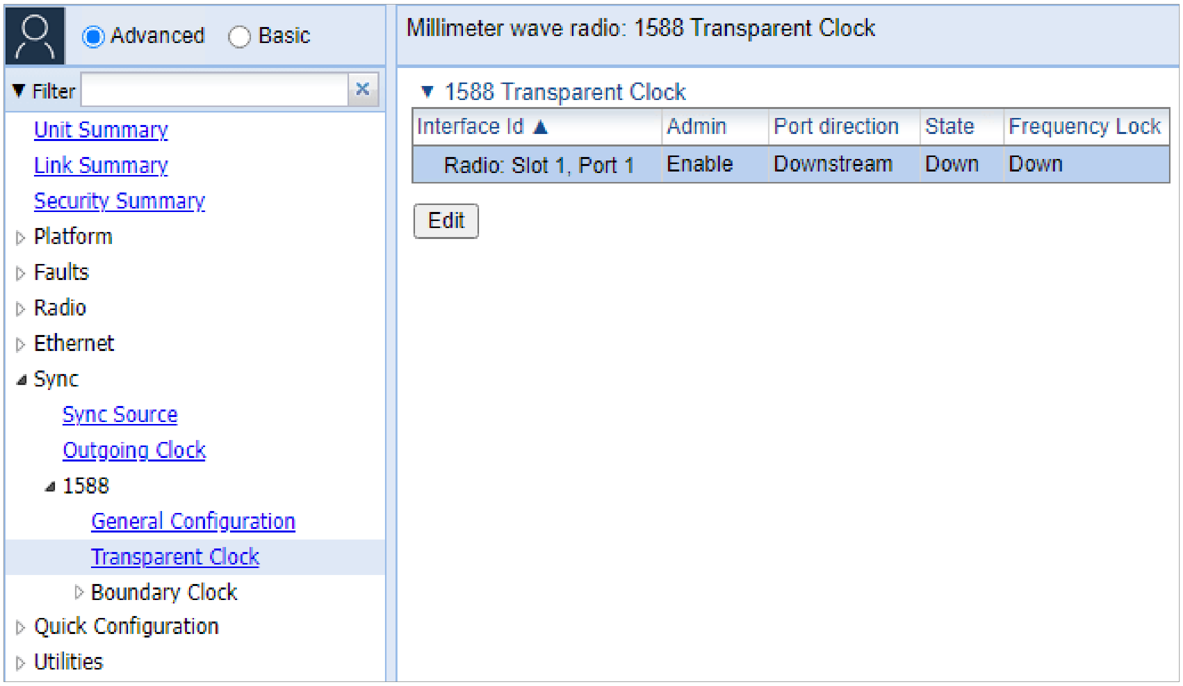
1588 - General Configuration

1588 PTP Enable

⚠ Disabling 1588 PTP can significantly impair time synchronization in the entire network.

7. In the **1588 PTP** field, select **Enable**.
8. Click **Apply**.
9. Select **Sync** > **1588** > **Transparent Clock**. The 1588 Transparent Clock page opens.

Figure 282 *1588 Transparent Clock Page (PTP 850EX)*



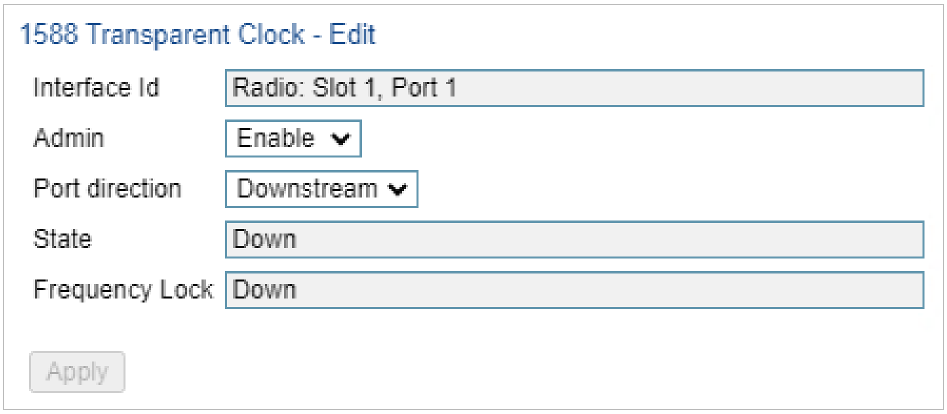
Millimeter wave radio: 1588 Transparent Clock

▼ 1588 Transparent Clock

Interface Id ▲	Admin	Port direction	State	Frequency Lock
Radio: Slot 1, Port 1	Enable	Downstream	Down	Down

10. Select the radio interface or Multi-Carrier ABC group and click **Edit**. The 1588 Transparent Clock – Edit page opens.

Figure 283 *1588 Transparent Clock – Edit Page*



1588 Transparent Clock - Edit

Interface Id: Radio: Slot 1, Port 1

Admin: Enable

Port direction: Downstream

State: Down

Frequency Lock: Down

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. In the Admin field, make sure Enable is selected.

Note

By default, 1588 Transparent Clock is enabled for all radio interfaces. However, you can disable it for a specific radio interface by selecting Disable in this field and clicking Apply.

13. Click Apply, then Close.
14. 11588 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
```

15. 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 (1588 General Configuration Page).
2. In the **1588 PTP** field, select **Disable**.
3. Click **Apply**.

Note

Disabling 1588 PTP can significantly impair time synchronization performance in the entire network.

Configuring 1588 Boundary Clock

Boundary Clock complies with ITU-T Telecom Profile G.8275.1. This enables PTP 850, with Boundary Clock, to meet the rigorous synchronization requirements of 5G networks.

The Boundary Clock in PTP 850 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 850 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 device.

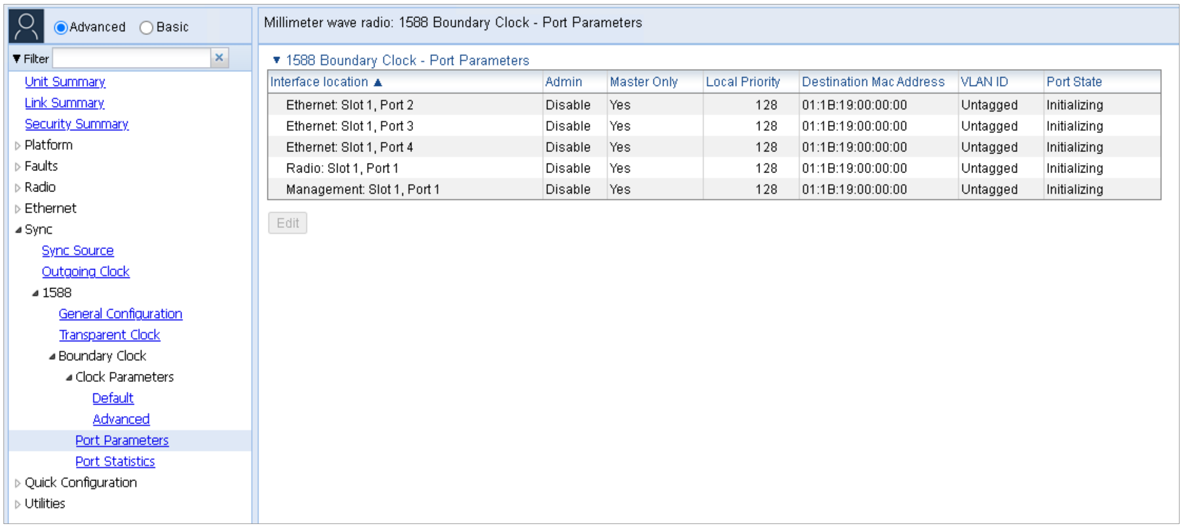
- 1588 BC can only be used in a chain or star topology. It cannot be used in a ring topology.
- 1588 BC is not supported when Master-Slave communication is using the IPv6 transport layer.

Enabling Boundary Clock

To enable Boundary Clock:

1. Select **Sync** > **1588** > **General Configuration**. The 1588 – General Configuration page opens (1588 General Configuration Page).
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.

Figure 284 *1588 Boundary Clock – Port Parameters Page (PTP 850EX)*



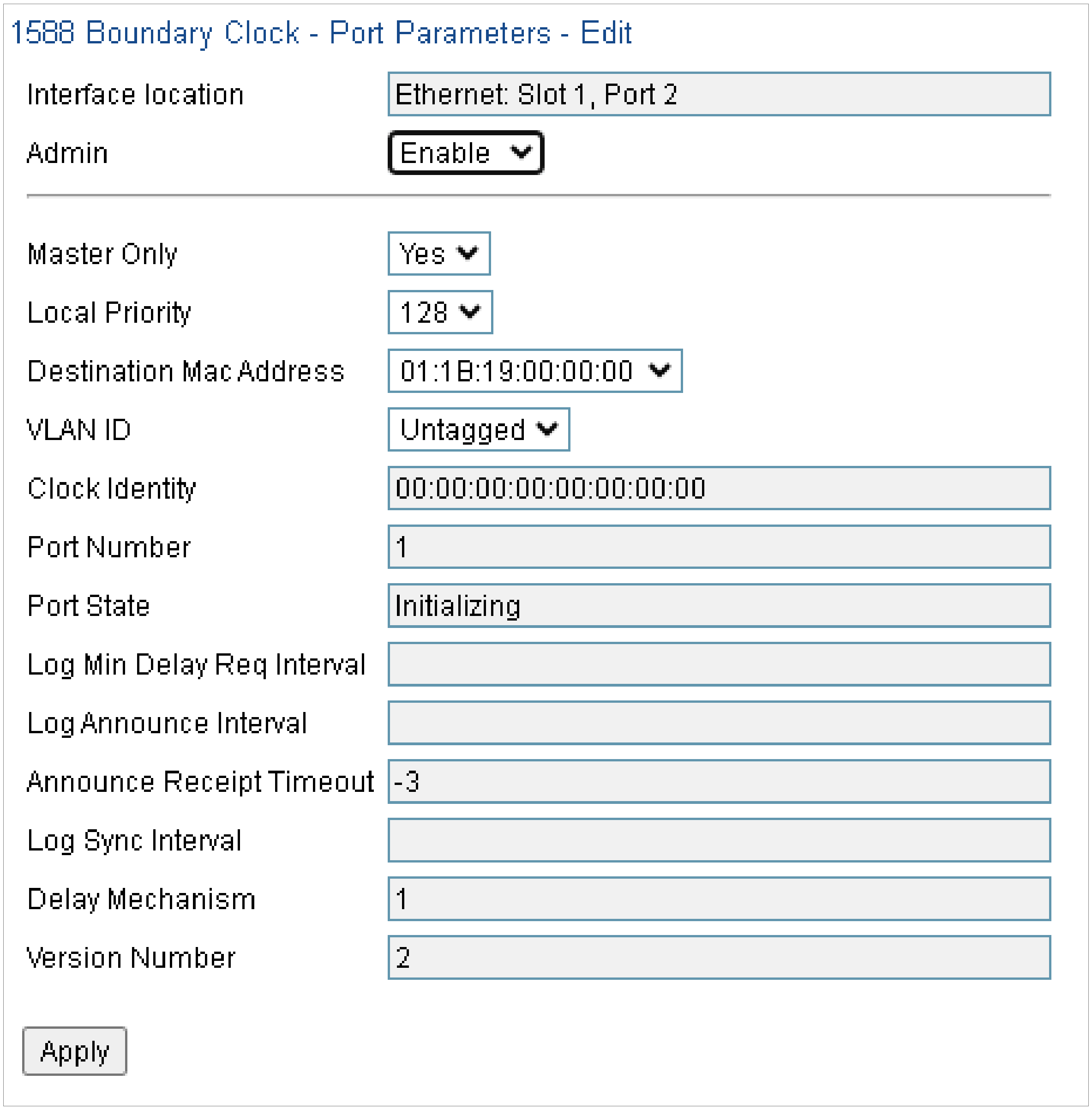
Millimeter wave radio: 1588 Boundary Clock - Port Parameters

▼ 1588 Boundary Clock - Port Parameters

Interface location ▲	Admin	Master Only	Local Priority	Destination Mac Address	VLAN ID	Port State
Ethernet: Slot 1, Port 2	Disable	Yes	128	01:1B:19:00:00:00	Untagged	Initializing
Ethernet: Slot 1, Port 3	Disable	Yes	128	01:1B:19:00:00:00	Untagged	Initializing
Ethernet: Slot 1, Port 4	Disable	Yes	128	01:1B:19:00:00:00	Untagged	Initializing
Radio: Slot 1, Port 1	Disable	Yes	128	01:1B:19:00:00:00	Untagged	Initializing
Management: Slot 1, Port 1	Disable	Yes	128	01:1B:19:00:00:00	Untagged	Initializing

5. Select an interface and click **Edit**. The 1588 Boundary Clock – Port Parameters – Edit page opens.

Figure 285 *1588 Boundary Clock – Port Parameters – Edit Page*



1588 Boundary Clock - Port Parameters - Edit

Interface location	Ethernet: Slot 1, Port 2
Admin	Enable
Master Only	Yes
Local Priority	128
Destination Mac Address	01:1B:19:00:00:00
VLAN ID	Untagged
Clock Identity	00:00:00:00:00:00:00:00
Port Number	1
Port State	Initializing
Log Min Delay Req Interval	
Log Announce Interval	
Announce Receipt Timeout	-3
Log Sync Interval	
Delay Mechanism	1
Version Number	2

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 850 node at any one time.

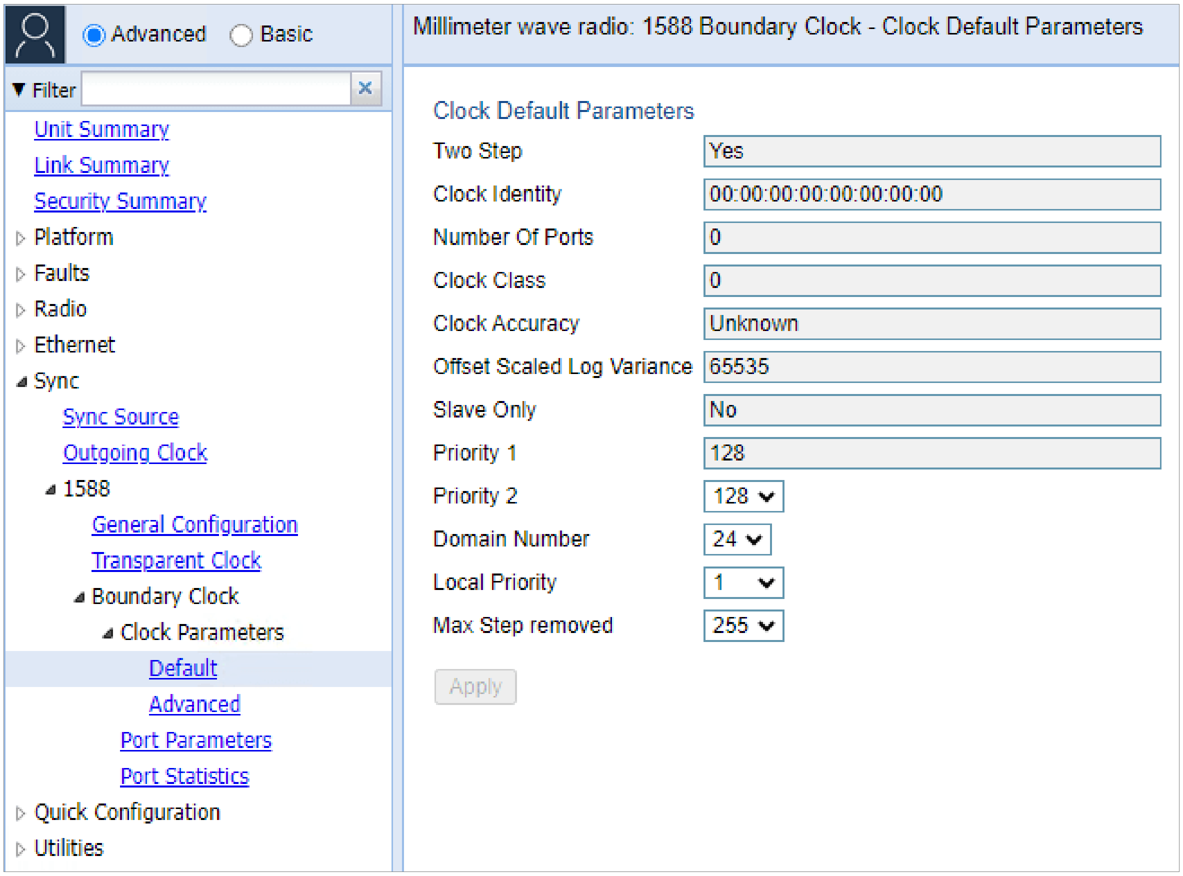
8. Optionally, in the **Local Priority** field, select a value between 1-255. The default value is 128. The Local Priority value is taken into account when two identical announce messages are received by at least two different ports. In such a case, the Boundary Clock mechanism selects the slave port 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. The **VLAN ID** field should be set to its default value of **Untagged**.
11. Click **Apply**.
12. Repeat these steps to add up to 16 interfaces to the unit's Boundary Clock node.
13. 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.
14. Add a port receiving synchronization from the customer side as a Sync source, with Sync Interface Priority 1. See Adding a Sync Source.
15. 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.
16. 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.
17. 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.
18. Verify that the Sync Interface Quality Status of the first Sync source is not Failure. See Viewing the Sync Source Status.

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 286 *1588 Boundary Clock – Clock Default Parameters Page*



Millimeter wave radio: 1588 Boundary Clock - Clock Default Parameters

Clock Default Parameters

Two Step	Yes
Clock Identity	00:00:00:00:00:00:00:00
Number Of Ports	0
Clock Class	0
Clock Accuracy	Unknown
Offset Scaled Log Variance	65535
Slave Only	No
Priority 1	128
Priority 2	128
Domain Number	24
Local Priority	1
Max Step removed	255

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 850'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 850 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**.

Boundary Clock Default Parameters lists and describes the read-only Boundary Clock default parameters.

Table 76 *Boundary Clock Default Parameters*

Parameter	Definition
Two Step	Indicates whether the Boundary Clock node is operating in two-step mode. For PTP

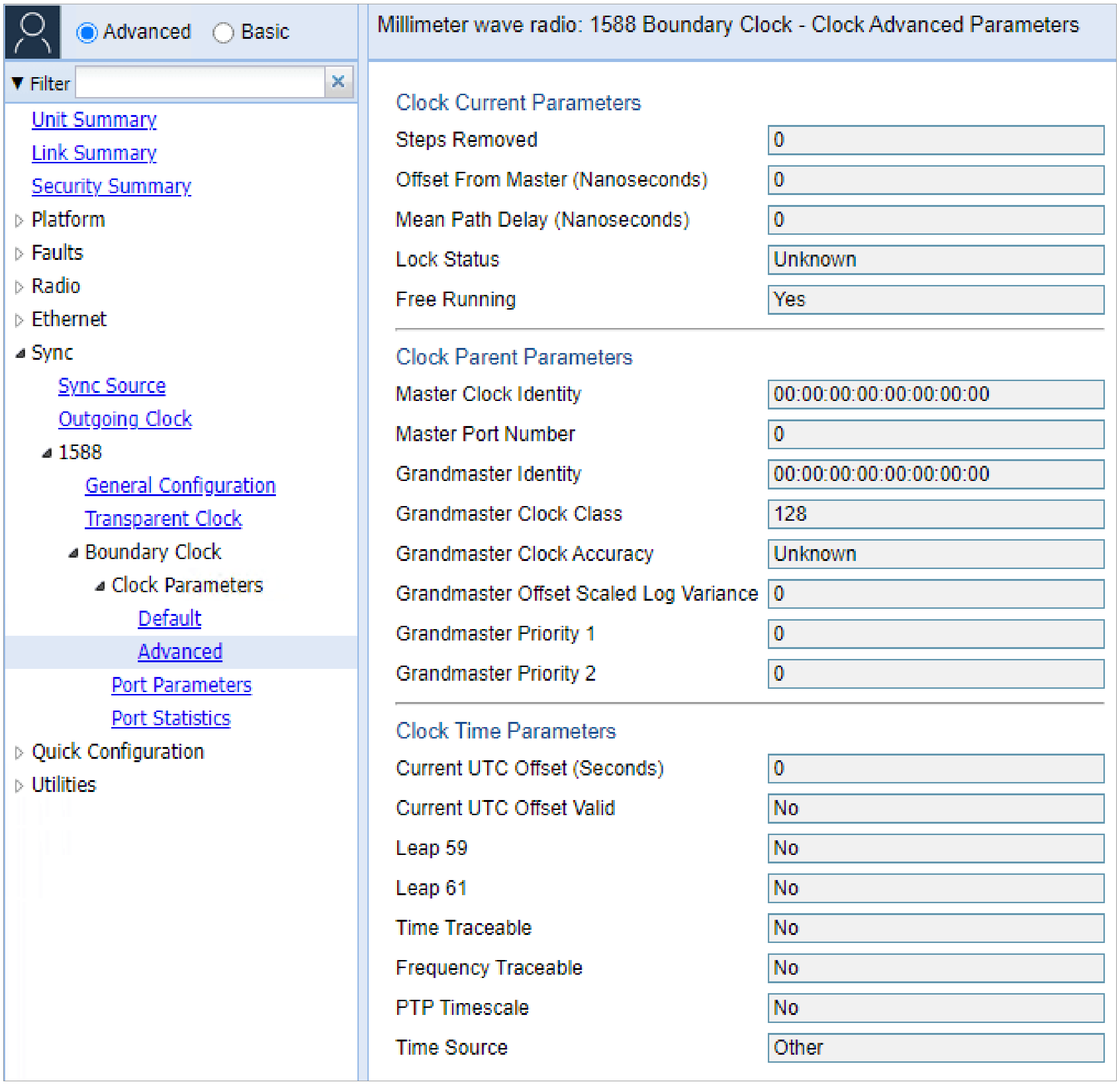
Parameter	Definition
	850EX, Two Step is always set to No.
Clock Identity	Identifies the system clock.
Number of Ports	Displays the number of ports on the unit on which Boundary Clock is enabled. The maximum is 16 per PTP 850 unit.
Clock Class	One of the elements of the clock quality, as defined in IEEE-1588.
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. This is always set to **No**.
Priority 1	Always displays 128.

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 287 *1588 Boundary Clock – Clock Advanced Parameters Page*



Millimeter wave radio: 1588 Boundary Clock - Clock Advanced Parameters

Clock Current Parameters

Steps Removed	0
Offset From Master (Nanoseconds)	0
Mean Path Delay (Nanoseconds)	0
Lock Status	Unknown
Free Running	Yes

Clock Parent Parameters

Master Clock Identity	00:00:00:00:00:00:00:00
Master Port Number	0
Grandmaster Identity	00:00:00:00:00:00:00:00
Grandmaster Clock Class	128
Grandmaster Clock Accuracy	Unknown
Grandmaster Offset Scaled Log Variance	0
Grandmaster Priority 1	0
Grandmaster Priority 2	0

Clock Time Parameters

Current UTC Offset (Seconds)	0
Current UTC Offset Valid	No
Leap 59	No
Leap 61	No
Time Traceable	No
Frequency Traceable	No
PTP Timescale	No
Time Source	Other

All of the advanced Boundary Clock parameters are read-only. Boundary Clock Advanced Parameters lists and describes the Boundary Clock advanced parameters.

Table 77 *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 850 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).

Parameter	Definition
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

To display the Boundary Clock port parameters:

1. Select **Sync** > **1588** > **Boundary Clock** > **Port Parameters**. The 1588 Boundary Clock – Port Parameters page opens (1588 Boundary Clock – Port Parameters Page (PTP 850EX)).
2. Select the port you want to configure and click **Edit**. The 1588 Boundary Clock – Port Parameters – Edit page opens (1588 Boundary Clock – Port Parameters – Edit Page).

For an explanation of the configurable fields, see Enabling Boundary Clock. Boundary Clock Port Parameters lists and describes the read-only Boundary Clock port parameters.

Table 78 *Boundary Clock Port Parameters*

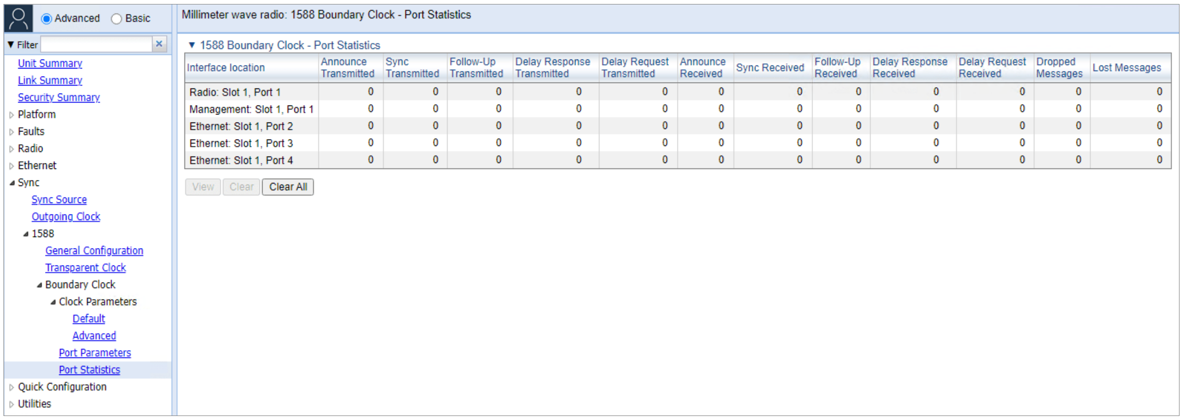
Parameter	Definition
Clock Identity	The PTP 850 unit's clock identity. The same value is used for every port that belongs to the Boundary Clock node.
Port Number	Displays the number of the port according to the activation sequence of every port.
Port State	Indicates whether the port is currently acting 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 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.

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 288 *1588 Boundary Clock – Port Statistics Page (PTP 850EX)*



Millimeter wave radio: 1588 Boundary Clock - Port Statistics

▼ 1588 Boundary Clock - Port Statistics

Interface location	Announce Transmitted	Sync Transmitted	Follow-Up Transmitted	Delay Response Transmitted	Delay Request Transmitted	Announce Received	Sync Received	Follow-Up Received	Delay Response Received	Delay Request Received	Dropped Messages	Lost Messages
Radio: Slot 1, Port 1	0	0	0	0	0	0	0	0	0	0	0	0
Management: Slot 1, Port 1	0	0	0	0	0	0	0	0	0	0	0	0
Ethernet: Slot 1, Port 2	0	0	0	0	0	0	0	0	0	0	0	0
Ethernet: Slot 1, Port 3	0	0	0	0	0	0	0	0	0	0	0	0
Ethernet: Slot 1, Port 4	0	0	0	0	0	0	0	0	0	0	0	0

- 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.

Boundary Clock Port Statistics lists and describes the Boundary Clock port statistics.

Table 79 *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.

Disabling 1588 PTP

To disable 1588 PTP synchronization on the device:

1. Select **Sync** > **1588** > **Boundary Clock** > **Port Parameters**. The 1588 Boundary Clock – Port Parameters page opens (1588 Boundary Clock – Port Parameters Page (PTP 850EX)).
2. Select an interface and click **Edit**. The 1588 Boundary Clock – Port Parameters – Edit page opens (1588 Boundary Clock – Port Parameters – Edit Page).
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 opens (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.

You can disable 1588 PTP synchronization on a specific interface without disabling it on the device. You can do this by disabling Transparent Clock on the interface, as follows:

1. Select Sync > 1588 > Boundary Clock > Port Parameters. The 1588 Boundary Clock – Port Parameters page opens (1588 Boundary Clock – Port Parameters Page (PTP 850EX)).
2. Select the interface and click Edit. The 1588 Boundary Clock – Port Parameters – Edit page opens (1588 Boundary Clock – Port Parameters – Edit Page).
3. In the Admin field, select Disable.

Note

It is important to disable Boundary Clock on the interface before disabling Transparent Clock.

4. Select **Sync** > **1588** > **Transparent Clock**. The 1588 Transparent Clock page opens (1588 Transparent Clock Page (PTP 850EX)).
5. Select a radio and click **Edit**. The 1588 Transparent Clock – Edit page opens (1588 Transparent Clock – Edit Page).
6. In the **Admin** field, select **Disable**.
7. Click **Apply**.

Access Management and Security

This section includes:

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

Quick Security Configuration

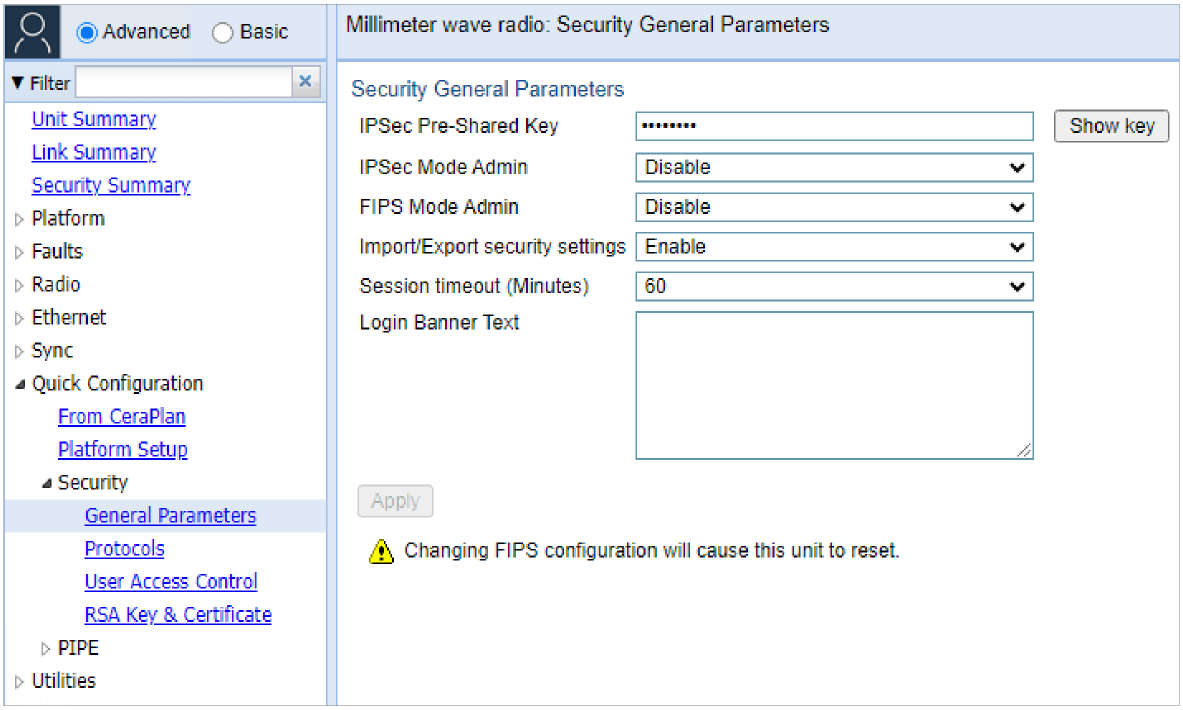
The Web EMS provides a set of Quick Configuration pages that enable you to quickly configure the unit's access and security parameters. This section describes these pages, with cross references to the sections in which each parameter is described in depth.

Quick Security Configuration – General Parameters Page

To configure the import and export security settings, session timeout, and a login banner:

1. Select **Quick Configuration** > **Security** > **General Parameters**. The Quick Configuration Security General Parameters page opens.

Figure 289 *Quick Configuration Security General Parameters Page*



Millimeter wave radio: Security General Parameters

Security General Parameters

IPSec Pre-Shared Key	••••••••
IPSec Mode Admin	Disable
FIPS Mode Admin	Disable
Import/Export security settings	Enable
Session timeout (Minutes)	60
Login Banner Text	

⚠ Changing FIPS configuration will cause this unit to reset.

2. The **IPSec Pre-Shared Key, IPSec Mode Admin**, and **FIPS Mode Admin** fields are not relevant for these products.

3. 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.

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, see Configuring the Session Timeout.

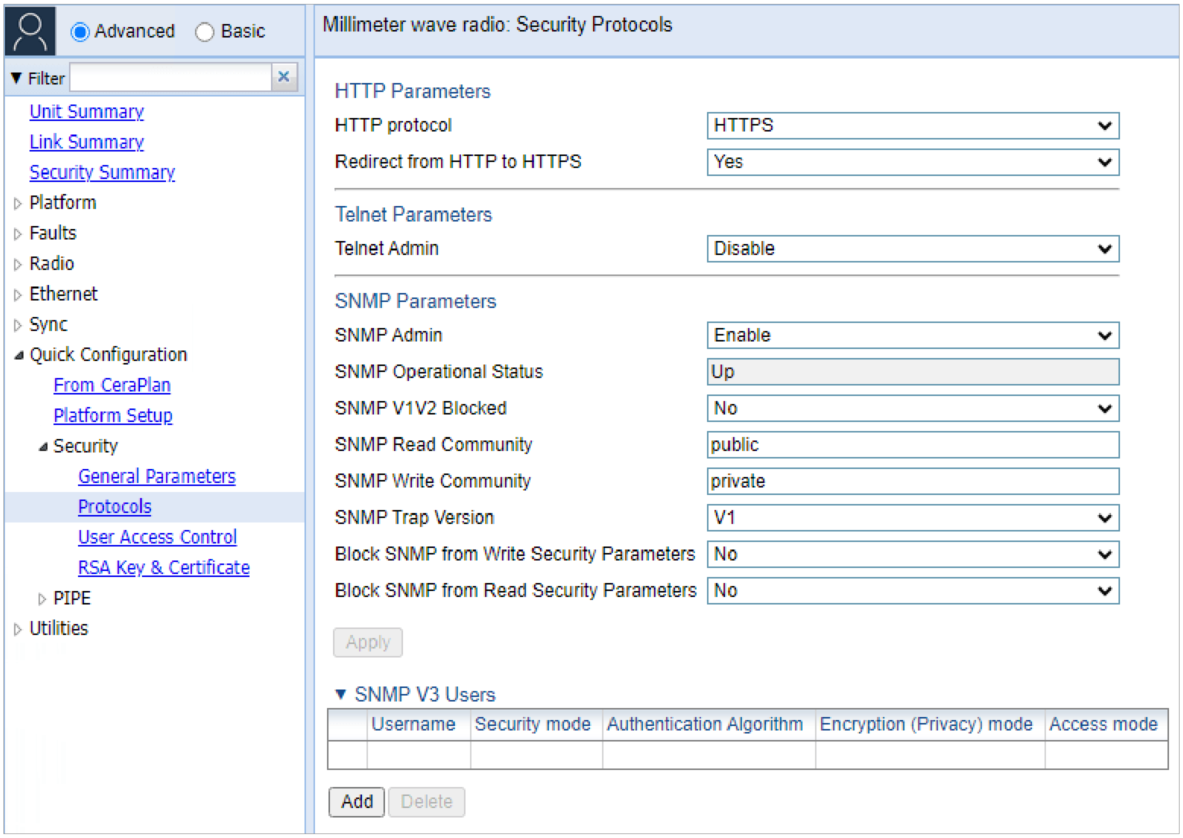
5. In the **Login Banner Text** field, you can define a login banner of up to 2,000 bytes. This banner will appear every time a user establishes a connection with the Web EMS. The banner appears before the login prompt, so that users will always see the login banner and must manually close the banner before logging in to the Web EMS. For details, see Defining a Login Banner.

Quick Security Configuration – Protocols Page

To configure the HTTP type, Telnet access, and SNMP parameters:

1. Select **Quick Configuration** > **Security** > **Protocols**. The Quick Configuration Security Protocols page opens.

Figure 290 *Quick Configuration Security Protocols Page*



Millimeter wave radio: Security Protocols

HTTP Parameters

HTTP protocol	HTTPS
Redirect from HTTP to HTTPS	Yes

Telnet Parameters

Telnet Admin	Disable

SNMP Parameters

SNMP Admin	Enable
SNMP Operational Status	Up
SNMP V1V2 Blocked	No
SNMP Read Community	public
SNMP Write Community	private
SNMP Trap Version	V1
Block SNMP from Write Security Parameters	No
Block SNMP from Read Security Parameters	No

▼ SNMP V3 Users

	Username	Security mode	Authentication Algorithm	Encryption (Privacy) mode	Access mode

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. If you select **HTTPS**, an additional field is displayed, the Redirect from **HTTP** to **HTTPS** field. This field enables you to block Port 80 when HTTPS is enabled. 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 enable or block telnet access to the unit. By default, telnet access is blocked (disabled). For details, see Enabling Telnet Access.

4. In the **SNMP Parameters** area, you can configure the unit's SNMP parameters. For details, see Configuring SNMP. In addition, you can configure the following parameters only in the Quick Configuration Security Protocols page:

   - In the **Block SNMP from Write Security Parameters** field, select Yes if you want to block SNMP from writing security parameters.
   - In the **Block SNMP from Read Security Parameters** field, select Yes if you want to block SNMP from reading security parameters.

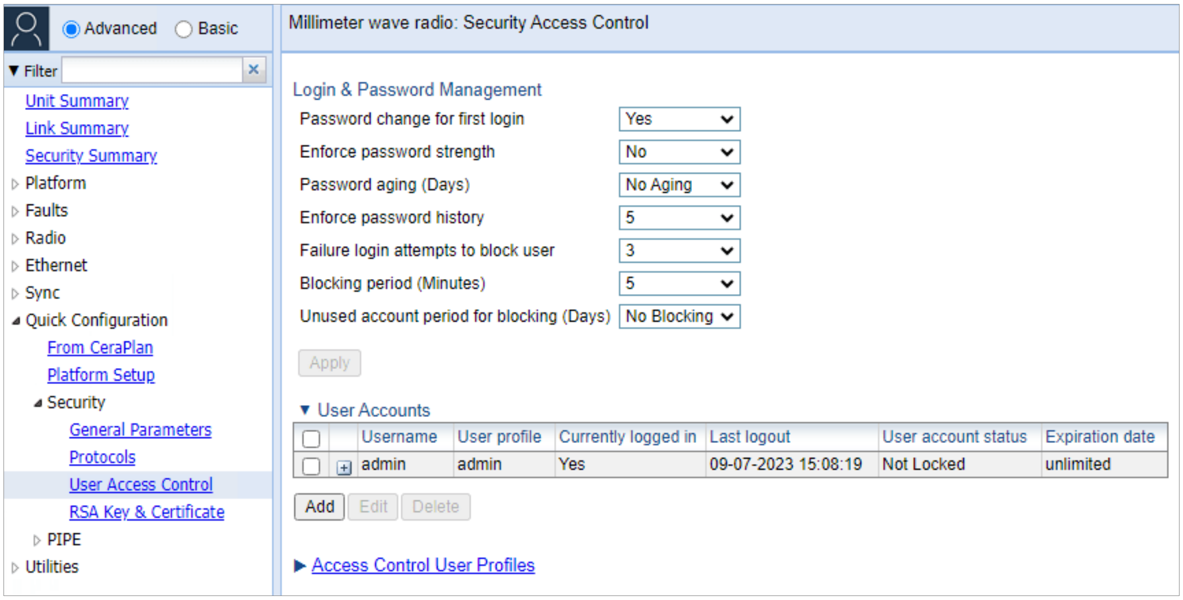
5. When you are finished editing the parameters described above, click **Apply**.
6. In the **SNMP V3 Users** are, you can click **Add** to add SNMP V3 users. For details, see Configuring SNMP.

Quick Security Configuration – Access Control Page

To configure parameters relating to users and login parameters:

1. Select **Quick Configuration** > **Security** > **User Access Control**. The Quick Configuration Security Protocols page opens.

   Figure 291 *Quick Configuration Security Access Control Page*



Millimeter wave radio: Security Access Control

Login & Password Management

Password change for first login	Yes
Enforce password strength	No
Password aging (Days)	No Aging
Enforce password history	5
Failure login attempts to block user	3
Blocking period (Minutes)	5
Unused account period for blocking (Days)	No Blocking

▼ User Accounts

□	Username	User profile	Currently logged in	Last logout	User account status	Expiration date
□	⊞ admin	admin	Yes	09-07-2023 15:08:19	Not Locked	unlimited

2. In the **Login & Password Management** area, you can configure enhanced security requirements for user passwords and for logging into the unit. For details, see Configuring the General Access Control Parameters and Configuring the Password Security Parameters.
3. When you are finished editing the login and password parameters, click **Apply**.
4. In the **User Accounts** area, you can configure individual users:
   - To add a user, click Add.
   - To edit an existing user, select the user in the User Accounts table and click Edit.

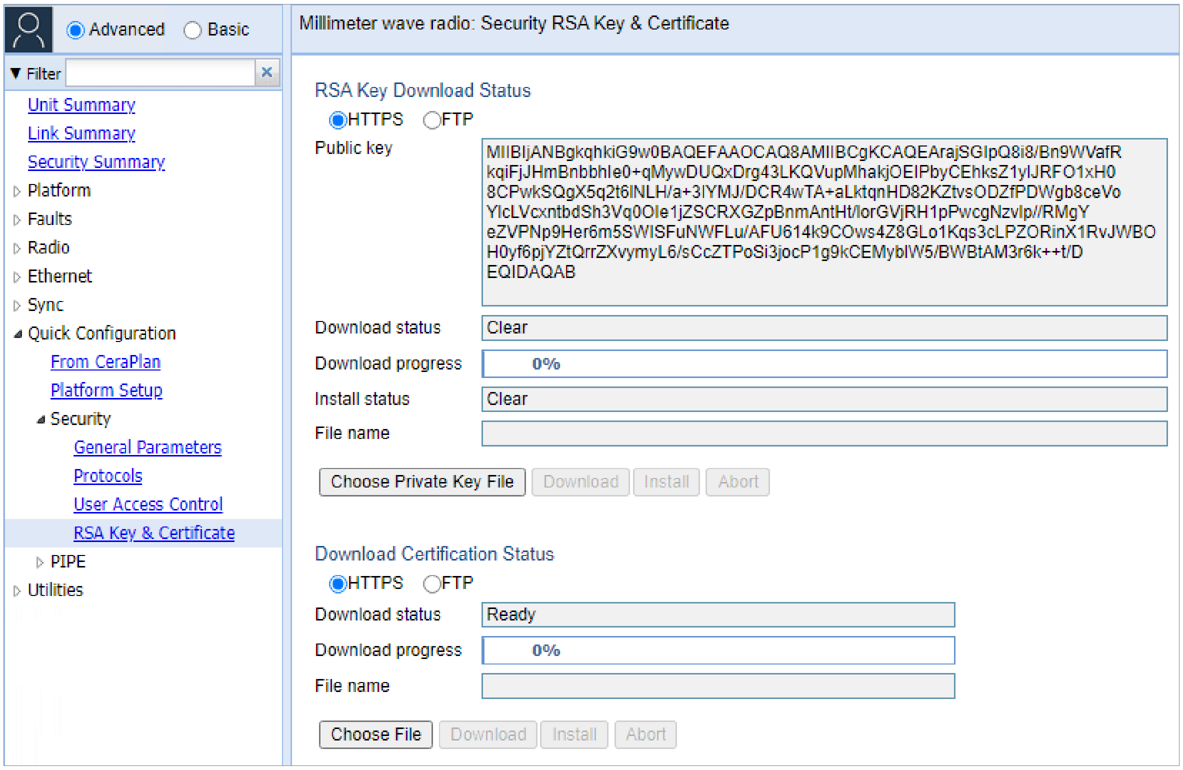
   For details, see Configuring Users.
5. To configure user profiles, click **Access Control User Profiles**. For details, see Configuring User Profiles.

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 292 *Quick Configuration Security RSA Key & Certificate Page*



Millimeter wave radio: Security RSA Key & Certificate

RSA Key Download Status

● HTTPS ○ FTP

Public key

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArajSGIpQ8i8/Bn9WVafR
kqiFjJHmBnbbhIe0+qMywDUQxDrg43LKQVupMhakjOEIPbyCEhksZ1yIJRFO1xH0
8CPwkSQgX5q2t6INLH/a+3IYMJ/DCR4wTA+aLktqnHD82KZtvsODZfPDWgb8ceVo
YIcLVcxntbdSh3Vq0OIe1jZSCRXGZpBnmAntHt/lorGVjRH1pPwcgNzvIp//RMgY
eZVPNp9Her6m5SWISFuNWFLu/AFU614k9COws4Z8GLo1Kqs3cLPZORinX1RvJWBO
H0yf6pjYZtQrrZXvymyL6/sCcZTPoSi3jocP1g9kCEMybIW5/BWBtAM3r6k++t/D
EQIDAQAB
```

Download status: Clear

Download progress: 0%

Install status: Clear

File name:

Download Certification Status

● HTTPS ○ FTP

Download status: Ready

Download progress: 0%

File name:

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.

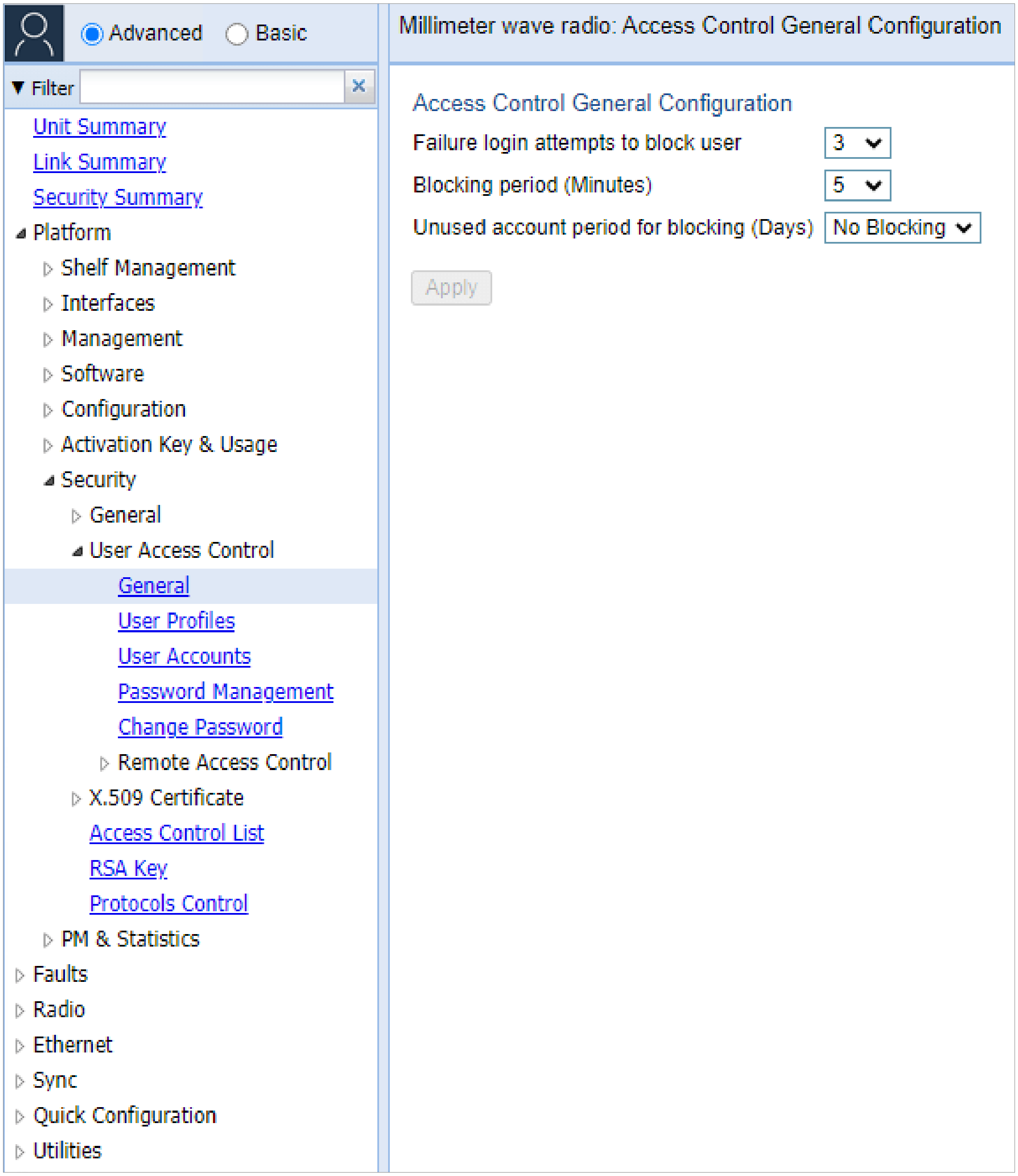
Configuring the General Access Control Parameters

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** > **User Access Control** > **General**. The Access Control General Configuration page opens.

Figure 293 *Access Control General Configuration Page*



Millimeter wave radio: Access Control General Configuration

Access Control General Configuration

Failure login attempts to block user: 3

Blocking period (Minutes): 5

Unused account period for blocking (Days): No Blocking

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.

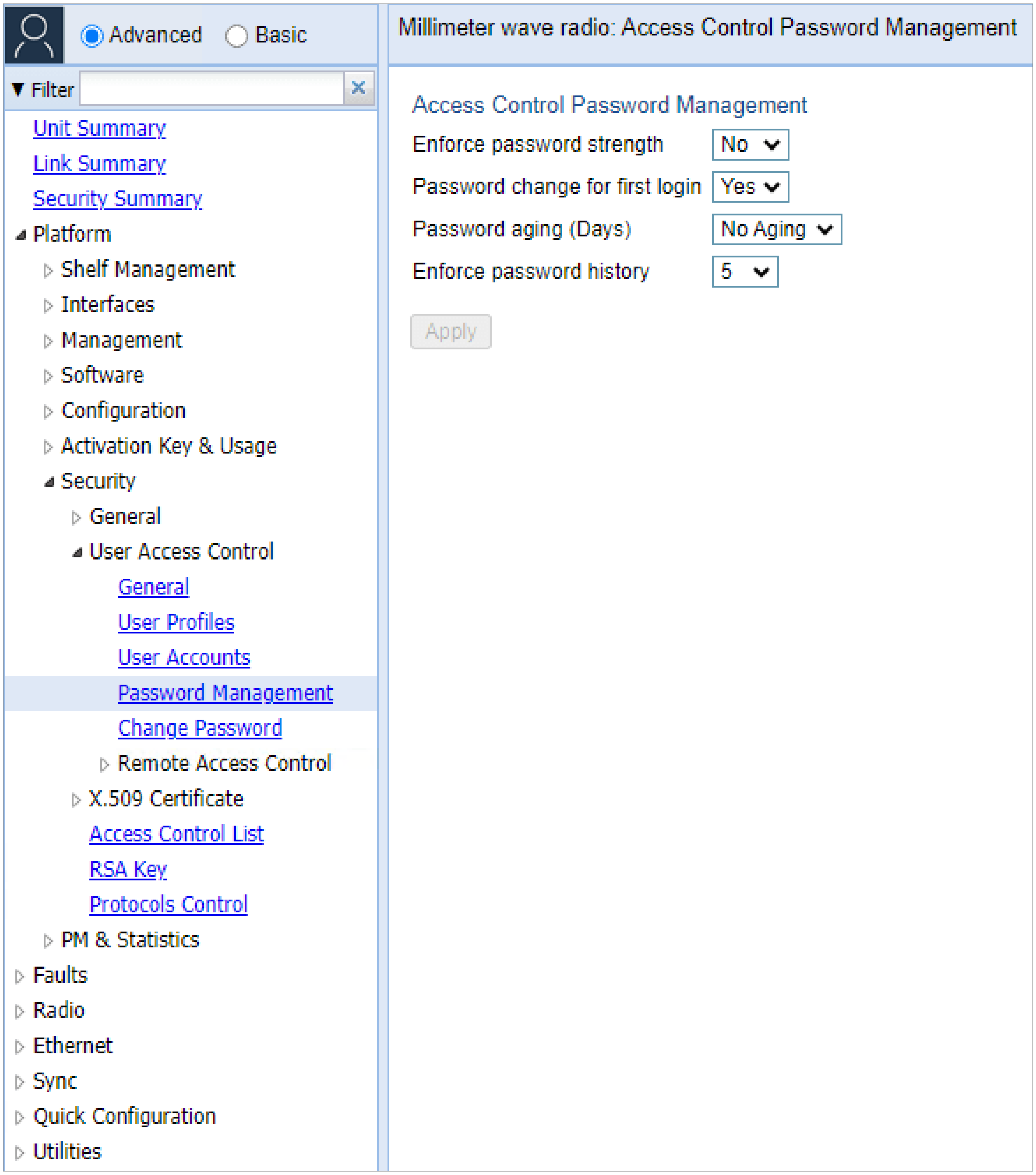
3. In the **Blocking period (Minutes)** field, enter the length of time, in minutes, that a user is prevented from logging into the system after the defined number of failed login attempts. Valid values are 1-60. The default value is 5.
4. In the **Unused account period for blocking (Days)** field, you 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 30-90 or **No Blocking**. If you enter **No Blocking**, this feature is disabled. The default value is **No Blocking**.
5. Click **Apply**.

Configuring the Password Security Parameters

To configure enhanced security requirements for user passwords:

1. Select **Platform** > **Security** > **User Access Control** > **Password Management**. The Access Control Password Management page opens.

Figure 294 *Access Control Password Management Page*



Millimeter wave radio: Access Control Password Management

Access Control Password Management

Enforce password strength	No
Password change for first login	Yes
Password aging (Days)	No Aging
Enforce password history	5

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.
    - 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*.

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**.

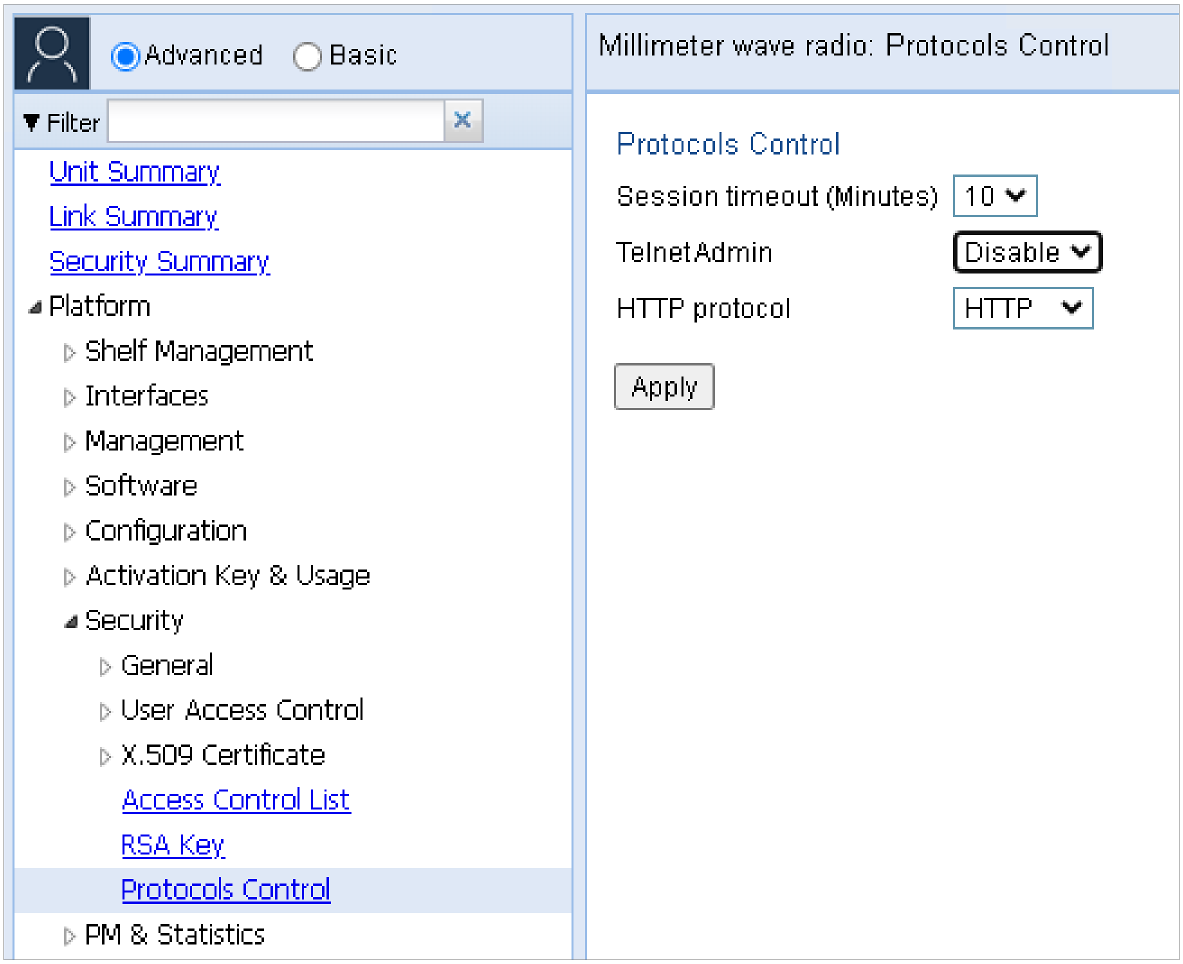
Configuring the Session Timeout

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 295 *Protocols Control Page*



Millimeter wave radio: Protocols Control

Protocols Control

Session timeout (Minutes) 10

TelnetAdmin Disable

HTTP protocol HTTP

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 Enabling Telnet Access.

3. Click Apply.

Configuring Users

This section includes:

- User Configuration Overview
- Configuring User Profiles
- Adding User Accounts

Related topics:

- Changing Your Password

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

> Note
>
> TDM is not relevant for PTP 850EX.

- 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.

Configuring User Profiles

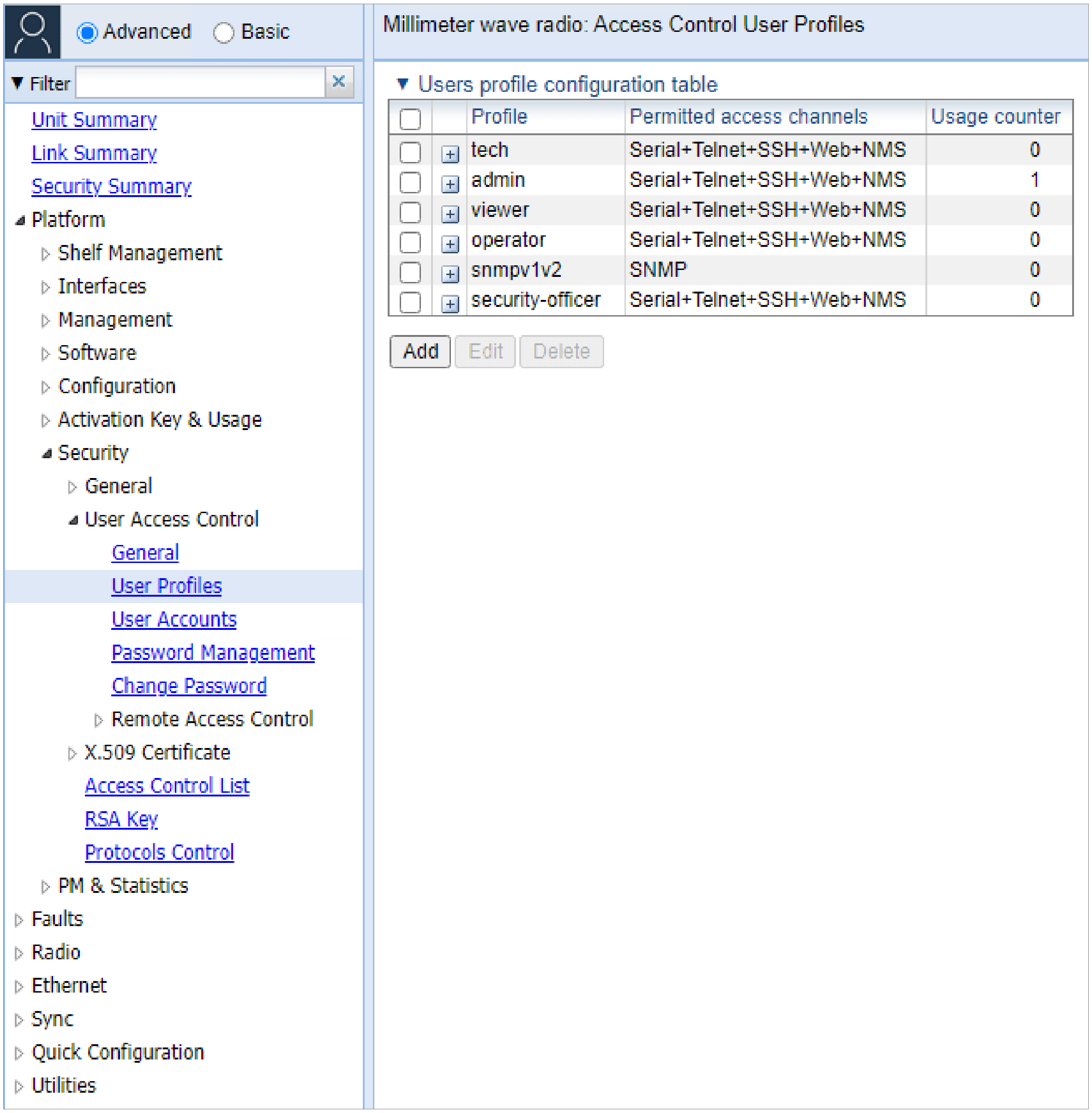
User profiles enable you to define system access levels. Each user must be assigned a user profile. Each user profile contains a detailed set of read and write permission levels per functionality group.

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.

To add a user profile:

1. Select **Platform** > **Security** > **User Access Control** > **User Profiles**. The Access Control User Profiles page opens.

Figure 296 *Access Control User Profiles Page*



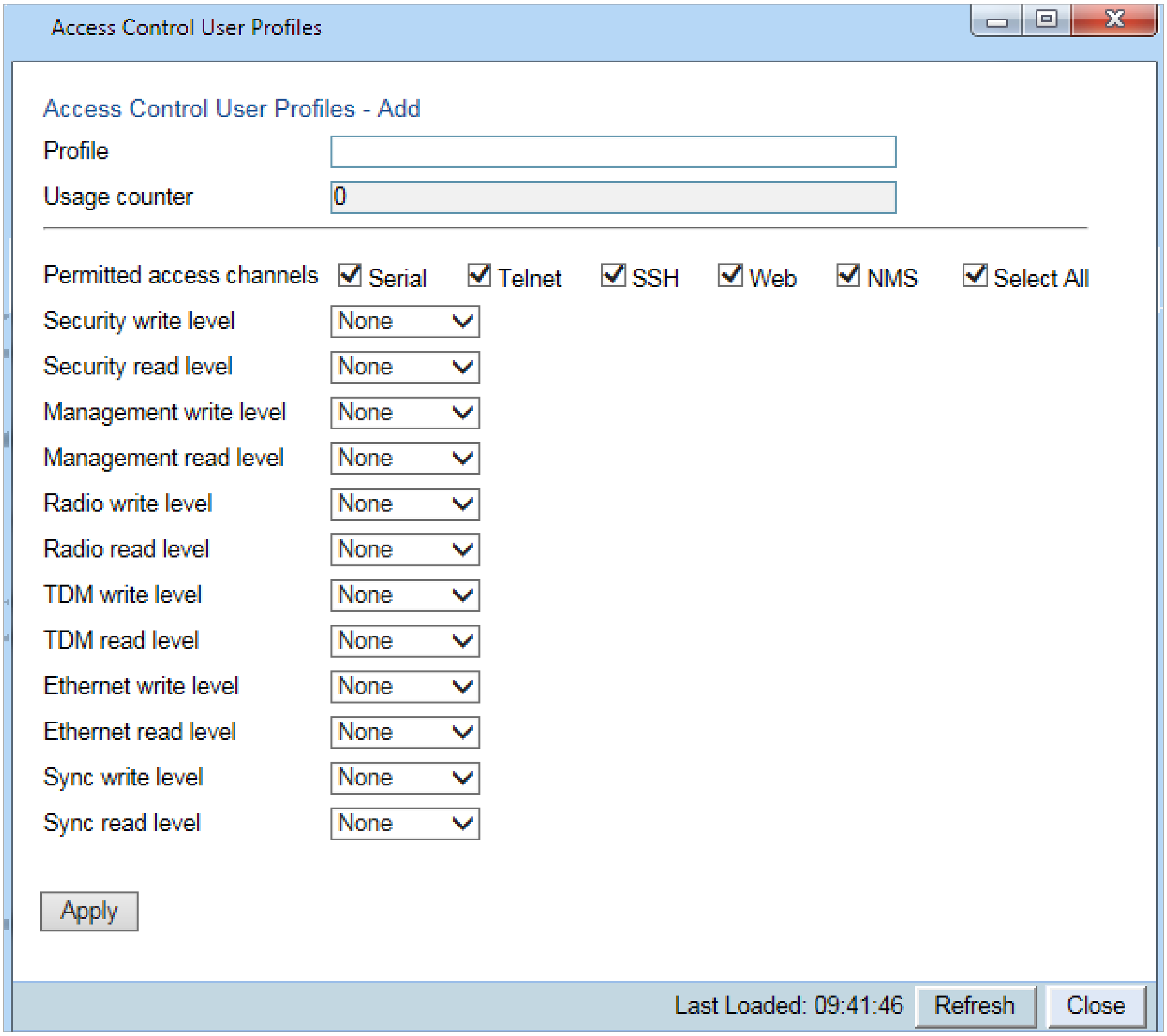
Millimeter wave radio: Access Control User Profiles

▼ Users profile configuration table

□		Profile	Permitted access channels	Usage counter
□	⊞	tech	Serial+Telnet+SSH+Web+NMS	0
□	⊞	admin	Serial+Telnet+SSH+Web+NMS	1
□	⊞	viewer	Serial+Telnet+SSH+Web+NMS	0
□	⊞	operator	Serial+Telnet+SSH+Web+NMS	0
□	⊞	snmpv1v2	SNMP	0
□	⊞	security-officer	Serial+Telnet+SSH+Web+NMS	0

2. Click Add. The Access Control User Profiles - Add page opens.

Figure 297 *Access Control User Profiles - Add Page*



Access Control User Profiles

Access Control User Profiles - Add

Profile	
Usage counter	0
Permitted access channels	☑ Serial ☑ Telnet ☑ SSH ☑ Web ☑ NMS ☑ Select All
Security write level	None
Security read level	None
Management write level	None
Management read level	None
Radio write level	None
Radio read level	None
TDM write level	None
TDM read level	None
Ethernet write level	None
Ethernet read level	None
Sync write level	None
Sync read level	None

Last Loaded: 09:41:46

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**
>
> **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.

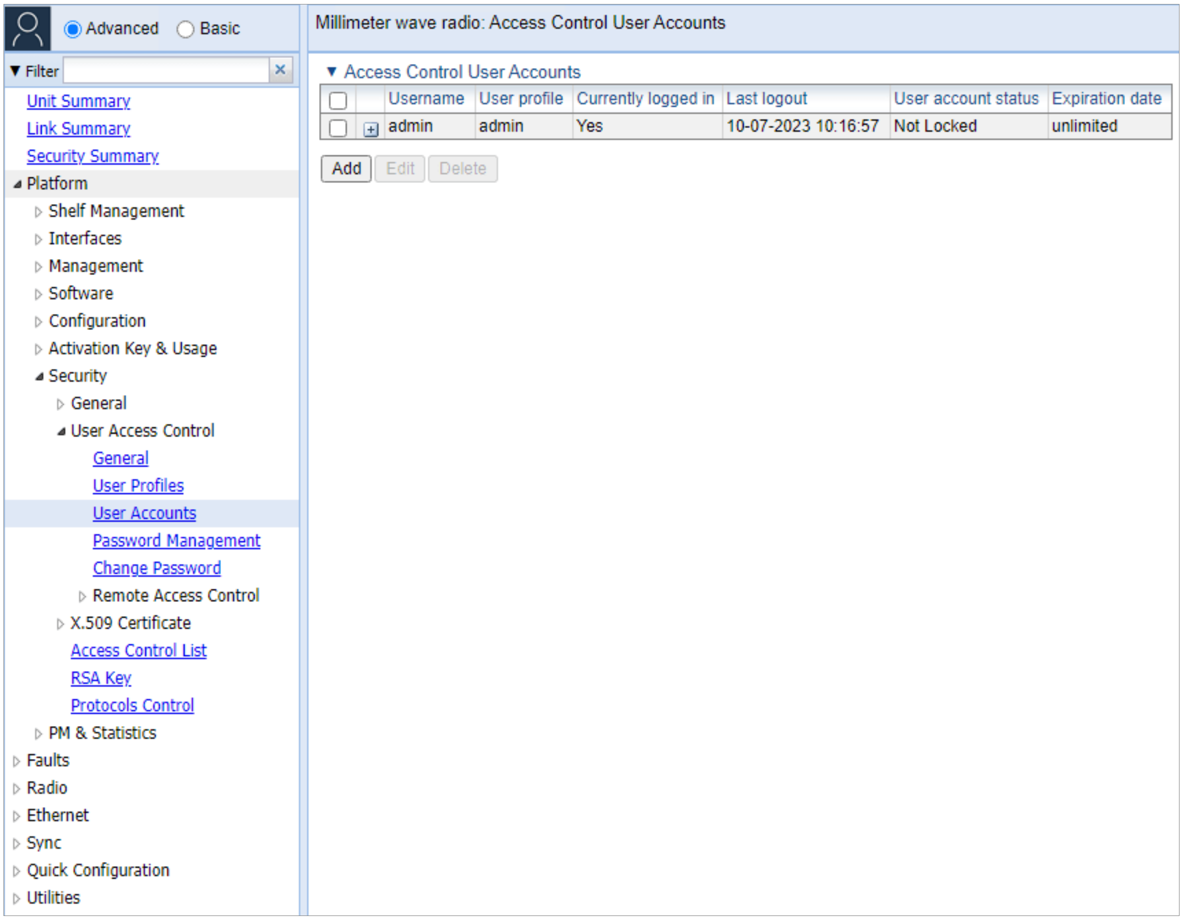
Adding User Accounts

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. See Configuring User Profiles.

To add a new user:

1. Select **Platform** > **Security** > **User Access Control** > **User Accounts**. The Access Control User Accounts page opens.

Figure 298 *Access Control User Accounts Page*



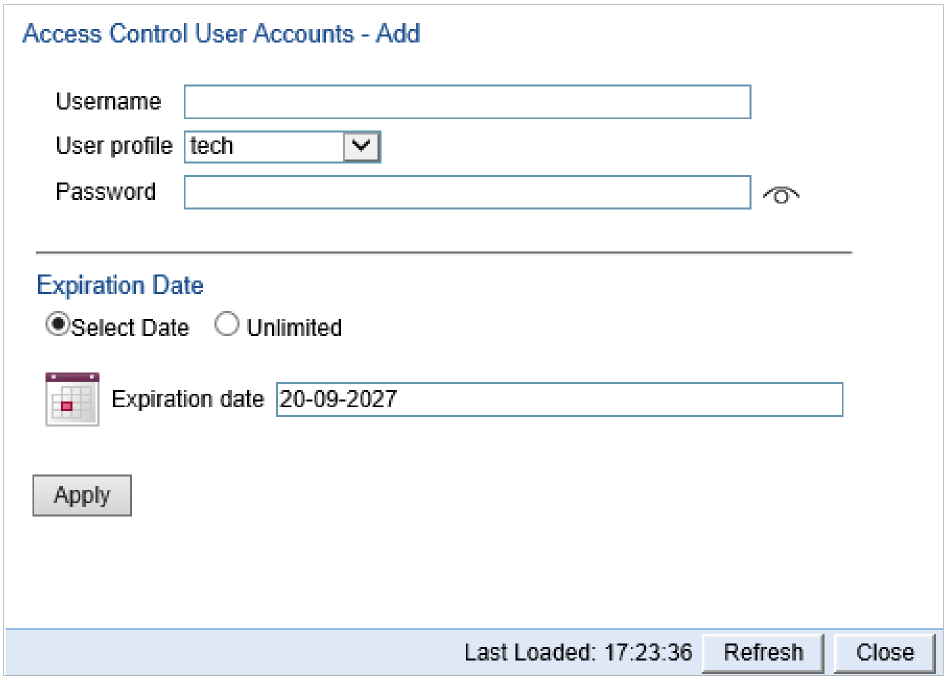
Millimeter wave radio: Access Control User Accounts

▼ Access Control User Accounts

□		Username	User profile	Currently logged in	Last logout	User account status	Expiration date
□	⊞	admin	admin	Yes	10-07-2023 10:16:57	Not Locked	unlimited

2. Click **Add**. The Access Control User Accounts - Add page opens.

Figure 299 *Access Control User Accounts - Add Page*



Access Control User Accounts - Add

Username

User profile: tech

Password

Expiration Date

● Select Date ○ Unlimited

Expiration date: 20-09-2027

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. See Configuring User Profiles.
5. In the **Password** field, enter a password for the user. 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.
   - 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**.

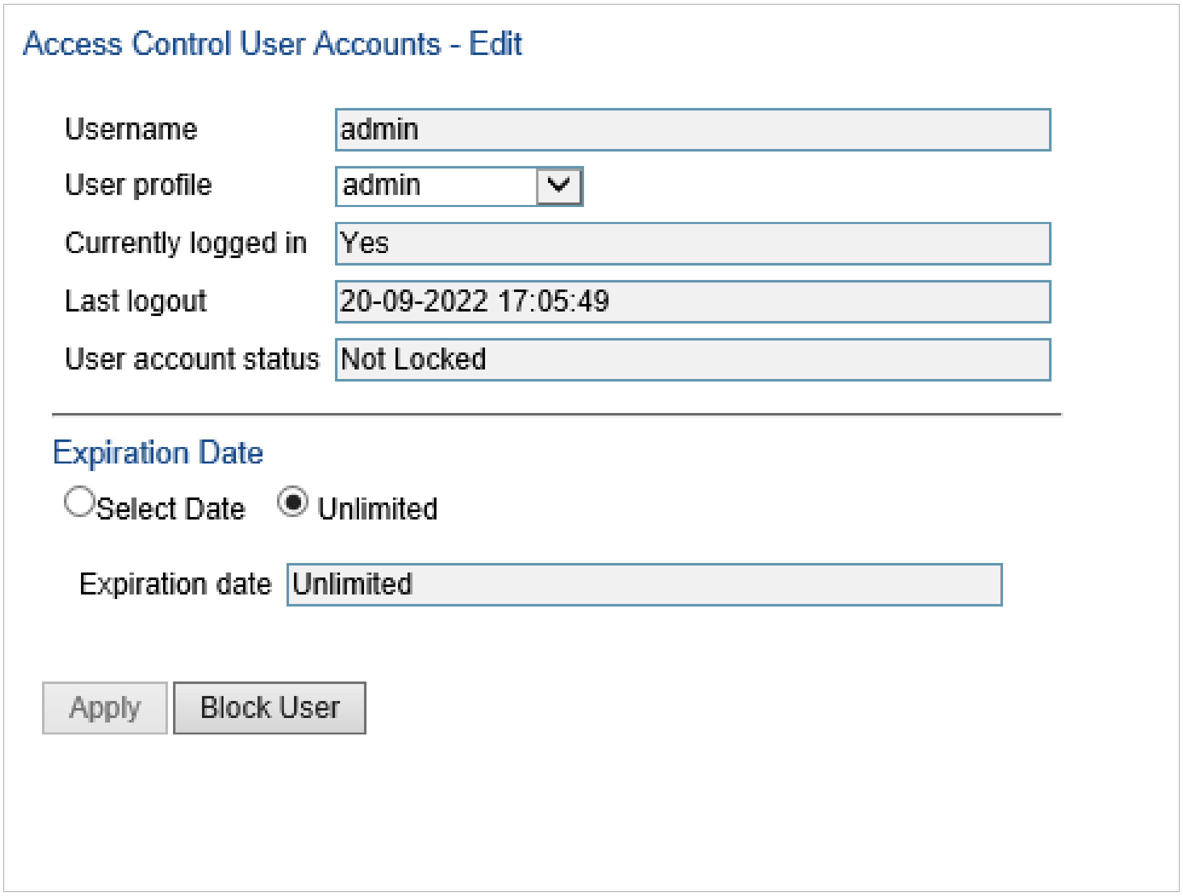
To delete a user, select the user and click **Delete**.

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 (Access Control User Accounts Page).
2. Select the user and click **Edit**. The Access Control User Accounts - Edit page opens.

Figure 300 *Access Control User Accounts - Edit Page*



Access Control User Accounts - Edit

Username	admin
User profile	admin
Currently logged in	Yes
Last logout	20-09-2022 17:05:49
User account status	Not Locked

Expiration Date

○ Select Date ● Unlimited

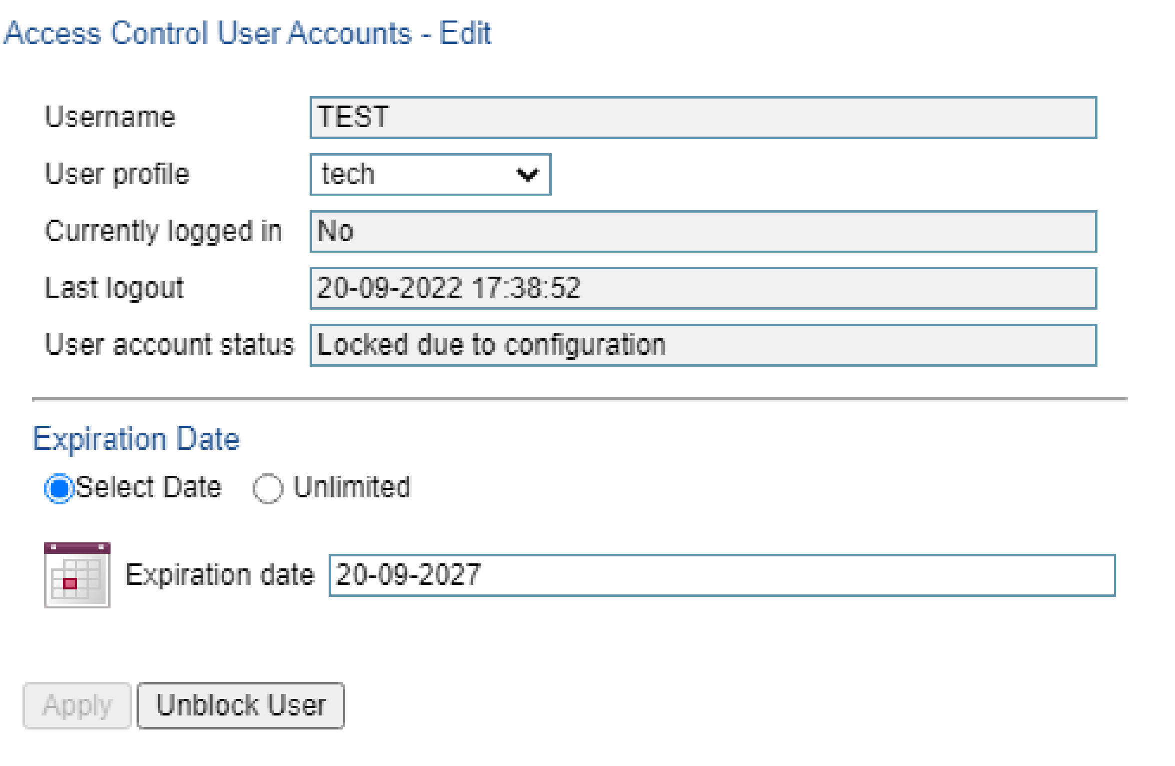
Expiration date: Unlimited

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. See Configuring the General Access Control Parameters.

   Figure 301 *Access Control User Accounts - Edit Page (User Blocked)*



Access Control User Accounts - Edit

Username	TEST
User profile	tech
Currently logged in	No
Last logout	20-09-2022 17:38:52
User account status	Locked due to configuration

Expiration Date

● Select Date ○ Unlimited

Expiration date 20-09-2027

4. Click **Apply**, then **Close**.

Configuring RADIUS

This section includes:

- RADIUS Overview
- Activating RADIUS Authentication

- Configuring the RADIUS Server Attributes
- Configuring a RADIUS Server

RADIUS Overview

The RADIUS protocol provides centralized user management services. PTP 850 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 850 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

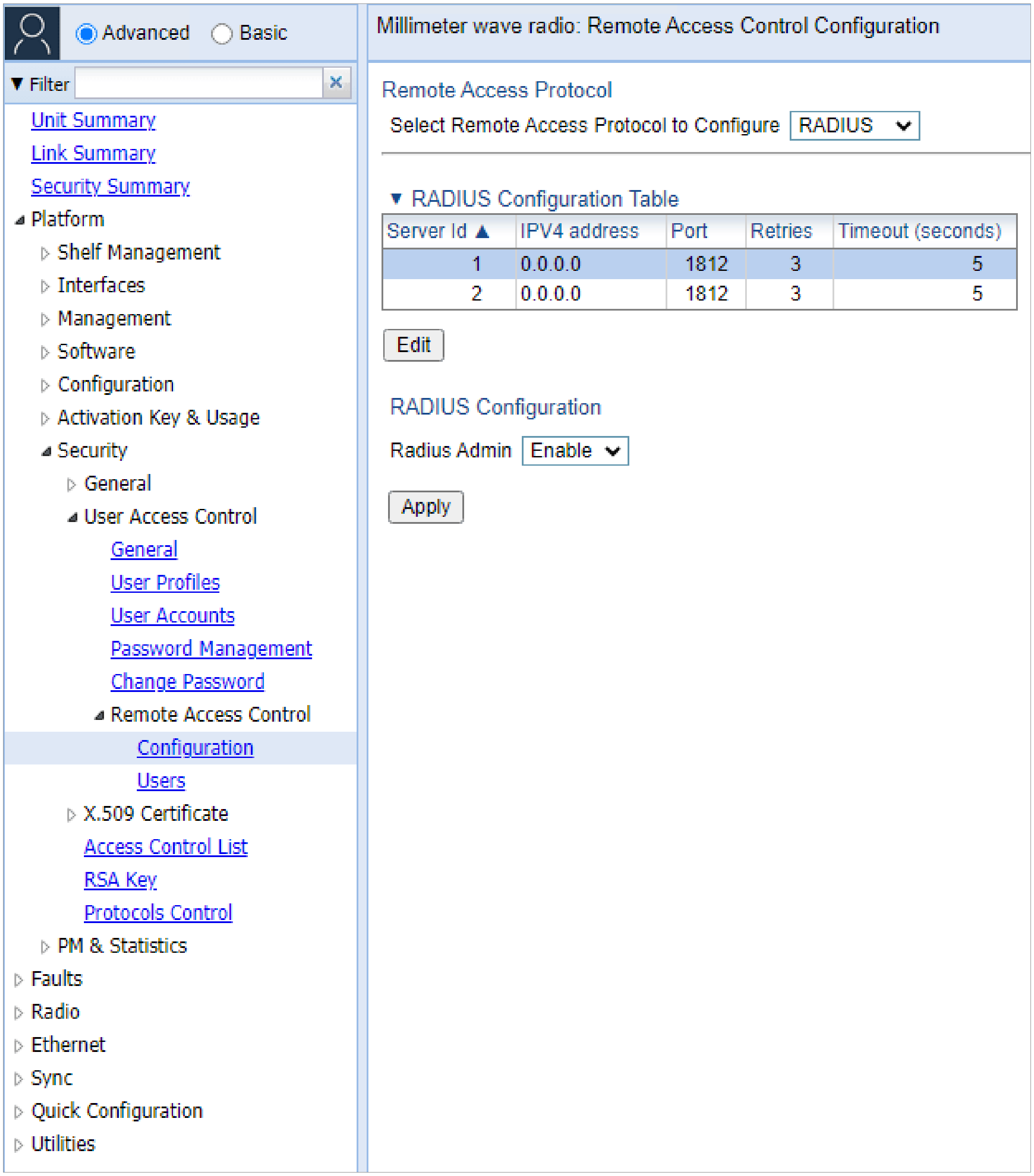
You can define up to two Radius servers. If you define two, one serves as the primary server and the other as the secondary server.

Activating RADIUS Authentication

To activate RADIUS authentication:

1. Select **Platform** > **Security** > **User Access Control** > **Remote Access Control** > **Configuration**. The Remote Access Control Configuration page opens.

Figure 302 *Remote Access Control Configuration Page (RADIUS)*



Millimeter wave radio: Remote Access Control Configuration

Remote Access Protocol

Select Remote Access Protocol to Configure: RADIUS

▼ RADIUS Configuration Table

Server Id ▲	IPV4 address	Port	Retries	Timeout (seconds)
1	0.0.0.0	1812	3	5
2	0.0.0.0	1812	3	5

RADIUS Configuration

Radius Admin: Enable

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

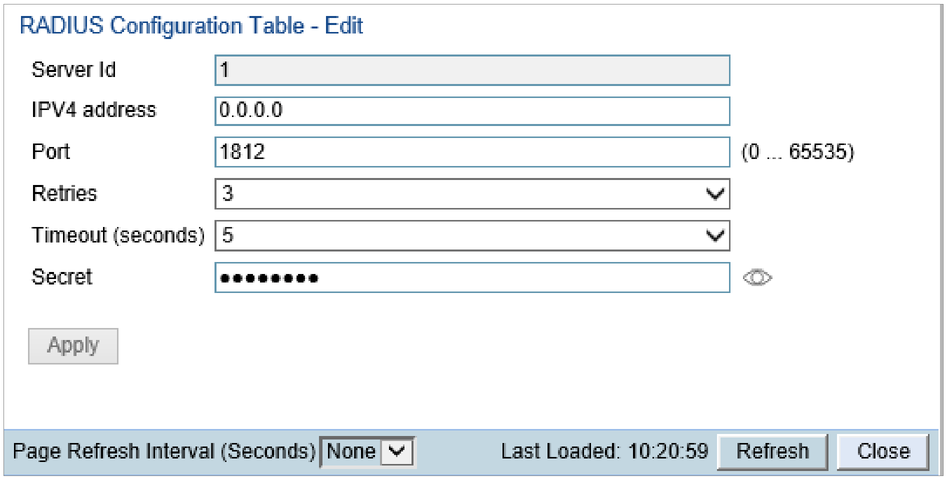
When the Protocol is changed, all active sessions are terminated when you click **Apply**.

Configuring the RADIUS Server Attributes

To configure the RADIUS server attributes:

1. Select **Platform** > **Security** > **User Access Control** > **Remote Access Control** > **Configuration**. The Remote Access Control Configuration page opens (Remote Access Control Configuration Page (RADIUS)). 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 303 *Radius Configuration – Edit Page*



RADIUS Configuration Table - Edit

Server Id	1
IPV4 address	0.0.0.0
Port	1812 (0 ... 65535)
Retries	3
Timeout (seconds)	5
Secret	●●●●●●●●

Page Refresh Interval (Seconds) None

Last Loaded: 10:20:59

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.
9. 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.

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 850 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

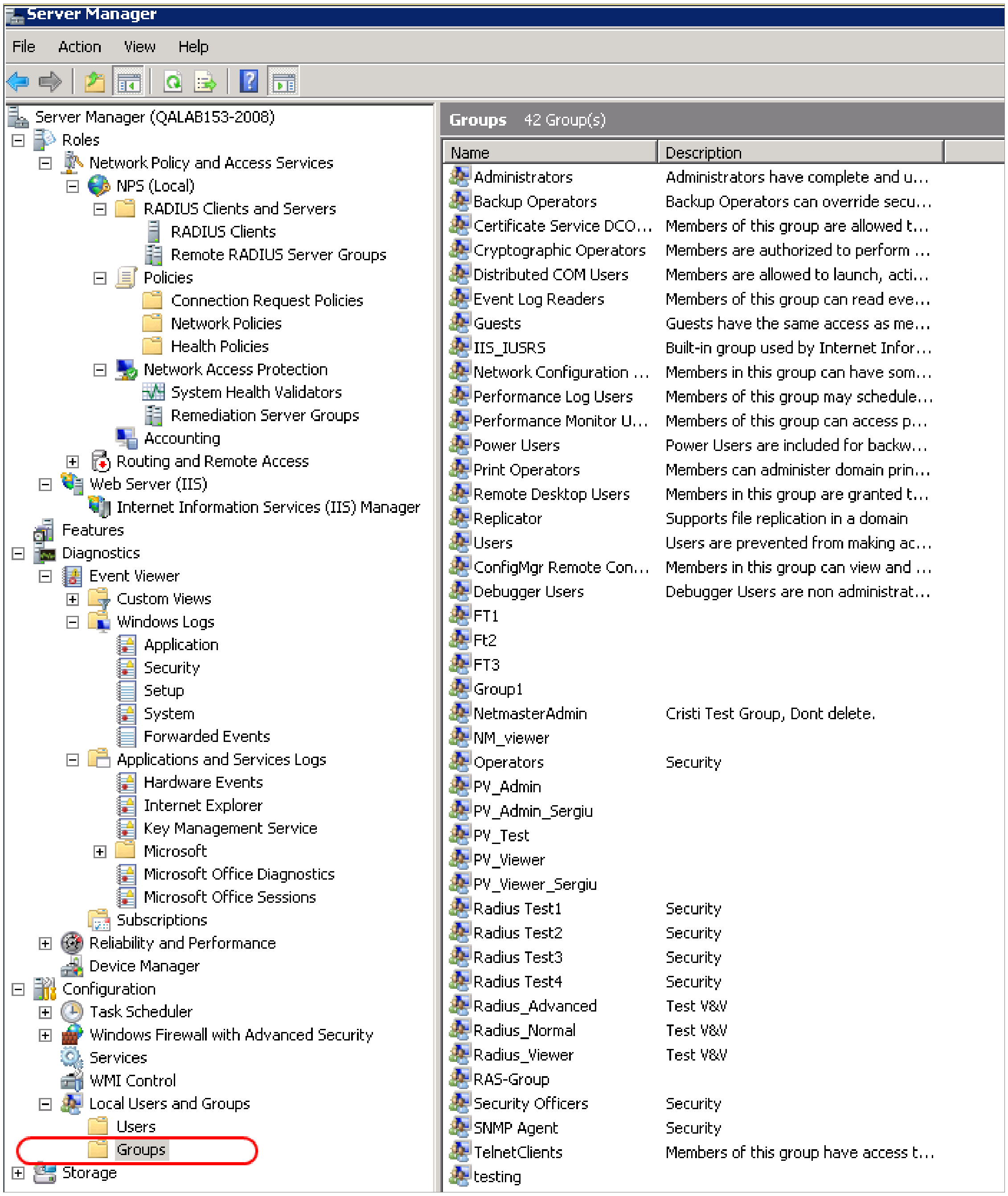
The following sub-sections describe how to configure a Win 2008 RADIUS Server to work with an PTP 850 device.

Step 1 – Creating Groups and Users

To create groups and users:

1. Create three user groups, as follows:
   - In the Server Manager, navigate to **Configuration** > **Local Users and Groups**.
   - Right click **Groups** and create the following three user groups:
     - Radius_Advanced
     - Radius_Normal
     - Radius_Viewer

Figure 304 *Server Manager – Creating User Groups*

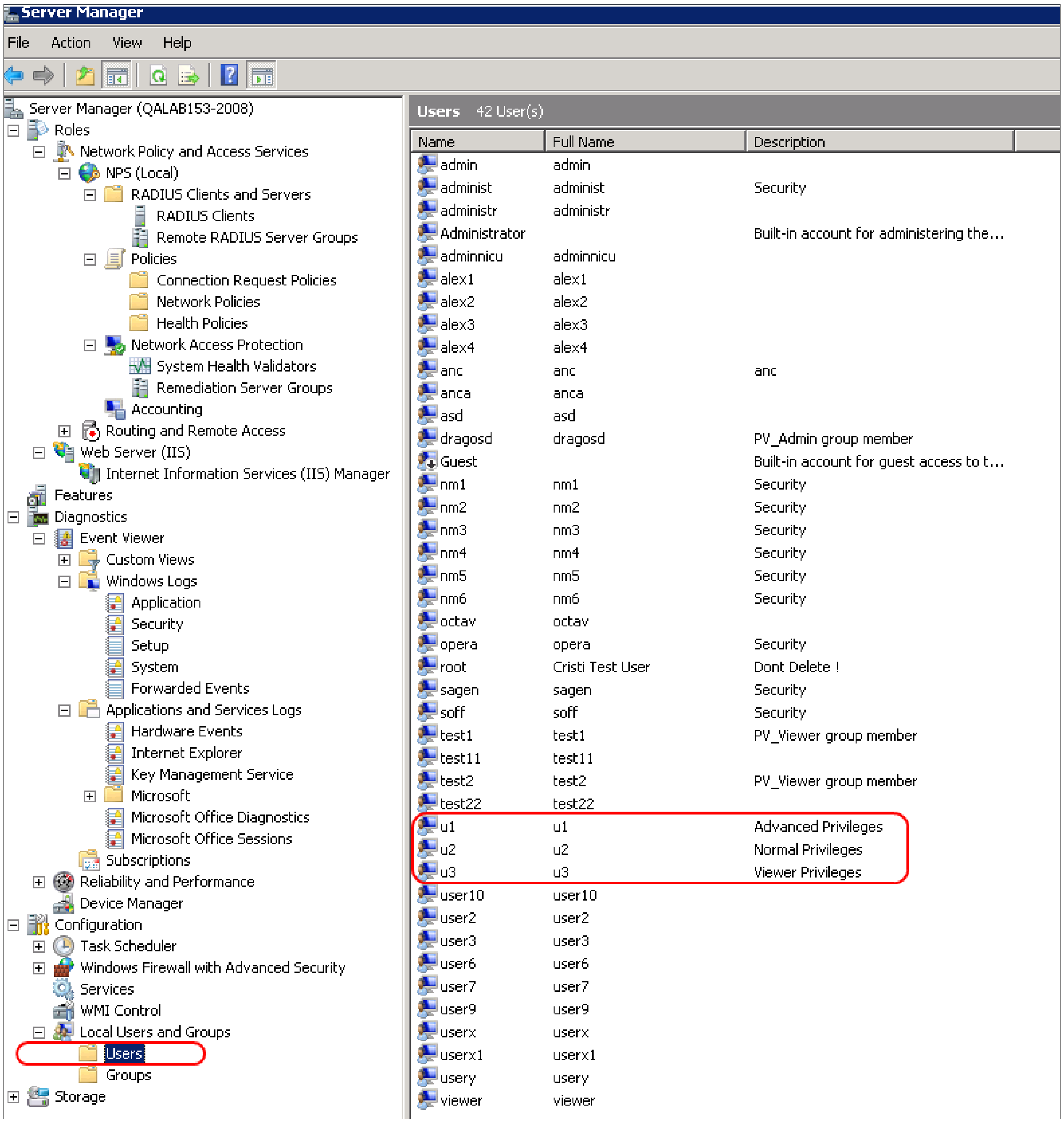


Name	Description
Administrators	Administrators have complete and u...
Backup Operators	Backup Operators can override secu...
Certificate Service DCO...	Members of this group are allowed t...
Cryptographic Operators	Members are authorized to perform ...
Distributed COM Users	Members are allowed to launch, acti...
Event Log Readers	Members of this group can read eve...
Guests	Guests have the same access as me...
IIS_IUSRS	Built-in group used by Internet Infor...
Network Configuration ...	Members in this group can have som...
Performance Log Users	Members of this group may schedule...
Performance Monitor U...	Members of this group can access p...
Power Users	Power Users are included for backw...
Print Operators	Members can administer domain prin...
Remote Desktop Users	Members in this group are granted t...
Replicator	Supports file replication in a domain
Users	Users are prevented from making ac...
ConfigMgr Remote Con...	Members in this group can view and ...
Debugger Users	Debugger Users are non administrat...
FT1	
Ft2	
FT3	
Group1	
NetmasterAdmin	Cristi Test Group, Dont delete.
NM_viewer	
Operators	Security
PV_Admin	
PV_Admin_Sergiu	
PV_Test	
PV_Viewer	
PV_Viewer_Sergiu	
Radius Test1	Security
Radius Test2	Security
Radius Test3	Security
Radius Test4	Security
Radius_Advanced	Test V&V
Radius_Normal	Test V&V
Radius_Viewer	Test V&V
RAS-Group	
Security Officers	Security
SNMP Agent	Security
TelnetClients	Members of this group have access t...
testing	

2. Create three users:

- u1
- u2
- u3

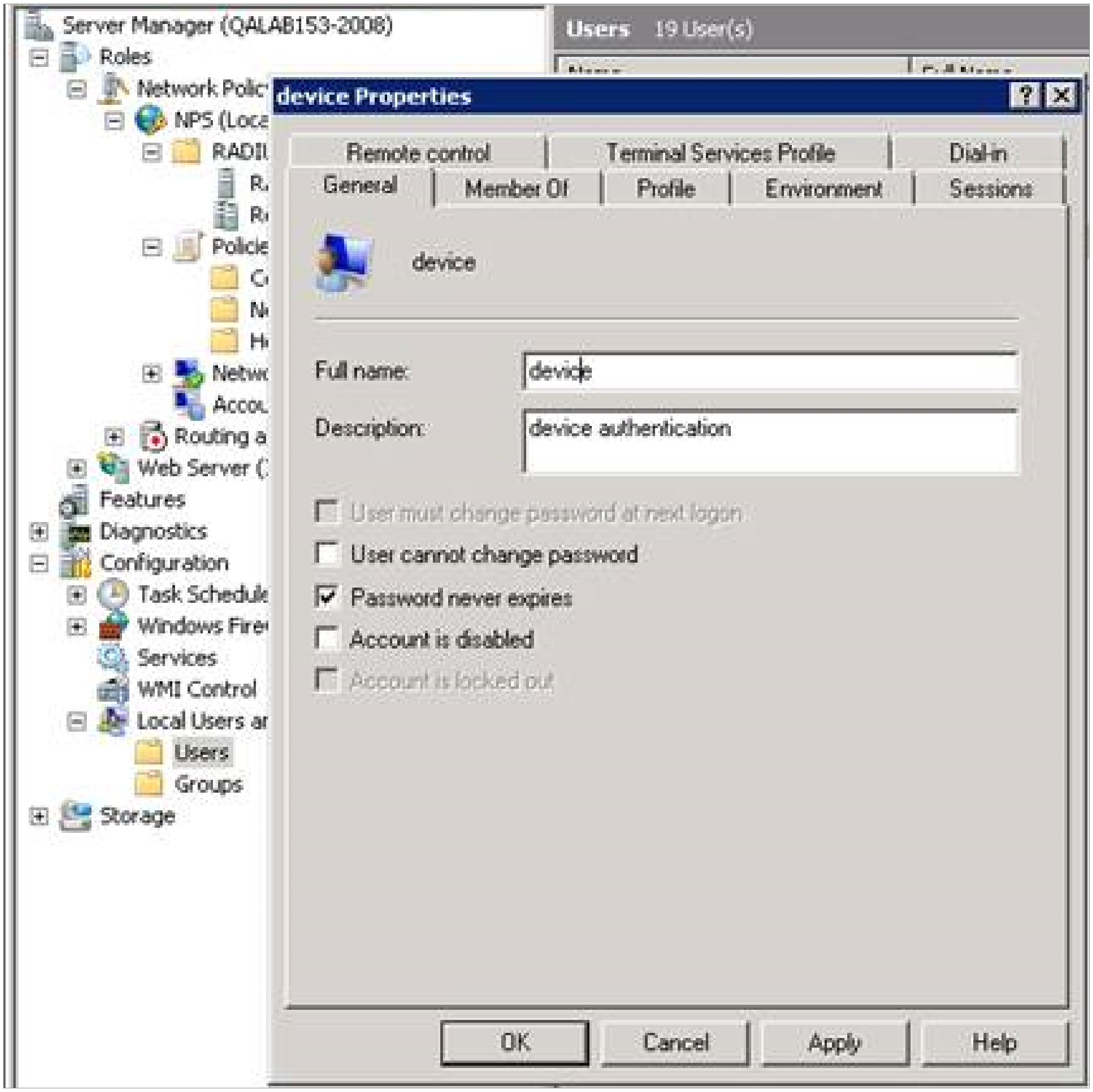
Figure 305 *Server Manager – Creating Users*



Name	Full Name	Description
admin	admin	
administ	administ	Security
administr	administr	
Administrator		Built-in account for administering the...
adminnicu	adminnicu	
alex1	alex1	
alex2	alex2	
alex3	alex3	
alex4	alex4	
anc	anc	anc
anca	anca	
asd	asd	
dragosd	dragosd	PV_Admin group member
Guest		Built-in account for guest access to t...
nm1	nm1	Security
nm2	nm2	Security
nm3	nm3	Security
nm4	nm4	Security
nm5	nm5	Security
nm6	nm6	Security
octav	octav	
opera	opera	Security
root	Cristi Test User	Dont Delete !
sagen	sagen	Security
soff	soff	Security
test1	test1	PV_Viewer group member
test11	test11	
test2	test2	PV_Viewer group member
test22	test22	
u1	u1	Advanced Privileges
u2	u2	Normal Privileges
u3	u3	Viewer Privileges
user10	user10	
user2	user2	
user3	user3	
user6	user6	
user7	user7	
user9	user9	
userx	userx	
userx1	userx1	
usery	usery	
viewer	viewer	

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 306 *Server Manager – User Password Settings*



device

Full name: device

Description: device authentication

□ User must change password at next logon

□ User cannot change password

☑ Password never expires

□ Account is disabled

□ Account is locked out

4. Attach each user to a group, as follows:

   - Attach u1 to Radius_Advanced
   - Attach u2 to Radius_Normal
   - Attach u3 to Radius_Viewer

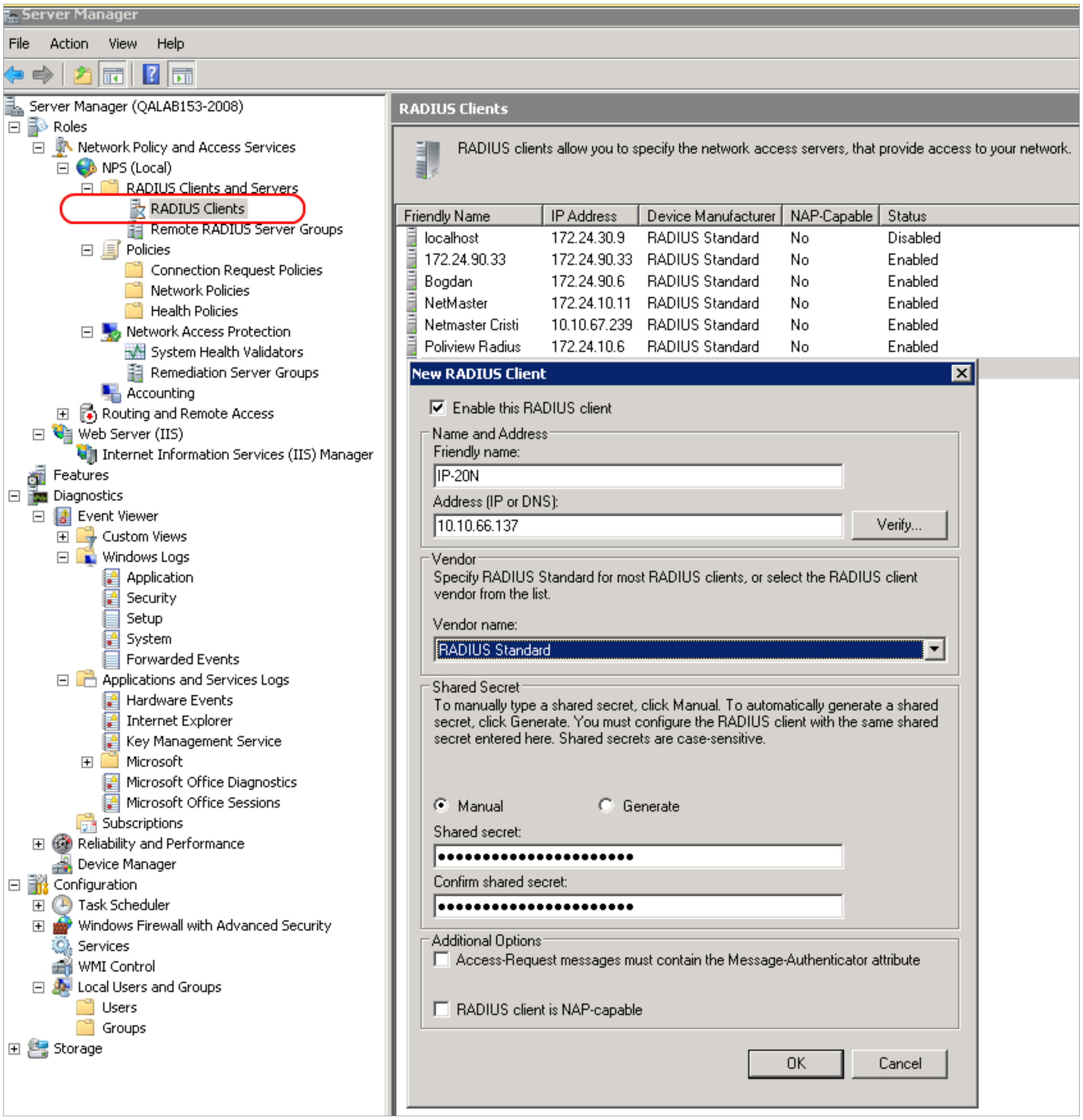
   Step 2 – Creating a RADIUS Client

   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.

Server Manager – Creating a RADIUS Client



RADIUS clients allow you to specify the network access servers, that provide access to your network.

Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
localhost	172.24.30.9	RADIUS Standard	No	Disabled
172.24.90.33	172.24.90.33	RADIUS Standard	No	Enabled
Bogdan	172.24.90.6	RADIUS Standard	No	Enabled
NetMaster	172.24.10.11	RADIUS Standard	No	Enabled
Netmaster Cristi	10.10.67.239	RADIUS Standard	No	Enabled
Poliview Radius	172.24.10.6	RADIUS Standard	No	Enabled

New RADIUS Client

☑ Enable this RADIUS client

Name and Address

Friendly name: IP-20N

Address (IP or DNS): 10.10.66.137 Verify...

Vendor

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name: RADIUS Standard

Shared Secret

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••••••••••••••••••••

Confirm shared secret: ••••••••••••••••••••••

Additional Options

□ Access-Request messages must contain the Message-Authenticator attribute

□ RADIUS client is NAP-capable

OK Cancel

3. In the New RADIUS Client window:

- Select the **Enable this RADIUS client** check box.
- Enter a descriptive **Friendly name** for the device, such as PTP 850.
- Enter the device IP **Address**.
- Select **RADIUS Standard** as the **Vendor name**.

- 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 (Radius Configuration – Edit Page).

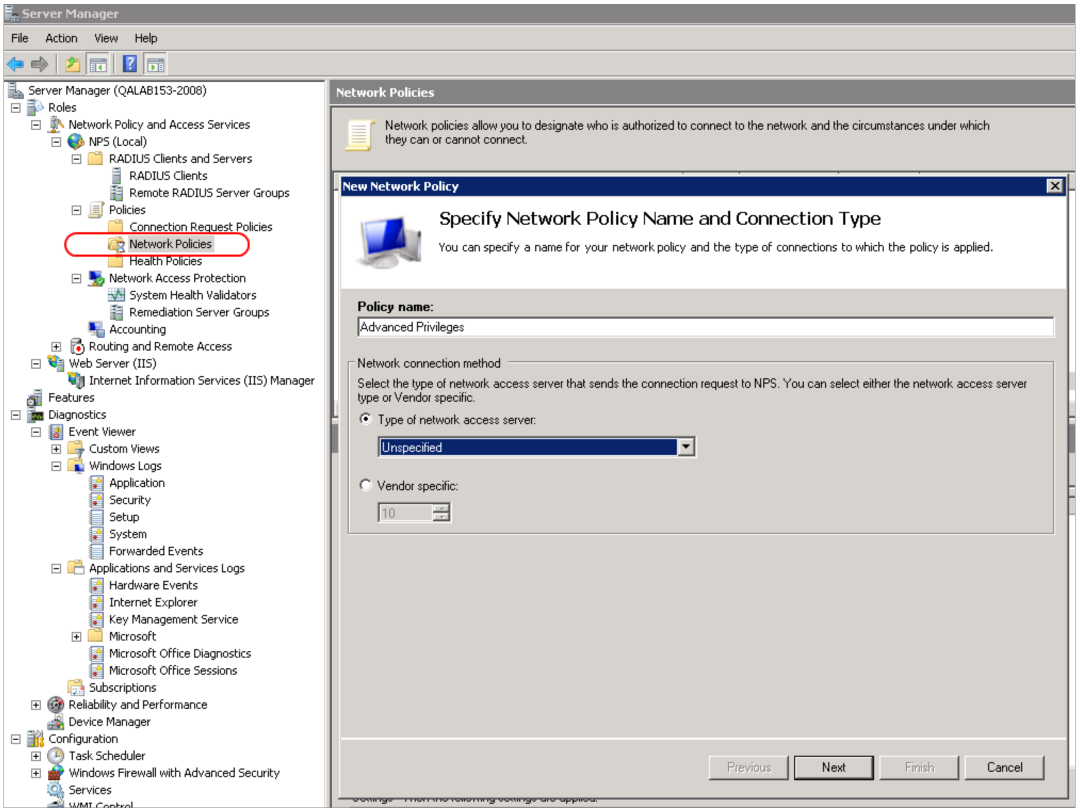
Step 3 – Creating a Network Policy

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 307 *Create Network Policy – Specify Name and Connection Type*



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name: Advanced Privileges

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.

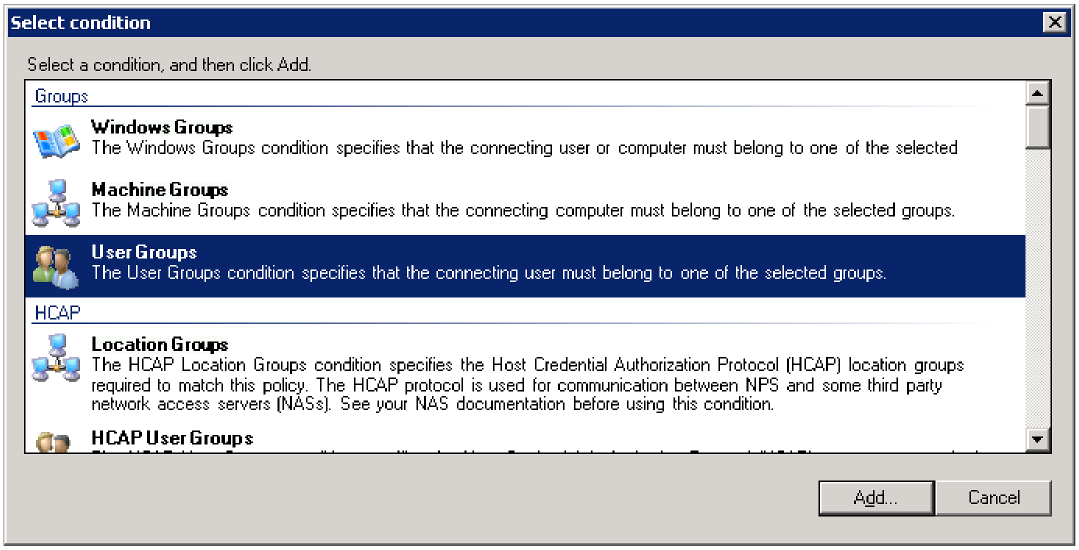
● Type of network access server: Unspecified

○ Vendor specific: 10

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 308 *Create Network Policy – Select Condition*



Select a condition, and then click Add.

Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected

Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.

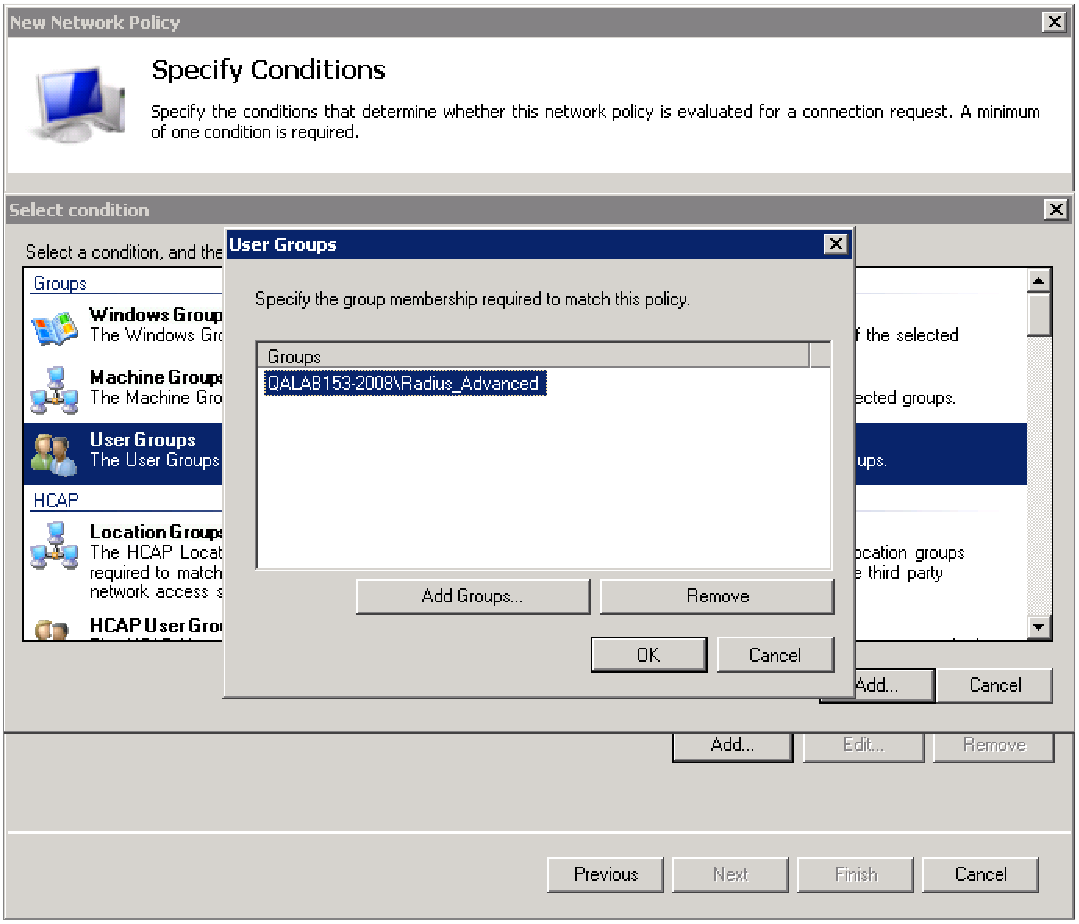
User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

Location Groups
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.

HCAP User Groups

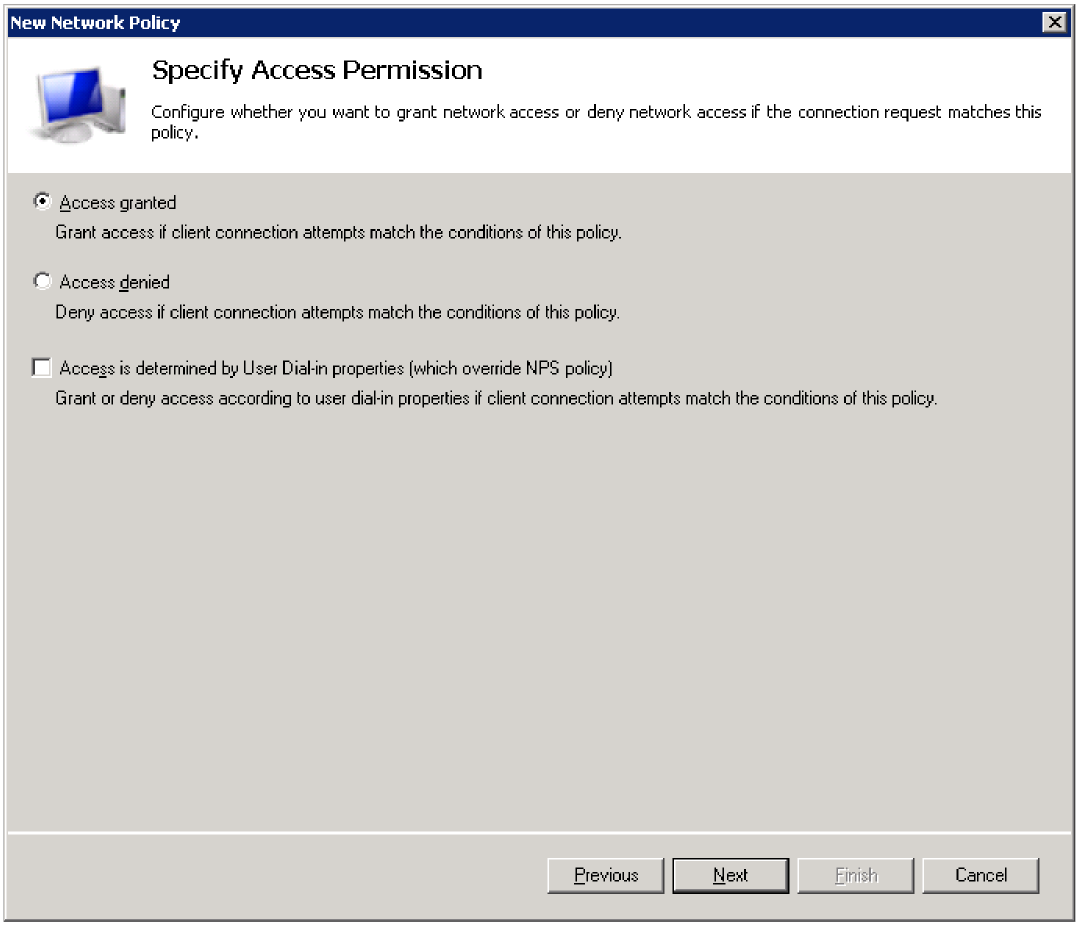
7. In the User Groups window that appears, click **Add Groups**.
8. In the Select Group window that appears, click **Advanced**.
9. In the Select Group window that appears, click **Find Now** to list all groups, and then select the appropriate group from the list: Radius_Advanced, Radius_Normal, or Radius_Viewer.
10. Click **OK**.

Figure 309 *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 310 *Create Network Policy – Specifying Access Permission*



New Network Policy

Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

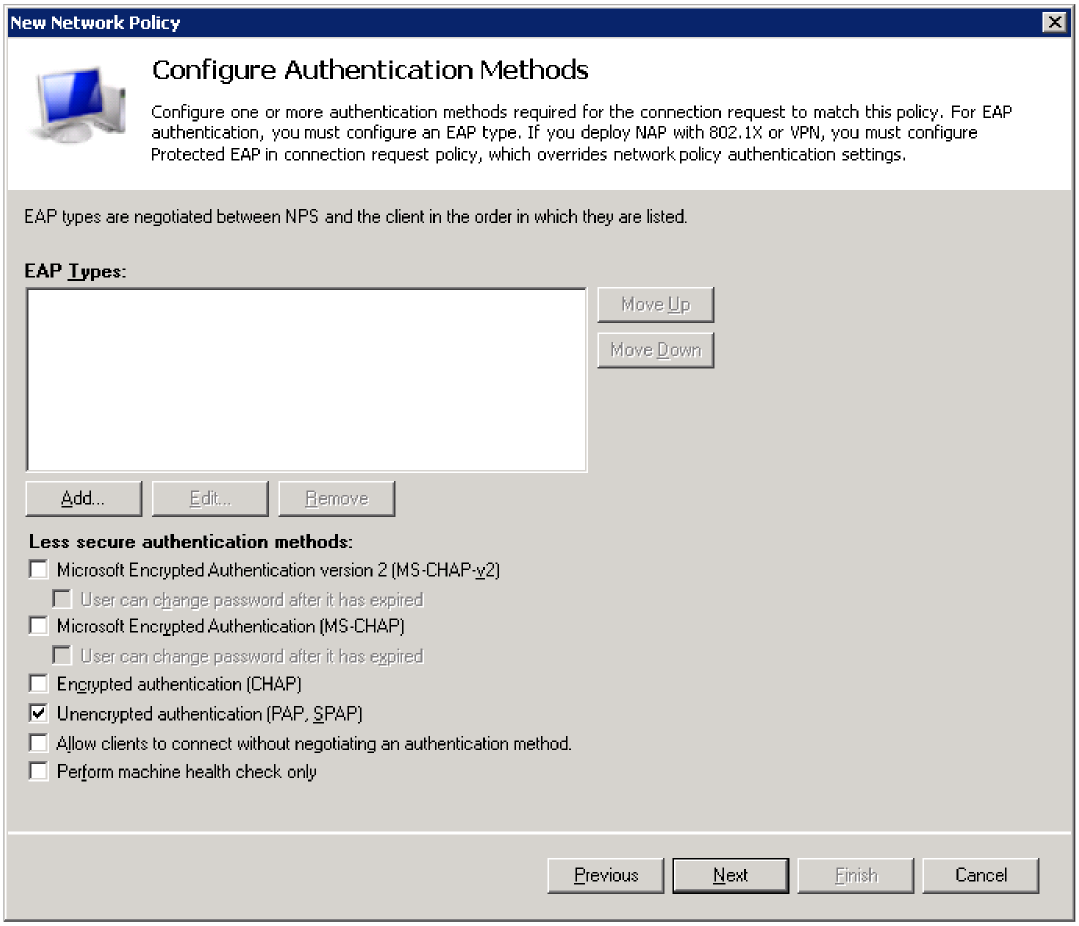
● Access granted
Grant access if client connection attempts match the conditions of this policy.

○ Access denied
Deny access if client connection attempts match the conditions of this policy.

□ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

14. Click **Next**.
15. In the Configure Authentication Methods window that appears, make sure only the **Unencrypted Authentication (PAP, SPAP)** option is selected.

Figure 311 *Create Network Policy – Configuring Authentication Methods*



Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Less secure authentication methods:

☐ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

☐ User can change password after it has expired

☐ Microsoft Encrypted Authentication (MS-CHAP)

☐ User can change password after it has expired

☐ Encrypted authentication (CHAP)

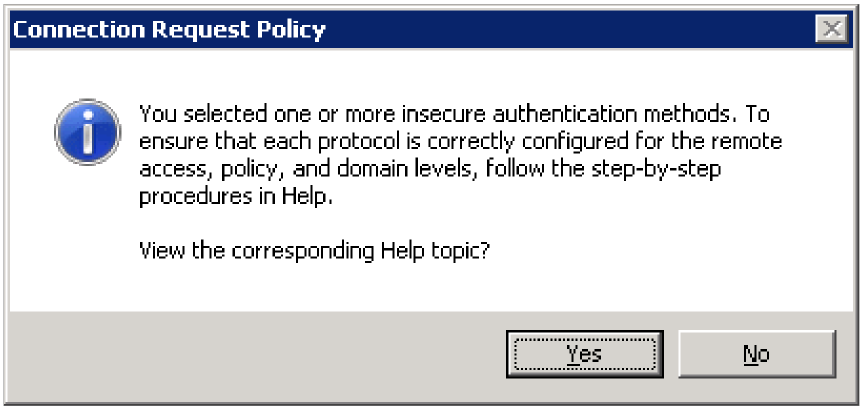
☑ Unencrypted authentication (PAP, SPAP)

☐ Allow clients to connect without negotiating an authentication method.

☐ Perform machine health check only

16. In the query window that appears, click **No**.

Figure 312 *Create Network Policy – Insecure Authentication Method Query*

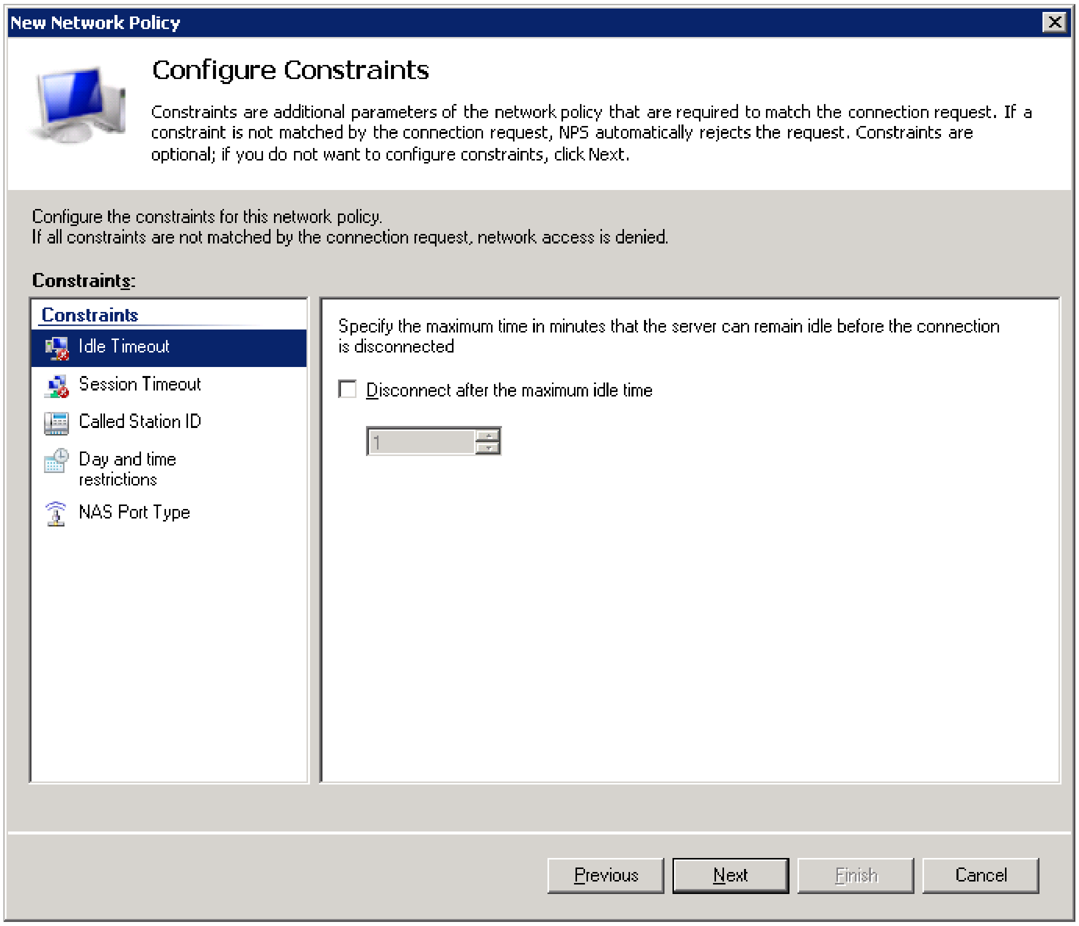


You selected one or more insecure authentication methods. To ensure that each protocol is correctly configured for the remote access, policy, and domain levels, follow the step-by-step procedures in Help.

View the corresponding Help topic?

17. In the Configure Constraints window that appears, click **Next**.

Figure 313 *Create Network Policy – Configuring Constraints*



New Network Policy

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

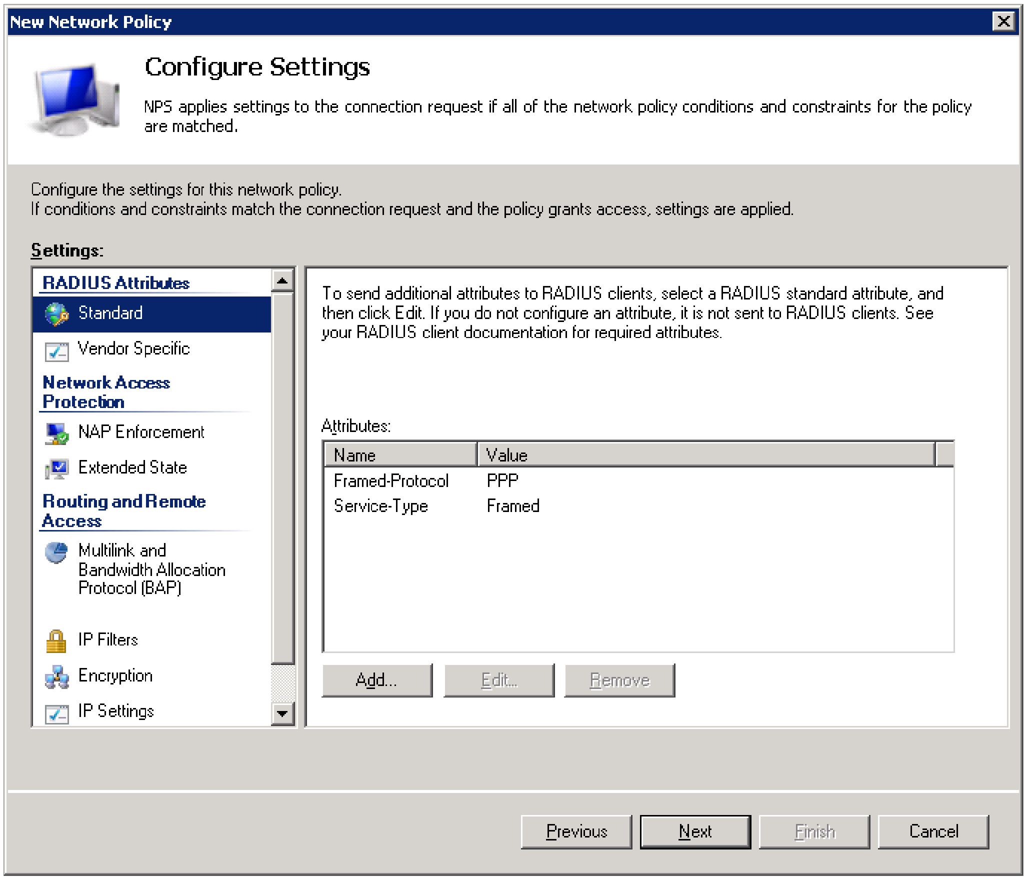
☐ Disconnect after the maximum idle time

1

18. In the Configure Settings window that appears:

- Remove all **Standard** RADIUS attributes. Make sure the Attributes table is empty.

Figure 314 *Create Network Policy – Configuring Settings*



New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

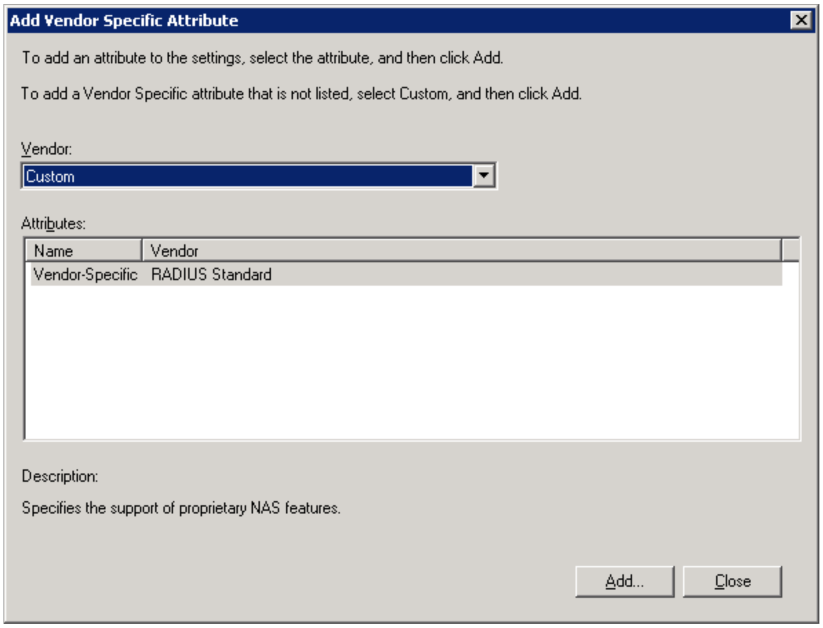
Name	Value
Framed-Protocol	PPP
Service-Type	Framed

- Select the **Vendor Specific** checkbox and click **Add** under the Attributes table.

19. In the Add Vendor Specific Attribute window that appears:

- Select **Custom** in the **Vendor** drop down field.
- Click **Add**.

Figure 315 *Create Network Policy – Adding Vendor Specific Attributes*



Add Vendor Specific Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.

Vendor: Custom

Attributes:

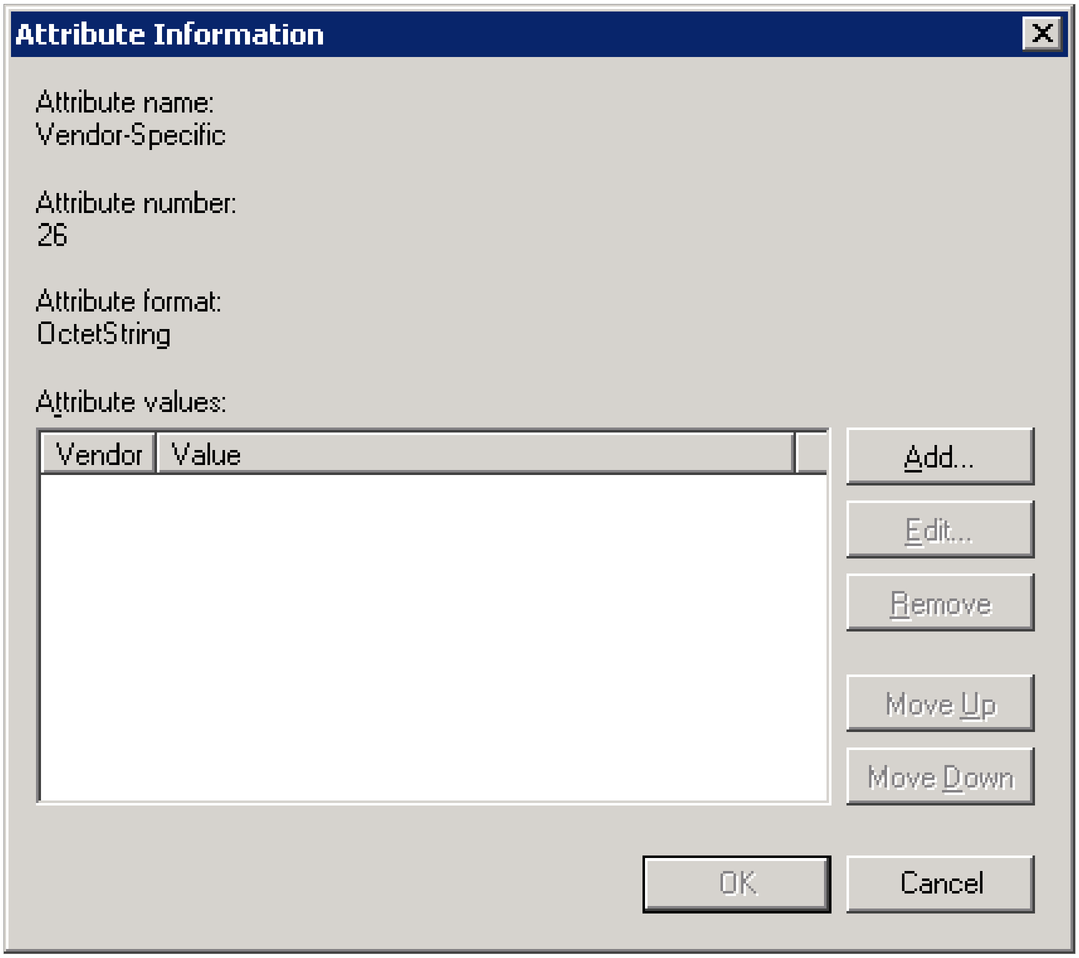
Name	Vendor
Vendor-Specific	RADIUS Standard

Description:

Specifies the support of proprietary NAS features.

20. In the Attribute Information window that appears, click **Add**.

Figure 316 *Create Network Policy – Selecting to Add Attribute Information*



Attribute Information

Attribute name:
Vendor-Specific

Attribute number:
26

Attribute format:
OctetString

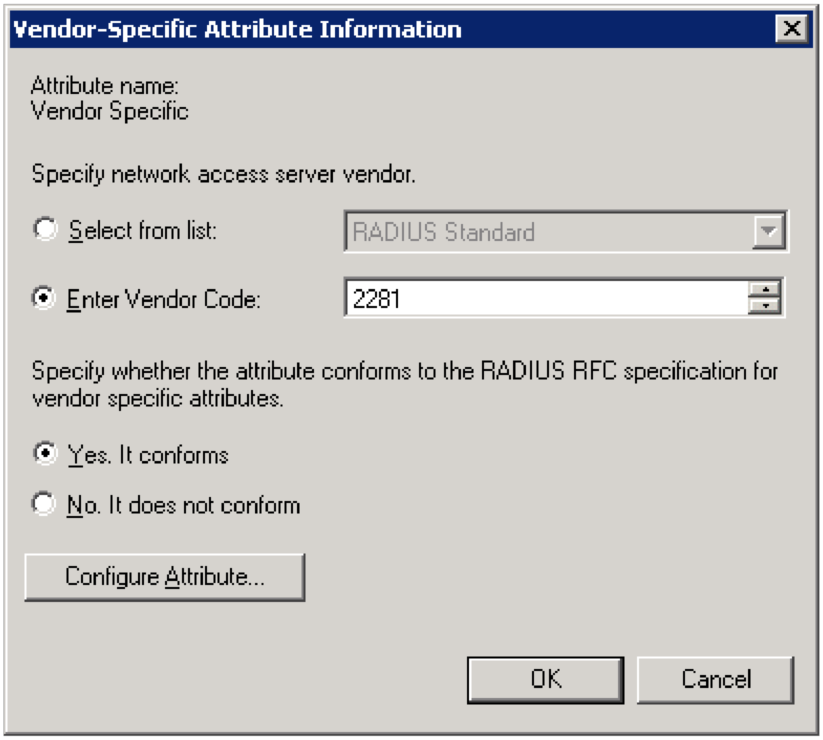
Attribute values:

Vendor	Value

21. In the Vendor-Specific Attribute Information window that appears:

- Select **Enter Vendor Code**.
- Enter **2281** in the **Enter Vendor Code** field.
- Select the option **Yes. It conforms**.
- Click **Configure Attribute**.

Figure 317 *Create Network Policy – Specifying the Vendor*


Vendor-Specific Attribute Information

Attribute name:
Vendor Specific

Specify network access server vendor.

○ Select from list: RADIUS Standard

● Enter Vendor Code: 2281

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

● Yes. It conforms

○ No. It does not conform

22. In the Configure VSA (RFC Compliant) window that appears, configure 13 attributes as follows:

    - 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:

      TDM is not relevant for PTP 850EX.

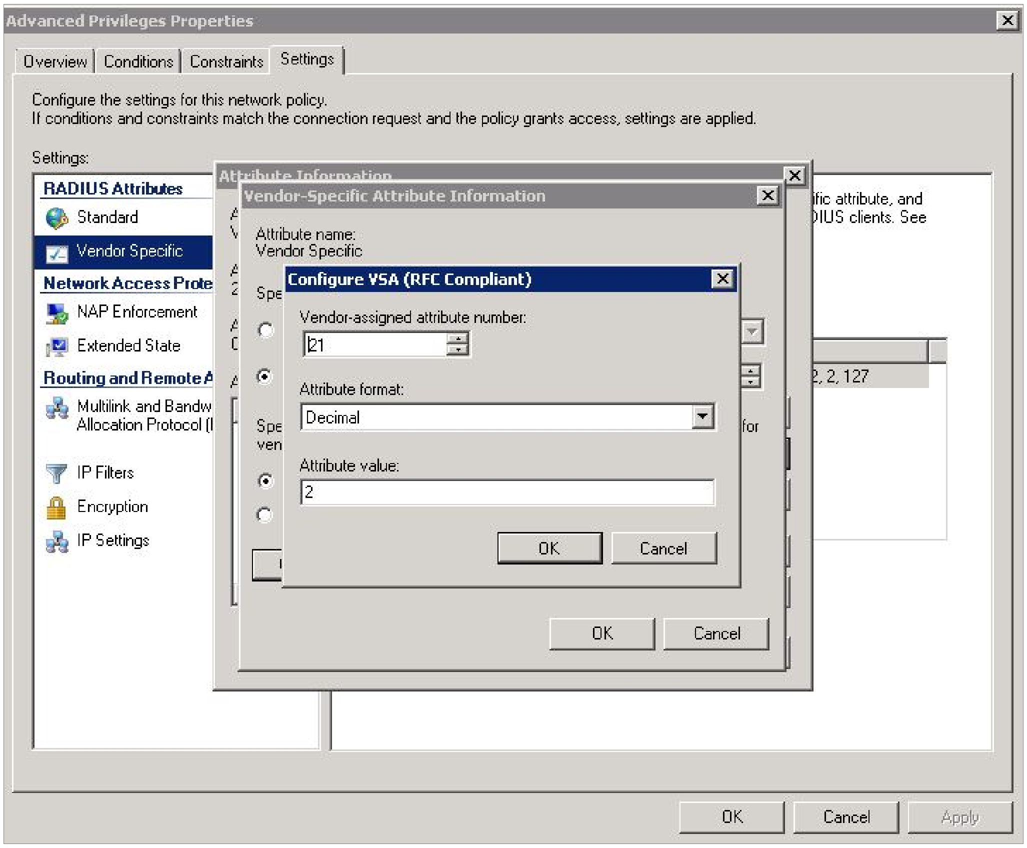
      2 = Advanced

      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 318 *Create Network Policy – Configuring Vendor-Specific Attribute Information*


Advanced Privileges Properties

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Vendor-Specific Attribute Information

Attribute name:
Vendor Specific

Configure VSA (RFC Compliant)

Vendor-assigned attribute number: 21

Attribute format: Decimal

Attribute value: 2

- 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

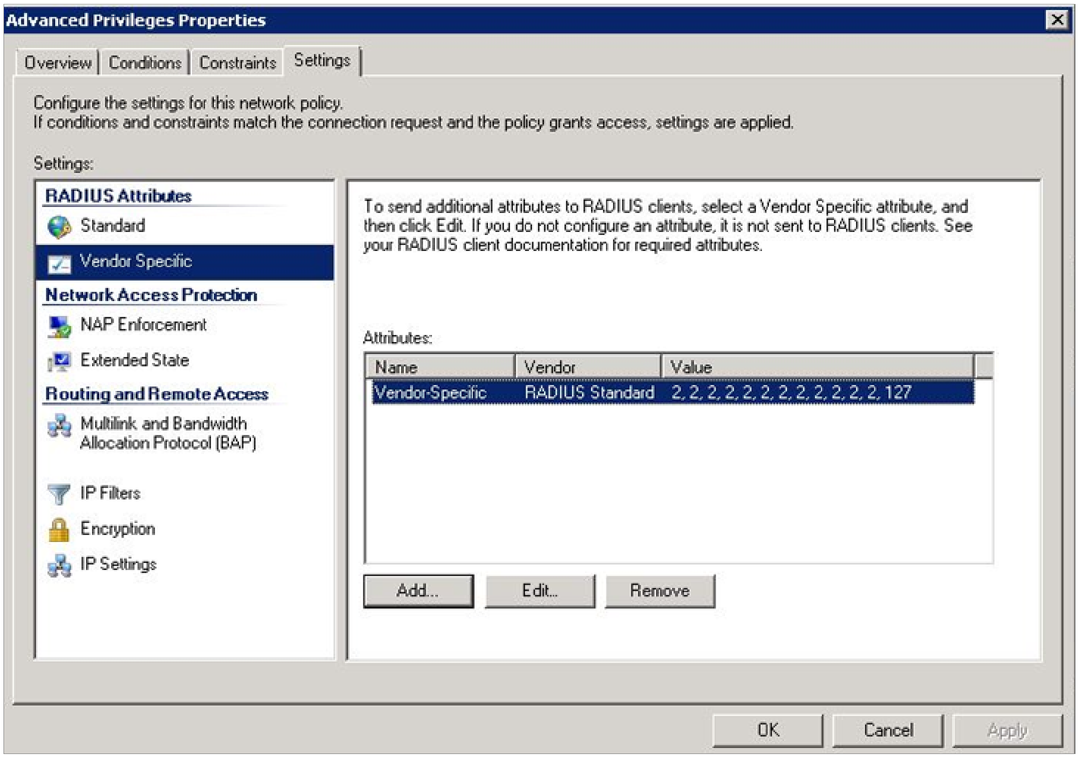
  Thus for example, enter **127** to allow access from all channels: Serial + Telnet + SSH + Web + NMS + SNMP +SNMPv3; Or enter **24** to allow access only from NMS + SNMP channels.

- 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 319 *Create Network Policy – Example of Vendor-Specific Attribute Configuration*



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
Vendor-Specific	RADIUS Standard	2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 127

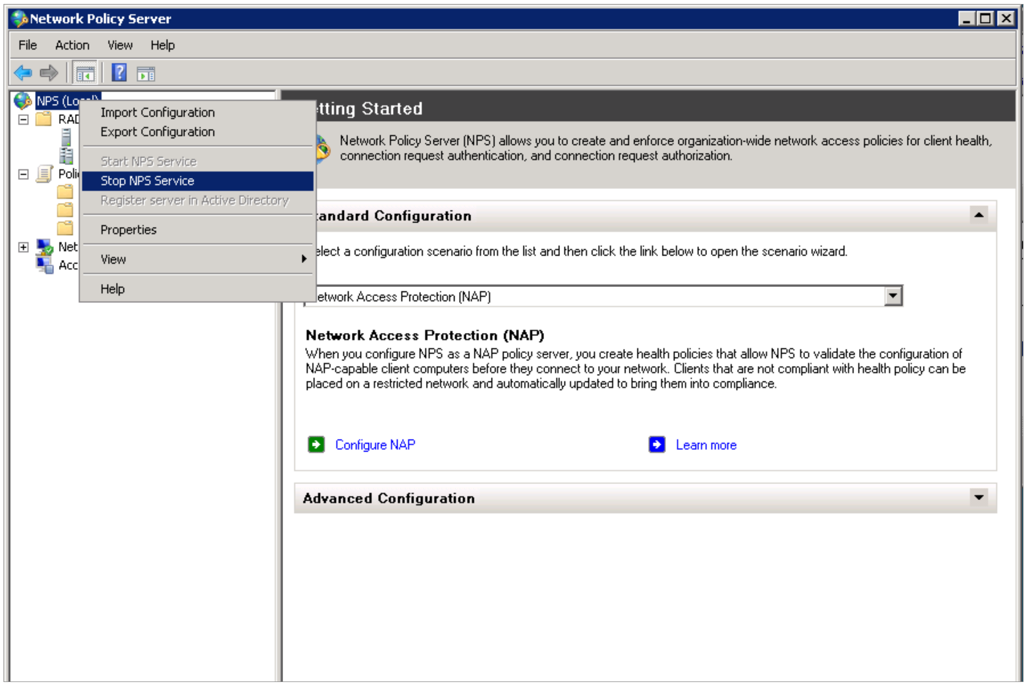
24. Close all opened windows and click **Next**.

25. In the Completing New Network Policy window, click **Finish**.

26. Reset the Network Policy Server (NPS) by stopping and starting the NPS service as follows:

    - Right click the **NPS (Local)** node, and select **Stop NPS Service**.
    - Right click the **NPS (Local)** node, and select **Start NPS Service**.

Figure 320 *Create Network Policy – Stopping/Starting NPS Services*



Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.

elect a configuration scenario from the list and then click the link below to open the scenario wizard.

When you configure NPS as a NAP policy server, you create health policies that allow NPS to validate the configuration of NAP-capable client computers before they connect to your network. Clients that are not compliant with health policy can be placed on a restricted network and automatically updated to bring them into compliance.

Configuring a Linux FreeRADIUS Server

The following sub-sections describe how to configure a Linux FreeRADIUS server to work with an PTP 850 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
```

2. 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 850 device with IP address 192.168.1.118:

      ```
      # IP50-EX
      client 192.168.1.118 {
        secret    = default_not_applicable
        shortname   = Cambium-PTP 850
      }
      ```

    - 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 (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 &

Configuring TACACS+

This section includes:

- TACACS+ Overview
- Activating TACACS+ Authentication and Authorization
- Configuring the TACACS+ Server Attributes
- Configuring a TACACS+ Server

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.

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.

Activating TACACS+ Authentication and Authorization

Before activating TACACS+, make sure to configure the TACACS+ servers and the TACACS+ server attributes. See:

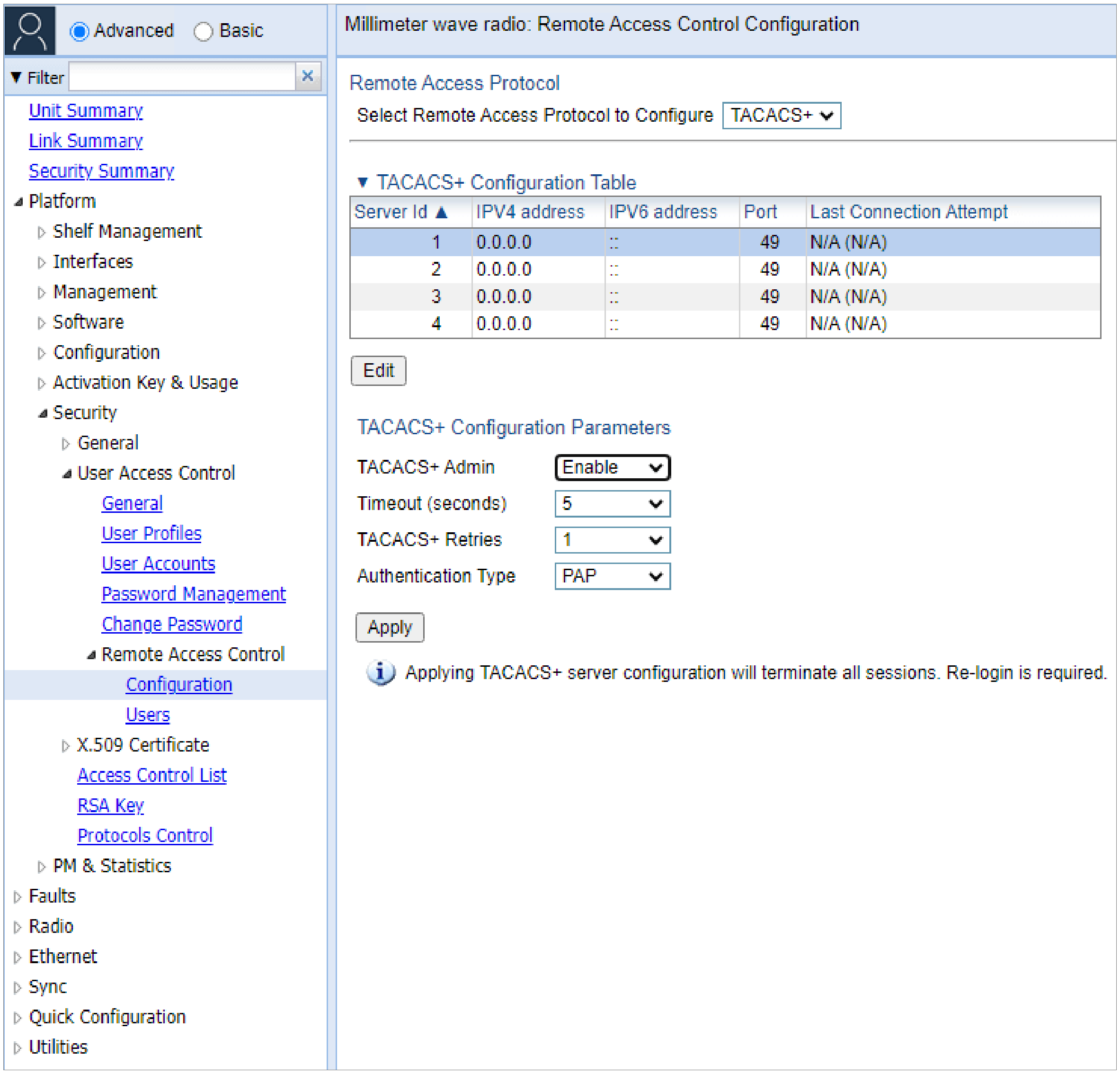
- Configuring the TACACS+ Server Attributes
- Configuring a TACACS+ Server

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 321 *Remote Access Control Configuration Page (TACACS+)*



Millimeter wave radio: Remote Access Control Configuration

Remote Access Protocol

Select Remote Access Protocol to Configure: TACACS+

TACACS+ Configuration Table

Server Id ▲	IPV4 address	IPV6 address	Port	Last Connection Attempt
1	0.0.0.0	::	49	N/A (N/A)
2	0.0.0.0	::	49	N/A (N/A)
3	0.0.0.0	::	49	N/A (N/A)
4	0.0.0.0	::	49	N/A (N/A)

TACACS+ Configuration Parameters

TACACS+ Admin	Enable
Timeout (seconds)	5
TACACS+ Retries	1
Authentication Type	PAP

Applying TACACS+ server configuration will terminate all sessions. Re-login is required.

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**.

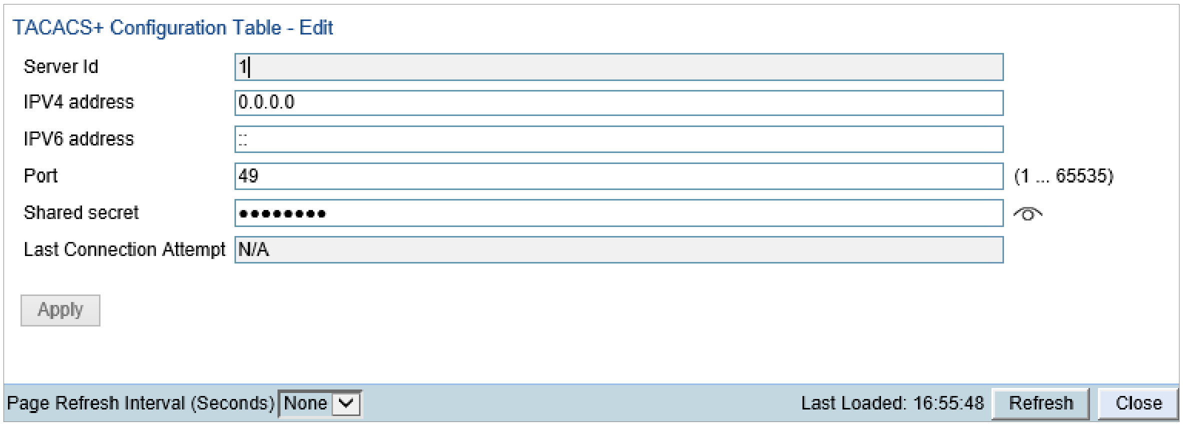
> **Note**
>
> When the Protocol is changed, all active sessions are terminated when you click **Apply**. Users must log in again via TACACS+.

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 (Remote Access Control Configuration Page (TACACS+)).
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 322 *TACACS+ Configuration – Edit Page*



TACACS+ Configuration Table - Edit

Server Id	1	
IPV4 address	0.0.0.0	
IPV6 address	::	
Port	49	(1 ... 65535)
Shared secret	●●●●●●●●●	
Last Connection Attempt	N/A	

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.

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

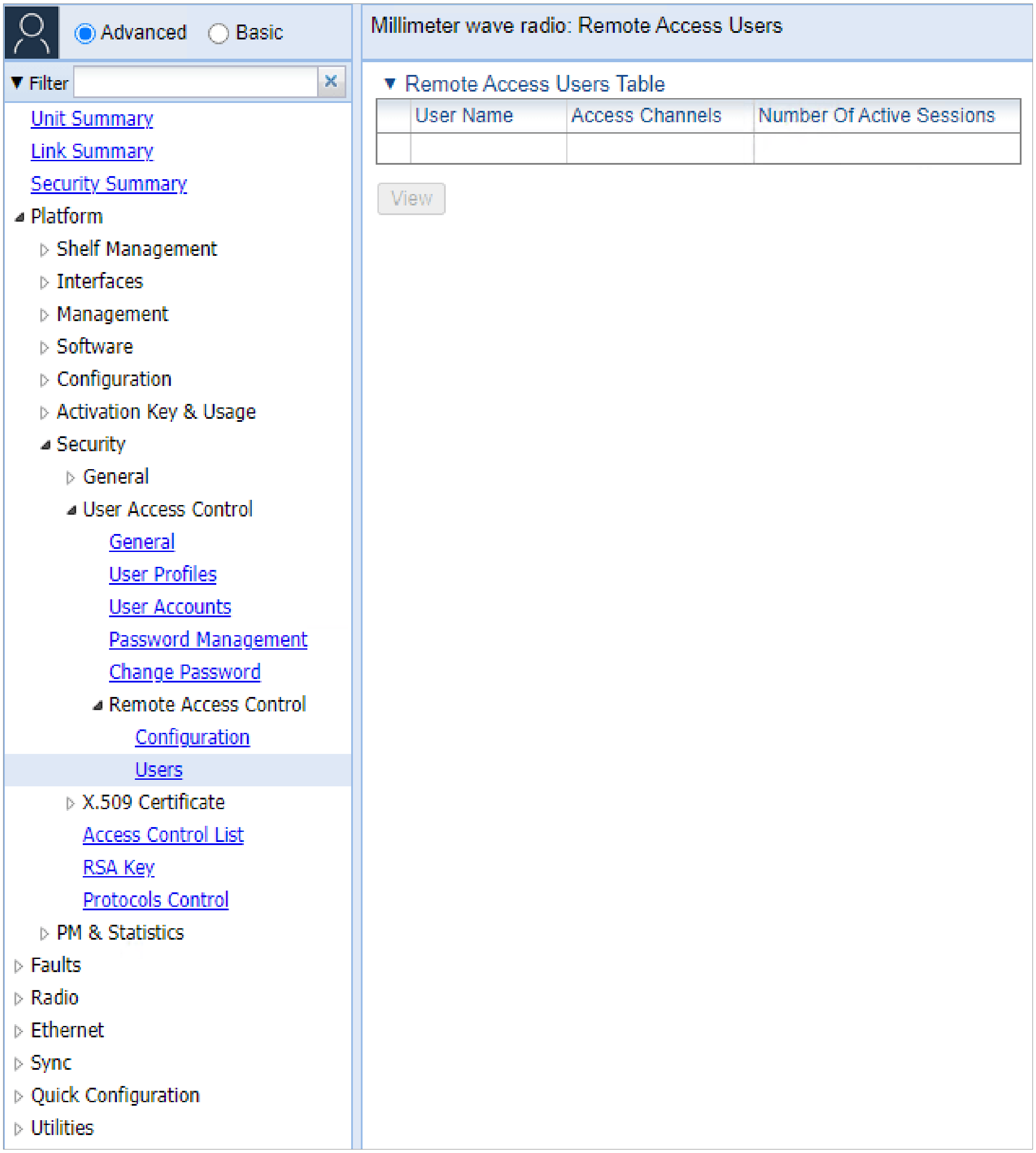
Viewing Remote Access User Connectivity and Permissions

You can view remote access user connectivity and permissions information for all RADIUS or TACACS+ users currently connected.

To view remote access users:

1. Select **Platform** > **Security** > **User Access Control** > **Remote Access Control** > **Users**. The Remote Access Users page opens.

Figure 323 *Remote Access Users Page*



Millimeter wave radio: Remote Access Users

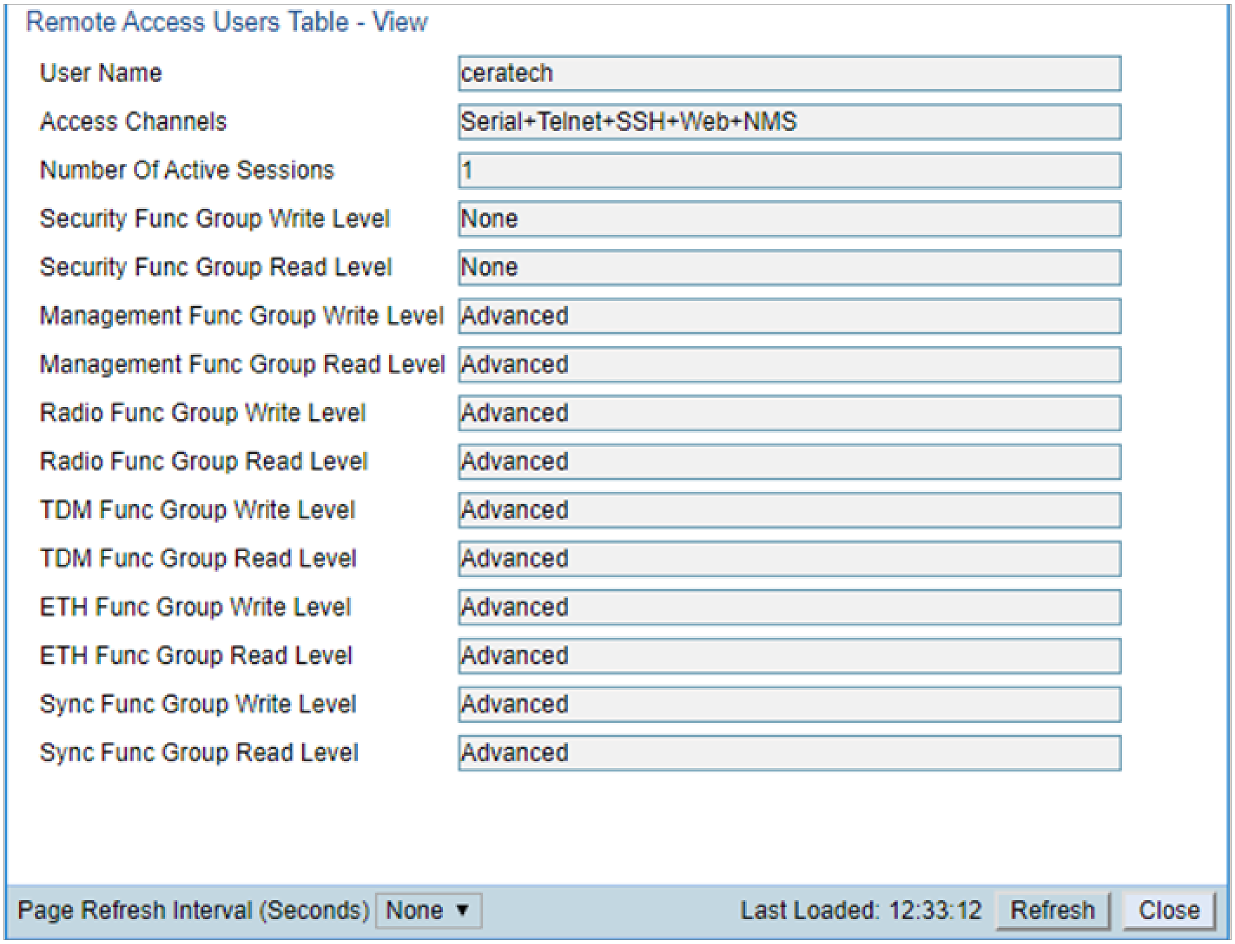
Remote Access Users Table

	User Name	Access Channels	Number Of Active Sessions

- 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 324 *Remote Access Users Table - View*



Remote Access Users Table - View

User Name	ceratech
Access Channels	Serial+Telnet+SSH+Web+NMS
Number Of Active Sessions	1
Security Func Group Write Level	None
Security Func Group Read Level	None
Management Func Group Write Level	Advanced
Management Func Group Read Level	Advanced
Radio Func Group Write Level	Advanced
Radio Func Group Read Level	Advanced
TDM Func Group Write Level	Advanced
TDM Func Group Read Level	Advanced
ETH Func Group Write Level	Advanced
ETH Func Group Read Level	Advanced
Sync Func Group Write Level	Advanced
Sync Func Group Read Level	Advanced

Page Refresh Interval (Seconds) None ▼

Last Loaded: 12:33:12

For each of the six functional groups (**Security, Management, Radio, TDM, Eth, Sync**), the page displays the Read access level (**None, Normal**, or **Advanced**), and the Write access level (**None, Normal**, or **Advanced**).

Note

TDM is not relevant for PTP 850EX.

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. See Enabling HTTPS.

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.

Generating a Certificate Signing Request (CSR) File

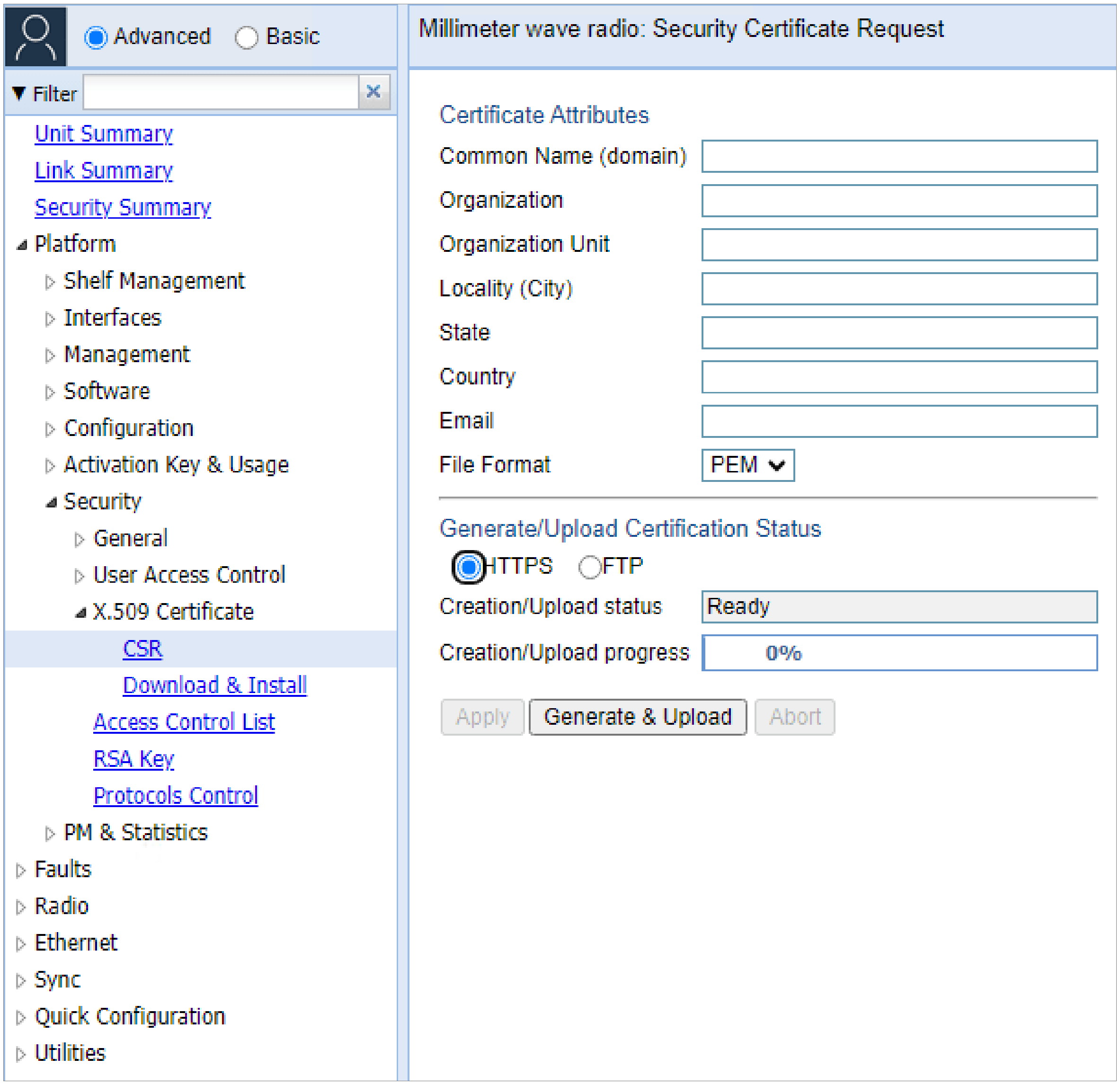
Note

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 325 *Security Certificate Request Page*



Millimeter wave radio: Security Certificate Request

Certificate Attributes

Common Name (domain)	
Organization	
Organization Unit	
Locality (City)	
State	
Country	
Email	
File Format	PEM

Generate/Upload Certification Status

● HTTPS ○ FTP

Creation/Upload status	Ready
Creation/Upload progress	0%

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.

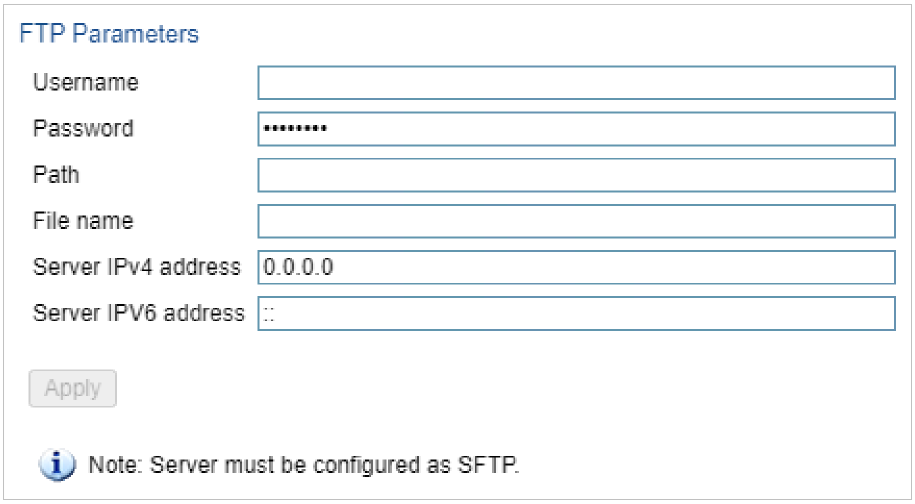
7. In the **Country** field, enter the two-letter ISO abbreviation for your country (e.g., US).

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 PEM or DER to determine the file format.

> **Note**
>
> In this version, only PEM is supported.

10. Click **Apply** to save your settings.
11. In the **Generate/Upload Certification Status**, select either **HTTPS** or **FTP**.
12. If you selected **FTP**:
    a. Click **FTP Parameters** to display the FTP Parameters page.

    Figure 326 *FTP Parameters Page (Security Certificate Request)*

    FTP Parameters

Username	
Password	••••••••
Path	
File name	
Server IPv4 address	0.0.0.0
Server IPV6 address	::

    Note: Server must be configured as SFTP.

    b. In the **Username** field, enter the user name you configured in the SFTP server.

    c. 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.

    d. 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 "//".

    e. In the **File Name** field, enter the name you want to give to the exported CSR.

    f. 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.

    g. 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.

    h. Click **Apply**, then **Close**, to save the FTP parameters and return to the Security Log Upload page.

13. Click **Generate & Upload**. The file is generated and uploaded.

The **Creation/Upload 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.

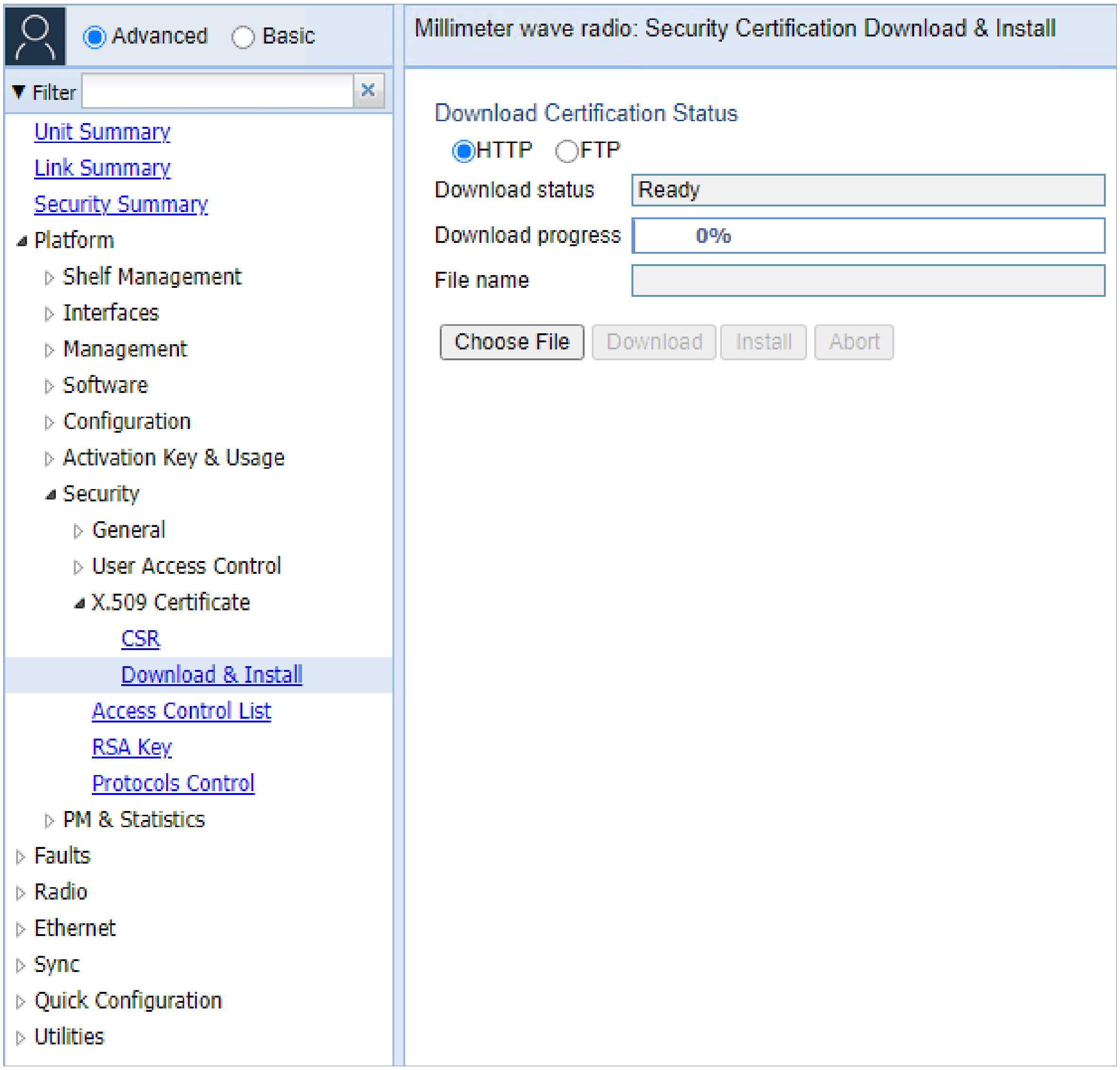
The **Creation/Upload progress** field displays the progress of any current CSR upload operation.

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 327 *Security Certification Download and Install Page*



Millimeter wave radio: Security Certification Download & Install

● Advanced ○ Basic

Download Certification Status

● HTTP ○ FTP

Download status: Ready

Download progress: 0%

File name:

2. If you selected **FTP,** click **FTP Parameters** to display the FTP Parameters page and configure the FTP parameters. See Step Generating a Certificate Signing Request (CSR) File.
3. Click **Download**. The certificate is downloaded.
4. Click **Install**. The certificate is installed on the PTP 850.

Enabling HTTPS

By default, HTTP is used by PTP 850 as its web interface protocol.

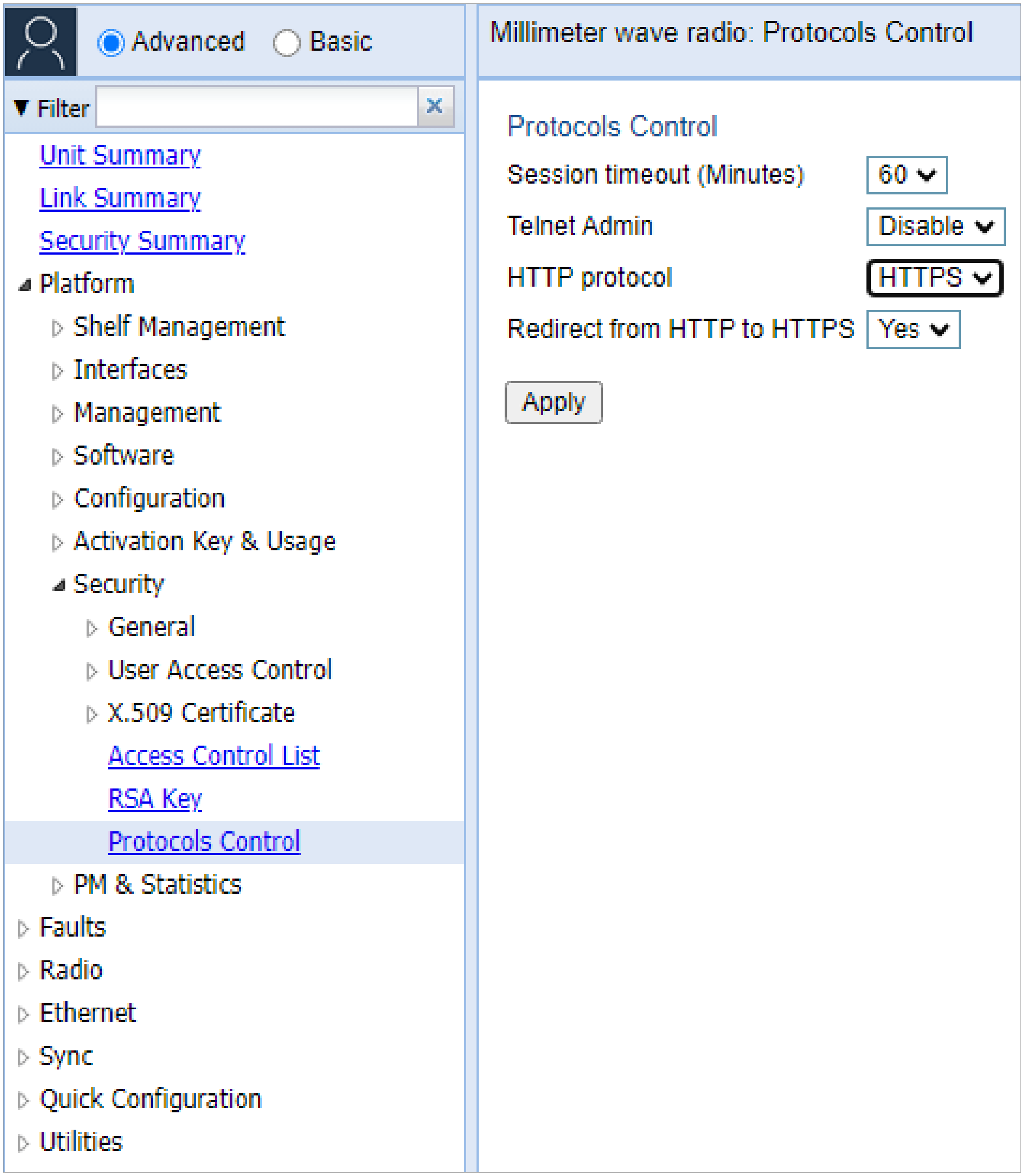
To enable HTTPS instead of HTTP:

1. Select **Platform** > **Security** > **Protocols Control**. The Protocols Control page opens (Protocols Control Page).

2. In the **HTTP protocol** field, select **HTTPS**. An additional field is displayed, the **Redirect from HTTP to HTTPS** field.
3. In the **Redirect from HTTP to HTTPS** field, select No to block Port 80 and redirect traffic to Port 443 or **Yes** if you do not want to block Port 80.

> **Note**
>
> Port 80 is the dedicated port for HTTP, and Port 443 is the dedicated port for HTTPS.

Figure 328 *Protocols Control Page – HTTPS Selected*



● Advanced ○ Basic

Millimeter wave radio: Protocols Control

Protocols Control

Session timeout (Minutes): 60

Telnet Admin: Disable

HTTP protocol: HTTPS

Redirect from HTTP to HTTPS: Yes

4. Click **Apply**. You will be required to login again after changing the protocol or changing the **Redirect from HTTP to HTTPS** setting.

Note

Make sure you have installed a valid certificate in the device before changing the web interface protocol to HTTPS. Failure to do this may prevent users from accessing the Web EMS.

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.

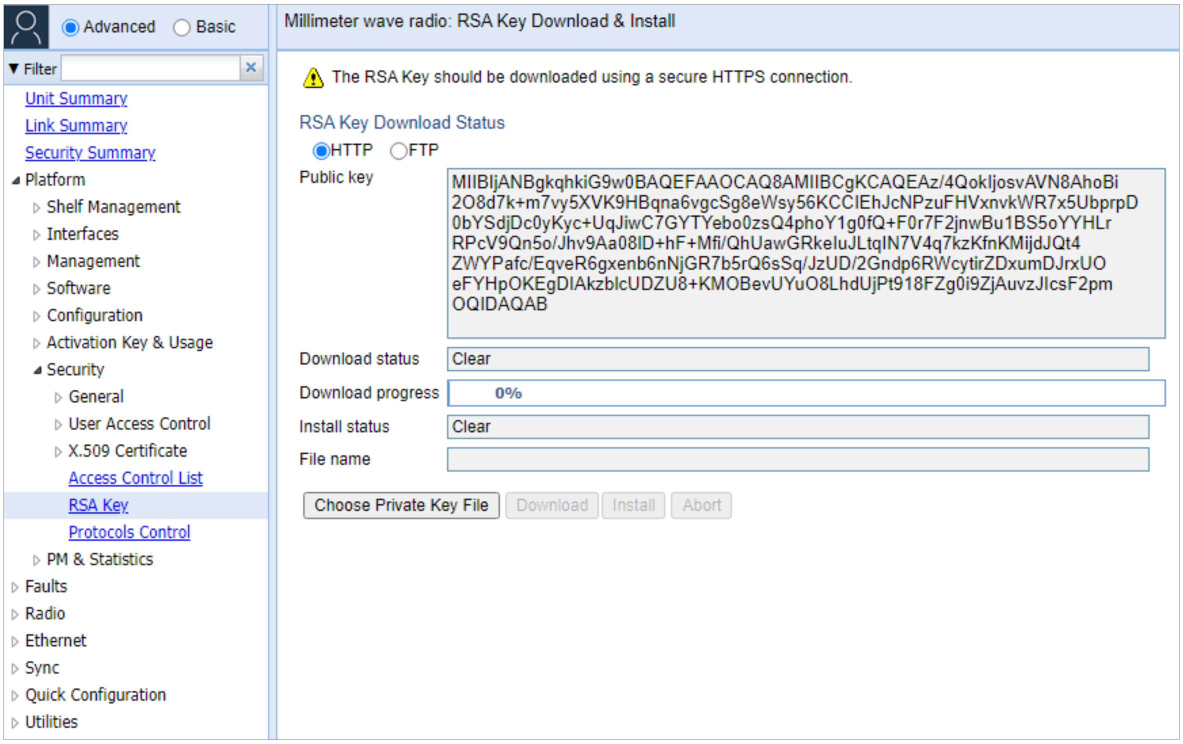
The following is an example of a valid RSA private key file:

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC+7jRmt27yF4xDh5Pc8w4ikvXUu32BI
0eOyELmeUBnEeIHbCOXD3upi8+ZnH51Q+8hzgoSqXgEYFgZMoF/sXCrO2yf62UJ5ohj3zadhx/7585zoG
wHtYz1S62hsa4+cdAl/i1Vbc6CoUBh5642XYje+Q+q1XJtObed884eaQcXUFLlBipYKvVx2kuelymansE91WJ
U+UjFlc3aiQG8qsSgW5Ar6wet0pXkP2Vdemo//QAXXjcTqqMBuizrlhlcvi+OKYFl9kSh21ZqSgjvK3cfAssCJ
BIY5d6t6bVkX9p2gjo/IPnErjAv7W6lZoemotb5KAeSHeR1sYTw17/xIpM7AgMBAAECggEAAwliLKQMOq4k
h/UXD/OPAlPDXyp1jjaTw8dBm811OG5wttzXGrxJ+OIFX5Rn79DbHnbayCiJL8tMe2dx5yhY+hA247roX3ua
0w57cuPxnp21izc+S0fC7H/TTM1jpRCbATparuTRMlitinZshJGA73Lsod3v36GEXxm/6dHnz/drCs2F4NdHW
pjMAAG/1CiBwut8jNkJUwa78Ivk3JF+XRoZ0txN2mIybQxxzjuNXqZbNO6H3Ua2u1iYyD+McfgOWCCUfSns
tGRhFg0OsQuqj6d74qKVQWaukEH91SVZHEoqX6DgpKy4INZBxORZmlTNmadwNhw5O7rvFxZ205u4gQ
KBgQDT5bXvc0Ok+Ypm2xnIbu2GFjxNYwYhR3TvHPy14NIO5Q9I/uDqwrSL1igzalr6EbZyLu8cDXa4aybrz
CyBfPeG89Qq+a6J3JR/RwJndLyjV4h5CT8Zy4O/wjgTrP3Rhq7LAbWgLjSaraflgruHTcnOifhkK7MK7Fr+xi2
IJfOKQQKBgQDmq1eYNzlMPlATESlsfbkcL49jSsu70kYg0g5Iol6+bVPo9K7mopICtWC/fwdNlUAfO+vr/231
YUfSo7YNEDNNRoT/NwvqqtAYxZaIUdIQxhMywF9jjYBBuq6+f/7+dwDfNBtMb2q7hceTdk6yZ8/MehCkvS
wOBmP+lq0FwTmmewKBgQClxmj31G1ve+rTXUZmkKIy7OJwiLAbCRRqnXr3r9Om43151i2QfJNTc1AwKVz
Tl1ftLNrUT5Q541qnzyxigaoFYmzy0jPCl1d128/9sE6EW87hImLDg3ynYQMOIaDRc1T8bXHyxzNQb9t+U+Dy
keD4POifNbD1MsRd3h1xDn/iAQKBgHmKpukJkCNgYgjp7g3AYR084izLaHZa4aDBjc0v4QQtzxzccJwN5S
mQMJ42bL6wecz7YeBEAshcrd+La42Oj7mUAtgHRTwtLOEgm6TQmANGmy8OtjRahs4bc5/lCZNDWS5C
4m9v9alBYFuO5wCSOqffWY20L9Zj/6RR+HEj0yCpAoGAHwrbRqPVZtZptFuNsCq130dtmqI7HFQAlqrc5D
wP7YSsznE6biHfLUw891xu0vmevALrCaoeOMaidugohgiorSJO4qk7I3XN3pUJhPYqbhtdCVnBI2Fm9pr3V
/SHGvrl1NW92cXObeQ2UEBiKPOyQKfOBlbac707u0HqaTu+/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 329 *RSA Key Download & Install Page (HTTP Selected)*



Millimeter wave radio: RSA Key Download & Install

The RSA Key should be downloaded using a secure HTTPS connection.

RSA Key Download Status

● HTTP ○ FTP

Public key

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAz/4QokljosvAVN8AhoBi
2O8d7k+m7vy5XVK9HBqna6vgcSg8eWsy56KCClEhJcNPzuFHVxnvkWR7x5UbprpD
0bYSdjDc0yKyc+UqJiwC7GYTYebo0zsQ4phoY1g0fQ+F0r7F2jnwBu1BS5oYYHLr
RPcV9Qn5o/Jhv9Aa08ID+hF+Mfi/QhUawGRkeluJLtqIN7V4q7kzKfnKMijdJQt4
ZWYPafc/EqveR6gxenb6nNjGR7b5rQ6sSq/JzUD/2Gndp6RWcytirZDxumDJrxUO
eFYHpOKEgDIAkzblcUDZU8+KMOBevUYuO8LhdUjPt918FZg0i9ZjAuvzJIcsF2pm
OQIDAQAB
```

Download status: Clear

Download progress: 0%

Install status: Clear

File name:

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.

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. See RSA File Download & Install Status Parameters.
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. See RSA File Download & Install Status Parameters.

> **Note**
>
> To discontinue the download process, click Abort.

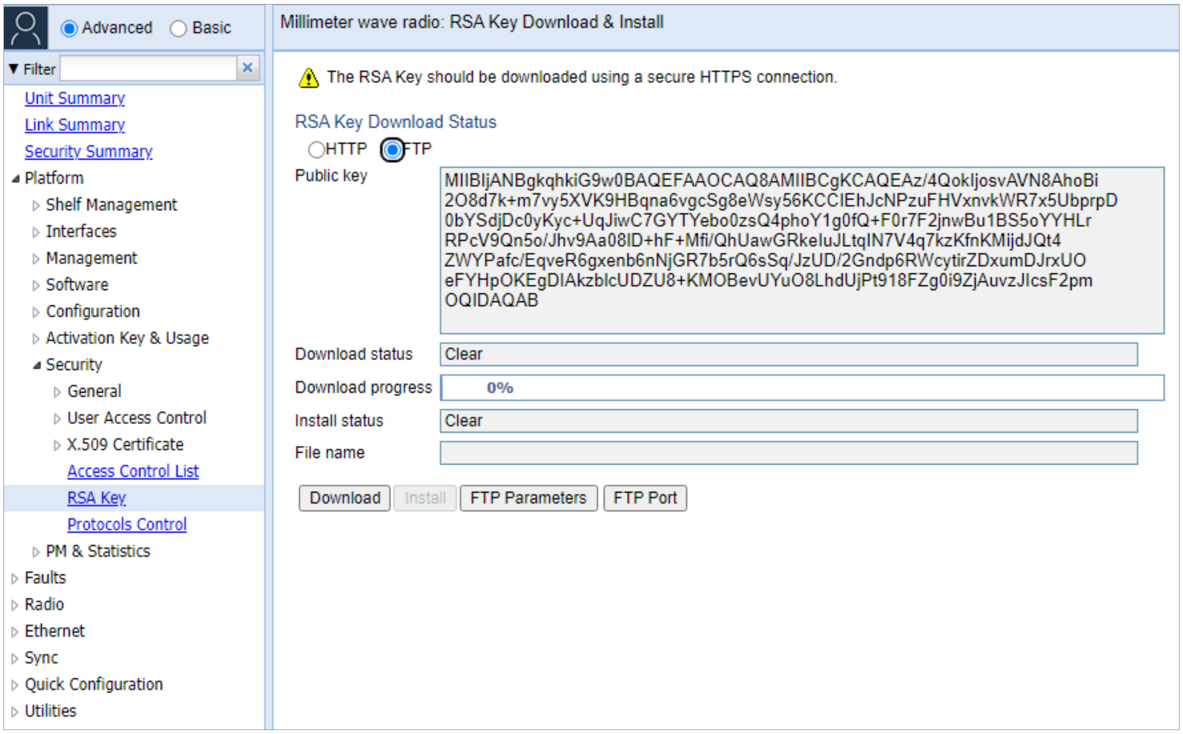
Downloading an RSA Key via SFTP

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 330 *RSA Key Download & Install Page (FTP Selected)*



Millimeter wave radio: RSA Key Download & Install

The RSA Key should be downloaded using a secure HTTPS connection.

RSA Key Download Status

○ HTTP ● FTP

Public key

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAz/4QokIjosvAVN8AhoBi
2O8d7k+m7vy5XVK9HBqna6vgcSg8eWsy56KCCIEhJcNPzuFHVxnvkWR7x5UbprpD
0bYSdjDc0yKyc+UqJiwC7GYTYebo0zsQ4phoY1g0fQ+F0r7F2jnwBu1BS5oYYHLr
RPcV9Qn5o/Jhv9Aa08ID+hF+Mfi/QhUawGRkeluJLtqIN7V4q7kzKfnKMijdJQt4
ZWYPafc/EqveR6gxenb6nNjGR7b5rQ6sSq/JzUD/2Gndp6RWcytirZDxumDJrxUO
eFYHpOKEgDIAkzblcUDZU8+KMOBevUYuO8LhdUjPt918FZg0i9ZjAuvzJIcsF2pm
OQIDAQAB
```

Download status: Clear

Download progress: 0%

Install status: Clear

File name:

3. Click **FTP Parameters** to display the FTP Parameters page and configure the FTP parameters. See Step Generating a Certificate Signing Request (CSR) File.

4. Click **Download**. The download begins. You can view the status of the download in the **Download Status** field. See RSA File Download & Install Status Parameters.

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. See RSA File Download & Install Status Parameters.

Note

To discontinue the download process, click Abort.

Table 80 *RSA File Download & Install Status Parameters*

Parameter	Definition
Download Status	The status of any pending RSA file download. Possible values are: • **Ready** – The default value, which appears when no download is in progress. • **In Progress** – The download is in progress.

Parameter	Definition
	- **Aborted** – 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: - **Success** – File downloaded and verified successfully. - **Failed** – File 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: - **Success** - **Failed**

Enabling Telnet Access

You can enable or disable telnet access to the unit. By default, telnet access is disabled.

To enable or disable telnet access:

1. Select **Platform** > **Security** > **Protocols Control**. The Protocols Control page opens (Protocols Control Page).
2. In the **Telnet Admin** field, select **Enable** to enable telnet access or **Disable** to disable telnet access. By default, telnet access is disabled (**Disable**).
3. Click **Apply**.

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.

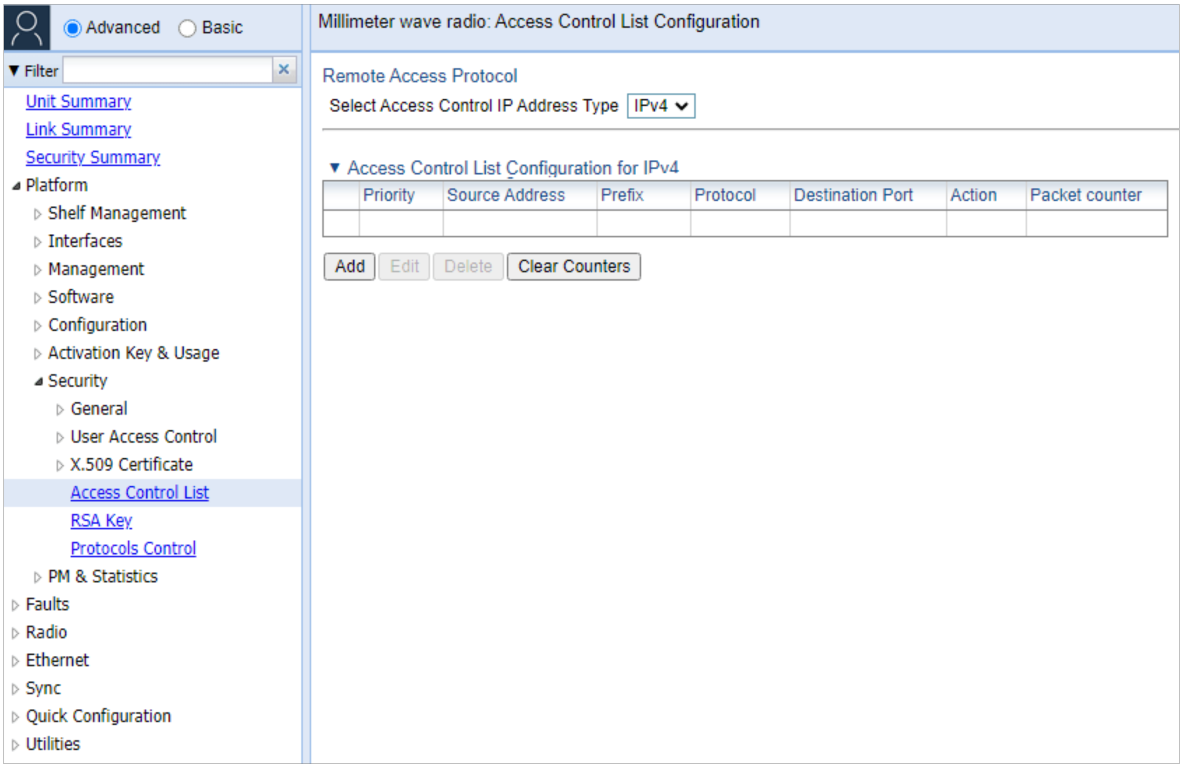
For example, to allow only packets from subnet 192.168.1/24 to ingress the management interface, you must configure the following rules:

- 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 331 *Access Control List Configuration Page*



Millimeter wave radio: Access Control List Configuration

Remote Access Protocol

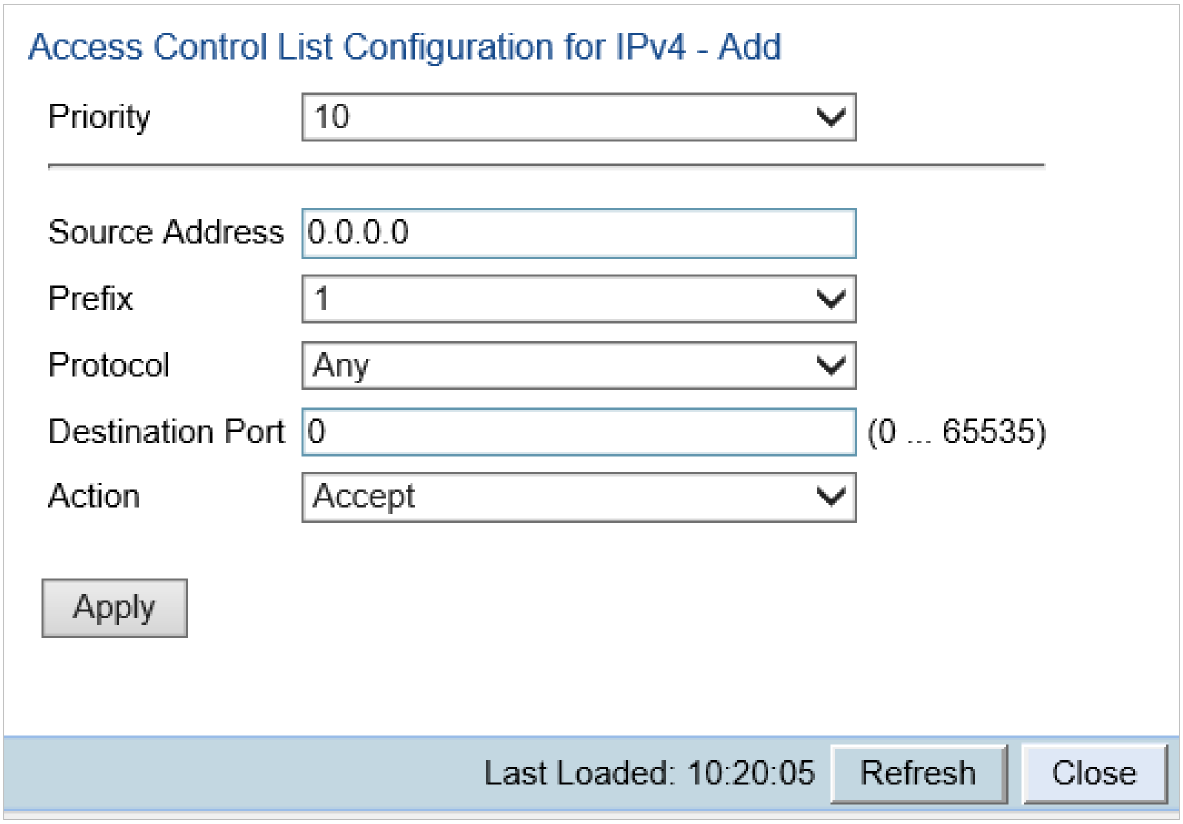
Select Access Control IP Address Type: IPv4

▼ Access Control List Configuration for IPv4

	Priority	Source Address	Prefix	Protocol	Destination Port	Action	Packet counter

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.

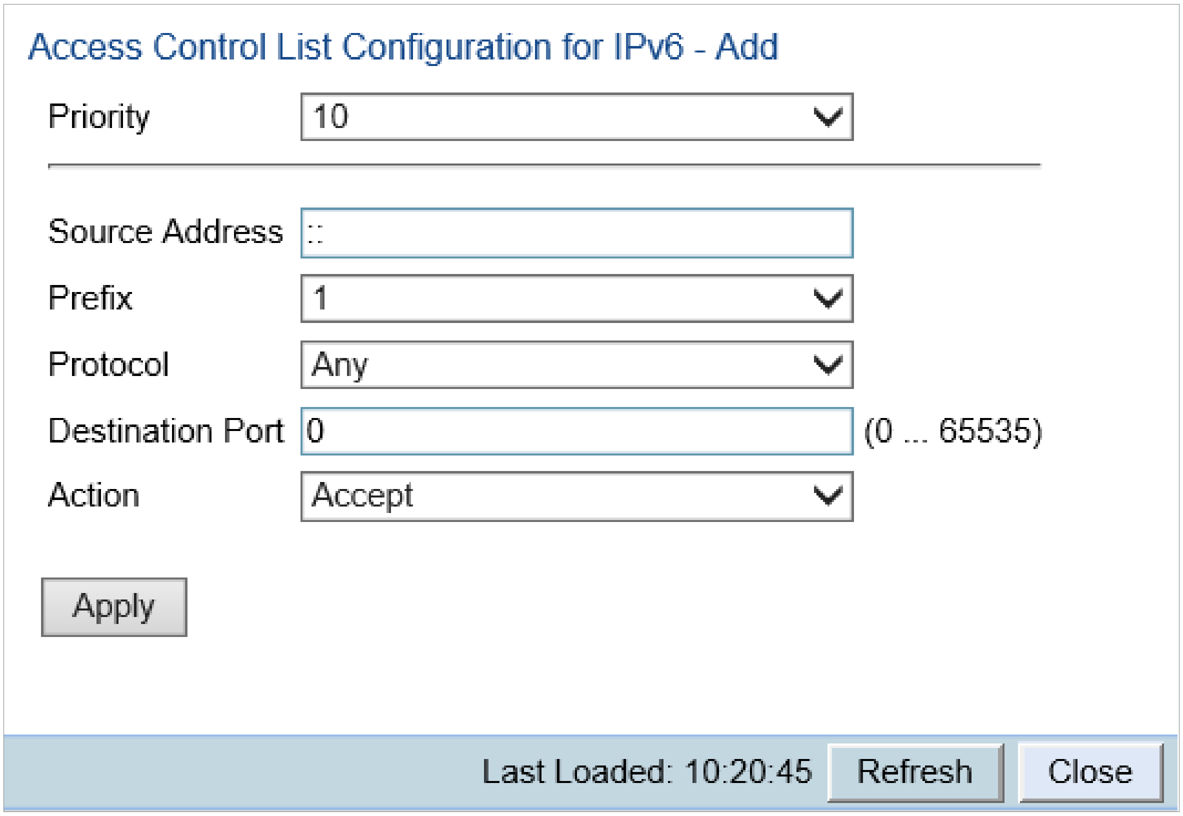
Figure 332 *Access Control List Configuration for IPv4 - Add*



Access Control List Configuration for IPv4 - Add

Priority	10
Source Address	0.0.0.0
Prefix	1
Protocol	Any
Destination Port	0 (0 ... 65535)
Action	Accept

Figure 333 *Access Control List Configuration for IPv6 - Add*



Access Control List Configuration for IPv6 - Add

Priority	10
Source Address	::
Prefix	1
Protocol	Any
Destination Port	0 (0 ... 65535)
Action	Accept

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**

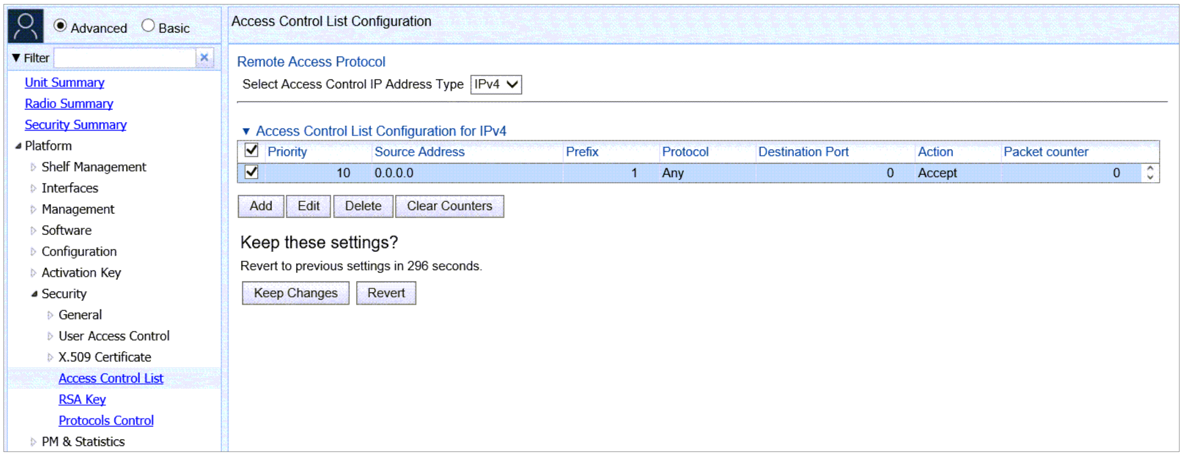
- **UDP**
- **ICMP (for IPv6, this appears as ICMPv6)**

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 Access Control List Configuration Page – Failsafe Timer. 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.

    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 334 *Access Control List Configuration Page – Failsafe Timer*



Access Control List Configuration

Remote Access Protocol

Select Access Control IP Address Type: IPv4

▼ Access Control List Configuration for IPv4

☑	Priority	Source Address	Prefix	Protocol	Destination Port	Action	Packet counter
☑	10	0.0.0.0	1	Any	0	Accept	0

Keep these settings?

Revert to previous settings in 296 seconds.

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.

Uploading the Security Log

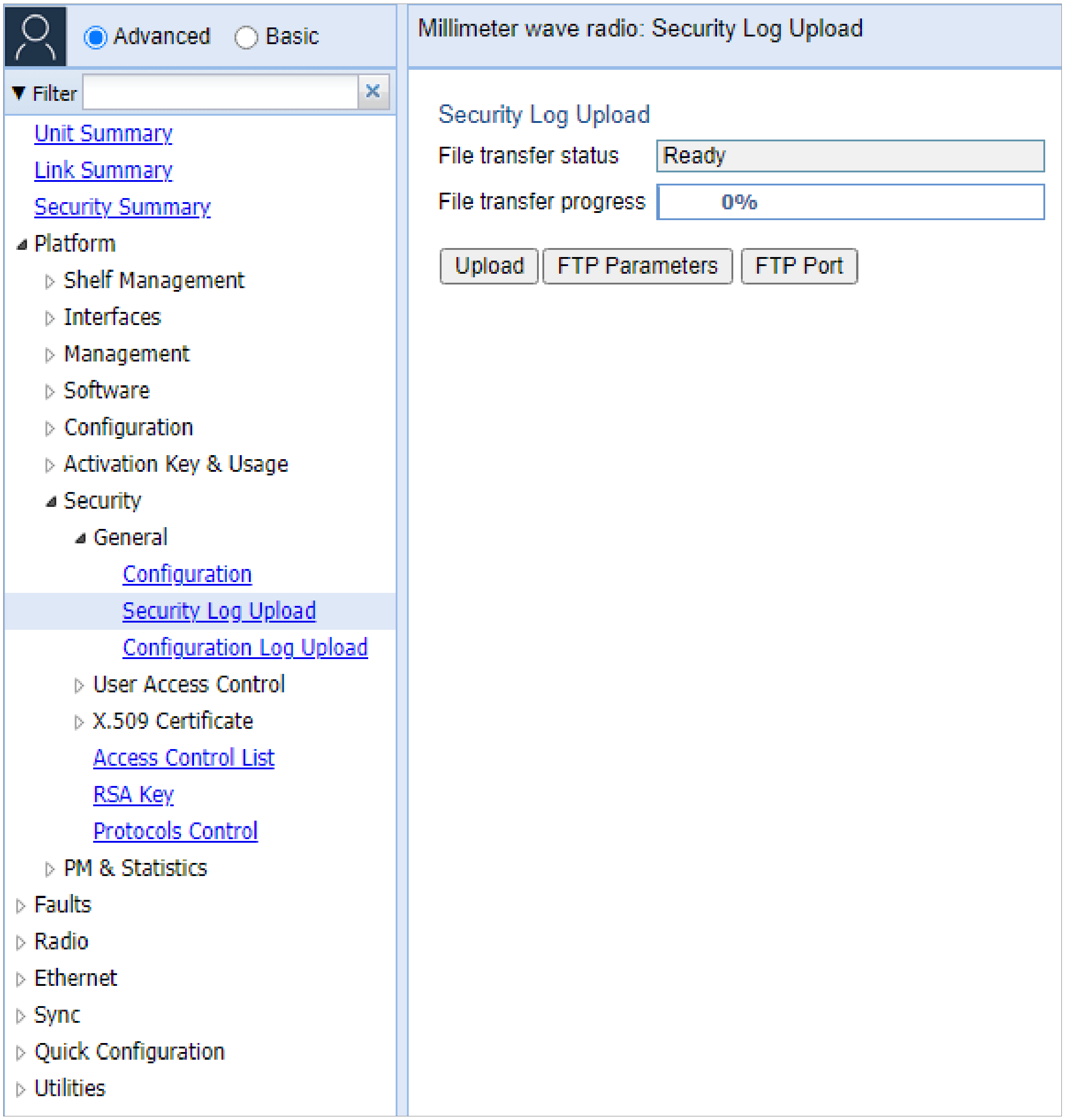
The security log is an internal system file which records all changes performed to any security feature, as well as all security related events.

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 335 *Security Log Upload Page*



Millimeter wave radio: Security Log Upload

Security Log Upload

File transfer status: Ready

File transfer progress: 0%

3. Click **FTP Parameters** to display the FTP Parameters page and configure the FTP parameters. See Step Generating a Certificate Signing Request (CSR) File

4. Click **Upload**. The upload begins.

The **File transfer 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.

Uploading the Configuration Log

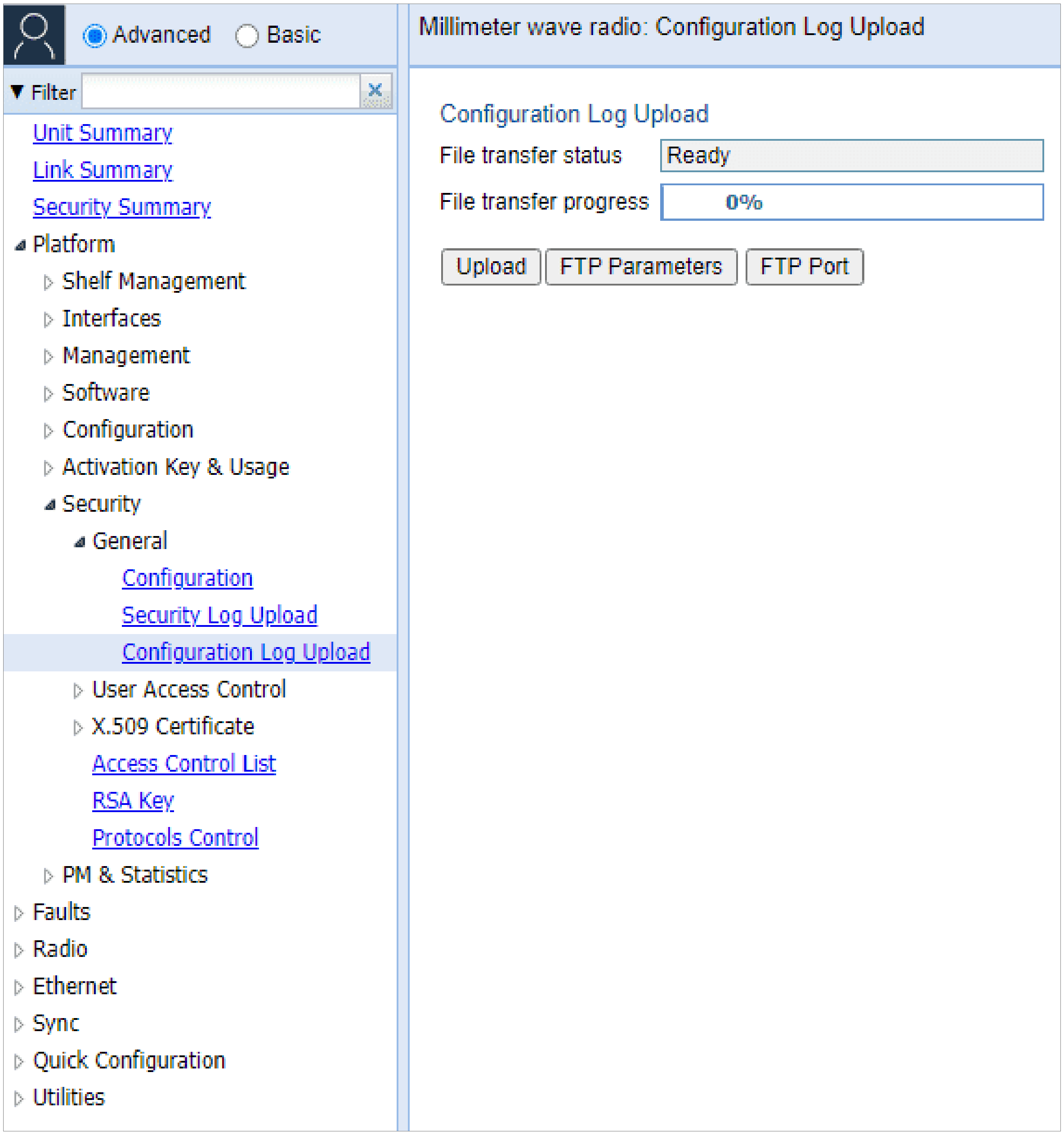
The configuration log lists actions performed by users to configure the system. This file is mostly used for security, to identify suspicious user actions. It can also be used for troubleshooting.

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 336 *Configuration Log Upload Page*



Millimeter wave radio: Configuration Log Upload

Configuration Log Upload

File transfer status: Ready

File transfer progress: 0%

3. Click **FTP Parameters** to display the FTP Parameters page and configure the FTP parameters. See Step Generating a Certificate Signing Request (CSR) File.

4. Click **Upload**. The upload begins.

The **File transfer 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.

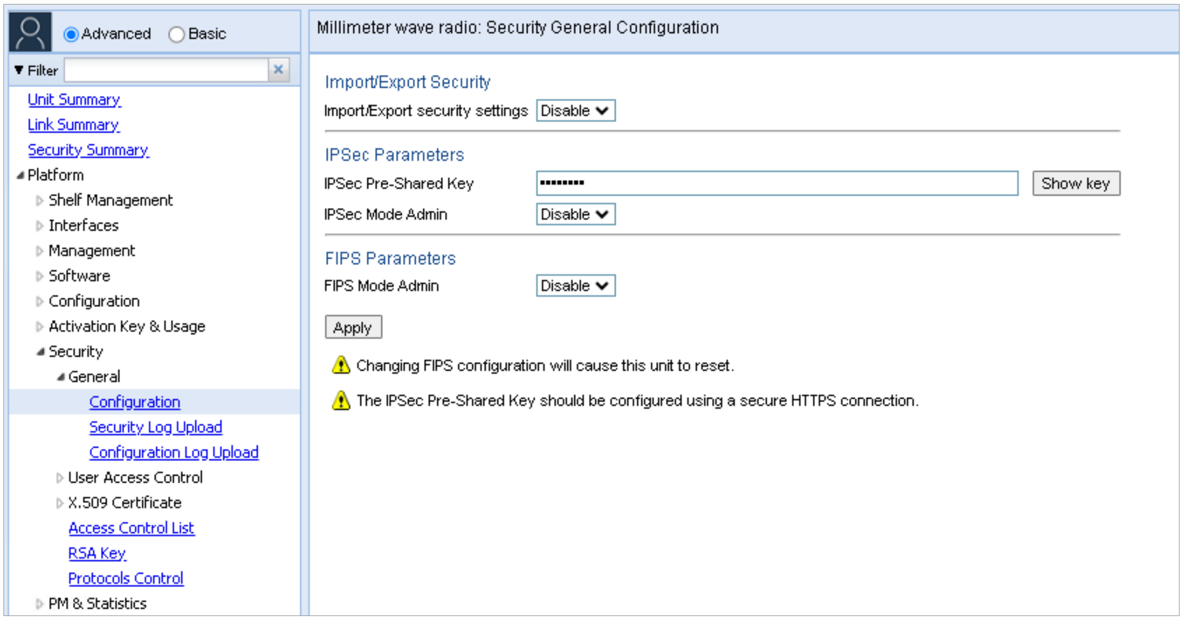
Importing and Exporting Security Settings

To determine whether security configurations are included in configuration backup files:

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

> **Note**
>
> This page is only available in Advanced mode.

Figure 337 *Security General Configuration Page*



Millimeter wave radio: Security General Configuration

Import/Export Security

Import/Export security settings: Disable

IPSec Parameters

IPSec Pre-Shared Key: ••••••••• Show key

IPSec Mode Admin: Disable

FIPS Parameters

FIPS Mode Admin: Disable

Apply

⚠ Changing FIPS configuration will cause this unit to reset.

⚠ The IPSec Pre-Shared Key should be configured using a secure HTTPS connection.

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.
3. Click **Apply**.

> Note
>
> The IPSec Parameters and FIPS parameters are not relevant to these products in the current System Release version. The **IPSec Mode Admin** and **FIPS Mode Admin** fields should be left at their default settings of **Disable**.

Note:

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. See Working in CW Mode (Single or Dual Tone) (CLI).

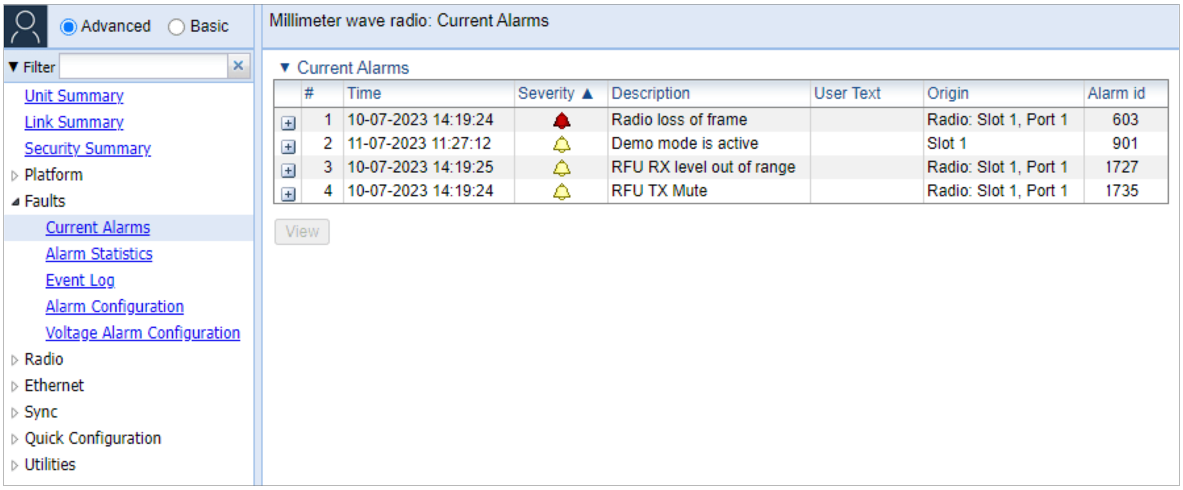
You can configure a wait time of up to 120 seconds after an alarm is cleared in the system before the alarm is actually reported as being cleared. This prevents traps flooding the NMS in the event that some external condition causes the alarm to be raised and cleared continuously. The timeout for trap generation can be configured via CLI. See Configuring a Timeout for Trap Generation (CLI).

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 Alarm Information.

Figure 338 *Current Alarms Page Example*



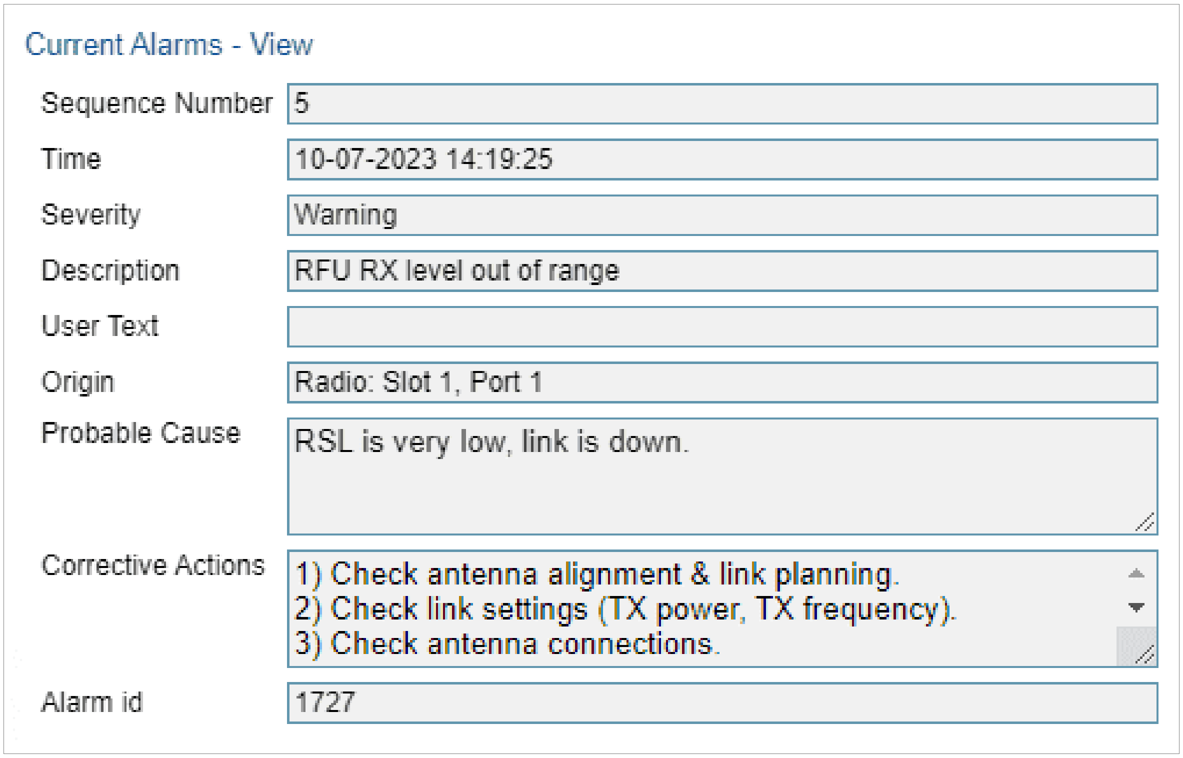
Millimeter wave radio: Current Alarms

Current Alarms

	#	Time	Severity ▲	Description	User Text	Origin	Alarm id
⊞	1	10-07-2023 14:19:24	▲	Radio loss of frame		Radio: Slot 1, Port 1	603
⊞	2	11-07-2023 11:27:12	△	Demo mode is active		Slot 1	901
⊞	3	10-07-2023 14:19:25	△	RFU RX level out of range		Radio: Slot 1, Port 1	1727
⊞	4	10-07-2023 14:19:24	△	RFU TX Mute		Radio: Slot 1, Port 1	1735

2. To view more detailed information about an alarm, click + at the beginning of the row or select the alarm and click **View**.

Figure 339 *Current Alarms - View Page*



Current Alarms - View

Sequence Number	5
Time	10-07-2023 14:19:25
Severity	Warning
Description	RFU RX level out of range
User Text	
Origin	Radio: Slot 1, Port 1
Probable Cause	RSL is very low, link is down.
Corrective Actions	1) Check antenna alignment & link planning. 2) Check link settings (TX power, TX frequency). 3) Check antenna connections.
Alarm id	1727

Table 81 *Alarm Information*

Parameter	Definition
Sequence Number (#)	A unique sequence number assigned to the alarm by the system.

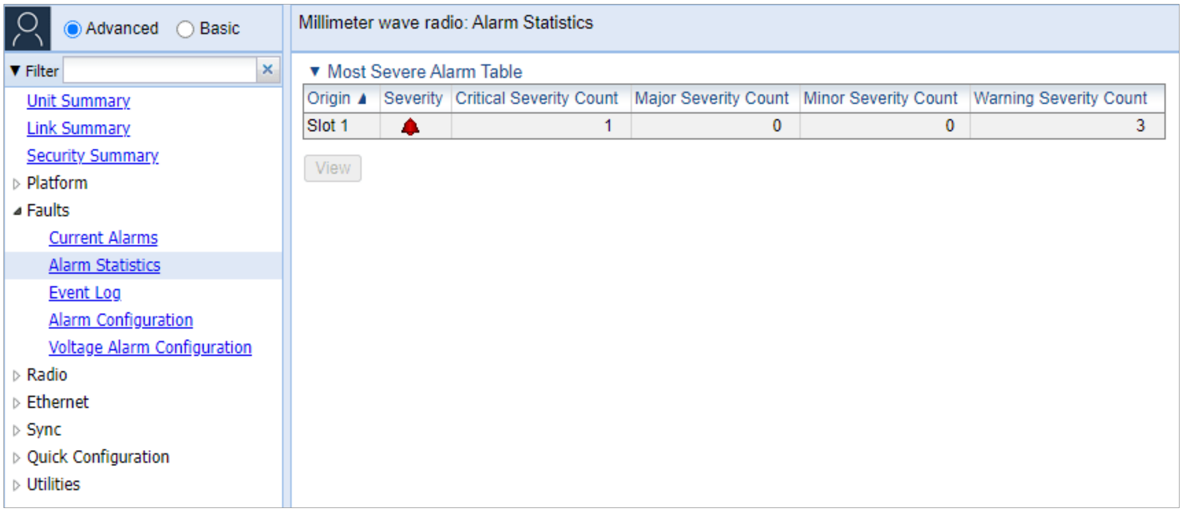
Parameter	Definition
Time	The date and time the alarm was triggered.
Severity	The severity of the alarm. In the Current Alarms table, the severity is indicated by a symbol. You can display a textual description of the severity by holding the cursor over the symbol. **Note:** You can edit the severity of alarm types in the Alarm Configuration page. See Editing Alarm Text and Severity and Disabling Alarms and Events.
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. See Editing Alarm Text and Severity and Disabling Alarms and Events
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.

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 340 *Alarm Statistics Page*



Millimeter wave radio: Alarm Statistics

▼ Most Severe Alarm Table

Origin ▲	Severity	Critical Severity Count	Major Severity Count	Minor Severity Count	Warning Severity Count
Slot 1	🔔	1	0	0	3

The Alarm Statistics page displays the number of current alarms per severity level for each module, interface, and virtual interface in the unit. Only modules and interfaces for which one or more alarms are currently raised are listed in the Alarm Statistics page.

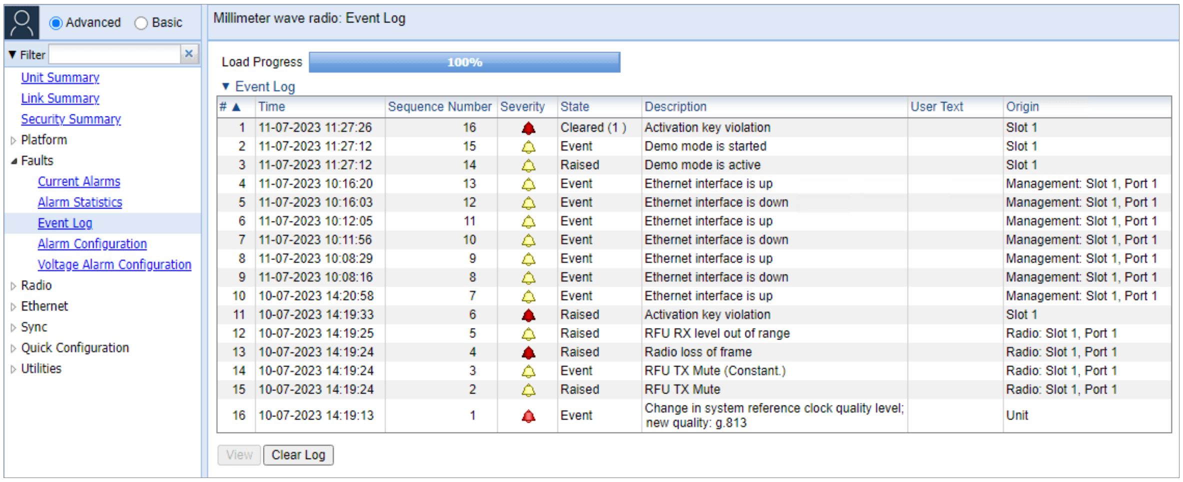
Viewing and Saving the Event Log

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 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 341 *Event Log*



Millimeter wave radio: Event Log

Load Progress 100%

▼ Event Log

# ▲	Time	Sequence Number	Severity	State	Description	User Text	Origin
1	11-07-2023 11:27:26	16	▲	Cleared (1)	Activation key violation		Slot 1
2	11-07-2023 11:27:12	15	△	Event	Demo mode is started		Slot 1
3	11-07-2023 11:27:12	14	△	Raised	Demo mode is active		Slot 1
4	11-07-2023 10:16:20	13	△	Event	Ethernet interface is up		Management: Slot 1, Port 1
5	11-07-2023 10:16:03	12	△	Event	Ethernet interface is down		Management: Slot 1, Port 1
6	11-07-2023 10:12:05	11	△	Event	Ethernet interface is up		Management: Slot 1, Port 1
7	11-07-2023 10:11:56	10	△	Event	Ethernet interface is down		Management: Slot 1, Port 1
8	11-07-2023 10:08:29	9	△	Event	Ethernet interface is up		Management: Slot 1, Port 1
9	11-07-2023 10:08:16	8	△	Event	Ethernet interface is down		Management: Slot 1, Port 1
10	10-07-2023 14:20:58	7	△	Event	Ethernet interface is up		Management: Slot 1, Port 1
11	10-07-2023 14:19:33	6	▲	Raised	Activation key violation		Slot 1
12	10-07-2023 14:19:25	5	△	Raised	RFU RX level out of range		Radio: Slot 1, Port 1
13	10-07-2023 14:19:24	4	▲	Raised	Radio loss of frame		Radio: Slot 1, Port 1
14	10-07-2023 14:19:24	3	△	Event	RFU TX Mute (Constant.)		Radio: Slot 1, Port 1
15	10-07-2023 14:19:24	2	△	Raised	RFU TX Mute		Radio: Slot 1, Port 1
16	10-07-2023 14:19:13	1	▲	Event	Change in system reference clock quality level; new quality: g.813		Unit

View   Clear Log

Note

Because it can contain up to 5,000 rows, the Event Log is loaded in chunks. The Load Progress bar at the top of the page indicates the percentage of rows that have been displayed. You can scroll through the results even before all the rows have been displayed. Clicking Refresh at the bottom right of the page begins the loading process over again.

Table 82 *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. See

Parameter	Definition
	Editing Alarm Text and Severity and Disabling Alarms and Events.
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. See Editing Alarm Text and Severity and Disabling Alarms and Events.
Origin	The module that generated the event.

Editing Alarm Text and Severity and Disabling Alarms and Events

You can view a list of alarm types, edit the severity level assigned to individual alarm types, disable alarms and events, and add additional descriptive text to individual alarm types.

This section includes:

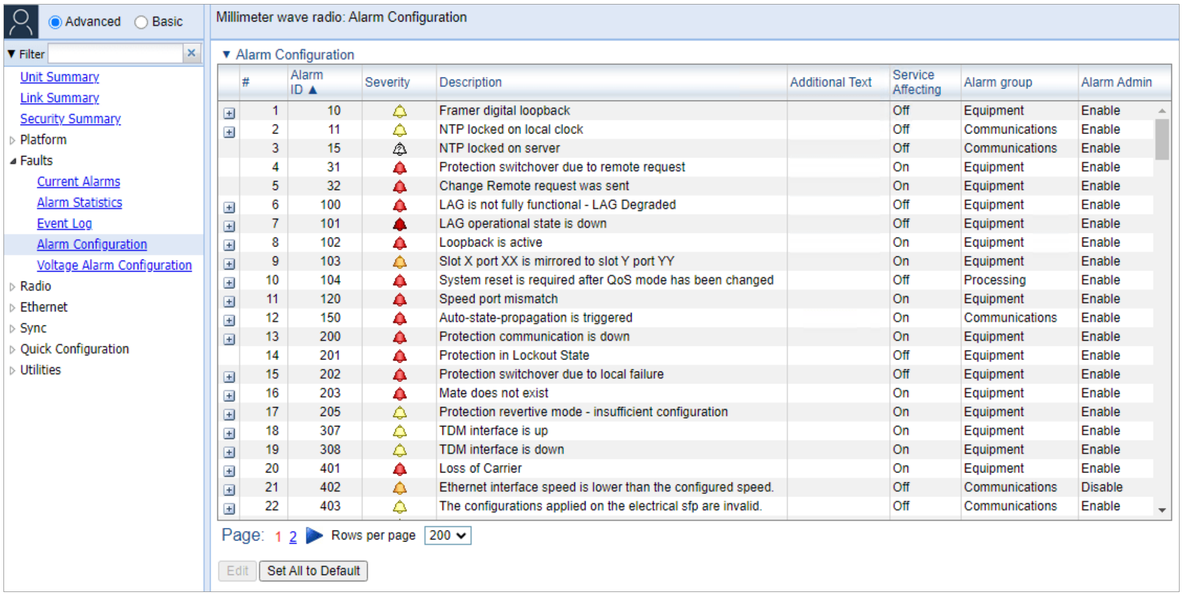
- Displaying Alarm Information
- Viewing the Probable Cause and Corrective Actions for an Alarm Type
- Editing an Alarm Type and Disabling Alarms and Events
- Enabling the Auto Negotiation Speed Alarm
- Setting Alarms to their Default Values

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, see Alarm Configuration Page Parameters.

Figure 342 *Alarm Configuration Page*



Millimeter wave radio: Alarm Configuration

▼ Alarm Configuration

	#	Alarm ID ▲	Severity	Description	Additional Text	Service Affecting	Alarm group	Alarm Admin
⊞	1	10	🔔	Framer digital loopback		Off	Equipment	Enable
⊞	2	11	🔔	NTP locked on local clock		Off	Communications	Enable
	3	15	🔔	NTP locked on server		Off	Communications	Enable
	4	31	🔔	Protection switchover due to remote request		On	Equipment	Enable
	5	32	🔔	Change Remote request was sent		On	Equipment	Enable
⊞	6	100	🔔	LAG is not fully functional - LAG Degraded		Off	Equipment	Enable
⊞	7	101	🔔	LAG operational state is down		Off	Equipment	Enable
⊞	8	102	🔔	Loopback is active		On	Equipment	Enable
⊞	9	103	🔔	Slot X port XX is mirrored to slot Y port YY		On	Equipment	Enable
⊞	10	104	🔔	System reset is required after QoS mode has been changed		Off	Processing	Enable
⊞	11	120	🔔	Speed port mismatch		On	Equipment	Enable
⊞	12	150	🔔	Auto-state-propagation is triggered		On	Communications	Enable
⊞	13	200	🔔	Protection communication is down		On	Equipment	Enable
	14	201	🔔	Protection in Lockout State		Off	Equipment	Enable
⊞	15	202	🔔	Protection switchover due to local failure		Off	Equipment	Enable
⊞	16	203	🔔	Mate does not exist		On	Equipment	Enable
⊞	17	205	🔔	Protection revertive mode - insufficient configuration		On	Equipment	Enable
⊞	18	307	🔔	TDM interface is up		On	Equipment	Enable
⊞	19	308	🔔	TDM interface is down		On	Equipment	Enable
⊞	20	401	🔔	Loss of Carrier		On	Equipment	Enable
⊞	21	402	🔔	Ethernet interface speed is lower than the configured speed.		Off	Communications	Disable
⊞	22	403	🔔	The configurations applied on the electrical sfp are invalid.		Off	Communications	Enable

Page: 1 2 ▶ Rows per page 200

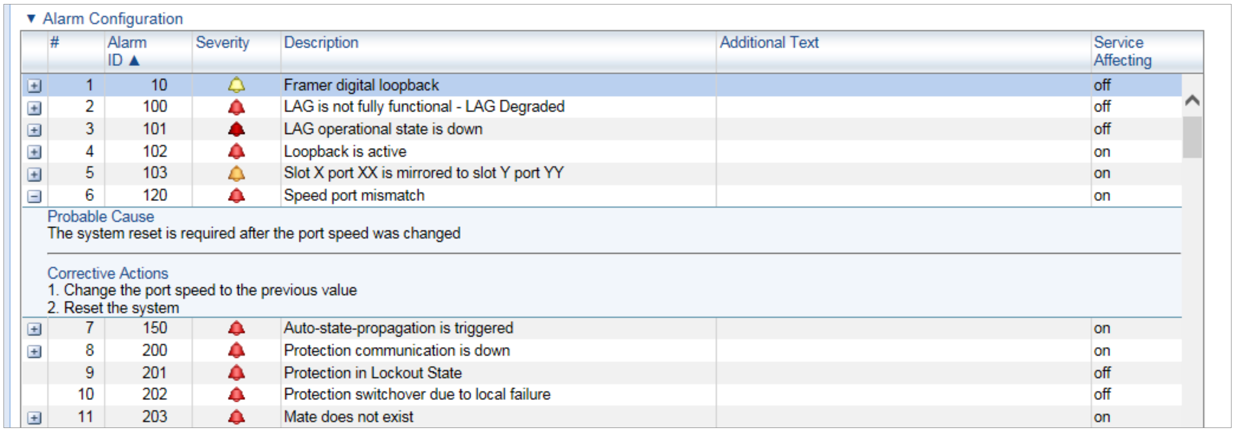
Table 83 *Alarm Configuration Page Parameters*

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. See Editing an Alarm Type and Disabling Alarms and Events.
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. See Editing an Alarm Type and Disabling Alarms and Events.
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. See Editing an Alarm Type and Disabling Alarms and Events and Enabling the Auto Negotiation Speed Alarm.

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 343 *Alarm Configuration Page – Expanded*



▼ Alarm Configuration

	#	Alarm ID ▲	Severity	Description	Additional Text	Service Affecting
⊞	1	10	🔔	Framer digital loopback		off
⊞	2	100	🔔	LAG is not fully functional - LAG Degraded		off
⊞	3	101	🔔	LAG operational state is down		off
⊞	4	102	🔔	Loopback is active		on
⊞	5	103	🔔	Slot X port XX is mirrored to slot Y port YY		on
⊟	6	120	🔔	Speed port mismatch		on

Probable Cause
The system reset is required after the port speed was changed

Corrective Actions
1. Change the port speed to the previous value
2. Reset the system

	#	Alarm ID ▲	Severity	Description	Additional Text	Service Affecting
⊞	7	150	🔔	Auto-state-propagation is triggered		on
⊞	8	200	🔔	Protection communication is down		on
	9	201	🔔	Protection in Lockout State		off
	10	202	🔔	Protection switchover due to local failure		off
⊞	11	203	🔔	Mate does not exist		on

Editing an Alarm Type and Disabling Alarms and Events

You can change the severity of an alarm type, reassign the Alarm group to which the alarm is assigned, 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.

Note

All alarms are enabled by default except the Auto Negotiation Speed alarm (Alarm ID 402). See Enabling the Auto Negotiation Speed Alarm.

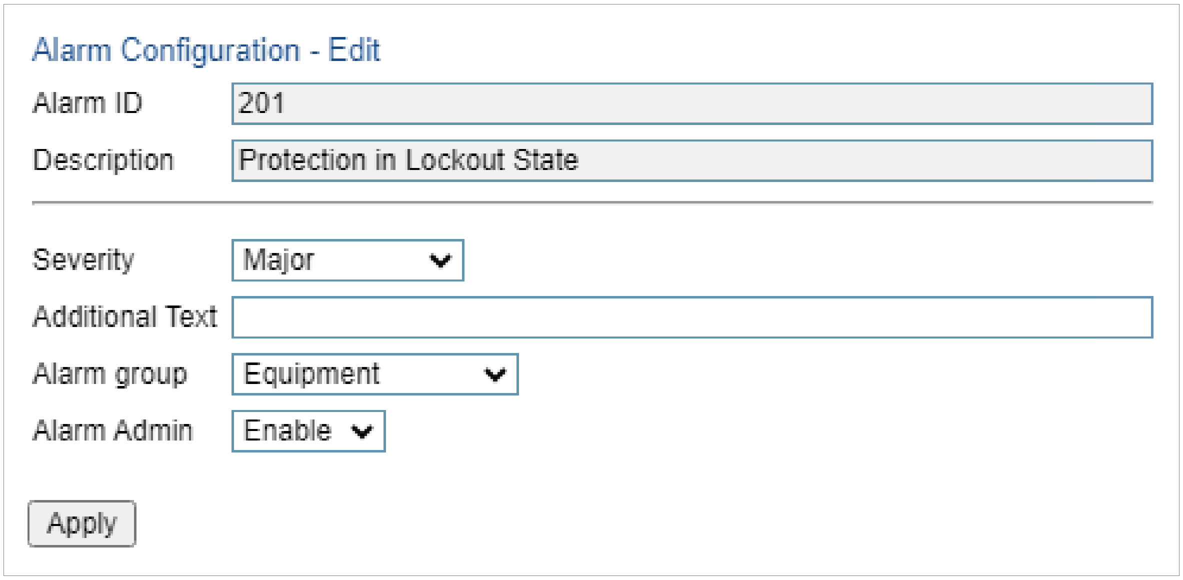
If you disable an alarm that is currently raised, the alarm is treated as if it has been cleared. If an alarm that has been disabled is enabled while it is in a raised state, the alarm is treated as if it has just been raised when it is enabled.

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, add additional text to the alarm type's description, and disable and enable alarms and events:

1. Select the alarm type in the Alarm Configuration page (Alarm Configuration Page).
2. Click **Edit**. The Alarm Configuration - Edit page opens.

Figure 344 *Alarm Configuration - Edit Page*



Alarm Configuration - Edit

Alarm ID: 201

Description: Protection in Lockout State

Severity: Major

Additional Text:

Alarm group: Equipment

Alarm Admin: Enable

3. Modify the **Severity** and/or **Additional Text** fields.
4. In the **Alarm group** field, you can re-assign the Alarm group to which the alarm belongs. The Alarm group is used to determine which alarms trigger an external alarm output.

Note

PTP 850EX do not support external alarm output.

5. To disable an alarm or event, select **Disable** in the **Alarm Admin** field. To re-enable an alarm or event, select **Enable** in the **Alarm Admin** field.
6. Click **Apply**, then **Close**.

Enabling the Auto Negotiation Speed Alarm

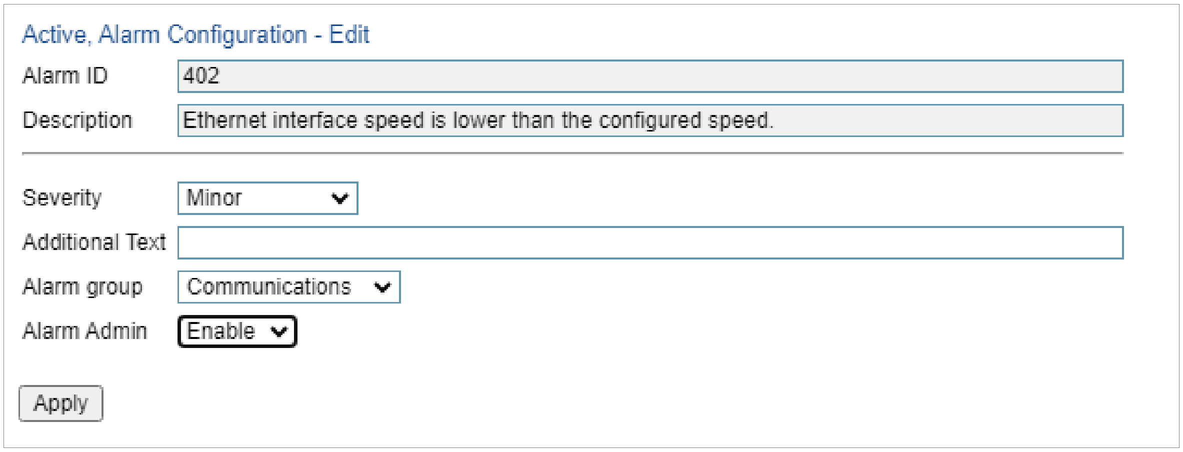
Alarm ID 402 is the Auto Negotiation Speed Alarm. When Auto Negotiation is enabled on an Ethernet interface, this alarm monitors the interface speed. The alarm is raised if the actual speed is lower than the configured speed. The alarm is cleared when any of the following occurs:

- 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 (Alarm Configuration Page).
2. Click **Edit**. The Alarm Configuration – Edit page opens.

Figure 345 *Alarm Configuration – Edit Page*



Active, Alarm Configuration - Edit

Alarm ID: 402

Description: Ethernet interface speed is lower than the configured speed.

Severity: Minor

Additional Text:

Alarm group: Communications

Alarm Admin: Enable

3. In the **Alarm Admin** field, select **Enable**.
4. Click **Apply**.

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 (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. See Enabling the Auto Negotiation Speed Alarm.

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 850EX devices 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

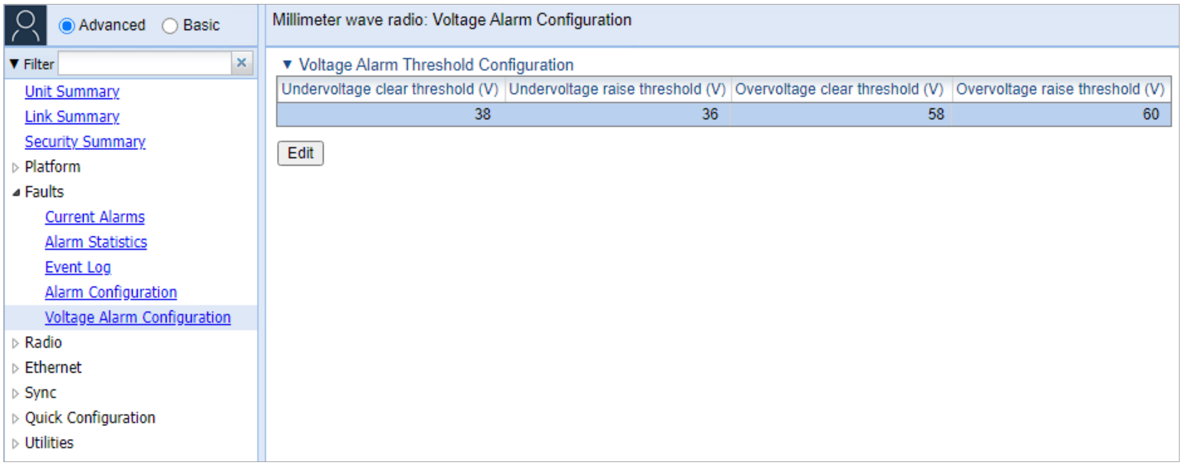
To configure voltage alarm thresholds:

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 346 *Voltage Alarm Configuration Page*



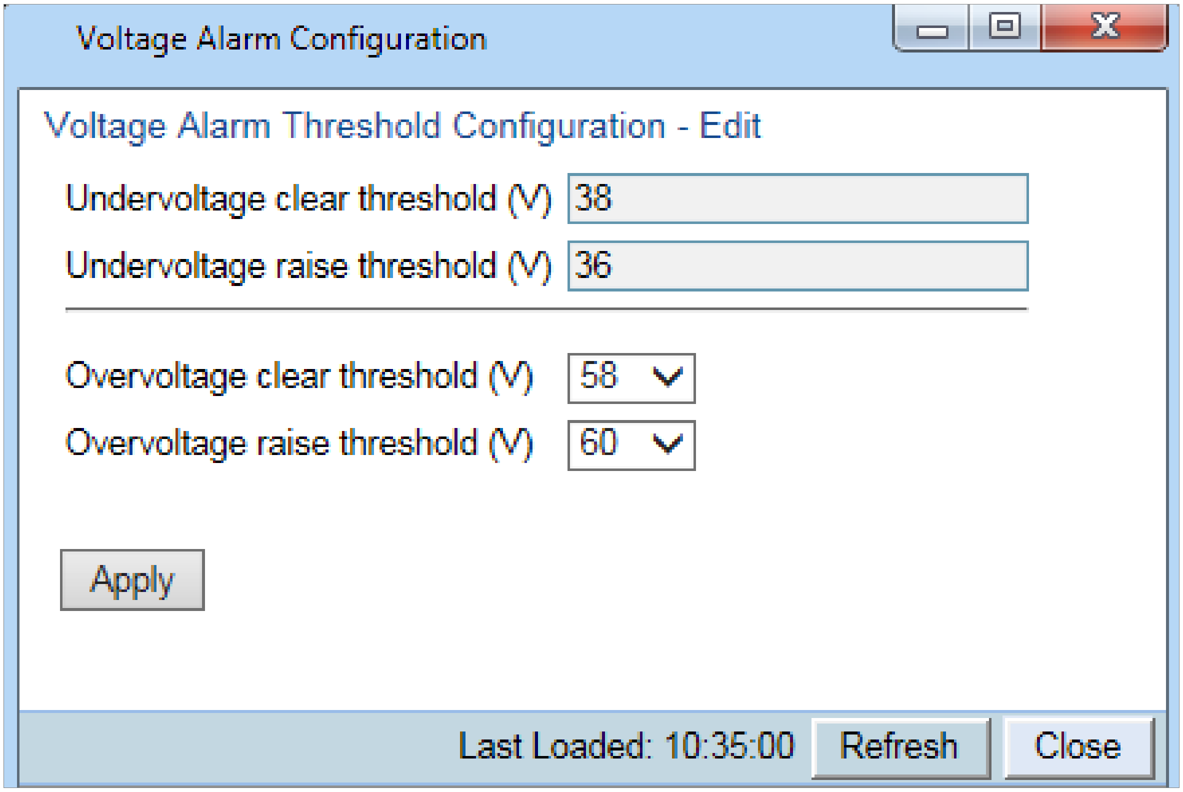
Millimeter wave radio: Voltage Alarm Configuration

Voltage Alarm Threshold Configuration

Undervoltage clear threshold (V)	Undervoltage raise threshold (V)	Overvoltage clear threshold (V)	Overvoltage raise threshold (V)
38	36	58	60

2. Click **Edit**. The Voltage Alarm Configuration – Edit page opens.

Figure 347 *Voltage Alarm Configuration – Edit Page*



Voltage Alarm Configuration

Voltage Alarm Threshold Configuration - Edit

Undervoltage clear threshold (V) 38

Undervoltage raise threshold (V) 36

Overvoltage clear threshold (V) 58

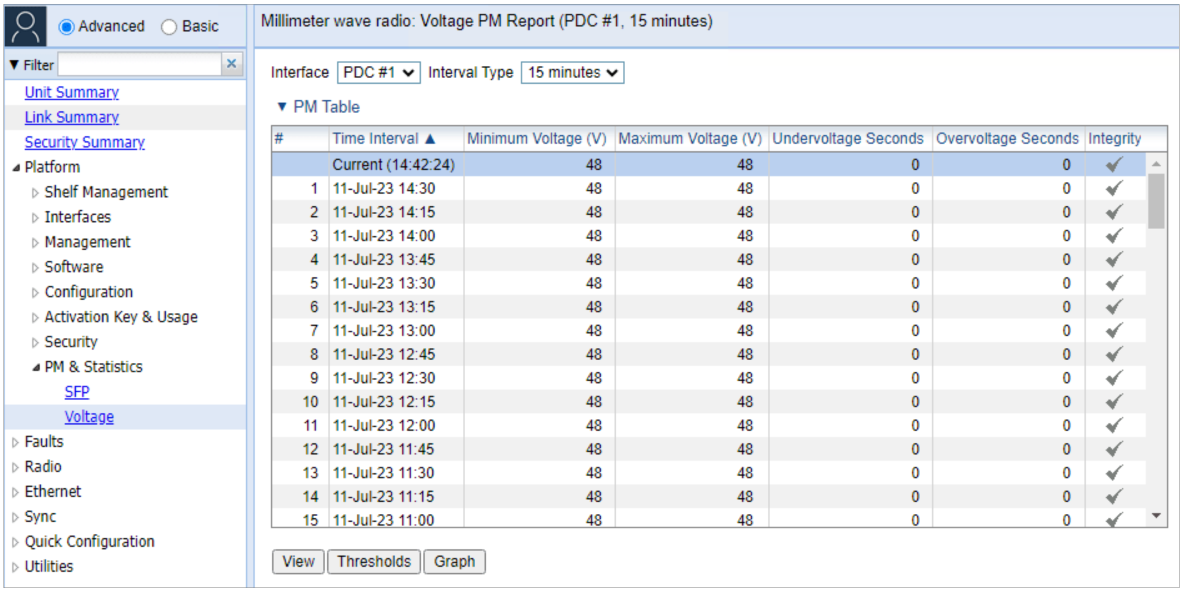
Overvoltage raise threshold (V) 60

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 348 *Voltage PM Report Page*



Millimeter wave radio: Voltage PM Report (PDC #1, 15 minutes)

Interface: PDC #1 | Interval Type: 15 minutes

#	Time Interval ▲	Minimum Voltage (V)	Maximum Voltage (V)	Undervoltage Seconds	Overvoltage Seconds	Integrity
	Current (14:42:24)	48	48	0	0	✓
1	11-Jul-23 14:30	48	48	0	0	✓
2	11-Jul-23 14:15	48	48	0	0	✓
3	11-Jul-23 14:00	48	48	0	0	✓
4	11-Jul-23 13:45	48	48	0	0	✓
5	11-Jul-23 13:30	48	48	0	0	✓
6	11-Jul-23 13:15	48	48	0	0	✓
7	11-Jul-23 13:00	48	48	0	0	✓
8	11-Jul-23 12:45	48	48	0	0	✓
9	11-Jul-23 12:30	48	48	0	0	✓
10	11-Jul-23 12:15	48	48	0	0	✓
11	11-Jul-23 12:00	48	48	0	0	✓
12	11-Jul-23 11:45	48	48	0	0	✓
13	11-Jul-23 11:30	48	48	0	0	✓
14	11-Jul-23 11:15	48	48	0	0	✓
15	11-Jul-23 11:00	48	48	0	0	✓

2. 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

The Interface field displays PDC #1.

Voltage PMs describes the Voltage PMs.

Table 84 *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.

Parameter	Definition
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.

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

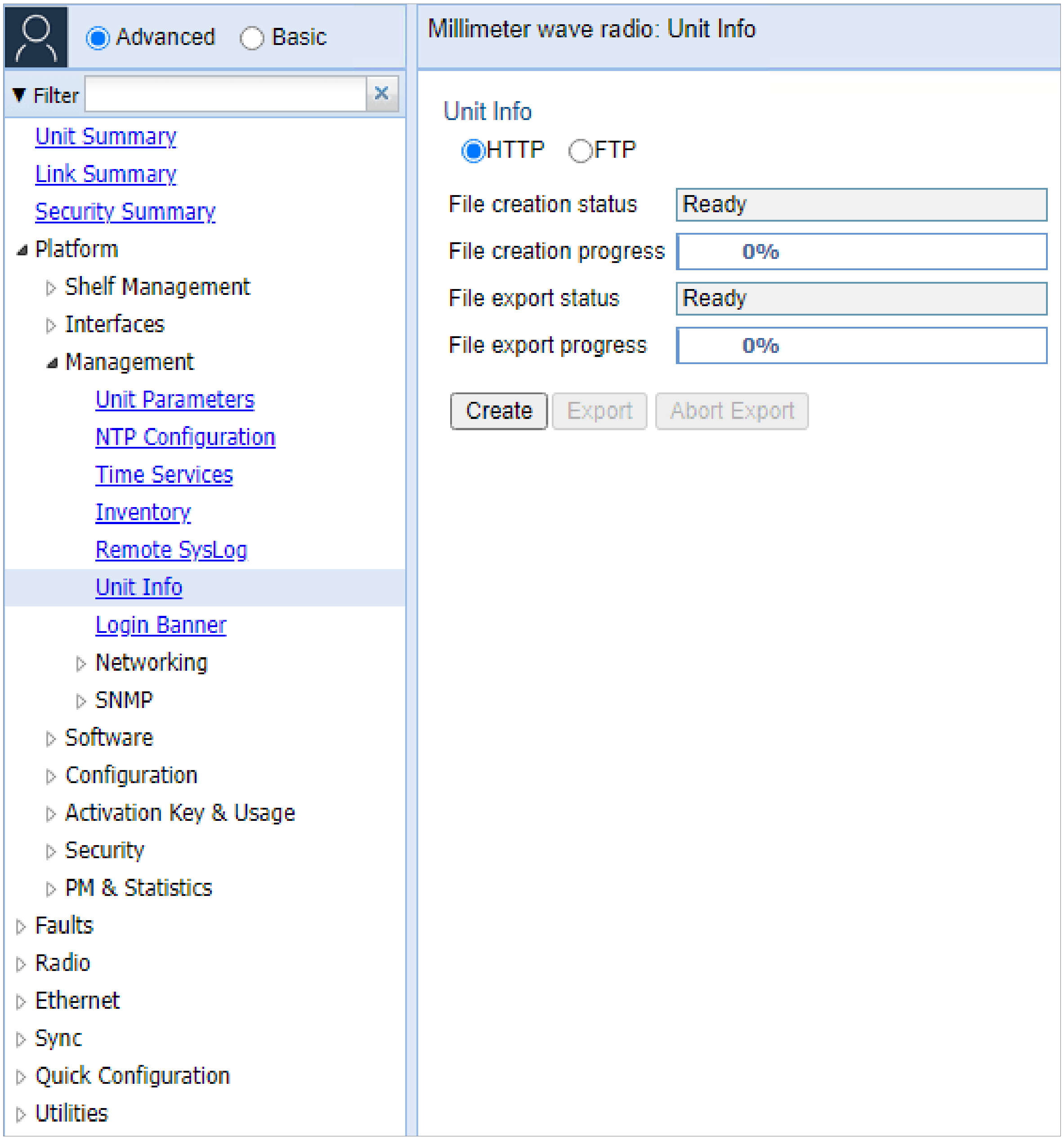
For troubleshooting, it is important that an updated configuration file be included in User Info files that are sent to customer support. To ensure that an up-to-date configuration file is included, it is recommended to back up the unit’s configuration before generating the Unit Info file.

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 with the **HTTP** option selected.

Figure 349 *Unit Info Page – HTTP/HTTPS Upload*



Millimeter wave radio: Unit Info

Unit Info

● HTTP ○ FTP

File creation status: Ready

File creation progress: 0%

File export status: Ready

File export progress: 0%

2. 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.

3. Click **Export**. The upload begins. The following fields display the status of the upload process:

   - **File Export 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 Export Progress** – Displays the progress of the current Unit Information file upload operation.

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, see Installing and Configuring an FTP or SFTP Server.

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. See Installing and Configuring an FTP or SFTP Server.
2. Select **Platform** > **Management** > **Unit Info**. The Unit Info page opens with the **HTTP** option selected (Unit Info Page – HTTP/HTTPS Upload).
3. Select FTP.
4. Click **FTP Parameters** to display the FTP Parameters page and configure the FTP parameters. See Step Generating a Certificate Signing Request (CSR) File.
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 export 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 export progress** – Displays the progress of the current Unit Information file upload operation.

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.

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. See Defining the IP Protocol Version for Initiating Communications.

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 Syslog Severity Values. The mapping depends on the type of log and the severity of the item, as shown in Syslog Severity Values.

Table 85 *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 Indeterminate	Warning – 4	Warning conditions
	Notice – 5	Normal but significant condition
Security Log or Configuration Log Entry	Informational – 6	Informational messages
	Debug – 7	Debug-level messages

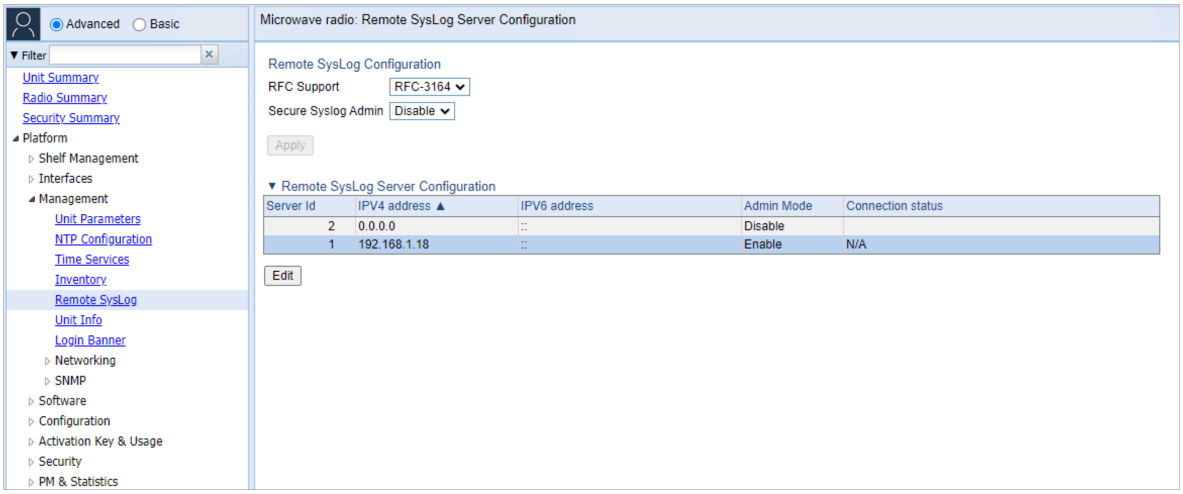
For example, a Major Alarm receives Syslog Priority 139. This is calculated as the Facility Value of 17, multiplied by 8, plus 3 based on the mapping in Syslog Severity Values.

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 350 *Remote SysLog Server Configuration Page*



Microwave radio: Remote SysLog Server Configuration

Remote SysLog Configuration

RFC Support: RFC-3164

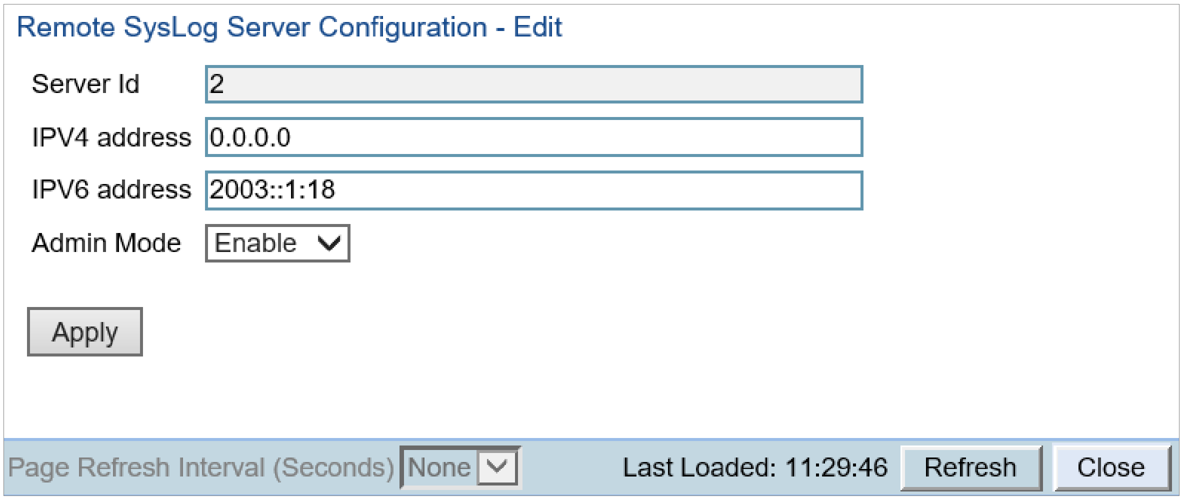
Secure Syslog Admin: Disable

Remote SysLog Server Configuration

Server Id	IPV4 address ▲	IPV6 address	Admin Mode	Connection status
2	0.0.0.0	::	Disable	
1	192.168.1.18	::	Enable	N/A

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 351 *Remote SysLog Server Configuration Page – Edit*



Remote SysLog Server Configuration - Edit

Server Id: 2

IPV4 address: 0.0.0.0

IPV6 address: 2003::1:18

Admin Mode: Enable

Page Refresh Interval (Seconds): None

Last Loaded: 11:29:46

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**.

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.

Performing Diagnostics

This section includes:

- Performing Radio Loopback
- Configuring Service OAM (SOAM) Fault Management (FM)

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.

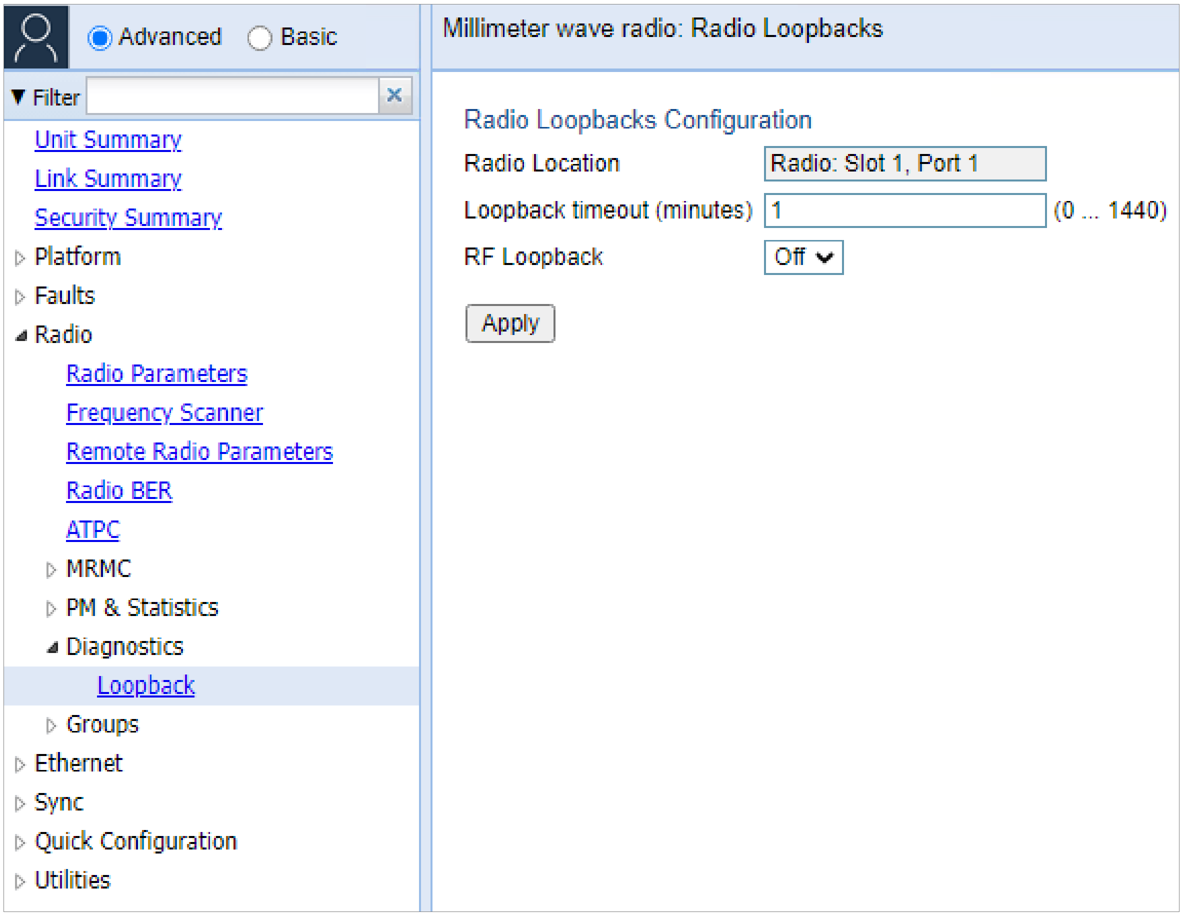
Setting radio loopback, either RF or IF, will cause full loss of the end-to-end traffic and in-band management to remote units. To avoid permanent loss of traffic and in-band management, it is recommended to set a loopback timeout.

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 352 *Radio Loopbacks Page*



Millimeter wave radio: Radio Loopbacks

Radio Loopbacks Configuration

Radio Location: Radio: Slot 1, Port 1

Loopback timeout (minutes): 1 (0 ... 1440)

RF Loopback: Off

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**.
4. Click **Apply**.

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 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
- Loopback

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.

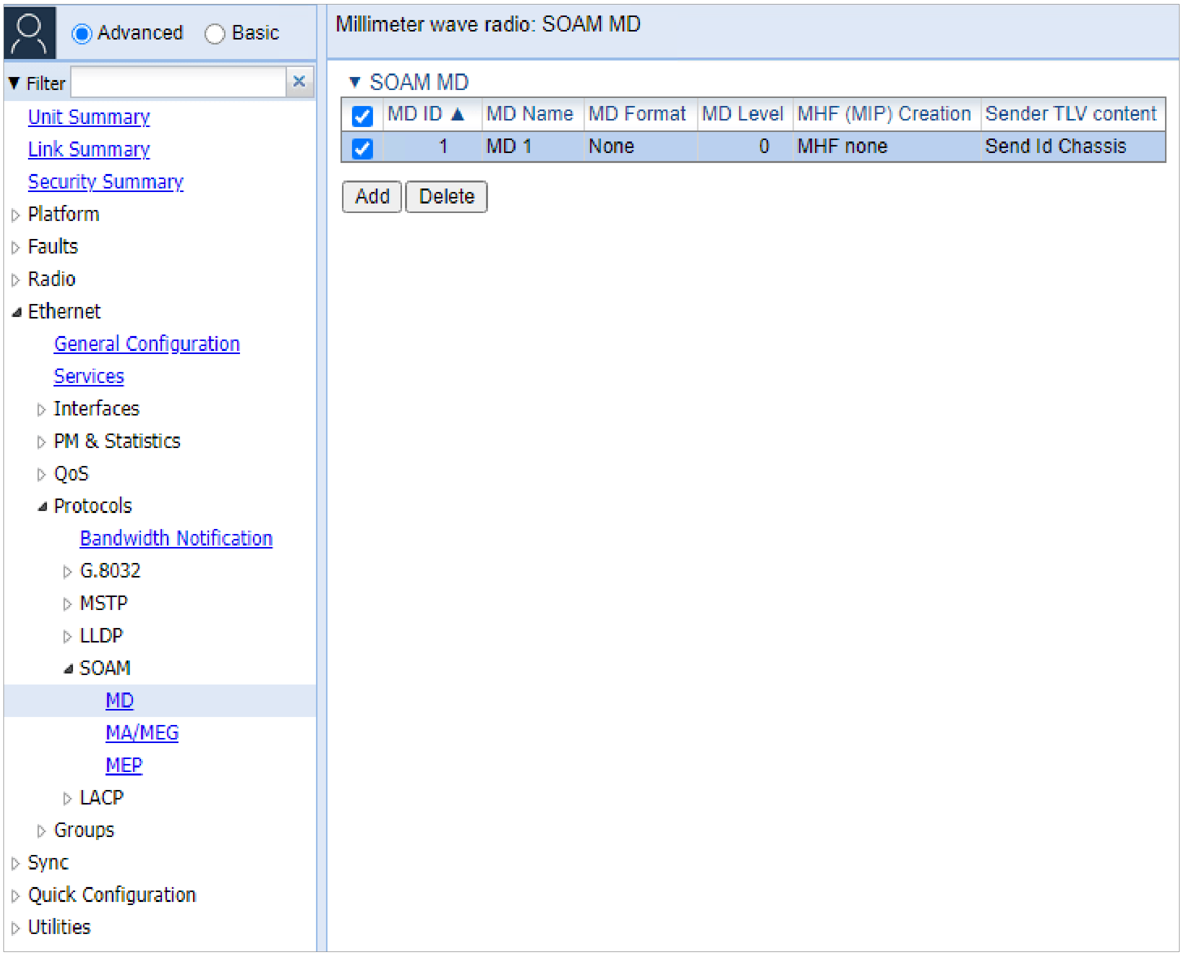
Configuring MDs

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 353 *SOAM MD Page*



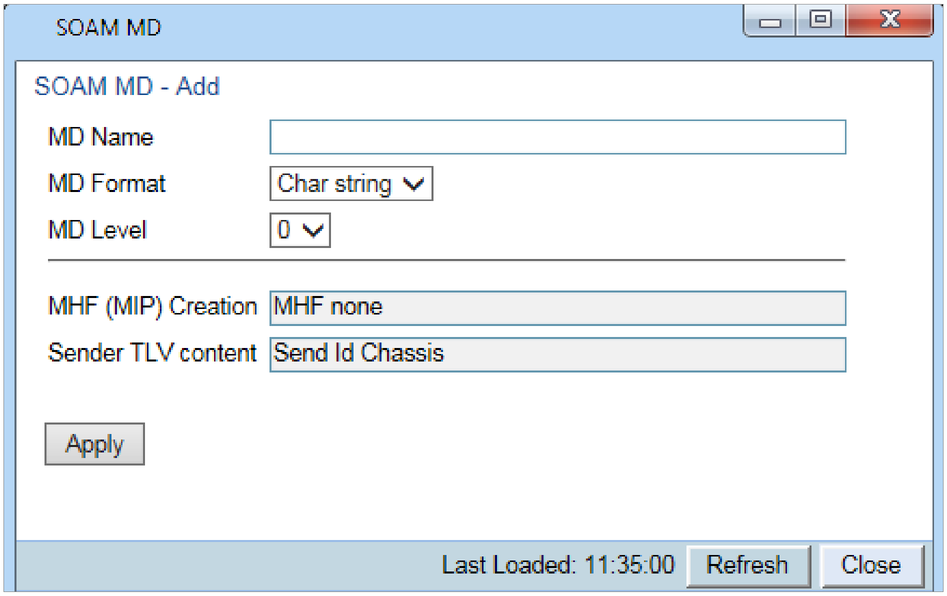
Millimeter wave radio: SOAM MD

▼ SOAM MD

☑	MD ID ▲	MD Name	MD Format	MD Level	MHF (MIP) Creation	Sender TLV content
☑	1	MD 1	None	0	MHF none	Send Id Chassis

2. Click **Add**. The SOAM MD – Add page opens.

Figure 354 *SOAM MD – Add Page*



SOAM MD

SOAM MD - Add

MD Name

MD Format: Char string

MD Level: 0

MHF (MIP) Creation: MHF none

Sender TLV content: Send Id Chassis

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 functionality.

5. In the **MD Level** field, select the maintenance level of the MD (0-7). 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 type 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 type 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 256 MEGs per network element. MEGs are classified as Fast MEGs or Slow MEGs according to the CCM interval (see SOAM MA/MEG Configuration Parameters):

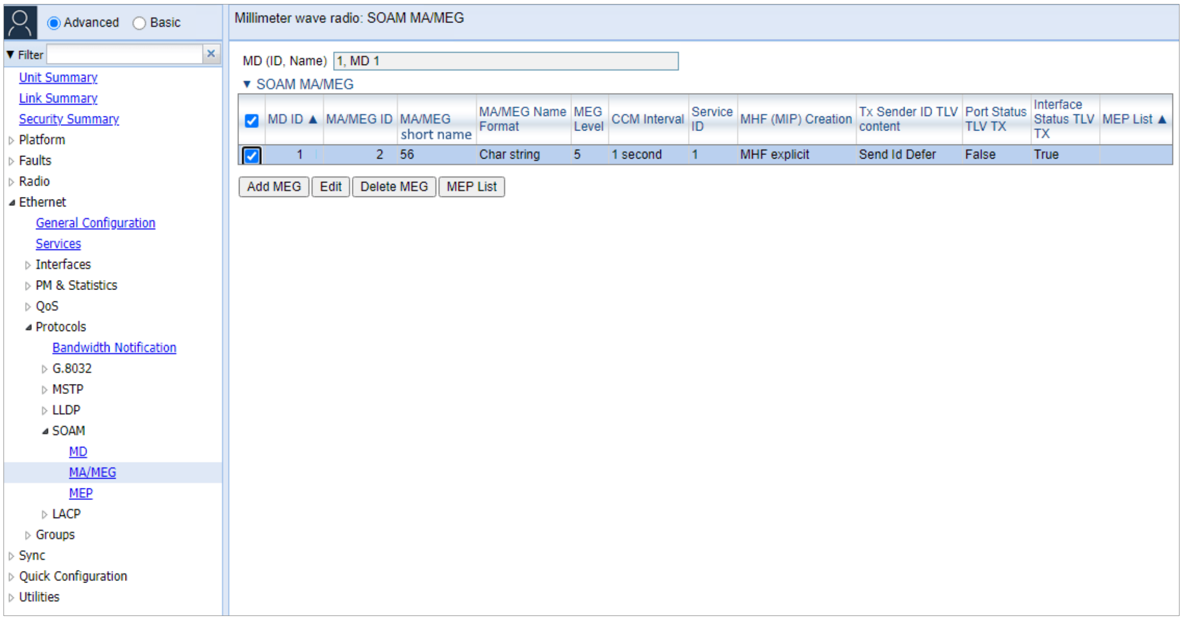
- Fast MEGs have a CCM interval of 1 second.
- Slow MEGs have a CCM interval of 10 seconds, 1 minute, or 10 minutes.

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 355 *SOAM MA/MEG Page*



Millimeter wave radio: SOAM MA/MEG

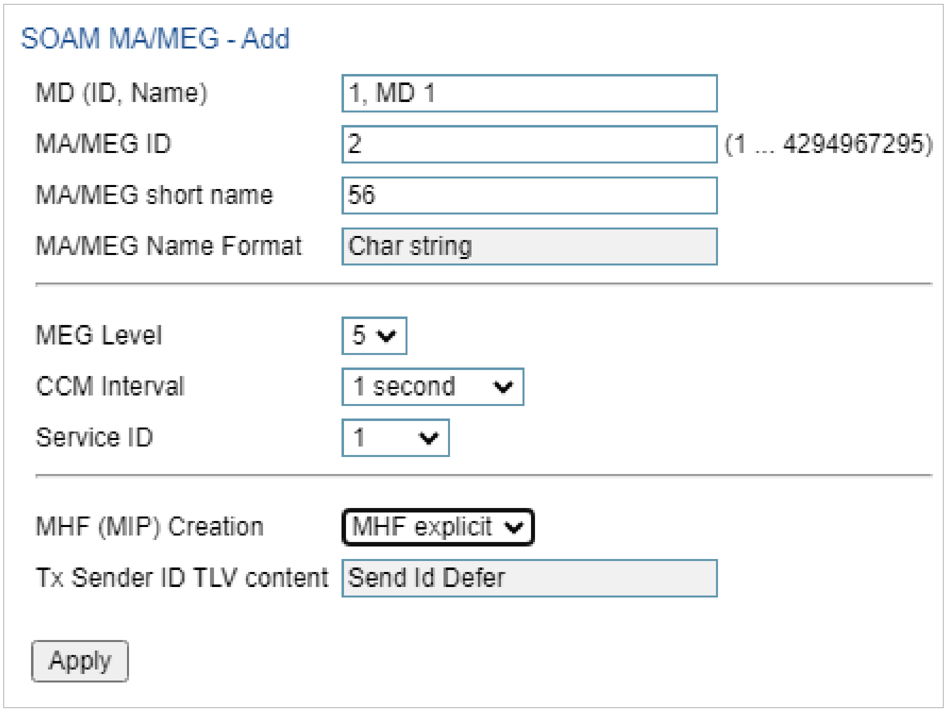
MD (ID, Name) 1, MD 1

▼ SOAM MA/MEG

☑	MD ID ▲	MA/MEG ID	MA/MEG short name	MA/MEG Name Format	MEG Level	CCM Interval	Service ID	MHF (MIP) Creation	Tx Sender ID TLV content	Port Status TLV TX	Interface Status TLV TX	MEP List ▲
☑	1	2	56	Char string	5	1 second	1	MHF explicit	Send Id Defer	False	True	

2. Click **Add MEG**. The SOAM MA/MEG – Add page opens.

Figure 356 *SOAM MA/MEG – Add Page*



SOAM MA/MEG - Add

MD (ID, Name)	1, MD 1	
MA/MEG ID	2	(1 ... 4294967295)
MA/MEG short name	56	
MA/MEG Name Format	Char string	
MEG Level	5	
CCM Interval	1 second	
Service ID	1	
MHF (MIP) Creation	MHF explicit	
Tx Sender ID TLV content	Send Id Defer	

3. Configure the fields described in SOAM MA/MEG Configuration Parameters.
4. Click **Apply**, then **Close**.

SOAM MA/MEG Status Parameters describes the status (read-only) fields in the SOAM MA/MEG Component table.

Table 86 *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).
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.

Parameter	Definition
	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: • 100 ms • 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.
Service ID	Select an Ethernet service to which the MEG belongs. You must define the service 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 87 *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	Sender ID TLV is transmitted.
Port Status TLV TX	Reserved for future use. No Port Status TLV is transmitted in the CCM frame.
Interface Status TLV TX	An Interface Status TLV is transmitted in the CCM frame, indicating the operational status of the interface on which the transmitting MEP is configured (Up or Down).
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.

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:

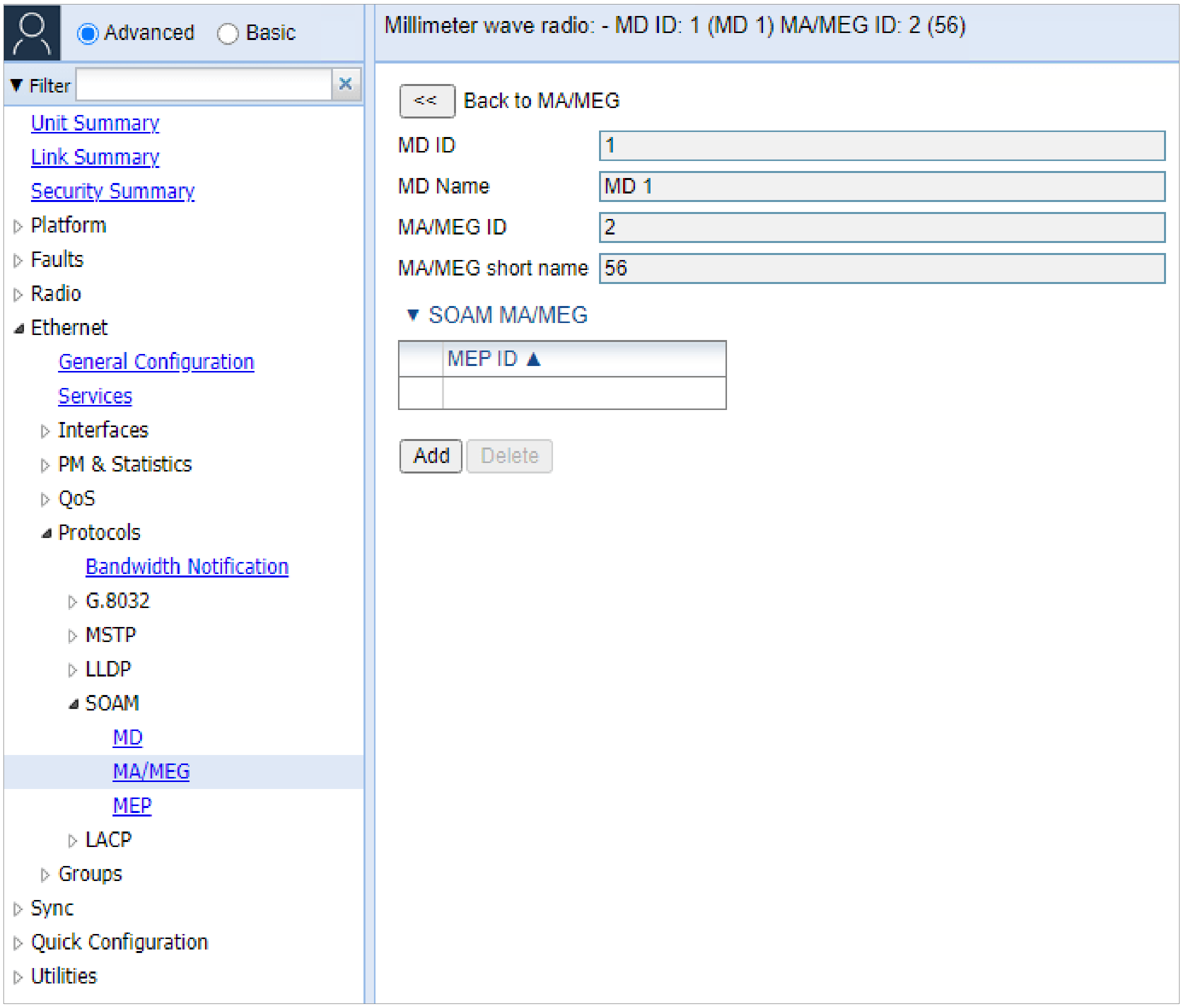
1. Add MEPs to the relevant MA/MEG. In this stage, you add both local and remote MEPs. The only thing you define at this point is the MEP ID. See Adding Local and Remote MEPs.
2. Configure the local MEPs. At this point, you determine which MEPs are local MEPs. The system automatically defines the other 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 357 *MEP List Page*

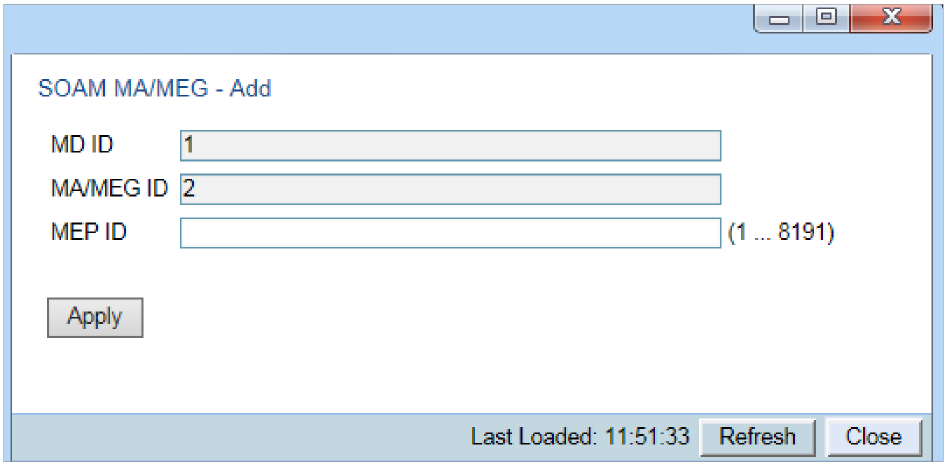


Millimeter wave radio: - MD ID: 1 (MD 1) MA/MEG ID: 2 (56)

MD ID	1
MD Name	MD 1
MA/MEG ID	2
MA/MEG short name	56

2. Click **Add**. The Add MEP page opens.

Figure 358 *Add MEP Page*



SOAM MA/MEG - Add

MD ID: 1

MA/MEG ID: 2

MEP ID: (1 ... 8191)

Last Loaded: 11:51:33

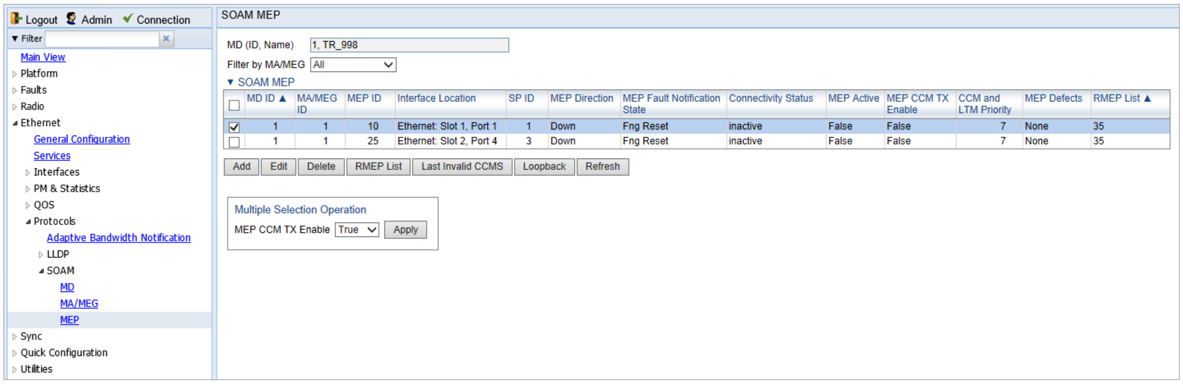
3. In the **MEP ID** field, enter a MEP ID (1-8191).
4. Click **Apply**, then **Close**.

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. SOAM MEP Parameters lists and describes the parameters displayed in the SOAM MEP page.

Figure 359 *SOAM MEP Page*



SOAM MEP

MD (ID, Name): 1, TR_998

Filter by MA/MEG: All

▼ SOAM MEP

□	MD ID ▲	MA/MEG ID	MEP ID	Interface Location	SP ID	MEP Direction	MEP Fault Notification State	Connectivity Status	MEP Active	MEP CCM TX Enable	CCM and LTM Priority	MEP Defects	RMEP List ▲
☑	1	1	10	Ethernet: Slot 1, Port 1	1	Down	Fng Reset	inactive	False	False	7	None	35
□	1	1	25	Ethernet: Slot 2, Port 4	3	Down	Fng Reset	inactive	False	False	7	None	35

Multiple Selection Operation

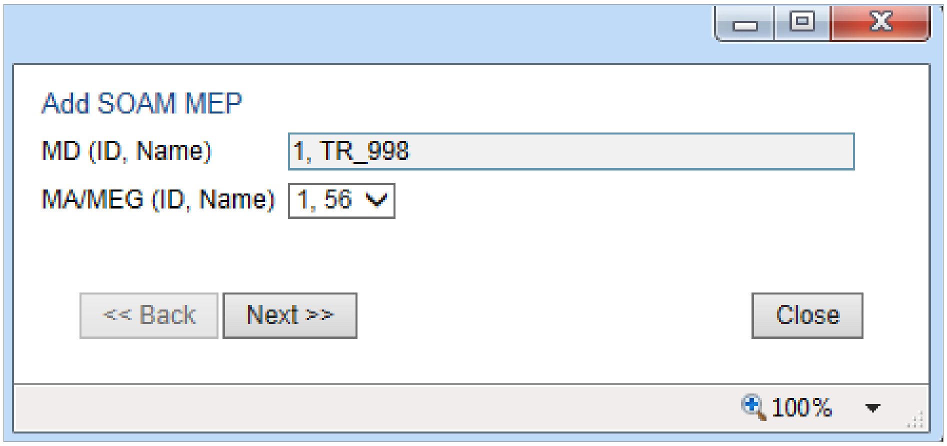
MEP CCM TX Enable: True

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 360 *Add SOAM MEP Wizard – Page 1*



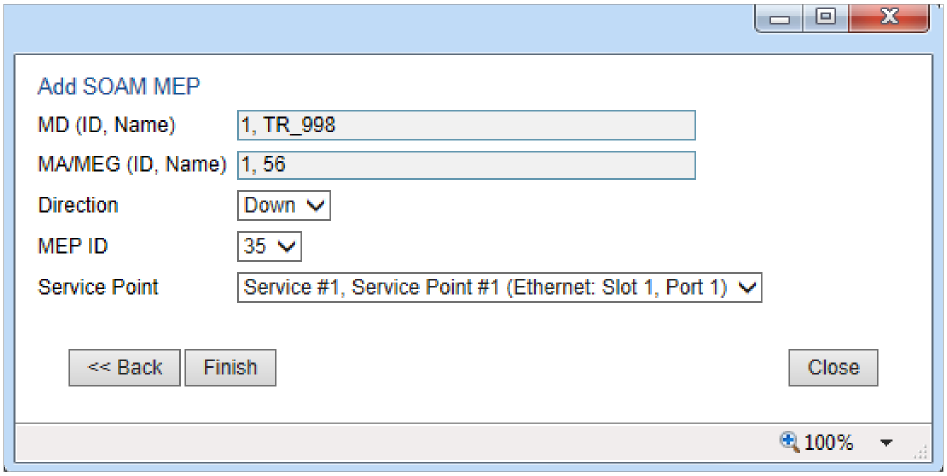
Add SOAM MEP

MD (ID, Name): 1, TR_998

MA/MEG (ID, Name): 1, 56

3. In the **MA/MEG Name** field, select an MA/MEG.
4. Click **Next**. Page 2 of the Add SOAM MEP wizard opens.

Figure 361 *Add SOAM MEP Wizard – Page 2*



Add SOAM MEP

MD (ID, Name): 1, TR_998

MA/MEG (ID, Name): 1, 56

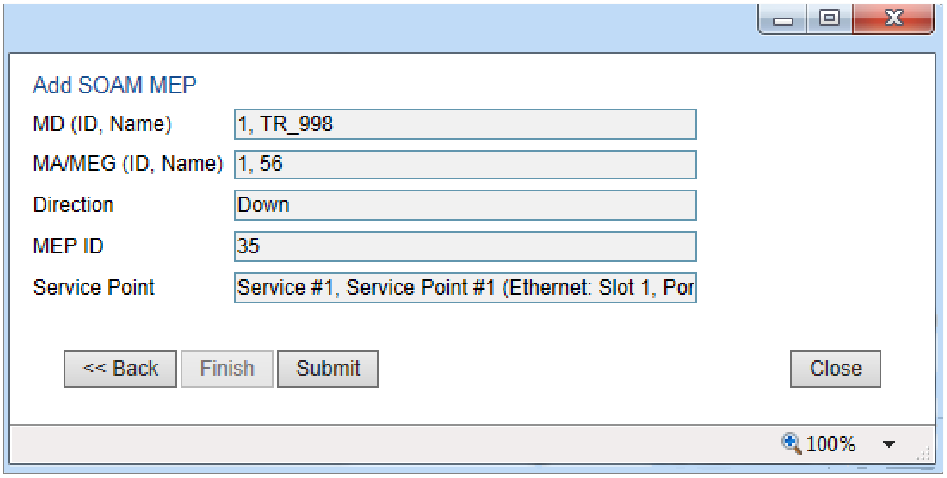
Direction: Down

MEP ID: 35

Service Point: Service #1, Service Point #1 (Ethernet: Slot 1, Port 1)

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 362 *Add SOAM MEP Wizard –Summary Page*



Add SOAM MEP

MD (ID, Name) 1, TR_998

MA/MEG (ID, Name) 1, 56

Direction Down

MEP ID 35

Service Point Service #1, Service Point #1 (Ethernet: Slot 1, Por

9. Verify that you want to submit the displayed parameters and click Submit.

Table 88 *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.
Service Point ID	The service point ID.
MEP Direction	**Up** or **Down**.
MEP Fault Notification State	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 (state = transient).
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:

Parameter	Definition
	- **inactive** – At least one of the remote MEPs is 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.

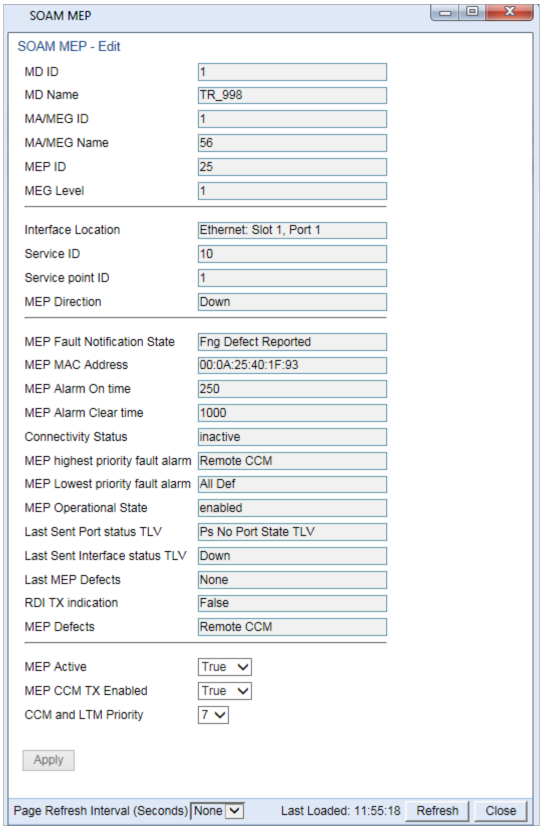
Enabling Local MEPs

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 (SOAM MEP Page), select the MEP you want to enable.
2. Click **Edit**. The SOAM MEP - Edit page opens.

Figure 363 *SOAM MEP - Edit Page*



SOAM MEP

SOAM MEP - Edit

MD ID	1
MD Name	TR_998
MA/MEG ID	1
MA/MEG Name	56
MEP ID	25
MEG Level	1
Interface Location	Ethernet: Slot 1, Port 1
Service ID	10
Service point ID	1
MEP Direction	Down
MEP Fault Notification State	Fng Defect Reported
MEP MAC Address	00:0A:25:40:1F:93
MEP Alarm On time	250
MEP Alarm Clear time	1000
Connectivity Status	inactive
MEP highest priority fault alarm	Remote CCM
MEP Lowest priority fault alarm	All Def
MEP Operational State	enabled
Last Sent Port status TLV	Ps No Port State TLV
Last Sent Interface status TLV	Down
Last MEP Defects	None
RDI TX indication	False
MEP Defects	Remote CCM
MEP Active	True
MEP CCM TX Enabled	True
CCM and LTM Priority	7

Page Refresh Interval (Seconds) None

Last Loaded: 11:55:18

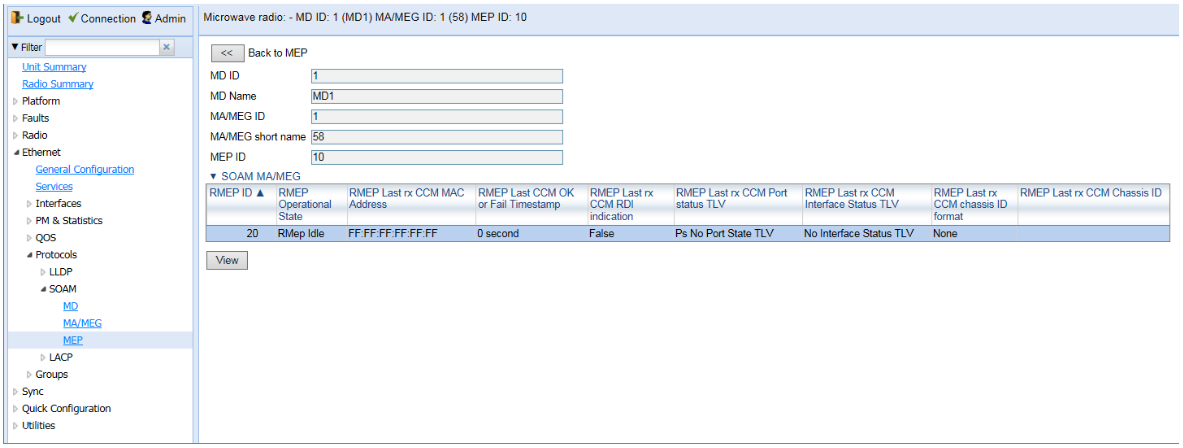
3. In the **MEP Active** field, select **True**.
4. In the **MEP CCM TX Enable** field, select **True**.
5. In the **CCM and LTM Priority** field, select the p-bit that will be included in CCMs sent by this MEP (0 to 7). It is recommended to select 7.
6. Click **Apply**, then **Close**.

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 (SOAM MEP Page).
2. Select a MEP and click RMEP List. The SOAM MEP DB table is displayed.

Figure 364 *SOAM MEP DB Table*



Microwave radio: - MD ID: 1 (MD1) MA/MEG ID: 1 (58) MEP ID: 10

Back to MEP

MD ID	1
MD Name	MD1
MA/MEG ID	1
MA/MEG short name	58
MEP ID	10

▼ SOAM MA/MEG

RMEP ID ▲	RMEP Operational State	RMEP Last rx CCM MAC Address	RMEP Last CCM OK or Fail Timestamp	RMEP Last rx CCM RDI indication	RMEP Last rx CCM Port status TLV	RMEP Last rx CCM Interface Status TLV	RMEP Last rx CCM chassis ID format	RMEP Last rx CCM Chassis ID
20	RMep Idle	FF:FF:FF:FF:FF:FF	0 second	False	Ps No Port State TLV	No Interface Status TLV	None	

SOAM MEP DB Table Parameters 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 89 *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.
RMEP Last rx CCM Interface Status TLV	Displays the operational status of the interface on which the remote MEP has been defined.

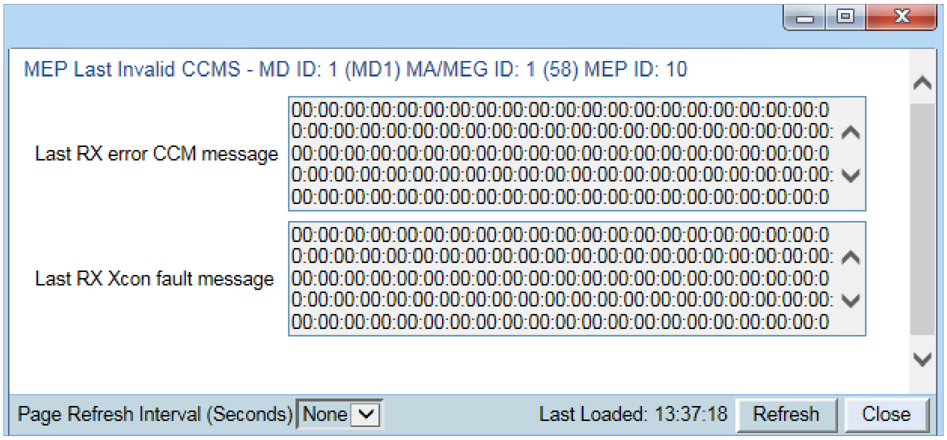
Parameter	Definition
RMEP Last rx CCM Chassis ID Format	Displays the format of the remote chassis (always the MAC address).
RMEP Last rx CCM Chassis ID	Displays the MAC address of the remote chassis.

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 (SOAM MEP Page).
2. Select a MEP and click **Last Invalid CCMS**. The MEP Last Invalid CCMS page opens.

Figure 365 *MEP Last Invalid CCMS Page*



MEP Last Invalid CCMS - MD ID: 1 (MD1) MA/MEG ID: 1 (58) MEP ID: 10

Last RX error CCM message

```
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0
0:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0
0:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0
```

Last RX Xcon fault message

```
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0
0:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0
0:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0
```

Page Refresh Interval (Seconds): None

Last Loaded: 13:37:18

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.

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. See Displaying MEP and Remote MEP Attributes (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:

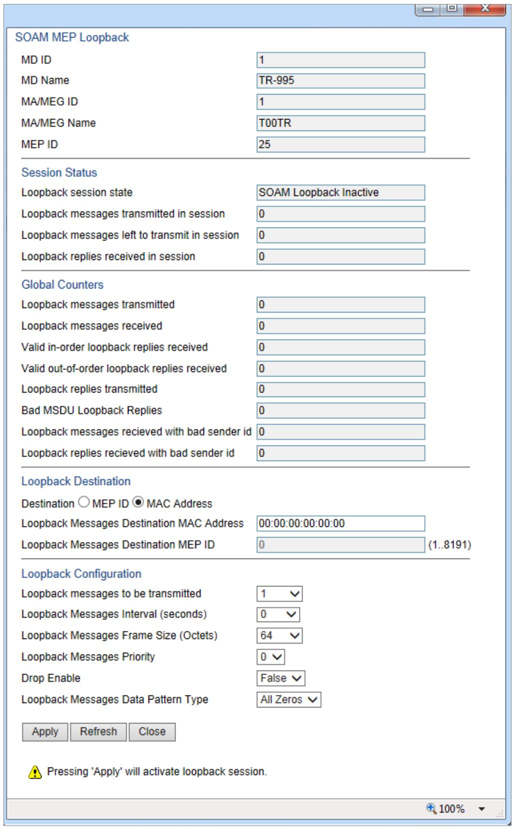
1. Create a MEG with the MHF none attribute on the intended Ethernet service. See Configuring MA/MEGs.
2. Select the MEG and click **Edit**. The SOAM MA/MEG – Edit page opens.
3. In the **MIP Creation** field, select **MHF Default**.
4. Click **Apply**, then **Close**.

Performing Loopback

To perform loopback on a MEP:

1. In the SOAM MEP page (SOAM MEP Page), select the MEP on which you want to perform the loopback.
2. Click **Loopback**. The SOAM MEP – Loopback page opens.

Figure 366 *SOAM MEP Loopback Page*



SOAM MEP Loopback

MD ID	1
MD Name	TR-995
MA/MEG ID	1
MA/MEG Name	T00TR
MEP ID	25

Session Status

Loopback session state	SOAM Loopback Inactive
Loopback messages transmitted in session	0
Loopback messages left to transmit in session	0
Loopback replies received in session	0

Global Counters

Loopback messages transmitted	0
Loopback messages received	0
Valid in-order loopback replies received	0
Valid out-of-order loopback replies received	0
Loopback replies transmitted	0
Bad MSDU Loopback Replies	0
Loopback messages recieved with bad sender id	0
Loopback replies recieved with bad sender id	0

Loopback Destination

Destination ○ MEP ID ● MAC Address

Loopback Messages Destination MAC Address	00:00:00:00:00:00
Loopback Messages Destination MEP ID	0 (1..8191)

Loopback Configuration

Loopback messages to be transmitted	1
Loopback Messages Interval (seconds)	0
Loopback Messages Frame Size (Octets)	64
Loopback Messages Priority	0
Drop Enable	False
Loopback Messages Data Pattern Type	All Zeros

⚠ Pressing 'Apply' will activate loopback session.

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 > Interfaces > 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>
```

Web EMS Utilities

This section includes:

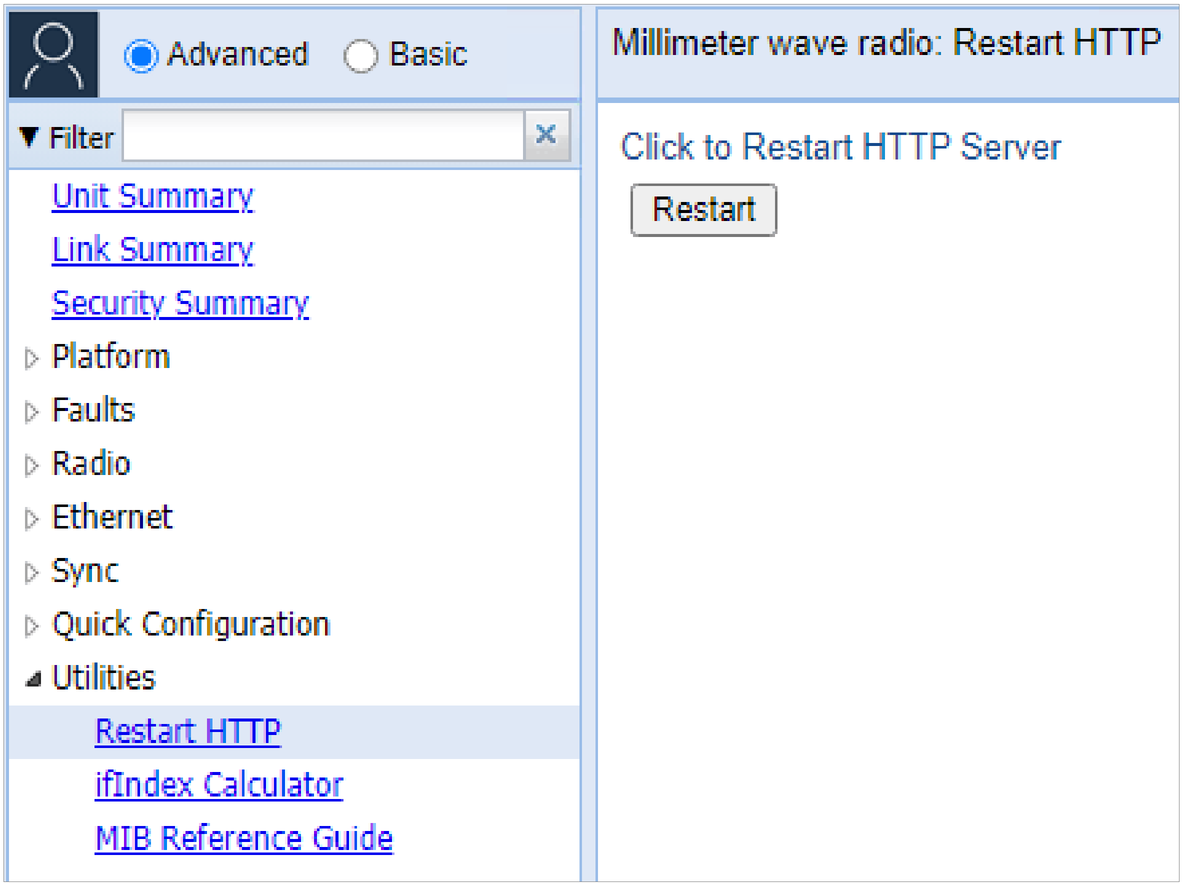
- Restarting the HTTP Server
- Calculating an ifIndex
- Displaying, Searching, and Saving a list of MIB Entities

Restarting the HTTP Server

To restart the unit's HTTP server:

1. Select **Utilities** > **Restart HTTP**. The Restart HTTP page opens.

   Figure 367 *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.

Calculating an ifIndex

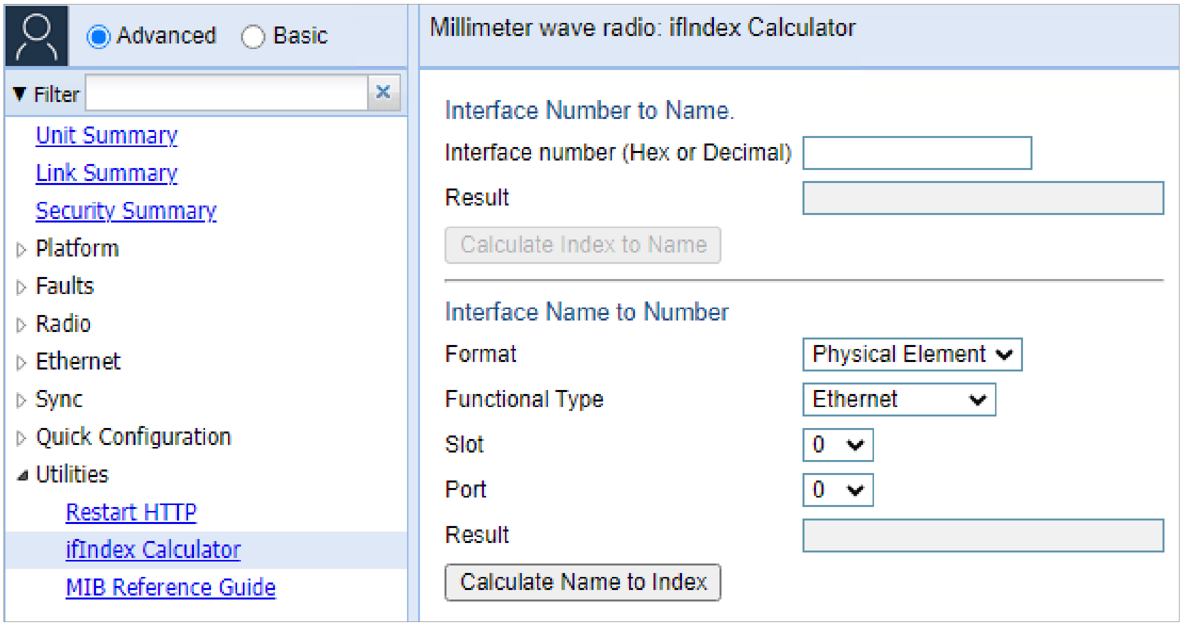
The ifIndex calculator enables you to:

- 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 368 *ifIndex Calculator Page*



Millimeter wave radio: ifIndex Calculator

Interface Number to Name.

Interface number (Hex or Decimal)

Result

Interface Name to Number

Format: Physical Element

Functional Type: Ethernet

Slot: 0

Port: 0

Result

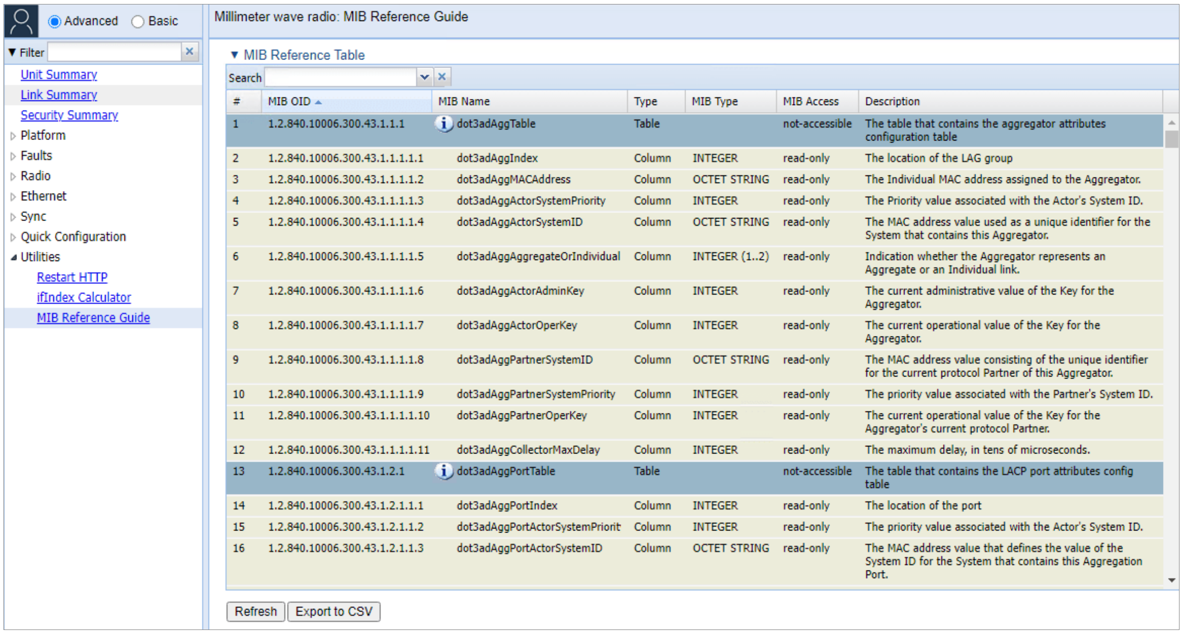
- If you have an ifIndex and you want to determine which hardware item in the unit it represents, enter the number in the **ifIndex number** field and click **Calculate Index to name**. A description of the object appears in the **Result** field.
- To determine the ifIndex of a hardware item in the unit, 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.

Displaying, Searching, and Saving a list of MIB Entities

To display a list of entities in the PTP 850 private MIB:

1. Select **Utilities** > **MIB Reference Guide**. The MIB Reference Guide page opens.

Figure 369 *MIB Reference Table Page*



Millimeter wave radio: MIB Reference Guide

MIB Reference Table

#	MIB OID	MIB Name	Type	MIB Type	MIB Access	Description
1	1.2.840.10006.300.43.1.1.1	dot3adAggTable	Table		not-accessible	The table that contains the aggregator attributes configuration table
2	1.2.840.10006.300.43.1.1.1.1.1	dot3adAggIndex	Column	INTEGER	read-only	The location of the LAG group
3	1.2.840.10006.300.43.1.1.1.1.2	dot3adAggMACAddress	Column	OCTET STRING	read-only	The Individual MAC address assigned to the Aggregator.
4	1.2.840.10006.300.43.1.1.1.1.3	dot3adAggActorSystemPriority	Column	INTEGER	read-only	The Priority value associated with the Actor's System ID.
5	1.2.840.10006.300.43.1.1.1.1.4	dot3adAggActorSystemID	Column	OCTET STRING	read-only	The MAC address value used as a unique identifier for the System that contains this Aggregator.
6	1.2.840.10006.300.43.1.1.1.1.5	dot3adAggAggregateOrIndividual	Column	INTEGER (1..2)	read-only	Indication whether the Aggregator represents an Aggregate or an Individual link.
7	1.2.840.10006.300.43.1.1.1.1.6	dot3adAggActorAdminKey	Column	INTEGER	read-only	The current administrative value of the Key for the Aggregator.
8	1.2.840.10006.300.43.1.1.1.1.7	dot3adAggActorOperKey	Column	INTEGER	read-only	The current operational value of the Key for the Aggregator.
9	1.2.840.10006.300.43.1.1.1.1.8	dot3adAggPartnerSystemID	Column	OCTET STRING	read-only	The MAC address value consisting of the unique identifier for the current protocol Partner of this Aggregator.
10	1.2.840.10006.300.43.1.1.1.1.9	dot3adAggPartnerSystemPriority	Column	INTEGER	read-only	The priority value associated with the Partner's System ID.
11	1.2.840.10006.300.43.1.1.1.1.10	dot3adAggPartnerOperKey	Column	INTEGER	read-only	The current operational value of the Key for the Aggregator's current protocol Partner.
12	1.2.840.10006.300.43.1.1.1.1.11	dot3adAggCollectorMaxDelay	Column	INTEGER	read-only	The maximum delay, in tens of microseconds.
13	1.2.840.10006.300.43.1.2.1	dot3adAggPortTable	Table		not-accessible	The table that contains the LACP port attributes config table
14	1.2.840.10006.300.43.1.2.1.1.1	dot3adAggPortIndex	Column	INTEGER	read-only	The location of the port
15	1.2.840.10006.300.43.1.2.1.1.2	dot3adAggPortActorSystemPriorit	Column	INTEGER	read-only	The priority value associated with the Actor's System ID.
16	1.2.840.10006.300.43.1.2.1.1.3	dot3adAggPortActorSystemID	Column	OCTET STRING	read-only	The MAC address value that defines the value of the System ID for the System that contains this Aggregation Port.

The MIB Reference Table is customized to the type of PTP 850 product you are using.

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 product or 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 **Export to CSV**.

Getting Started (CLI)

This section includes:

General (CLI)

Before a remote connection 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. See Changing the Management IP Address (CLI).

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

- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0

⚠ **Warning!**

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.

Establishing a Connection (CLI)

Connect the PTP 850 unit to a PC by means of a TP 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 operating the system. See Changing the Management IP Address (CLI) and Changing Your Password (CLI).

PTP 850 products only support strong ciphers for secure communication protocols such as SSH. In some cases, this may lead to a failure to connect if your SSH client is using old, less secure ciphers. If this occurs, it is recommended to update to a new client version using stronger ciphers.

For a list of supported ciphers, refer to *Annex A – Supported Ciphers for Secured Communication Protocols* in the Release Notes for the System Release version you are using.

PC Setup (CLI)

To obtain contact between the PC and the PTP 850 unit, it is necessary to configure 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. See Changing the Management IP Address (CLI) and Changing Your Password (CLI).

Logging On (CLI)

Use an SSH connection to manage the PTP 850 via CLI. You can use any standard SSH client, such as PuTTy or ZOC Terminal. You can also simply enter the command ssh <ip address> from the CMD window on your PC or laptop.

The default IP address of the unit is 192.168.1.1. Establish an SSH connection to the unit using the default IP address. The command syntax is ssh[user@host[:port]]. Otherwise, the system automatically uses the system name as user. For example:

```
C:\Users\johndoe>ssh 192.168.1.1
giganet\johndoe@192168.1.1’s password:
```

For example:

login:

When you have connected to the unit, a login prompt appears. At the prompt, enter the default login user name: admin

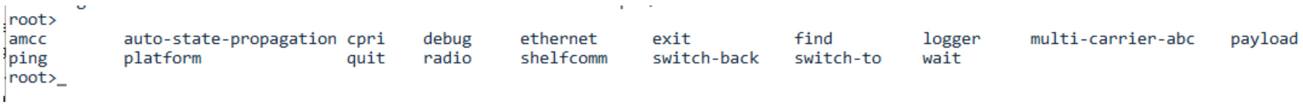
A password prompt appears. Enter the default password: admin

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>
```

General CLI Commands

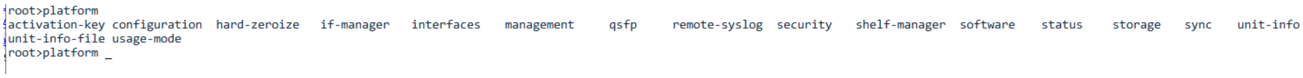
To display all command levels available from your current level, press <TAB> twice. For example, if you press <TAB> twice at the root level, the following is displayed:



```
root>
amcc        auto-state-propagation cpri    debug    ethernet    exit         find        logger      multi-carrier-abc    payload
ping        platform               quit    radio    shelfcomm   switch-back  switch-to   wait
root>_
```

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 hard-zeroize  if-manager  interfaces  management  qsfp  remote-syslog security  shelf-manager software  status  storage  sync  unit-info
unit-info-file usage-mode
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).

Changing Your Password (CLI)

It is recommended to change your default Admin password as soon as you have logged into the system. If the default Admin password is not changed within ten days after the first unit boot up, an alarm is raised:

- 5051 – 'admin' user password needs to be changed (Alarm)

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*.

See Configuring the Password Security Parameters (CLI).

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 850 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).

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

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 90 *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).
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 91 *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).

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
```

Enabling Dynamic IPv6 Addresses Via DHCPv6 (CLI)

Related Topics:

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

Optionally, you can configure the device to obtain its IPv6 address automatically from a DSCP server. To configure the device to IPv6 Automatic mode, use the following command:

```
root> platform management ip set ipv6-assignment dhcp
```

To set the device back to manual mode, use the following command:

```
root> platform management ip set ipv6-assignment manual
```

Once IPv6 Automatic mode is enabled, the previously configured IPv6 address is stored but not used by the device. It is used again if and when IPv6 Automatic mode is disabled. Therefore, before enabling IPv6 Automatic mode, you should record the IPv6 Link Local Address. To display the IPV6 Link Local Address, use the following command:

```
root> platform management ip show ipv6-status
```

This command also indicates whether the current mode is Automatic (DHCP) or Manual. In Manual mode, the IPv6 Address column is populated. It is not populated in Automatic (DHCP) mode.

```
IPv6 Link Local Address   IPv6 Default Gateway   IPv6 Address   IPv6 Prefix Length
===========================================================================
====
fe80::20a:25ff:fe5f:df74   fe80::4255:39ff:fe8d:afcd  ::          128
root>
```

After enabling IPv6 Automatic mode, you can use the IPv6 Link Local Address to re-connect to the device if the DHCPv6 server is unavailable. You can also use the device's IPv4 address.

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. To clear the DUID, use the following command:

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

Configuring DSCP/TC for Management (CLI)

In certain situations, 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. See Configuring Ingress Path Classification on a Logical Interface.
- For the management service, the CoS Mode must be set to Preserve-SP-COS-Decision. See Configuring a Service’s CoS Mode and Default CoS (CLI).

To configure a DSCP value for management connections that use IPv4 protocol, use the following command:

```
root> platform management cos set dscp <0-63> ip-address-family ipv4
```

To configure a TC value for management connections that use IPv6 protocol, use the following command:

```
root> platform management cos set dscp <0-63> ip-address-family ipv6
```

To configure the same DCSP and TC value for management connections that use either IPv4 or IPv6 protocol, use the following command:

```
root> platform management cos set dscp <0-63>
```

To display DSCP value configured for management connections that use IPv4 protocol, use the following command:

```
root> platform management cos show ip-address-family ipv4
```

To display TC value configured for management connections that use IPv6 protocol, use the following command:

```
root> platform management cos show ip-address-family ipv6
```

To display both the DSCP and the TC values configured for management connections, use the following command:

```
root> platform management cos show
```

Configuring the Activation Key (CLI)

This section includes:

- Viewing the Activation Key Status Parameters (CLI)
- Entering the Activation Key (CLI)
- Activating Demo Mode (CLI)
- Activation Key Reclaim (CLI)
- Displaying a List of Activation-Key-Enabled Features (CLI)

Note

For an explanation of Activation Keys, see Activation Key Overview.

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 information
```

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.

Activating Demo Mode (CLI)

To activate demo mode, enter the following command in root view:

```
root> platform activation-key set demo admin enable
```

To display the current status of demo mode, enter the following command in root view:

```
root> platform activation-key show demo status
```

Activation Key Reclaim (CLI)

If it is necessary to deactivate an PTP 850 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 850 unit. To display the Validation Number, enter the following command in root view:

```
root> platform activation-key show all
```

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
```

Setting the Time and Date (Optional) (CLI)

Related Topics:

- Configuring NTP (CLI)

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 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 92 *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
```

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 93 *Daylight Savings Time CLI Parameters*

Parameter	Input Type	Permitted Values	Description
month	Number	1 - 12	This parameter operates according to the selected Policy, as described above. The default value is 1 (January).
day	Number	1 – 31	This parameter operates according to the selected Policy, as described above. The default value is 1.
time			The Time at which DST begins, in the format 00:00. The default value is 02:00 (2:00 AM).
day-of-week	Variable	sun mon tue wed thu fri sat	This parameter operates according to the selected Policy, as described above. The default value is sun.
offset	Number	0 – 23	The required offset, in hours, for Daylight Savings Time. Only positive offset is supported.
start-date-month	Number	1 – 12	The month when Daylight Savings Time begins.
start-date-day	Number	1 – 31	The date in the month when Daylight Savings Time begins.
end-date-month	Number	1 – 12	The month when Daylight Savings Time ends.
end-date-day	Number	1 – 31	The date in the month when Daylight Savings Time ends.

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
root>
```

Enabling the Interfaces (CLI)

By default:

- Ethernet traffic interfaces are disabled and must be manually enabled.
- The Ethernet management interface is enabled.
- Radio interfaces are enabled.

Note

For PTP 850EX, Ethernet Slot 1, Ports 2, 3, and 4 are supported. Management Slot 1 Port 1 is also supported for management.

For PTP 850EX, support for traffic with the Management port is planned for future release.

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 display the status of all the interfaces in the unit, enter the following command in root view:

```
root> platform if-manager show interfaces
```

Table 94 *Interface Configuration CLI Parameters*

Parameter	Input Type	Permitted Values	Description
interface-type	Variable	ethernet radio management	ethernet – an Ethernet traffic interface. radio – a radio interface. management – the management interface
slot	Number	Ethernet: 1 Radio: 1	The slot on which the interface is located.
port	Number	Ethernet: • PTP 850EX: 2-4 Radio: • PTP 850EX: 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 3:

```
root> platform if-manager set interface-type ethernet slot 1 port 3 admin
up
```

The following command enables the 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
```

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.

Displaying Available MRMC Scripts (CLI)

To display all scripts that are available for a specific radio carrier in your unit:

For PTP 850EX, use the following command to enter radio view:

```
root> radio slot 1 port 1
```

Enter the following command in radio view:

```
radio[1/x]>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 95 *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:

```
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]>
```

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.

Notes

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.

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 96 *MRMC Script Assignation to Radio Carrier CLI Parameters*

Parameter	Input Type	Permitted Values	Description
script-id	Number	See Radio Profiles for PTP 850EX	The ID of the script you want to assign to the radio carrier.
modulation	Variable	adaptive fixed	Determines whether ACM is enabled (adaptive) or disabled (fixed).
max-profile	Number	See Radio Profiles for PTP 850EX	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	See Radio Profiles for PTP 850EX	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. If you do not include this parameter in the command, the minimum profile is set at the default value of 0.
profile	Number	See Radio Profiles for PTP 850EX	Fixed ACM mode only: The profile in which the system will operate

Notes

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, see Radio Profiles for PTP 850EX. Note that 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 an PTP 850EX:

```
radio[1/1]>mrmc set acm-support script-id 5703 modulation adaptive max-
profile 9 min-profile 3
```

Configuring the Radio Parameters (CLI)

In order to establish a radio link, you must:

- Enter radio view.
- 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**).

Entering Radio View (CLI)

To view and configure radio parameters, you must first enter the radio's view level in the CLI.

For PTP 850EX, use the following command to enter radio view:

```
root> radio slot 1 port 1
```

The following prompt appears:

```
radio[1/x]>
```

Muting and Unmuting a Radio (CLI)

To mute or unmute the radio, enter the following command in radio view:

```
radio[1/x]>rf mute set admin <on|off>
```

To configure a timed mute, enter the following command in radio view:

```
radio[1/x]>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. 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.

To display the mute status of a radio, enter the following command in radio view:

```
radio[1/x]>rf mute show status
```

The following command mutes the radio:

```
radio[1/x]>rf mute set admin on
```

The following command unmutes the radio:

```
radio[1/x]>rf mute set admin off
```

The following command configures a timed mute. This mute will automatically expire in 30 minutes.

```
radio[1/x]>rf mute set admin on-with-timer timeout-value 30
```

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/x]>rf set tx-frequency <0-4294967295> local-remote
<enable|disable>
```

The following command sets the TX frequency of the radio in an PTP 850EX device 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 850EX device 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
```

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, as described in Enabling ACM with Adaptive Transmit Power (CLI).

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/1]>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.

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.

```
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.

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).

Configuration Guide (CLI)

System Configurations (CLI)

This section lists the basic configurations, with links to configuration instructions.

Table 97 *System Configurations (CLI)*

Configuration	Supported Products	Link to Configuration Instructions
1+0	PTP 850EX	Configuring a 1+0 Link Using the Quick Configuration Wizard
Link Aggregation (LAG)	PTP 850EX	Configuring Link Aggregation (LAG) (CLI)

Configuring Multi-Carrier ABC (CLI)

This section includes:

- 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)

Multi-Carrier ABC Overview (CLI)

For an overview of Multi-Carrier ABC, see Multi-Carrier ABC Overview.

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
   multi-carrier-abc enhanced-group-id [1] slot [1]> exit
   ```

Removing Members from a Multi-Carrier ABC Group (CLI)

To remove members from a Multi-Carrier ABC group:

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. See Removing Members from a Multi-Carrier ABC Group (CLI).
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
   ```

Configuring XPIC (CLI)

For a general explanation of XPIC, see XPIC Overview.

Configuring the Radio Carriers for XPIC (CLI)

You must create and enable a single AMCC (XPIC) group on both sides of the link. The group must include both carriers on the device, with opposite polarizations.

Configuring the Radio Carriers for XPIC (CLI)

To configure the radio carriers for XPIC:

1. Configure the radio carriers 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).

Note

If you are not sure which scripts support XPIC, see Radio Profiles for PTP 850EX.

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 internal
   ```

   The following should appear:

   ```
   group_id 1, group_type xpic created
   ```

4. Attach the radio carriers to the AMCC (XPIC) group. To attach the radio carrier(s), 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
   xpic-group[1]>amcc attach slot 1 port 2

   Note

   It does not matter which interface is Member 1 and which interface is Member 2. In any event, port 1 is the vertical radio carrier and port 2 is the horizontal radio carrier.

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.

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 first 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
   ```

3. Remove the second radio carrier from the group. To remove the second radio carrier from the group, enter the following command in group view:

   ```
   xpic-group[1]>amcc detach slot 1 port 2
   ```

4. 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
   ```

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
```

The following is displayed:

```
group_id 1 group_type xpic group_sub_type internal
```

Alternatively, enter the following command in root view:

```
root>amcc show group_id 1 group_type xpic
```

The following is displayed:

```
group_id 1 group_type xpic group_sub_type internal
```

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 XPIC status of each carrier, enter the following command in group view:

```
xpic-group[1]>show members
```

The following output indicates that the status is normal:

```
slot 1 port 1 role n/a state Idle
slot 1 port 2 role n/a 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**. See Enabling the Interfaces (CLI).
- **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).

Configuring Link Aggregation (LAG) (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.

Note

LACP is planned for future release.

This section explains how to configure LAG and includes the following topics:

- Configuring a LAG Group (CLI)
- Configuring Multi-Homing (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)

Note

For an overview of LAG, see LAG Overview.

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>
```

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
```

Note

See LAG Overview for an explanation of Multi-Homing.

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
```

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 98 *LAG Group CLI Parameters*

Parameter	Input Type	Permitted Values	Description
lagid	Variable	lag1 lag2 lag3 lag4	The ID for the LAG.
slot	Number	Ethernet: 1 Radio: 1	
Port	Number	Ethernet: 2-4	The port number of the interface.

Parameter	Input Type	Permitted Values	Description
		Radio: 1 Management: 1	

The following commands create a LAG with the ID lag1. The LAG includes Ethernet interfaces 2 and 3 and radio interface 1. Multi Homing for ETH-BN and CSF messages is enabled on the LAG.

```
root> platform if-manager set interface-type ethernet slot 1 port 2 admin
down
root> ethernet interfaces eth slot 1 port 2
eth type eth [1/2]>
eth type eth [1/2]> static-lag add lagid lag1
eth type eth [1/2]> exit
root>
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> 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 2 admin
up
root> platform if-manager set interface-type ethernet slot 1 port 3 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>
```

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#[1/2]
Eth#[1/3]
Radio#[1/1]

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)      1/2
Member Port#(2)      1/3
Member Port#(3)      1/1

eth group [lag2]> operational state show
Port operational state: up.
eth group [lag2]>
```

The following commands remove port 3 from the LAG:

```
root> platform if-manager set interface-type ethernet slot 1 port 3 admin
down
root> ethernet interfaces group lag2
eth group [lag2]>
eth group [lag2]> port static-lag remove member interface eth slot 1 port
3
```

Enabling and Disabling the LAG Group Shutdown in Case of Degradation Event Option (CLI)

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]>
```

Unit Management (CLI)

This section includes:

Related topics:

- Setting the Time and Date (Optional) (CLI)
- Uploading Unit Info (CLI)
- Changing the Management IP Address (CLI)

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
```

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.

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[1/1]>remote-unit set ip-address <ipv4-address>
```

To display the remote radio’s IP Address, enter the following command in radio view:

```
radio[1/1]>remote-unit show ip-address
```

To set the remote radio’s subnet mask, enter the following command in radio view:

```
radio[1/1]>remote-unit set subnet-mask IP <subnet-mask>
```

To display the remote radio’s subnet mask, enter the following command in radio view:

```
radio[1/1]>remote-unit show subnet-mask
```

To set the remote radio’s default gateway, enter the following command in radio view:

```
radio[1/1]>remote-unit set default-gateway IP <ipv4-address>
```

To display the remote radio’s default gateway, enter the following command in radio view:

```
radio[1/1]>remote-unit show default-gateway
```

Table 99 *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
```

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[1/1]>remote-unit set ip-address-ipv6 <ipv6-address>
```

To display the remote radio’s IP Address, enter the following command in radio view:

```
radio[1/1]>remote-unit show ip-address-ipv6
```

To set the remote radio’s prefix length, enter the following command in radio view:

```
radio[1/1]>remote-unit set prefix-length <prefix-length >
```

To display the remote radio's prefix-length, enter the following command in radio view:

```
radio[1/1]>remote-unit show prefix-length
```

To set the remote radio's default gateway, enter the following command in radio view:

```
radio[1/1]>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[1/1]>remote-unit show default-gateway-ipv6
```

To configure the remote unit to obtain an IPv6 address automatically from a DHCPv6 server, enter the following command in radio view:

```
radio[x/x]>remote-unit set ipv6-assignment dhcp
```

To configure the remote unit for manual configuration of the IPv6 address, enter the following command in radio view:

```
radio[x/x]>remote-unit set ipv6-assignment manual
```

To display the current IPv6 address assignment mode, enter the following command in radio view:

```
radio[x/x]>remote-unit show ipv6-assignment
```

Note

By default, the IPv6 assignment mode is Manual. For further information, see Enabling Dynamic IPv6 Addresses Via DHCPv6 (CLI).

To display all the current IPv6 address parameters, enter the following command in radio view:

```
radio[x/x]>remote-unit show ipv6-status
```

For example:

```
radio [1/1]>remote-unit show ipv6-status
remote IPv6 assignment mode is: manual
remote IPv6 address is: 2001:1111:1111:1111:4a9:fe56:8be1:e6e5
remote IPv6 prefix length is: 64
remote IPv6 default gateway is: fe80::1e6a:7aff:fecb:6399
remote IPv6 link-local address is: fe80::3e4c:d0ff:feaf:5852
radio [1/1]>
```

When DHCP Automatic mode is configured, the link-local address can be used to re-connect to the device if the DHCPv6 server is unavailable.

Table 100 *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.

Parameter	Input Type	Permitted Values	Description
			should be different for each RADIUS client

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
```

Configuring SNMP (CLI)

PTP 850 supports SNMP v1, V2c, and v3. You can set community strings for access to PTP 850 units.

PTP 850 supports 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)

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>
```

To unblock or block SNMPv1 and SNMPv2 access, enter the following command in root view:

```
root> platform security protocols-control snmp v1v2-block set <set-block>
```

Table 101 *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.
read-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 v1v2-block set no
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
```

Configuring SNMPv3 (CLI)

The following commands are relevant for SNMPv3.

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 102 *SNMPv3 CLI Parameters*

Parameter	Input Type	Permitted Values	Description
v3-user-name	Text String		An SNMPv3 user name.
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	None DES AES	Defines the encryption (privacy) protocol to be used for this user.
v3-auth-algorithm	Variable	None SHA SHA256 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-256, 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 SHA256 v3-access-mode readWrite
```

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
```

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 103 *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 root> platform management ip set ip-address-family <IPv4|IPv6> is IPv4, enter the destination IPv4 address. Traps will be sent to this IP address.
manager-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	If the IP protocol selected in root> platform management ip set ip-address-family <IPv4|IPv6> 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	Enter the community string for the SNMP read community.

Parameter	Input Type	Permitted Values	Description
		community.	
manager-v3-user	Text String.	The name of a V3 user defined in the system.	If the SNMP Trap version selected in root> platform security protocols-control snmp version set <version> 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-ipv4 192.168.1.250 manager-ipv6 none
manager-port 164 manager-community private manager-v3-user user manager-
description text
root> platform security protocols-control snmp trap-manager heartbeat
manager-id 2 manager-heartbeat 12
```

Configuring the Internal Ports for FTP or SFTP (CLI)

By default, the following 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>
```

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.

Note

Make sure to use the original System Release software file, without any modification. Otherwise the software download process will fail.

This section includes:

- Viewing Current Software Versions (CLI)
- Configuring a Software Download (CLI)
- Downloading a Software Package (CLI)
- Installing and Upgrading Software (CLI)

Note

For an explanation of software management, see Upgrading the Software.

Viewing Current Software Versions (CLI)

To display the software version running and downloaded on the unit, enter the following command in root view:

```
root> platform software show versions
```

The following appears:

- **Downloaded Version** – The version, if any, that has been downloaded from the server but not yet installed. Upon installation and reset, this version will become the Running Version.
- **Installed Version** – The software version currently running on the unit.

To display more detailed information about software component versions, enter the following command in root view:

```
root> platform software show versions all
```

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 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 software upgrade. For details, see Installing and Configuring an FTP or SFTP Server.

Note

For SFTP downloads, be aware that only certain ciphers are supported. For a list of supported ciphers, refer to Annex A – Supported Ciphers for Secured Communication Protocols in the Release Notes for the product and System Release version you are using.

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 root> platform management ip set ip-address-family <IPv4|IPv6> 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 root> platform management ip set ip-address-family <IPv4|IPv6> 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 104 *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.
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. 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
```

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
```

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:

Note

- 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
  ```

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.

Importing and exporting configuration files can be done using HTTP, HTTPS, FTP, or SFTP. However, import and export using HTTP or HTTPS must be performed using the Web EMS. See Backing Up and Restoring Configurations.

Configuration files can only be copied between units of the same type, i.e., PTP 850EX to PTP 850EX.

> **Note**
>
> You can also write CLI scripts that will automatically execute a series of commands when the configuration file is restored. For information, see Editing CLI Scripts (CLI).

This section includes:

- 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)

> **Note**
>
> For an overview of configuration management, see Backing Up and Restoring Configurations.

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 root> platform management ip set ip-address-family <IPv4|IPv6> 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 root> platform management ip set ip-address-family <IPv4|IPv6> 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 105 *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 "//".
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
```

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>
```

To enhance unit security, you can configure the unit to exclude security configurations from configuration backup files. To configure this parameter, use the following command.

```
root> platform security general import-export set admin <enable|disable>
```

Use *disable* to exclude security configurations from configuration backup files, and *enable* to include security configurations in configuration backup files. The default setting is *enable*.

Figure 370 *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
```

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 (CLI) and Backing up and Exporting a Configuration File (CLI).

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 106 *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
```

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 command is executed. During initialization following the reset, execution of the CLI script continues from the following command.

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.

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
```

Resetting the Remote Unit (CLI)

To initiate a hard (cold) 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.

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 107 *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
```

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>
```

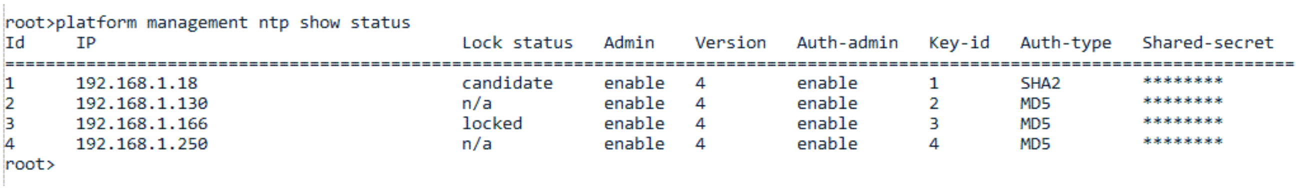
To display the current configuration of all the defined NTP servers, enter the following command in root view:

```
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:

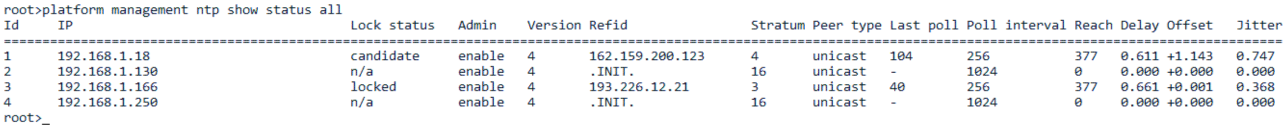
```
root> platform management ntp show status all
```

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 NTP Status Parameters.



```
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 108 *NTP CLI Parameters*

Parameter	Input Type	Permitted Values	Description
index	Number	1-4	Determines the NTP server being configured. You can configure up to four NTP servers.
admin	Variable	enable disable	Enter **enable** or **disable** to enable or disable the NTP server.
authentication	Variable	enable disable	Enter **enable** or **disable** to enable or disable NTP authentication. By default, NTP authentication is disabled.
key	Number	1-65535	Only necessary if you are enabling NTP authentication. The key identifier as included in the client requests and identifies the shared secret the client is using for message authentication.
auth-type	Variable	md5 sha1 sha2-256	Only necessary if you are enabling NTP authentication. The message authentication code type for NTP authentication. The default value is sha1.
secret	Number	Depends on the auth-type: • md5 – 8-32 characters • sha1	Only necessary if you are enabling NTP authentication. The shared secret for NTP authentication.

Parameter	Input Type	Permitted Values	Description
		(default) – 8-40 characters - sha2-256 – 8-64 characters	
ipv4	Dotted decimal format.	Any valid IPv4 address.	Enter the IP address of the NTP server.
ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	Enter the IP address of the NTP server.
ntp-version	Variable	ntpv3 ntpv4	Enter the NTP version you want to use. NTP v4 provides interoperability with NTP v3 and with SNTP.

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
```

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:

```
System information:
card-name : PTP 850
Subtype : 0x000002F0
part number :
serial number :
company name : Cambium Networks Ltd.
product name : PTP 850
product description : All outdoor system
```

Displaying SFP DDM and Inventory Information (CLI)

Static and dynamic monitoring is available for all SFP, SFP+, and SFP28 modules used on PTP 850EX devices.

Dynamic monitoring (DDM) PMs are also available.

Note

DDM parameters are not relevant for electrical SFPs.

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.

These alarms are based on thresholds defined by the SFP module vendor, which are static. They also display the actual RX or TX values as of the time when the alarm was raised, which are dynamic. The dynamic values are not changed as long as the alarm is still raised. They are only updated if the alarm is cleared, then raised again.

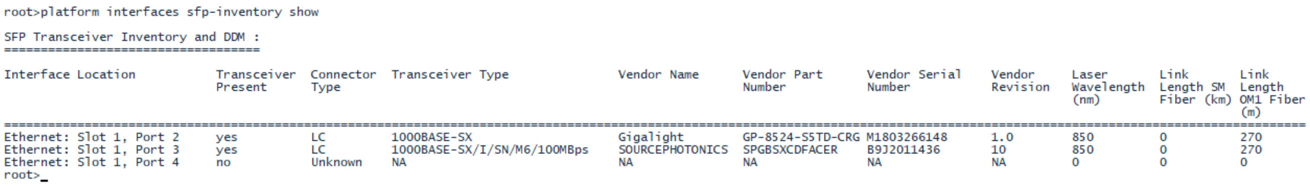
If there is no signal on the interface, a Loss of Carrier alarm (LOC) is raised, and this alarm masks the DDM alarms.

Displaying Static Information about an SFP Module (CLI)

To display static information about an SFP module, 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  Connector  Transceiver Type                Vendor Name      Vendor Part      Vendor Serial    Vendor     Laser       Link       Link
                             Present      Type                                                        Number           Number           Revision   Wavelength  Length SM  Length
                                                                                                                                                   (nm)        Fiber (km) OM1 Fiber
                                                                                                                                                                          (m)
====================================================================================================================================================================================
Ethernet: Slot 1, Port 2     yes          LC         1000BASE-SX                     Gigalight        GP-8524-S5TD-CRG M1803266148      1.0        850         0          270
Ethernet: Slot 1, Port 3     yes          LC         1000BASE-SX/I/SN/M6/100MBps     SOURCEPHOTONICS  SPGBSXCDFACER    B9J2011436       10         850         0          270
Ethernet: Slot 1, Port 4     no           Unknown    NA                              NA               NA               NA               NA         0           0          0
root>_
```

Table 109 *SFP Inventory Parameters (CLI) (PTP 850EX)*

Parameter	Description
Transceiver Present	Indicates whether an SFP module is attached to the interface.
Connector Type	Always displays LC.
transceiver Type	Displays a description of the SFP module.
Vendor Name	Displays the name of the SFP's vendor.
Vendor Part Number	Displays the vendor's part number for the SFP module.
Vendor Serial	Displays the vendor's serial number for the SFP module.

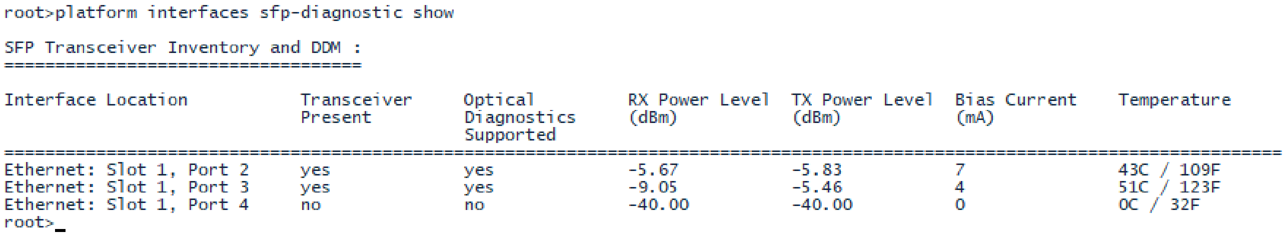
Parameter	Description
Number	
Vendor Revision	Displays the revision number of the serial number provided by the vendor for the SFP module.
Laser Wavelength (nm)	Display’s the SFP module’s laser wavelength. For CSFP modules, two wavelengths are displayed. This parameters is not relevant for copper SFPs.
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 (m)	The maximum length of the cable (in meters) for OM3 multi-mode fiber cables.
Optical Diagnostics Supported	Displays whether the SFP module supports DDM monitoring. For modules that do not support DDM monitoring, the parameters described in SFP Digital Diagnostic Monitoring (DDM) Parameters (CLI) (PTP 850EX) are not available.

Displaying Dynamic (DDM) Information about an SFP Module (CLI)

To display dynamic information about an SFP module, 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
                             Present         Diagnostics     (dBm)           (dBm)           (mA)
                                             Supported
==============================================================================================================================
Ethernet: Slot 1, Port 2     yes             yes             -5.67           -5.83           7               43C / 109F
Ethernet: Slot 1, Port 3     yes             yes             -9.05           -5.46           4               51C / 123F
Ethernet: Slot 1, Port 4     no              no              -40.00          -40.00          0               0C / 32F
root>_
```

Table 110 *SFP Digital Diagnostic Monitoring (DDM) Parameters (CLI) (PTP 850EX)*

Parameter	Description
Transceiver Present	Indicates whether an SFP module is attached to the interface.
RX Power Level (dBm)	The SFP module’s current RX power signal strength (in dBm).
TX Power Level (dBm)	The SFP module’s current TX power signal strength (in dBm).

Parameter	Description
Bias Current (mA)	The laser bias current of the SFP module (in mA)
Temperature	The current temperature of the SFP module (displayed in both C° and F°).

Note

Tx Power level DDM is not supported for QSFP (P5) – 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 module is inserted in the port.

Displaying DDM PMs about an SFP Module (CLI)

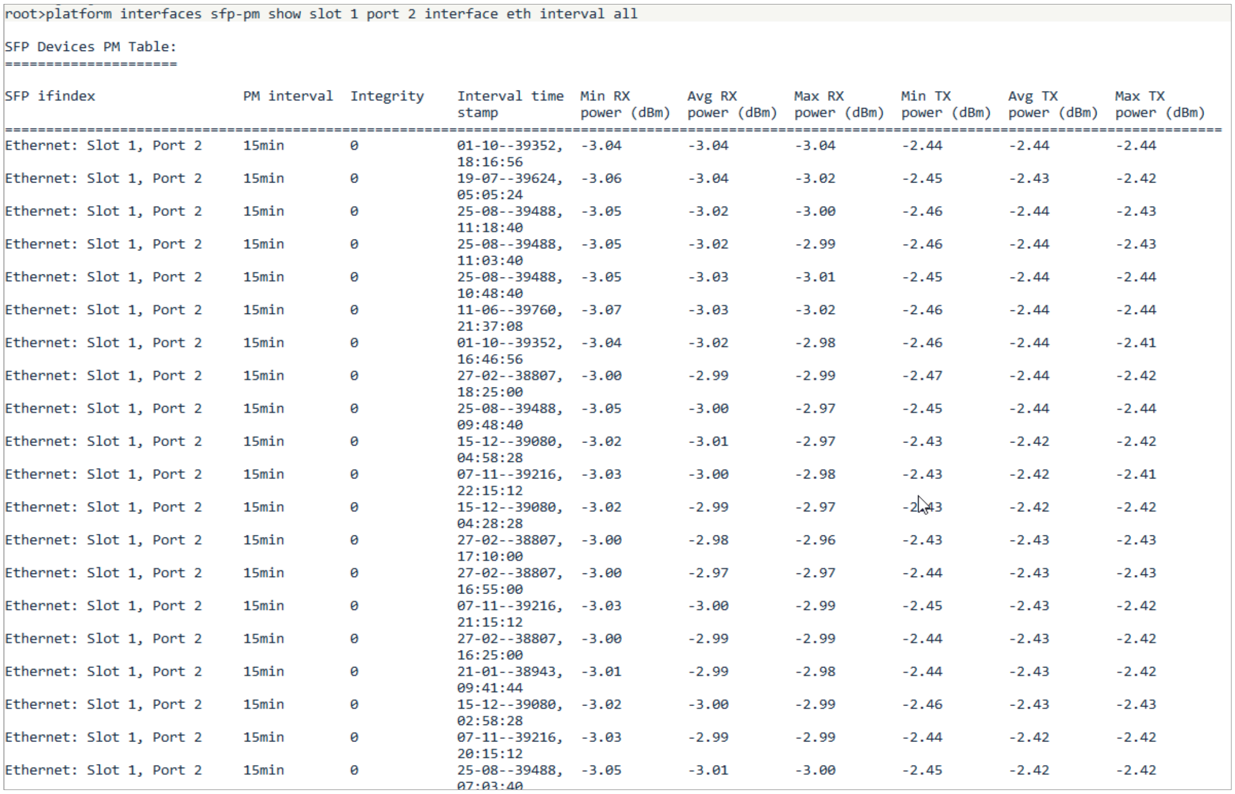
DDM PMs can be displayed for 15-minute and 24-hour intervals. For each interval, the following PMs are displayed:

- 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)

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 2 interface eth interval all

SFP Devices PM Table:
=====================

SFP ifindex                  PM interval  Integrity    Interval time Min RX       Avg RX       Max RX       Min TX       Avg TX       Max TX
                                                       stamp         power (dBm)  power (dBm)  power (dBm)  power (dBm)  power (dBm)  power (dBm)
====================================================================================================================================================
Ethernet: Slot 1, Port 2     15min        0            01-10--39352, -3.04        -3.04        -3.04        -2.44        -2.44        -2.44
                                                       18:16:56
Ethernet: Slot 1, Port 2     15min        0            19-07--39624, -3.06        -3.04        -3.02        -2.45        -2.43        -2.42
                                                       05:05:24
Ethernet: Slot 1, Port 2     15min        0            25-08--39488, -3.05        -3.02        -3.00        -2.46        -2.44        -2.43
                                                       11:18:40
Ethernet: Slot 1, Port 2     15min        0            25-08--39488, -3.05        -3.02        -2.99        -2.46        -2.44        -2.43
                                                       11:03:40
Ethernet: Slot 1, Port 2     15min        0            25-08--39488, -3.05        -3.03        -3.01        -2.45        -2.44        -2.44
                                                       10:48:40
Ethernet: Slot 1, Port 2     15min        0            11-06--39760, -3.07        -3.03        -3.02        -2.46        -2.44        -2.44
                                                       21:37:08
Ethernet: Slot 1, Port 2     15min        0            01-10--39352, -3.04        -3.02        -2.98        -2.46        -2.44        -2.41
                                                       16:46:56
Ethernet: Slot 1, Port 2     15min        0            27-02--38807, -3.00        -2.99        -2.99        -2.47        -2.44        -2.42
                                                       18:25:00
Ethernet: Slot 1, Port 2     15min        0            25-08--39488, -3.05        -3.00        -2.97        -2.45        -2.44        -2.44
                                                       09:48:40
Ethernet: Slot 1, Port 2     15min        0            15-12--39080, -3.02        -3.01        -2.97        -2.43        -2.42        -2.42
                                                       04:58:28
Ethernet: Slot 1, Port 2     15min        0            07-11--39216, -3.03        -3.00        -2.98        -2.43        -2.42        -2.41
                                                       22:15:12
Ethernet: Slot 1, Port 2     15min        0            15-12--39080, -3.02        -2.99        -2.97        -2.43        -2.42        -2.42
                                                       04:28:28
Ethernet: Slot 1, Port 2     15min        0            27-02--38807, -3.00        -2.98        -2.96        -2.43        -2.43        -2.43
                                                       17:10:00
Ethernet: Slot 1, Port 2     15min        0            27-02--38807, -3.00        -2.97        -2.97        -2.44        -2.43        -2.43
                                                       16:55:00
Ethernet: Slot 1, Port 2     15min        0            07-11--39216, -3.03        -3.00        -2.99        -2.45        -2.43        -2.42
                                                       21:15:12
Ethernet: Slot 1, Port 2     15min        0            27-02--38807, -3.00        -2.99        -2.99        -2.44        -2.43        -2.42
                                                       16:25:00
Ethernet: Slot 1, Port 2     15min        0            21-01--38943, -3.01        -2.99        -2.98        -2.44        -2.43        -2.42
                                                       09:41:44
Ethernet: Slot 1, Port 2     15min        0            15-12--39080, -3.02        -3.00        -2.99        -2.46        -2.43        -2.43
                                                       02:58:28
Ethernet: Slot 1, Port 2     15min        0            07-11--39216, -3.03        -2.99        -2.99        -2.44        -2.42        -2.42
                                                       20:15:12
Ethernet: Slot 1, Port 2     15min        0            25-08--39488, -3.05        -3.01        -3.00        -2.45        -2.42        -2.42
                                                       07:03:40
```

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.

Radio Configuration (CLI)

This section includes:

- Viewing and Configuring the Remote Radio Parameters (CLI)
- Configuring ATPC and ATPC Override Timer (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 Link Aggregation (LAG) (CLI)

Note

To view and configure radio parameters, you must first enter the radio's view level in the CLI. For details, refer to Entering Radio View (CLI).

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)

Displaying Communication Status with the Remote Radio (CLI)

To display the communication status with the remote radio, enter the following command in radio view:

```
radio[1/1]>remote-unit communication status show
```

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
```

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 111 *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. 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 with a timeout of 1 hour:

```
radio[1/1]>remote-unit mute set admin on-with-timer timeout-value 60
```

The following command mutes the remote radio with no timeout:

```
radio[1/1]>remote-unit mute set admin on
```

The following command unmutes the remote radio:

```
radio[1/1]>remote-unit mute set admin off
```

Displaying the Remote Radio’s RX Level (CLI)

To display the remote radio’s RX level, enter the following command in radio view:

```
radio[1/1]>remote-unit show rx-level
```

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[1/1]>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[1/1]>remote-unit show tx-level
```

Table 112 *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[1/1]>remote-unit set tx-level 10
```

Configuring Remote ATPC (CLI)

To set the RX reference level for ATPC on the remote radio, enter the following command in radio view:

```
radio[1/1]>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[1/1]>remote-unit atpc show ref-level
```

Table 113 *Remote Radio ATPC CLI Parameters*

Parameter	Input Type	Permitted Values	Description
ref-level	Number	-70 - -30	The RX reference level for the ATPC mechanism.

The following command sets the ATPC RX reference level of the remote radio to -55:

```
radio[1/1]>remote-unit atpc set ref-level -55
```

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[1/1]>remote-unit show most-severe-alarm
```

Configuring ATPC and ATPC Override Timer (CLI)

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 Redundancy, the ATPC override state is propagated to the standby unit in the event of switchover.

Notes

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[1/1]>atpc set admin <admin>
```

To display whether or not ATPC is enabled, enter the following command in radio view:

```
radio[1/1]>atpc show admin
```

To set the RX reference level for ATPC, enter the following command in radio view

```
radio[1/1]>atpc set rx-level atpc_ref_rx_level <rx-level>
```

Note

It is recommended to set the ATPC Reference RX Level to a value that is 10 dB better than the RSL threshold for the maximum ACM profile configured for the radio, in order to account for normal fluctuations in the link quality.

To display the RX reference level for ATPC, enter the following command in radio view:

```
radio[1/1]>atpc show rx-level
```

To set an ATPC override timer, enter the following command in radio view:

```
radio[1/1]>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[1/1]>atpc override set admin <override admin>
```

To display whether or not ATPC override is enabled, enter the following command in radio view:

```
radio[1/1]>atpc override show admin
```

To display the ATPC override timeout, enter the following command in radio view:

```
radio[1/1]>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[1/1]>atpc set override-tx-level <override-tx-level>
```

To display the ATPC override TX power, enter the following command in radio view:

```
radio[1/1]>atpc show override tx-level
```

To display the current ATPC override state, enter the following command in radio view:

```
radio[1/1]>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[1/x]>atpc set override-cancel
```

Table 114 *Radio ATPC CLI Parameters*

Parameter	Input Type	Permitted Values	Description
admin	Variable	enable disable	Enables or disables ATPC mode.
rx-level	Number	-70 - -30	The RSL reference level for the ATPC mechanism. When ATPC is enabled, it adjusts the TX power dynamically to preserve this RSL level.
timeout	Number	0-1800	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.
override admin	Variable	enable disable	Enables or disables ATPC override.

Parameter	Input Type	Permitted Values	Description
override-tx-level	Number	-50 - 50	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 radio type.

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[1/x]>atpc set admin enable
radio[1/x]>atpc set rx-level atpc_ref_rx_level -55
radio[1/x]>atpc set override timeout 900
radio[1/x]>atpc override set admin enable
radio[1/x]> atpc set override-tx-level 18
```

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)
- Displaying Traffic PMs (CLI)

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[1/x]>modem show status
```

The following is a sample output of the modem show status command:

```
MSE[db]: -99.00
  Defective Blocks count: 0
  Raw Defective Blocks count: 0
  Current Tx profile: 0
  Current Tx QAM: 2
  Current Tx rate(Kbps): 0
  Current Rx profile: 0
  Current Rx QAM: 2
  Current Rx rate(Kbps): 47535
```

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[1/1]>modem clear counters
```

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 [1/x]>framer pm-aggregate show interval 15min
```

The following is a partial sample output of the framer pm-aggregate show interval 15min command:

```
radio [x/x]>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 [x/x]>
```

To display modem BER PMs in daily intervals, enter the following command in radio view:

```
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 [x/x]>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 [x/x]>
```

Table 115 *Aggregate PMs (CLI)*

Parameter	Description
Interval	The number of the interval: 1-29 for daily PM reports, and 1-95 for 15-minute PM reports, plus an additional interval with the index “0”, which represents the interval currently in progress.
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.
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.

Displaying BER Level and Configuring BER Parameters (CLI)

To display the current BER level, enter the following command in radio view:

```
radio [1/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 unit 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 in radio view:

```
radio [1/x]>modem excessive-ber set threshold <threshold>
```

To display the excessive BER threshold, enter the following command in radio view:

```
radio [1/x]>modem excessive-ber show threshold
```

Table 116 *Excessive BER CLI Parameters*

Parameter	Input Type	Permitted Values	Description
admin	Variable	enable disable	Enables or disables propagation of excessive BER as a fault.

Parameter	Input Type	Permitted Values	Description
threshold	Variable	1e-3 1e-4 1e-5 1e-6 1e-7 1e-8 1e-9 1e-10	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 [x/x]>modem excessive-ber set threshold 1e-5
```

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 in radio view:

```
radio [1/x]>rf pm-rsl set threshold1 <threshold1> threshold2 <threshold2>
```

Table 117 *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 [x/x]>rf pm-rsl set threshold1 -30 threshold2 -60
```

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 in radio view:

```
radio [1/x]>rf pm-tsl set threshold -15
```

Table 118 *TSL Thresholds CLI Parameters*

Parameter	Input Type	Permitted Values	Description
threshold	Number	-10 - 50	The TSL threshold (dBm).

The following command sets the TSL threshold to 10 dBm:

```
radio [x/x]>rf pm-tsl set threshold 10
```

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.

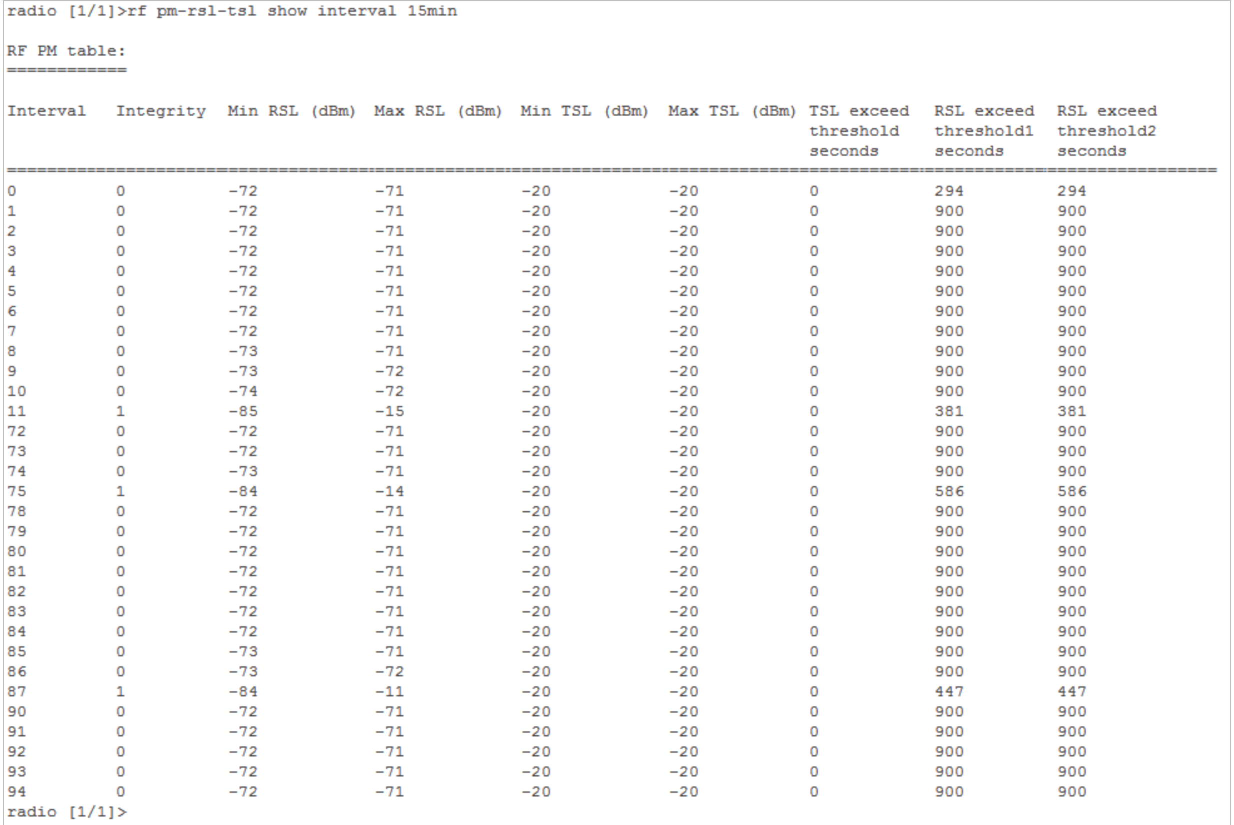
To display RSL and TSL PMs in 15-minute intervals, enter the following command in radio view:

```
radio [1/x]>rf pm-rsl-tsl show interval 15min
```

To display RSL and TSL PMs in daily intervals, enter the following command in radio view:

```
radio [1/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 119 *RSL and TSL PMs (CLI)*

Parameter	Description
Interval	The number of the interval: 1-29 for daily PM reports, and 1-95 for 15-minute PM reports, plus an additional interval with the index “0”, which represents the interval currently in progress.
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
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).

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 in radio view:

```
radio [1/x]>modem signal-degrade set threshold 1e-7
```

To display the Signal Degrade BER threshold, enter the following command in radio view:

```
radio [1/x]>modem signal-degrade show threshold
```

Table 120 *Signal Level Threshold CLI Parameters*

Parameter	Input Type	Permitted Values	Description
threshold	Variable	1e -6 1e -7 1e -8 1e -9 1e -10 1e-11 1e-12 1e-13 1e-14 1e-15	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 [1/x]>modem signal-degrade set threshold 1e-7
```

Configuring the MSE Thresholds and Displaying the MSE PMs (CLI)

To configure the MSE (Mean Square Error) threshold, enter the following command in radio view:

```
radio [1/x]>modem set mse-exceed threshold <threshold>
```

To display the currently configured MSE threshold, enter the following command in radio view:

```
radio [1/x]>modem show threshold-mse-exceed
```

Table 121 *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 in radio view:

```
radio [1/x]>modem pm-mse show interval 15min
```

The following is a partial sample output of the modem pm-mse show interval 15min command:

```
radio [x/x]>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 [1/x]>
```

To display MSE (Mean Square Error) PMs in daily intervals, enter the following command in radio view:

```
radio [1/x]>modem pm-mse show interval 24hr
```

The following is sample output of the modem pm-mse show interval 24hr command:

```
radio [x/x]>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 [1/x]>modem
```

Table 122 *MSE PMs (CLI)*

Parameter	Description
Interval	The number of the interval: 1-29 for daily PM reports, and 1-95 for 15-minute PM reports, plus an additional interval with the index “0”, which represents the interval currently in progress.
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 [1/x]>modem set mse-exceed threshold -30
```

Configuring the XPI Thresholds and Displaying the XPI PMs (CLI)

> **Note**
>
> For PTP 850EX, XPIC is planned for future release.

To configure the modem XPI threshold for calculating XPI Exceed Threshold seconds, enter the following command in radio view:

```
radio[1/x]>modem set threshold-xpi-exceed threshold <threshold>
```

To display the currently configured XPI threshold, enter the following command in radio view:

```
radio[1/x]>modem show threshold-xpi-below
```

Table 123 *XPI Threshold CLI Parameters*

Parameter	Input Type	Permitted Values	Description
threshold	Number	0-99	The XPI threshold.

To display XPI PMs in 15-minute intervals, enter the following command in radio view:

```
radio[1/x]>modem pm-xpi show interval 15min
```

The following is a partial sample output of the modem pm-xpi show interval 15min command:

```
radio [1/x]>modem pm-xpi show interval 15min

Modem XPI PM Table:
===================

Interval  Integrity  Min XPI (dB)  Max XPI (dB)   XPI below
                           threshold
                           seconds
================================================================
1     1      55.00     0.00      0
2     1      55.00     0.00      0
3     1      55.00     0.00      0
4     1      55.00     0.00      0
5     1      55.00     0.00      0
6     1      55.00     0.00      0
7     1      55.00     0.00      0
8     1      55.00     0.00      0
9     1      55.00     0.00      0
10    1      55.00     0.00      0
11    1      55.00     0.00      0
12    1      55.00     0.00      0
13    1      55.00     0.00      0
14    1      55.00     0.00      0
15    1      55.00     0.00      0
16    1      55.00     0.00      0
17    1      55.00     0.00      0
18    1      55.00     0.00      0
19    1      55.00     0.00      0
20    1      55.00     0.00      0

radio [1/x]>
```

To display XPI PMs in daily intervals, enter the following command in radio view:

```
radio[1/x]>modem pm-xpi show interval 24hr
```

The following is a partial sample output of the modem pm-xpi show interval 24hr command:

```
radio [1/x]>modem pm-xpi show interval 24hr

Modem XPI PM Table:
===================

Interval  Integrity  Min XPI (dB)  Max XPI (dB)  XPI below
                           threshold
                           seconds
===============================================================
1     1      55.00     0.00      0
2     1      55.00     0.00      0
3     1      55.00     0.00      0
4     1      55.00     0.00      0
5     1      55.00     0.00      0
6     1      55.00     0.00      0
7     1      55.00     0.00      0
8     1      55.00     0.00      0
9     1      55.00     0.00      0
10    1      55.00     0.00      0
11    1      55.00     0.00      0
12    1      55.00     0.00      0
13    1      55.00     0.00      0
14    1      55.00     0.00      0
15    1      55.00     0.00      0
16    1      55.00     0.00      0
17    1      55.00     0.00      0
18    1      55.00     0.00      0
19    1      55.00     0.00      0
20    1      55.00     0.00      0

radio [x/x]>
```

Table 124 *XPI PMs (CLI)*

Parameter	Description
Interval	The number of the interval: 1-29 for daily PM reports, and 1-95 for 15-minute PM reports, plus an additional interval with the index “0”, which represents the interval currently in progress.
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[1/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 display the number of seconds each carrier operated at each ACM profile for these 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 [1/x]>mrmc pm-acm set threshold1 <threshold1> threshold2
<threshold2>
```

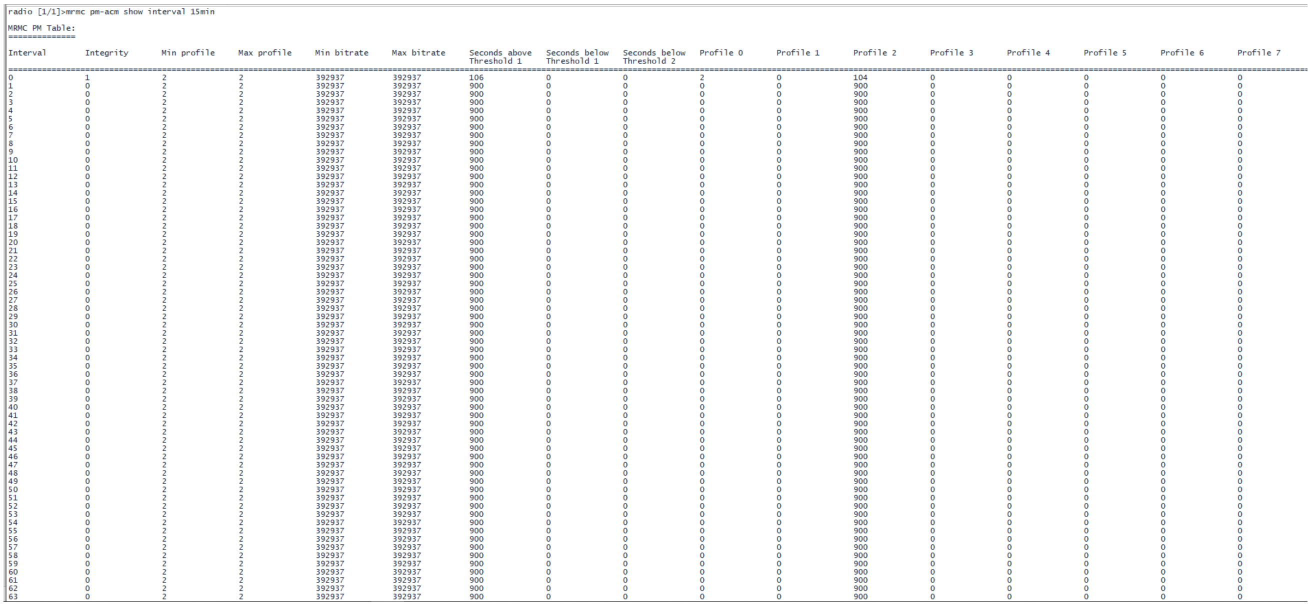
To display the ACM thresholds, enter the following command in radio view:

```
radio [1/x]>mrmc pm-acm get thresholds
```

To display ACM PMs in 15-minute intervals, enter the following command in radio view:

```
radio [1/x]>mrmc pm-acm show interval 15min
```

The following is a partial sample output of the modem pm-acm show interval 15min command:

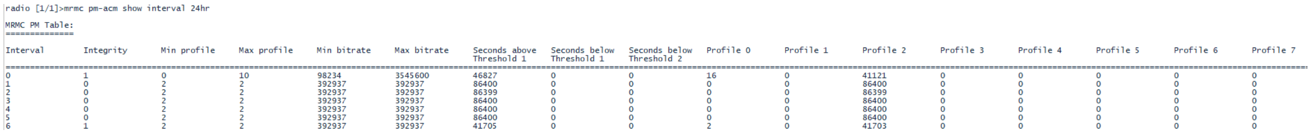


```
radio [1/1]>mrmc pm-acm show interval 15min

MRMC PM Table:
==============

Interval        Integrity       Min profile     Max profile     Min bitrate     Max bitrate     Seconds above   Seconds below   Seconds below   Profile 0       Profile 1       Profile 2       Profile 3       Profile 4       Profile 5       Profile 6       Profile 7
                                                                                                Threshold 1     Threshold 1     Threshold 2
==============================================================================================================================================================================================================================================================================
0               1               2               2               392937          392937          106             0               0               2               0               104             0               0               0               0               0
1               0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
2               0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
3               0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
4               0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
5               0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
6               0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
7               0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
8               0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
9               0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
10              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
11              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
12              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
13              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
14              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
15              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
16              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
17              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
18              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
19              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
20              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
21              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
22              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
23              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
24              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
25              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
26              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
27              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
28              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
29              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
30              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
31              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
32              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
33              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
34              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
35              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
36              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
37              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
38              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
39              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
40              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
41              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
42              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
43              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
44              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
45              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
46              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
47              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
48              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
49              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
50              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
51              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
52              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
53              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
54              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
55              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
56              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
57              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
58              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
59              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
60              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
61              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
62              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
63              0               2               2               392937          392937          900             0               0               0               0               900             0               0               0               0               0
```

To display ACM PMs in daily intervals, enter the following command in radio view:

```
radio [1/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   Seconds below   Seconds below   Profile 0       Profile 1       Profile 2       Profile 3       Profile 4       Profile 5       Profile 6       Profile 7
                                                                                                Threshold 1     Threshold 1     Threshold 2
==============================================================================================================================================================================================================================================================================
0               1               0               10              98234           3545600         46827           0               0               16              0               41121           0               0               0               0               0
1               0               2               2               392937          392937          86400           0               0               0               0               86400           0               0               0               0               0
2               0               2               2               392937          392937          86399           0               0               0               0               86399           0               0               0               0               0
3               0               2               2               392937          392937          86400           0               0               0               0               86400           0               0               0               0               0
4               0               2               2               392937          392937          86400           0               0               0               0               86400           0               0               0               0               0
5               0               2               2               392937          392937          86400           0               0               0               0               86400           0               0               0               0               0
6               1               2               2               392937          392937          41705           0               0               2               0               41703           0               0               0               0               0
```

Table 125 *ACM PMs and ACM Profile Thresholds (CLI)*

Parameter	Description
Interval	The number of the interval: 1-29 for daily PM reports, and 1-95 for 15-minute PM reports, plus an additional interval with the index “0”, which represents the interval currently in progress.
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.
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.

Displaying Traffic PMs (CLI)

This section includes:

- Displaying Capacity PMs (CLI)
- Displaying Throughput PMs (CLI)
- Displaying Utilization PMs and Configuring Utilization Thresholds (CLI)

Displaying Capacity PMs (CLI)

You can display capacity PMs for the 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.

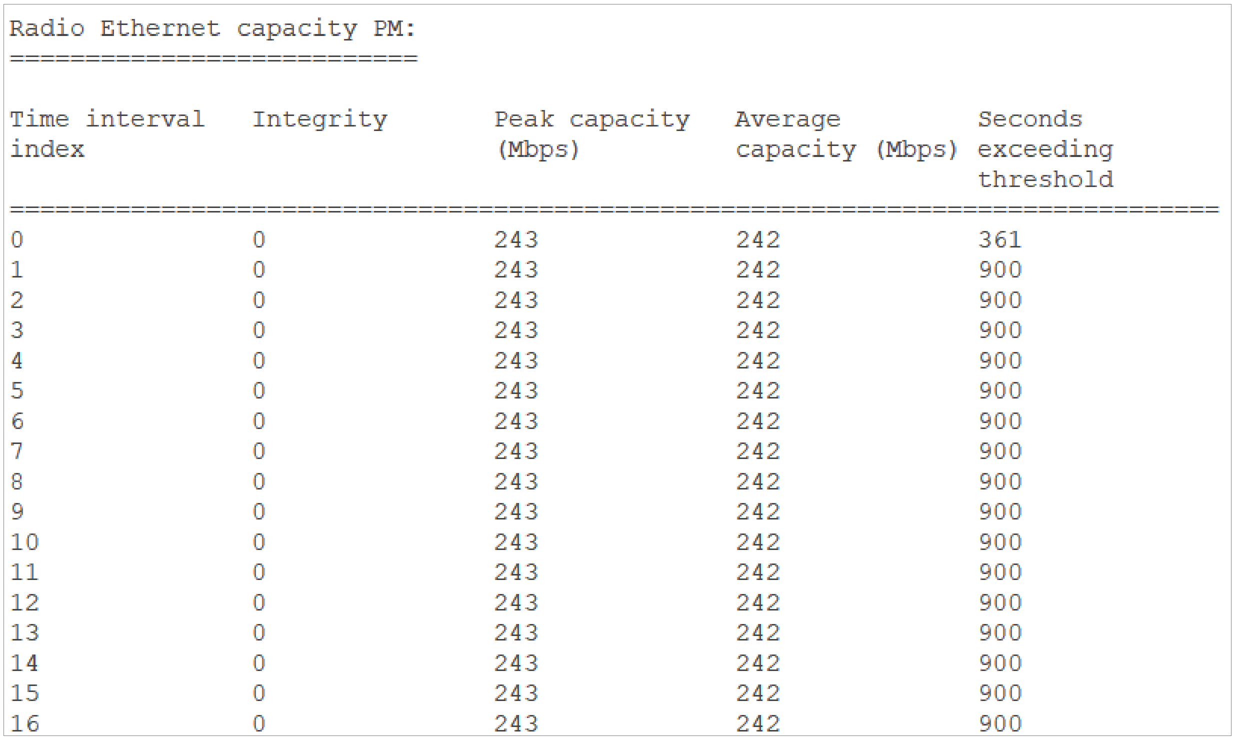
To display capacity PMs per radio in 15-minute intervals, enter the following command in radio view:

```
radio [1/X]> traffic capacity show pm interval 15min
```

To display capacity PMs per radio in daily intervals, enter the following command in radio view:

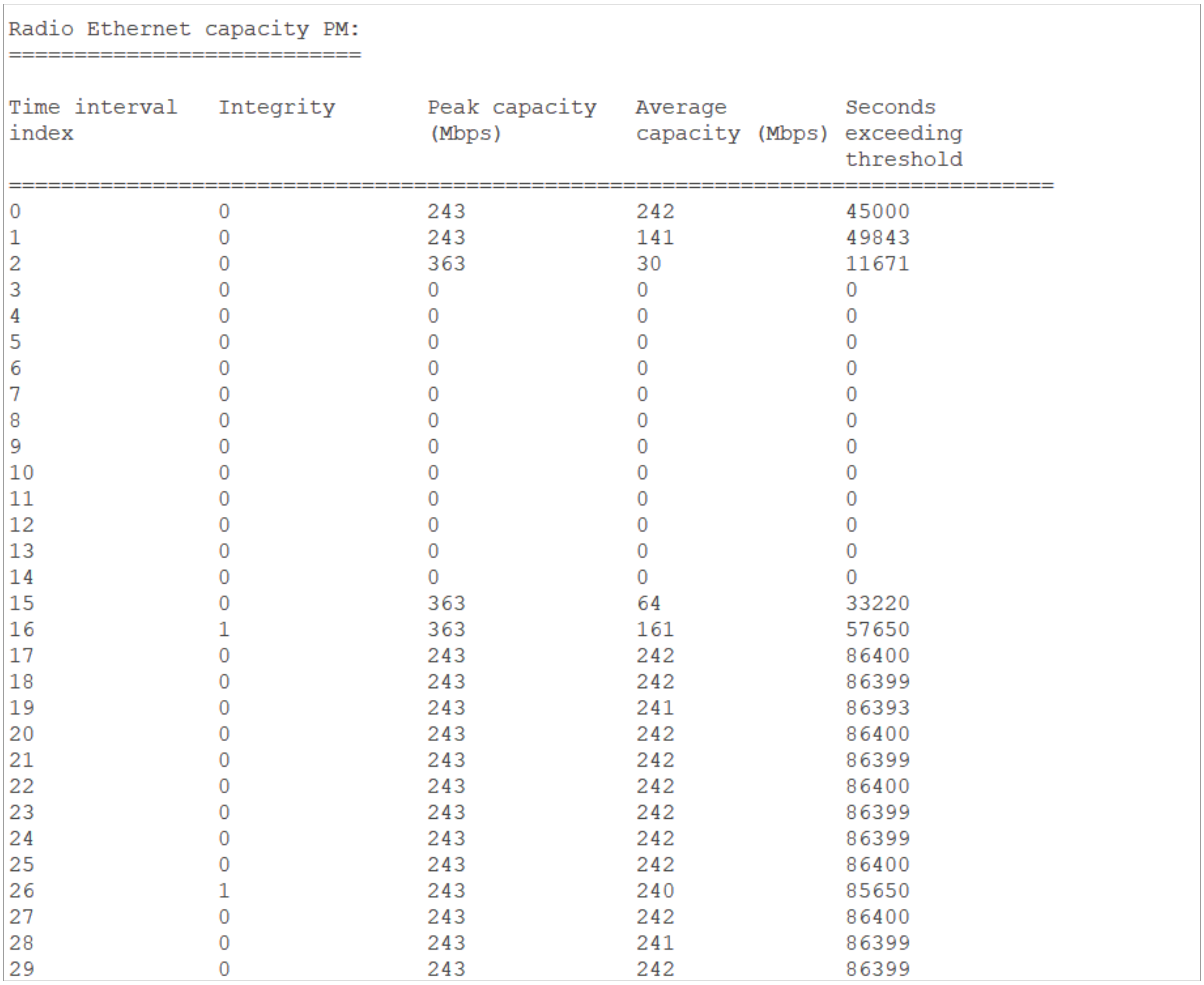
```
radio [1/x]> traffic capacity show pm interval 24hr
```

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 [1/x]> traffic capacity set pm-threshold <0-4294967295>
```

To display the threshold for capacity PMs, enter the following command in radio view:

```
radio [1/x]> traffic capacity show pm-threshold
```

Capacity/Throughput PMs (CLI) describes the capacity PMs.

Table 126 *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.

Parameter	Definition
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.

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.

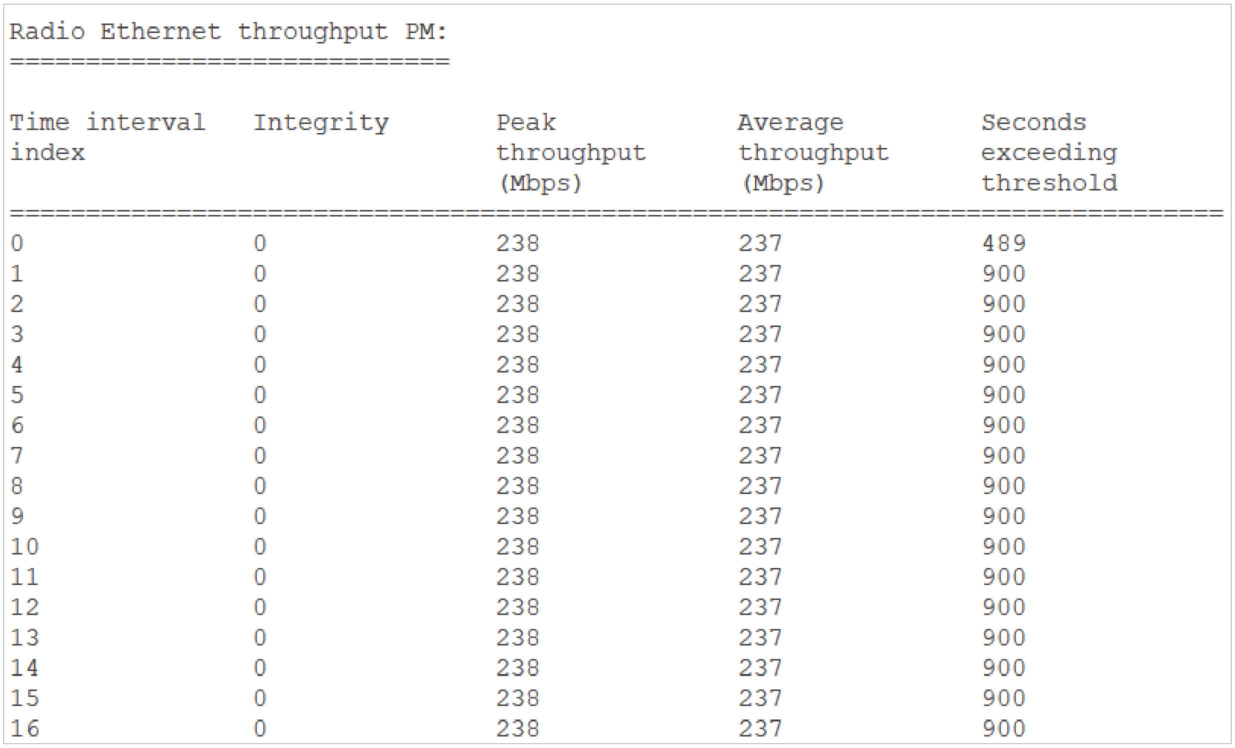
To display throughput PMs per radio in 15-minute intervals, enter the following command in radio view:

```
radio [1/x]> traffic throughput show pm interval 15min
```

To display throughput PMs per radio in daily intervals, enter the following command in radio view:

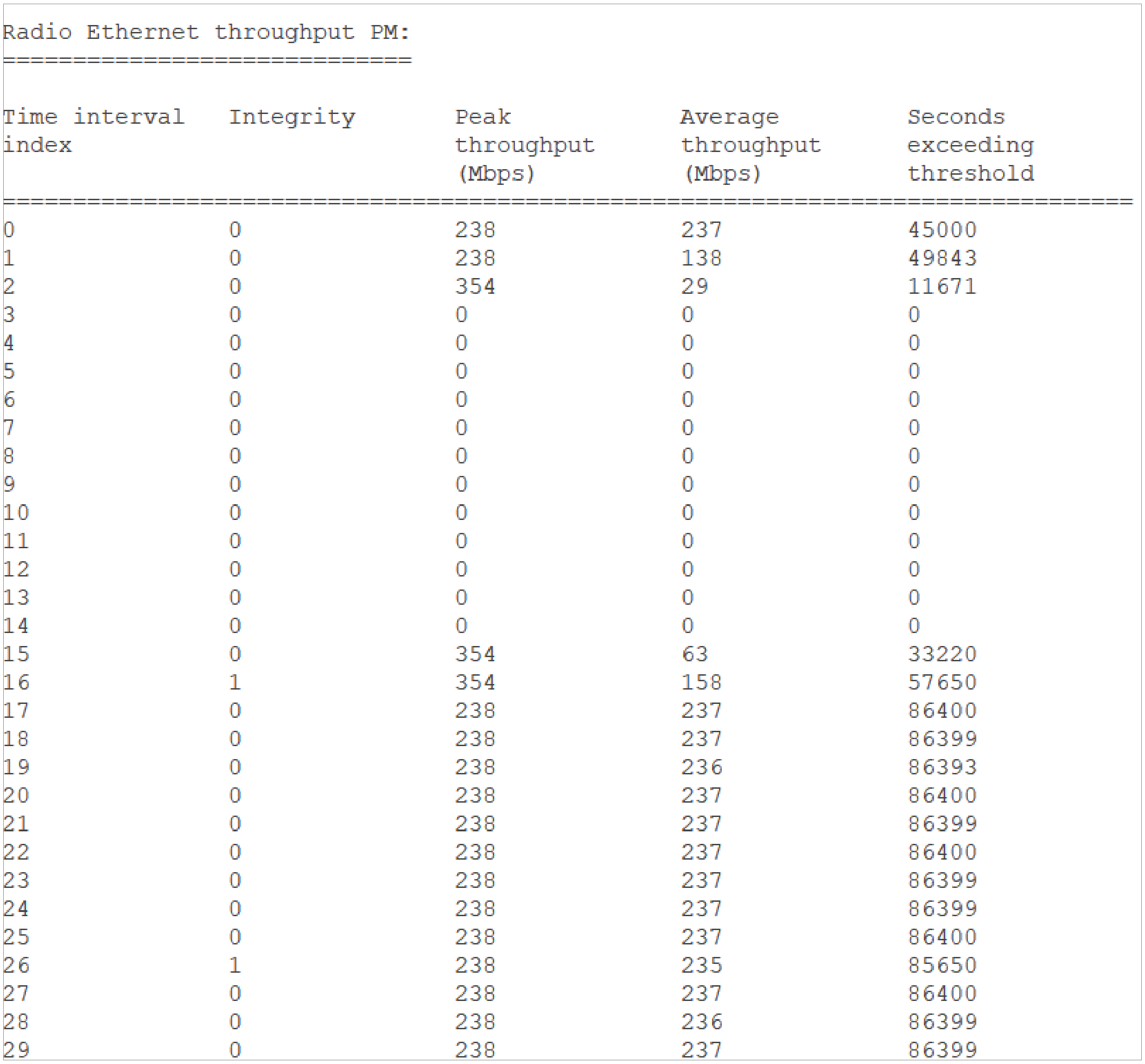
```
radio [1/x]> traffic throughput show pm interval 24hr
```

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 [1/x]> traffic throughput set pm-threshold <0-4294967295>
```

To display the threshold for capacity PMs, enter the following command in radio view:

```
    radio [1/x]> traffic throughput show pm-threshold
```

Throughput PMs (CLI) describes the throughput PMs.

Table 127 *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.

Parameter	Definition
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.

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.

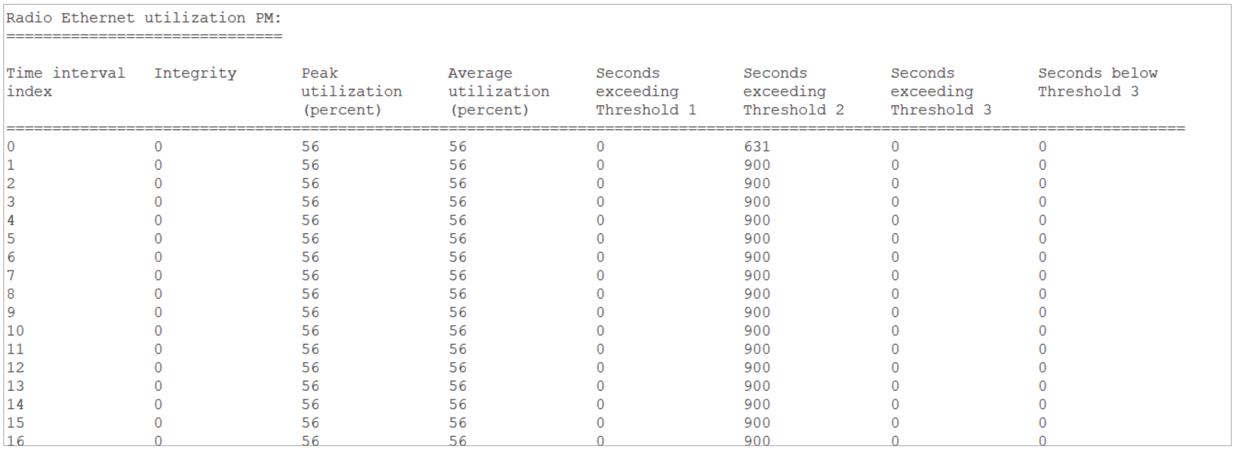
To display radio utilization PMs per radio or Multi-Carrier ABC group in 15-minute intervals, enter the following command in radio view:

```
radio [1/1]> 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:

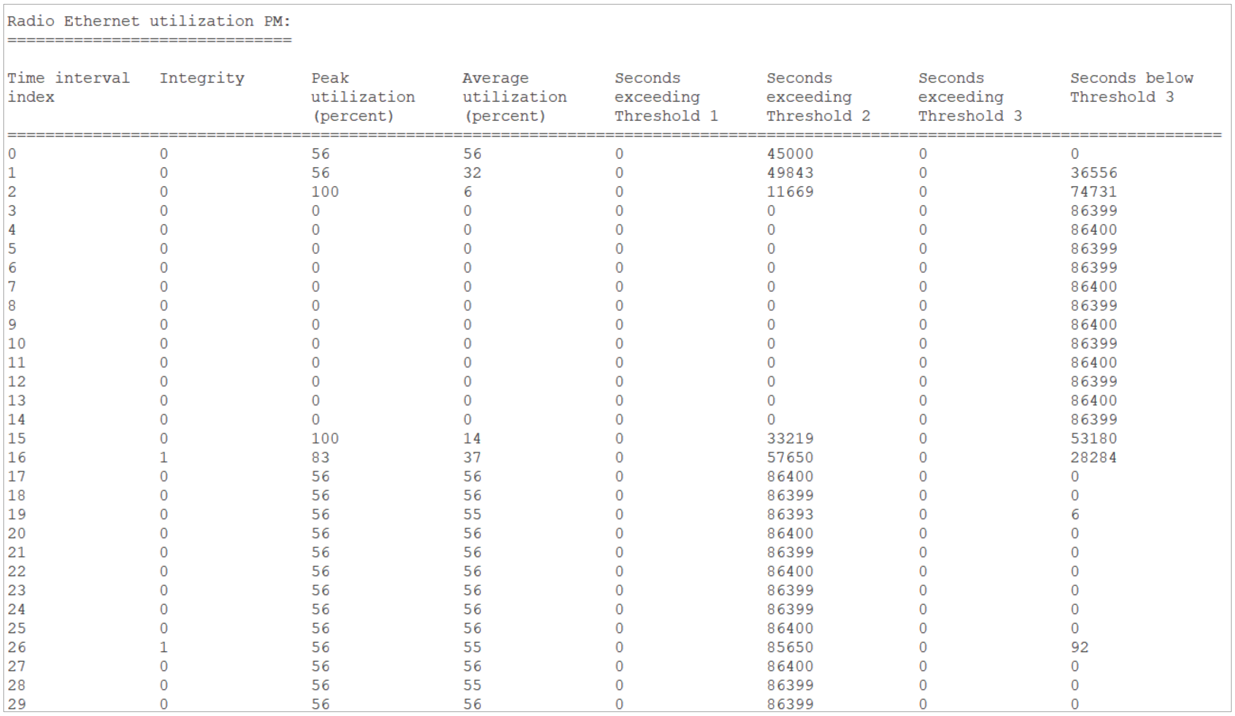
```
radio [1/1]> traffic utilization show pm interval 24hr
```

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 [1/1]> 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 [1/1]> traffic utilization show pm-thresholds
```

Utilization PMs (CLI) describes the utilization PMs.

Table 128 *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	Indicates the average utilization of the radio capacity for the selected radio or group

Parameter	Definition
utilization (percent)	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).

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:

- Quality of Service (QoS) (CLI)
- Configuring Link Aggregation (LAG) (CLI)
- Ethernet Protocols (CLI)

Configuring Ethernet Services (CLI)

This section includes:

- Defining Services (CLI)
- Configuring Service Points (CLI)
- Configuring the MAC Address Forwarding Table (CLI)

Note

For an overview of Ethernet services and provisioning guidelines, see Ethernet Services Overview and General Guidelines for Provisioning Ethernet Services.

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.

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 129 *Adding Ethernet Service CLI Parameters*

Parameter	Input Type	Permitted Values	Description
service type	Variable	p2p mp	Defines the service type: p2p - Point-to-Point

Parameter	Input Type	Permitted Values	Description
			mp – Multipoint
sid	Number	• Any unused value from 1-4095	A unique ID for the service. Once you have added the service, you cannot change the Service ID. Service ID 1025 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 <1-4095>
```

The following command enters service view for the service with Service ID 10:

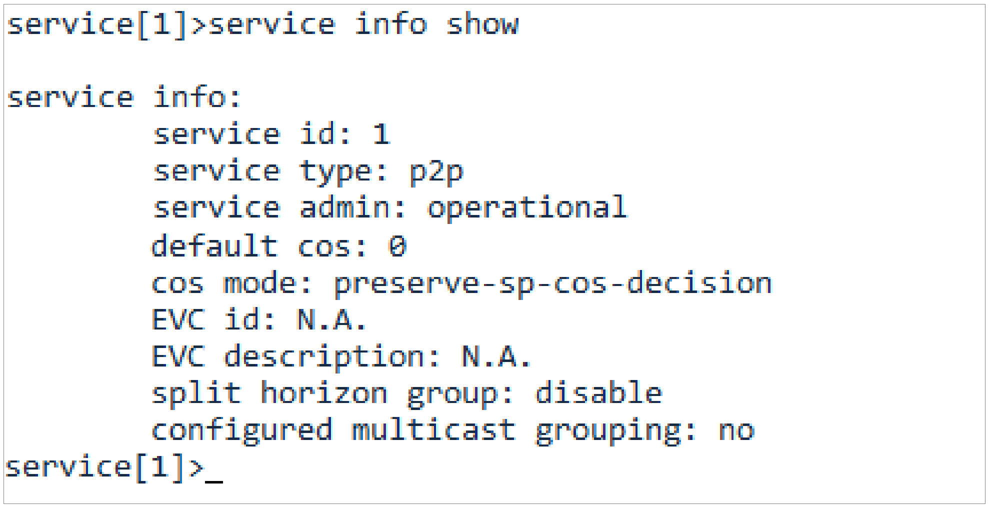
```
root> ethernet service sid 10
service[10]>
```

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:

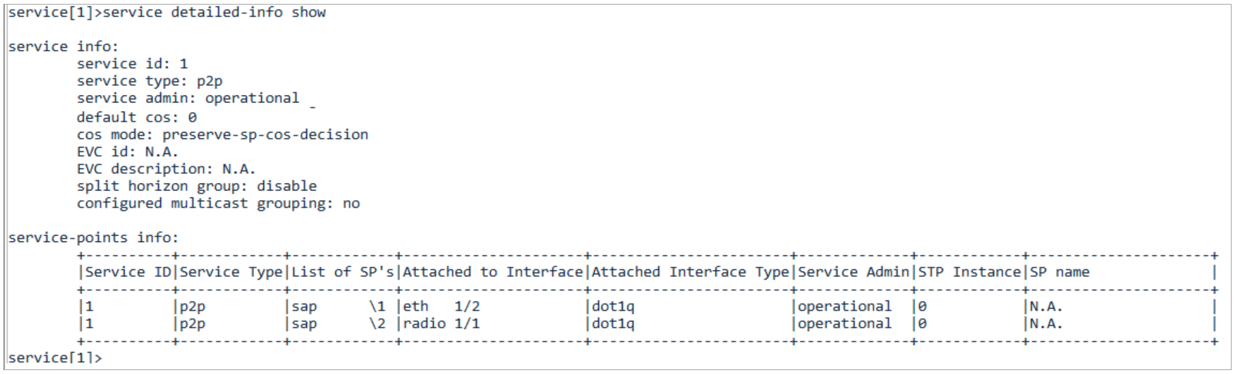


```
service[1]>service info show

service info:
        service id: 1
        service type: p2p
        service admin: operational
        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:

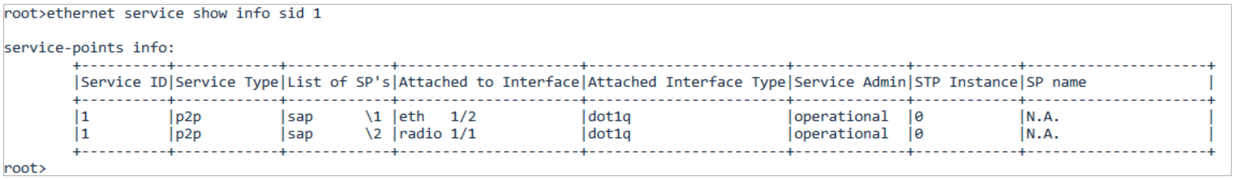


```
service[1]>service detailed-info show

service info:
        service id: 1
        service type: p2p
        service admin: operational
        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-points info:
        +----------+------------+------------+---------------------+-----------------------+-------------+------------+---------------------+
        |Service ID|Service Type|List of SP's|Attached to Interface|Attached Interface Type|Service Admin|STP Instance|SP name              |
        +----------+------------+------------+---------------------+-----------------------+-------------+------------+---------------------+
        |1         |p2p         |sap      \1 |eth    1/2           |dot1q                  |operational  |0           |N.A.                 |
        |1         |p2p         |sap      \2 |radio 1/1            |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 <1-4095>
```

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         |sap      \1 |eth    1/2           |dot1q                  |operational  |0           |N.A.                 |
        |1         |p2p         |sap      \2 |radio 1/1            |dot1q                  |operational  |0           |N.A.                 |
        +----------+------------+------------+---------------------+-----------------------+-------------+------------+---------------------+
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 130 *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 131 *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-

Parameter	Input Type	Permitted Values	Description
			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 132 *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 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 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 <1-4095>
```

Use the following command to delete a range of services:

```
root>ethernet service delete sid <1-4095> to <1-4095>
```

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
```

Configuring Service Points (CLI)

This section includes:

- Service Point Classification (CLI)
- Adding a Service Point (CLI)
- Configuring Service Point Ingress Attributes (CLI)
- Configuring Service Point Egress Attributes (CLI)
- Removing the Outer VLAN Tag on the Ingress Service Point (CLI)
- Displaying Service Point Attributes (CLI)
- Deleting a Service Point (CLI)

Note

For an explanation of service points, see Ethernet Service Points Overview.

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.

Legal Service Point – Interface Type Combinations per Interface – SAP and SNP and Legal Service Point – Interface Type Combinations per Interface – Pipe and MNG show which service point – Interface Type combinations can co-exist on the same interface.

Table 133 *Legal Service Point – Interface Type Combinations per Interface – SAP and SNP*

SP Type	SP Type Attached Interface Type	SAP 802.1q	Bundle-C	Bundle-S	All to One	Q in Q	SNP 802.1q	S-Tag
SAP	802.1q	Yes	Yes	No	No	No	No	No
	Bundle-C	Yes	Yes	No	No	No	No	No
	Bundle-S	No	No	Yes	No	Yes	No	No
	All to One	No	No	No	Only 1 All to One SP Allowed	No	No	No
	Q in Q	No	No	Yes	No	Yes	No	No
SNP	802.1q	No	No	No	No	No	Yes	No
	S-Tag	No	No	No	No	No	No	Yes
Pipe	802.1q	No	No	No	No	No	No	No
	S-Tag	No	No	No	No	No	No	No
MNG	802.1q	Yes	Yes	No	No	No	Yes	No
	Q in Q	No	No	Yes	No	Yes	No	No
	S-Tag	No	No	No	No	No	No	Yes

Table 134 *Legal Service Point – Interface Type Combinations per Interface – Pipe and MNG*

SP Type	SP Type Attached Interface Type	Pipe 802.1q	S-Tag	MNG 802.1q	Q in Q	S-Tag
SAP	802.1q	No	No	Yes	No	No
	Bundle-C	No	No	Yes	No	No
	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
Pipe	802.1q	Only one Pipe SP Allowed	No	Yes	No	No
	S-Tag	No	Only one Pipe	No	No	Yes

SP Type	SP Type Attached Interface Type	Pipe 802.1q	S-Tag	MNG 802.1q	Q in Q	S-Tag
			SP Allowed			
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.

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> slot <slot> port <port> sp-name <sp-name> service-
bundle-id <service-bundle-id>
```

To add a service point with an All-to-One interface type to a Multi-Carrier ABC group, 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>
group-on-slot enhanced-abc slot 1 group-id <1-4> 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> slot <slot> port <port> vlan <vlan> sp-name <sp-name>
service-bundle-id <service-bundle-id>
```

To add a service point with an Dot1q interface type to a Multi-Carrier ABC group, 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> group-
on-slot enhanced-abc slot 1 group-id <1-4> 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> 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 to a Multi-Carrier ABC group, 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> group-
on-slot enhanced-abc slot 1 group-id <1-4> 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> slot <slot> port <port> sp-name <sp-name> service-
bundle-id <service-bundle-id>
```

To add a service point with an Bundle-C interface type to a Multi-Carrier ABC group, 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>
group-on-slot enhanced-abc slot 1 group-id <1-4> 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> slot <slot> port <port> [outer-vlan <outer-
vlan>|vlan <vlan>] sp-name <sp-name> service-bundle-id <service-bundle-id>
```

To add a service point with an Bundle-S interface type to a Multi-Carrier ABC group, 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>
group-on-slot enhanced-abc slot 1 group-id <1-4> sp-name [outer-
vlan <outer-vlan>|vlan <vlan>] <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> 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 service point with a Q-in-Q interface type to a Multi-Carrier ABC group, 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> group-
on-slot enhanced-abc slot 1 group-id <1-4> 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> slot <slot> port <port> sp-name <sp-name> service-
bundle-id <service-bundle-id>
```

To add a Pipe service point to a Multi-Carrier ABC group, 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> group-
on-slot enhanced-abc slot 1 group-id <1-4> sp-name <sp-name> service-
bundle-id <service-bundle-id>
```

Table 135 *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.	This ID is unique within the service.

Parameter	Input Type	Permitted Values	Description
		1-30 for MNG services.	
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, use the group parameter instead of the interface parameter.
group	Variable	lag1 lag2 lag3 lag4	When you are defining the service point on a LAG (lag1 - lag4), use this parameter instead of the interface parameter to identify the group. The group must be defined before you add the service point. When group is used, the slot and port parameters should not be included.
slot	Number	Ethernet: 1 Radio: 1	
port	Number	Ethernet: • PTP 850EX: 2-4 Radio: • PTP 850EX: 1	The port or radio carrier on which the service point is located.
vlan	Number or Variable	1-4097	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	1-4097	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	1-4097	Defines the C-VLAN classified to the service point.

Parameter	Input Type	Permitted Values	Description
			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).
service-bundle-id	Number	1	This parameter is optional. The only available Service Bundle ID is 1.

The following command adds an SAP service point with Service Point ID 10 to Service 37 on an PTP 850EX, 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
1 port 1 vlan 100 sp-name Radio
```

The following command adds an SAP service point with Service Point ID 10 to Service 37 on an PTP 850EX, 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 1 port 1 sp-name "all-to-one"
```

The following command adds an SNP service point with Service Point ID 10 to Service 37 on an PTP 850EX, 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
1 port 1 vlan 100 sp-name Radio
```

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 Eth 3.

```
service[1]>sp add sp-type pipe int-type dot1q spid 1 interface eth slot 1
port 3 sp-name pipe_dot1q
```

The following commands create a Smart Pipe service between Eth 3 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 3 sp-name test1
service[10]>
service[10]>sp add sp-type pipe int-type s-tag spid 2 interface radio slot
1 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 136 *Enable/Disable Broadcast Frames 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 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 137 *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.
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. **Note:** For Bundle-S and Bundle-C service points, if Cos Overwrite Valid is set to True, the CoS and Color defined in the Attached VLAN page has priority over the interface decision, but not over a MAC DA match.
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 138 *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)
- 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)

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 139 *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
```

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 140 *C-VLAN 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.
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
```

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 141 *S-VLAN CoS Preservation CLI Parameters*

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for	The Service Point ID.

Parameter	Input Type	Permitted Values	Description
		MNG services.	
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
```

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 classify untagged frames 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 attach untagged spid <sp-id>
```

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 removed 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 142 *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	The C-VLAN at the beginning of the range of the VLAN Bundle.
to-vlan	Number	1-4094	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 classifies untagged frames to Service Point 1 in Service 37:

```
service[37]>sp bundle attach untagged spid 1
```

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
```

The following command removes untagged frames to Service Point 1 in Service 37:

```
service[37]>sp bundle remove untagged spid 1
```

Removing the Outer VLAN Tag on the Ingress Service Point (CLI)

The following command can be used to remove the outer VLAN tag on an ingress service point. This command should only be used in very specific instances.

```
service[x]>sp ingress-remove-outer-vlan set spid <1-32> admin
<enable|disable>
```

For example, the following commands remove the outer VLAN tag on Service Point ID 1 belonging to Service ID 1:

```
root>ethernet service sid 1
service[1]>sp ingress-remove-outer-vlan set spid 1 admin enable
```

To determine whether this command is active, enter the following command in service view:

```
service[x]>sp ingress-remove-outer-vlan show spid <1-32>
```

For example, enter the following commands to display the status of this command for Service Point ID 1 belonging to Service ID 1:

```
root>ethernet service sid 1
service[1]> sp ingress-remove-outer-vlan show spid 1
```

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 143 *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 144 *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
```

Configuring the MAC Address Forwarding Table (CLI)

This section includes:

- MAC Address Forwarding Table Overview (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)
- Flushing the MAC Address Forwarding Table (CLI)
- Enabling MAC Address Learning on a Service Point (CLI)

MAC Address Forwarding Table Overview (CLI)

The device can learn up to 32K Ethernet source MAC addresses. The size of the MAC address table is for the device as a whole, and is not configurable.

When a frame arrives via a specific service point, the learning mechanism checks the MAC forwarding table to determine whether that frame's source MAC address is known to the service. If the MAC address is not found, the learning mechanism adds it to the table under the specific service point.

In parallel with the learning process, the forwarding mechanism searches the service's MAC forwarding table for the frame's destination 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.

In addition to the dynamic learning mechanism, you can add static MAC addresses for static routing in each service.

You can manually clear all the dynamic entries from the MAC forwarding table. You can also delete static entries per service.

The system also provides an automatic flush process. An entry is erased from the table as a result of:

- The global aging time expires for the entry.
- Loss of carrier occurs on the interface with which the entry is associated.
- Resiliency protocols, such as MSTP or G.8032.

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 145 *MAC Address Forwarding Table Aging Time CLI Parameters*

Parameter	Input Type	Permitted Values	Description
time	Number	15 – 1649	The global aging time for the MAC address forwarding table, in seconds.

The following command sets the global aging time to 1500 seconds:

```
root> ethernet service learning-ageing-time set time 1500
```

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. 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 146 *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.

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
```

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
```

To display the MAC address forwarding table for the entire unit, enter the following command:

```
root> ethernet generalcfg mac-learning-table show
```

To display 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
```

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 147 *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
```

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)

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 148 *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.

For example, the following command sets the system S-VLAN ethertype to 0x88a8:

```
root> ethernet generalcfg ethertype set svlan-value 0x88a8
```

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
```

Configuring the MRU (CLI)

To define the global size (in bytes) of the Maximum Receive Unit (MRU), enter the following command in root view:

To display the system MRU, enter the following command in root view:

```
root> ethernet generalcfg mru set size <size>
root> ethernet generalcfg mru show
```

Table 149 *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.

For example, the following command sets the system MRU to 9612:

```
root> ethernet generalcfg mru set size 9612
```

S-VLAN Ethertype 0x8100 (CISCO Mode) (CLI)

When the S-VLAN Ethertype is set to 0x8100 (CISCO mode), another VLAN tag is added at the egress s-tag service point.

To remove this additional VLAN tag, the following commands can be used:

1. 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 by using the following command:

```
service[x]>sp ingress-remove-outer-vlan set spid <1-32> admin enable
```

For more information on usage of these command, see Removing the Outer VLAN Tag on the Ingress Service Point (CLI).

2. 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, use the following command:

```
service[x]>sp cvlan-preservation-mode set spid 1 mode disable
```

For more information on usage of these command, see Configuring C-VLAN Preservation (CLI).

Configuring Ethernet Interfaces (CLI)

Related Topics:

- Enabling the Interfaces (CLI)
- Configuring Ethernet Services (CLI)
- Quality of Service (QoS) (CLI)

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 on the physical interface level. Ethernet services, QoS, and OAM characteristics are configured on the logical interface level.

Note

When 25 Gbps ports are connected to third-party equipment:, the 25 Gbps ports on the third-party equipment must be configured to RS_FEC Clause 108. The RS_FEC Clause 108 configuration must be per the IEEE 802.3 standard for 25G SR and 25G L.

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 Media Type (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)

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:

```
root> ethernet interfaces group <group>
```

Table 150 *Entering Interface View CLI Parameters*

Parameter	Input Type	Permitted Values	Description
slot	Number	Ethernet: 1 Management: 1 Radio: 1	
port	Number	Ethernet: • PTP 850EX: 2-4 Radio: • PTP 850EX: 1	The port number of the interface.

Parameter	Input Type	Permitted Values	Description
group	Variable	lag1 lag2 lag3 lag4	To enter interface view for a LAG (lag1 - lag4), enter the group.

The following command enters interface view for Ethernet 3:

```
root> ethernet interfaces eth slot 1 port 3
```

The following prompt appears:

```
eth type eth [1/3]>
```

The following command enters interface view for radio interface 1:

```
root> ethernet interfaces radio slot 1 port 1
```

The following prompt appears:

```
radio [1/1]>
```

Note

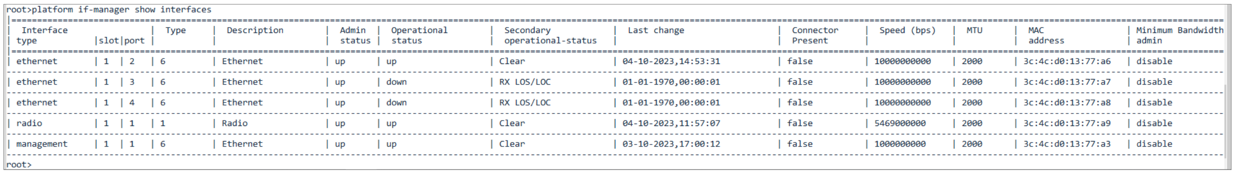
For simplicity, the examples in the following sections show the prompt for an Ethernet interface.

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  | 2   | 6        | Ethernet            | up     | up                | Clear                  | 04-10-2023,14:53:31         | false       | 10000000000   | 2000    | 3c:4c:d0:13:77:a6  | disable
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| ethernet    | 1  | 3   | 6        | Ethernet            | up     | down              | RX LOS/LOC             | 01-01-1970,00:00:01         | false       | 10000000000   | 2000    | 3c:4c:d0:13:77:a7  | disable
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| ethernet    | 1  | 4   | 6        | Ethernet            | up     | down              | RX LOS/LOC             | 01-01-1970,00:00:01         | false       | 10000000000   | 2000    | 3c:4c:d0:13:77:a8  | disable
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| radio       | 1  | 1   | 1        | Radio               | up     | up                | Clear                  | 04-10-2023,11:57:07         | false       | 5469000000    | 2000    | 3c:4c:d0:13:77:a9  | disable
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| management  | 1  | 1   | 6        | Ethernet            | up     | up                | Clear                  | 03-10-2023,17:00:12         | false       | 1000000000    | 2000    | 3c:4c:d0:13:77:a3  | disable
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
root>
```

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 3:

```
eth type eth [1/3]>summary show
```

The following command shows the operational state of Eth 3:

```
eth type eth [1/3]>operational state show
```

Configuring an Interface’s Media Type (CLI)

The Media Type attribute defines the physical interface Layer 1 media type. The Media Type for Ethernet interfaces must be sfp.

To configure an Ethernet interface’s Media Type, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>media-type state set <media type>
```

Table 151 *Interface Media Type CLI Parameters*

Parameter	Input Type	Permitted Values	Description
media-type	Variable	auto-type rj45 sfp	Select the physical interface layer 1 media type: **auto-type** – Only relevant for Ethernet interfaces. The system detects whether the optical or electrical port is being used. Auto-type can only be used when the interface speed is set to 1000 Mbps. **RJ45**– An electrical (RJ-45) Ethernet interface. **SFP**– An optical (SFP) Ethernet interface.

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 [1/x]>speed-and-duplex state set <speed-and-duplex state>
```

Table 152 *Interface Speed and Duplex State CLI Parameters*

Parameter	Input Type	Permitted Values	Description
speed-and-duplex state	Variable	'10hd' '10fd' '100hd' '100fd' '1000fd' ‘2500fd’ ‘10000fd’	This parameter sets the maximum speed and the duplex state of the interface. See Ethernet Port Speed and Auto Negotiation Options for available options per interface.

The following command sets Eth 2 to 1 Gbps, full duplex:

```
      eth type eth [1/1]>speed-and-duplex state set '1000fd'
```

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 [1/x]>autoneg state set <autoneg state>
```

Table 153 *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 available options per interface, see Ethernet Port Speed and Auto Negotiation Options.

The following command enables auto negotiation for Eth 3:

```
      eth type eth [1/3]>autoneg state set on
```

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 [1/x]>ifg set <ifg>
```

Table 154 *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 Eth 3 to 12:

```
      eth type eth [1/3]>ifg set 12
```

The following displays the currently configured ifg for GbE 1:

```
      eth type eth [1/3]>ifg get
```

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 [1/x]>preamble set <preamble>
```

Table 155 *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 Eth 3 to 8:

```
eth type eth [1/3]>preamble set 8
```

The following command displays the current preamble for Eth 3:

```
eth type eth [1/3]>preamble get
```

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 [1/x]>description set <description>
```

To delete a description, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>description delete
```

To display an interface's description, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>description show
```

Table 156 *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 Eth 3:

```
eth type eth [1/3]>description set Line
```

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. You can create multiple pairs using the same Monitored Interface and multiple Controlled Interfaces.

The Monitored Interface is a radio interface 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.

Note

A radio interface that belongs to a LAG group cannot be used as a 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. 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 <1-2> radio-port 1 llf-id <llf-id>
```

To configure propagation of a Multi-Carrier ABC group failure to an Ethernet port, use the following command:

```
root> auto-state-propagation add eth-port-to-multi-radio-group eth-slot 1
eth-port <eth-port> multi-radio-group <1-4> slot 1 type Enhanced <llf-id>
```

To enable automatic state propagation on an Ethernet port, determine whether remote interface failures are also propagated, enable ASP Management Safe 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>
```

Notes

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 157 *Automatic State Propagation to an Ethernet Port CLI Parameters*

Parameter	Input Type	Permitted Values	Description
eth-port	Number	2-4	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 Interface 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 with radio interface 2.
asp-admin	Variable	enable disable	Enables or disables automatic state propagation on the Ethernet interface.
remote-fault-	Variable	enable disable	Determines whether faults on the remote radio interface or group are propagated to the local Ethernet interface.

Parameter	Input Type	Permitted Values	Description
trigger-admin			
csf-mode-admin	Variable	enable disable	Enables or disables 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.
trigger-delay	Number	0-10000	Sets a trigger delay time, in milliseconds. When a triggering event takes place, the ASP mechanism does not propagate the event until this delay time has elapsed. By default, the trigger-delay is 0 (no delay time).

The following commands configure and enable automatic state propagation on an PTP 850EX to propagate faults from the radio interface to Ethernet ports 3 and 4. ASP Management Safe 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 3 radio-slot 1
radio-port 1 llf-id 1
root> auto-state-propagation add eth-port-to-radio eth-slot 1 eth-port 4 radio-slot 1
radio-port 1 llf-id 2
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 trigger-delay 100
root> auto-state-propagation configure eth-port eth-slot 1 eth-port 4 asp-admin
enable remote-fault-trigger-admin enable csf-mode-admin disable
```

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
```

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 (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:

- Displaying RMON Statistics (CLI)
- Configuring Ethernet Port PMs and PM Thresholds (CLI)
- Displaying Ethernet Port PMs (CLI)
- Clearing Ethernet Port PMs (CLI)

Displaying RMON Statistics (CLI)

PTP 850 stores and displays statistics in accordance with RMON and RMON2 standards.

Note

RMON counters per frame size are not available for individual radio interfaces and radio groups.

To display RMON statistics for a physical interface, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>rmon statistics show clear-on-read <clear-on-read>
layer-1 <layer-1>
```

Table 158 *Interface Statistics (RMON) 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 enter interface view for Eth 3, and clear the statistics after displaying them.

```
root> ethernet interfaces eth slot 1 port 3
```

eth type eth [1/3]>rmon statistics show clear-on-read yes layer-1 yes

The following commands enter interface view for the radio carrier, and display statistics for the interface, without clearing the statistics.

```
root> ethernet interfaces radio slot <1-2> port 1
```

eth type radio[1/1]>rmon statistics show clear-on-read no layer-1 no

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 [1/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 [1/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 [1/x]> pm show configuration
```

Table 159 *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 3, 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 3
eth type eth [1/3]>pm set admin enable
eth type eth [1/3]>pm set thresholds rx-layer1-rate-threshold 850000000
tx-layer1-rate-threshold 850000000
```

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 [1/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 [1/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 [1/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 [1/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 [1/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 [1/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 [1/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 [1/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 [1/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 [1/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 [1/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 [1/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 [1/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 [1/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 [1/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 [1/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 [1/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 [1/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 [1/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 [1/x]> pm show tx-bytes-layer2 interval 24hr
```

Table 160 *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.

Parameter	Definition
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.
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	The average rate of TX multicast packets per second for the measured time interval.

Parameter	Definition
Packets	
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).
Average TX Bytes in Layer2	The average TX rate, in bytes per second, for the measured time interval (excluding preamble and IFG).

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 [1/x]> pm clear-all
```

Quality of Service (QoS) (CLI)

This section includes:

- Configuring Classification (CLI)
- Configuring Policers (Rate Metering) (CLI)
- Configuring Marking (CLI)
- Configuring WRED (CLI)
- Configuring Egress Shaping (CLI)
- Configuring Scheduling (CLI)
- Displaying Egress PMs and Statistics (CLI)

Configuring Classification (CLI)

This section includes:

- Configuring VLAN Classification and Override (CLI)
- Configuring DSCP Classification (CLI)
- Configuring MPLS Classification (CLI)
- Configuring 802.1p Classification (CLI)
- Configuring a Default CoS (CLI)
- Configuring Ingress Path Classification on a Service Point (CLI)
- Configuring Ingress Path Classification on a Service (CLI)

Note

For an overview of PTP 850’s hierarchical classification mechanism, see Classification Overview and Configuring Ingress Path Classification on a Logical Interface.

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 [1/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 [1/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 [1/x]>vlan-cos-override delete outer-vlan-id <outer-vlan-id>
inner-vlan-id <inner-vlan-id>
```

Table 161 *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-idandinner-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 Eth 3 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 [1/3]>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 Eth 3 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 [1/3]>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 Eth 3, with S-VLAN ID 10 and C-VLAN ID 20:

```
eth type eth [1/3]>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 Eth 3:

```
eth type eth [1/3]>vlan-cos-override show all
```

The following command deletes the VLAN to CoS and Color override mapping for frames that ingress on Eth 3, with S-VLAN ID 10 and C-VLAN ID 20:

```
eth type eth [1/3]>vlan-cos-override delete outer-vlan-id 10 inner-vlan-id
20
```

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.

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 [1/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 [1/x]>classification show 802.1p state
```

Table 162 *Trust Mode for DSCP CLI Parameters*

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. • un-trust – The interface does not consider DSCP during classification.

The following command enables DSCP trust mode for Eth 3:

```
eth type eth [1/3]>classification set ip-dscp trust
```

The following command disables DSCP trust mode for Eth 3:

```
eth type eth [1/3]>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 42.

The following table shows the pre-defined entries in the DSCP classification table.

Table 163 *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
51	110011	DSCP_51	6	Green
52	110100	DSCP_52	6	Green
54	110110	DSCP_54	6	Green

DSCP	DSCP (bin)	Description	CoS (Configurable)	Color (Configurable)
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> dscp_description <description>
```

To add an entry to the DSCP classification table, enter the following command:

```
root> ethernet qos dscp-mapping-tbl add dscp <dscp> cos <cos> color
<color> dscp_description <description>
```

To delete an entry from the DSCP classification table, enter the following command:

```
root> ethernet qos dscp-mapping-tbl delete dscp <dscp>
```

To display the DSCP classification table, enter the following command:

```
root> ethernet qos dscp-mapping-tbl show
```

Table 164 *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.
description	String		A description of the entry.

The following command maps frames with DSCP value of 10 to CoS 1 and Green color, and changes the description of the table entry to AFC11:

```
root> ethernet qos dscp-mapping-tbl set dscp 10 cos 1 color green dscp_
description AFC11
```

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.

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>
```

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 165 *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 3:

```
eth type eth [1/3]>classification set mpls trust
```

The following command disables MPLS trust mode for GbE 3:

```
eth type eth [1/3]>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 166 *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 167 *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
```

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 168 *802.1p Trust Mode CLI Parameters*

Parameter	Input Type	Permitted Values	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). • un-trust – The interface does not consider 802.1 UP bits during classification.

The following command enables 802.1p trust mode for Eth 3:

```
eth type eth [1/3]>classification set 802.1p trust
```

The following command disables 802.1p trust mode for GbE 3:

```
eth type eth [1/3]>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 169 *C-VLAN 802.1 UP and CFI Bit Classification Table Default Values*

802.1 UP	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

802.1 UP	CFI	CoS (configurable)	Color (configurable)
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 170 *C-VLAN 802.1 UP and CFI Bit Classification Table CLI Parameters*

Parameter	Input Type	Permitted Values	Description
802.1p	Number	0 – 7	The User Priority (UP) bit to be mapped.
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	Green yellow	The Color assigned to 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 171 *S-VLAN 802.1 UP and DEI Bit Classification Table Default Values*

802.1 UP	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

802.1 UP	DEI	CoS (Configurable)	Color (Configurable)
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 172 *S-VLAN 802.1 UP and DEI Bit Classification Table CLI Parameters*

Parameter	Input Type	Permitted Values	Description
802.1p	Number	0 – 7	The User Priority (UP) bit to be mapped.
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	green yellow	The Color assigned to frames with the designated UP and CFI.

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 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 [1/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 [1/x]>classification show default-cos
```

Table 173 *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 Eth 3 as 7:

```
eth type eth [1/3]>classification set default-cos 7
```

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).

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).

Configuring Policers (Rate Metering) (CLI)

This section includes:

- 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)
- Attaching a Rate Meter (Policer) to a Service Point (CLI)
- Configuring the Line Compensation Value for a Rate Meter (Policer) (CLI)

Note

For an overview of Rate Metering (Policing), see Policer (Rate Metering) Overview.

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 174 *Rate Meter Profile CLI Parameters*

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 – 250	A unique ID for the rate meter (policer) profile.
cir	Number	0 – 25000000	The Committed Information Rate (CIR) for the policer, in kbps. If the value is 0, all incoming CIR traffic is dropped. The default value is 84.
cbs	Number	0 – 8192	The Committed Burst Rate (CBR) for the rate meter (policer), in Kbytes.
eir	Number	0 – 25000000	The Excess Information Rate (EIR) for the policer, in kbps. If the value is 0, all incoming EIR traffic is dropped. The default value is 84.
ebs	Number	0 – 8192	The Excess Burst Rate (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 kbps
- CBS – 5 Kbytes
- EIR – 64,000 kbps
- 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 kbps
- CBS – 5 Kbytes
- EIR – 128,000 kbps
- EBS – 5 Kbytes
- Color Aware mode
- Coupling Flag enabled

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
```

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
```

Attaching a Rate Meter (Policer) to an Interface (CLI)

On the logical interface level, you can assign rate meter (policer) profiles per frame type (unicast, unknown unicast, multicast, and broadcast).

This section includes:

- Assigning a Rate Meter (Policer) for Unicast Traffic (CLI)
- Assigning a Rate Meter (Policer) for Unknown Unicast Traffic (CLI)
- Assigning a Rate Meter (Policer) for Unknown Unicast Traffic (CLI)
- Assigning a Rate Meter (Policer) for Broadcast Traffic (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 [1/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 [1/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 [1/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 [1/x]>rate-meter unicast delete
```

Table 175 *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 Eth 3, and enables rate metering on the port:

```
eth type eth [1/3]>rate-meter unicast add capability admin-state enable
profile-id 1
```

The following command changes the rate meter (policer) profile for unicast traffic on Eth 7 to 4:

```
eth type eth [1/3]>rate-meter unicast edit admin-state enable profile-id 4
```

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 176 *Assigning Rate Meter for Unknown Unicast Traffic CLI Parameters*

Parameter	Input Type	Permitted Values	Description
admin-state	Variable	enable disable	Enables or disables rate metering on unknown 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 unknown unicast traffic on Eth 2, and enables rate metering on the port:

```
eth type eth [1/2]>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 [1/2]>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 [1/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 [1/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 [1/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 [1/x]>rate-meter multicast delete
```

Table 177 *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 Eth 3, and enables rate metering on the port.

```
eth type eth [1/3]>rate-meter multicast add capability admin-state enable
profile-id 1
```

The following command changes the rate meter (policer) profile for multicast traffic on Eth 3 to 4:

```
eth type eth [1/3]>rate-meter 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 [1/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 [1/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 [1/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 [1/x]>rate-meter broadcast delete
```

Table 178 *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 Eth 3, and enables rate metering on the port.

```
eth type eth [1/3]>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 3 to 4:

```
eth type eth [1/3]>rate-meter broadcast edit admin-state enable profile-id
4
```

Attaching a Rate Meter (Policer) to a Service Point (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 delete 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 delete spid <spid>
```

Table 179 *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.	The Service

Parameter	Input Type	Permitted Values	Description
		1-30 for MNG services.	Point ID.
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 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
```

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 [1/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 [1/x]>rate-meter-compensation-value get
```

Table 180 *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 Eth 3 to 20:

```
eth type eth [1/3]>rate-meter-compensation-value set 20
```

Configuring Marking (CLI)

This section includes:

- Configuring Marking Mode on a Service Point (CLI)
- Modifying the Marking Values (CLI)

Note

For a description of Marking, see Marking Overview.

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 181 *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.
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.

Parameter	Input Type	Permitted Values	Description
			For information about configuring CoS Preservation, refer to CoS Preservation and Modification on a Service Point (CLI).

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
```

Modifying the Marking Values (CLI)

The 802.1Q and 802.1AD User Priority (UP) Marking table enables you to modify the mapping of CoS and Color to UP bits and the mapping of Color to CFI/DEI bits. The mapping is implemented when Marking is enabled.

Table 182 *Marking Table for 802.1Q and 802.1AD UP Bits*

CoS	Color	802.1Q (Configurable)	802.1AD (Configurable)
0	Green	0	0
0	Yellow	0	0
1	Green	1	1
1	Yellow	1	1
2	Green	2	2
2	Yellow	2	2
3	Green	3	3
3	Yellow	3	3
4	Green	4	4
4	Yellow	4	4
5	Green	5	5
5	Yellow	5	5
6	Green	6	6
6	Yellow	6	6
7	Green	7	7
7	Yellow	7	7

To modify the 802.1Q CoS and Color to UP 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>
```

To display the 802.1Q CoS and Color to UP bit mapping table, enter the following command in root view:

```
root> ethernet qos 802.1q-up-bits-marking-tbl show
```

To modify the 802.1AD CoS and Color to UP 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>
```

To display the 802.1AD CoS and Color to UP bit mapping table, enter the following command in root view:

```
root> ethernet qos 802.1ad-up-bits-marking-tbl show
```

To modify the Color to CFI/DEI bit mapping, enter the following command in root view:

```
root> ethernet marking color set green-cfi-dei <cfi> yellow-cfi-dei <cfi>
```

To display the Color to CFI/DEI bit mapping, enter the following command in root view:

```
root> ethernet marking color show
```

Table 183 *Marking Mapping 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.
cfi	Number	0 – 1	The CFI/DEI bit value assigned to matching frames.

The following command maps CoS 0, Green, to 802.1Q UP bit 0:

```
root> ethernet qos 802.1q-up-bits-marking-tbl set cos 0 color green 802.1p
0
```

The following command marks CoS 5, Yellow, to 802.1AD UP bit 5:

```
root> ethernet qos 802.1ad-up-bits-marking-tbl set cos 5 color yellow
802.1p 5 dei 1
```

The following command maps Green to CFI/DEI bit 0 and Yellow to CFI/DEI bit 1:

```
root> ethernet marking color set green-cfi-dei 0 yellow-cfi-dei 1
```

Configuring WRED (CLI)

This section includes:

- Configuring WRED Profiles (CLI)
- Assigning a WRED Profile to a Queue (CLI)

Note

For a description of WRED, see WRED Overview.

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 184 *WRED Profile CLI Parameters*

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 - 30	A unique ID to identify the profile.
green-min-threshold	Number	24 - 8192	The minimum throughput 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 throughput 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 throughput of yellow frames for queues with this profile, in Kbytes. When this value is reached, the system begins

Parameter	Input Type	Permitted Values	Description
			dropping yellow frames in the queue.
yellow-max-threshold	Number	24 - 8192	The maximum throughput 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.

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%

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 [1/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 [1/x]> wred show profile-id service-bundle-id <service-
bundle-id> cos <cos>
```

Table 185 *Assigning WRED Profile to Queue CLI Parameters*

Parameter	Input Type	Permitted Values	Description
service-bundle-id	Number	1	H-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.

The following command assigns WRED Profile 2 to the CoS 0 queue in Service Bundle 1, on Eth 7:

```
eth type eth [1/7]> 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 [1/7]> wred show profile-id service-bundle-id 1 cos 0
```

Configuring Egress Shaping (CLI)

This section includes:

- Configuring Queue Shaper Profiles (CLI)
- Attaching a Shaper Profile to a Queue (CLI)
- Configuring Egress Line Compensation for Shaping (CLI)
- Configuring Service Bundle Shapers (CLI)

Note

For a description of Egress Shaping, see Egress Shaping Overview.

Configuring Queue Shaper Profiles (CLI)

Queue shaper profiles must be configured via the Web EMS. See Configuring Queue Shaper Profiles.

Note

Support for queue shaper profile configuration via the CLI is planned for future release.

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 [1/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 [1/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 [1/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 [1/x]> queue-shaper delete service-bundle-id <service-bundle-
id> cos <cos>
```

Table 186 *Attaching Shaper Profile to Queue CLI Parameters*

Parameter	Input Type	Permitted Values	Description
service-bundle-id	Number	1	The service bundle to which you are attaching the queue shaper profile. The only supported value is 1.
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.
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 Eth 2, and enables shaping on these queues:

```
eth type eth [1/2]> 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 [1/2]> queue-shaper edit service-bundle-id 1 cos 0 admin-
state enable profile-id 2
```

Configuring Egress Line Compensation for Shaping (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 [1/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 [1/x]>shaping-compensation-value get
```

Table 187 *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
```

Configuring Service Bundle Shapers (CLI)

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 <0-25000000> shaper-profile-name <string> cbs <1-
4096> pbs
```

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 <0-25000000>
shaper-profile-name <string> cbs <1-4096>
```

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	Input Type	Permitted Values	Description
profile-id	Number	1 – 32	A unique ID that identifies the profile. 1 is a pre-defined service bundle shaper profile and cannot be edited.
cir	Number	0 – 25000000	The Committed Information Rate (CIR) assigned to the profile, in kbps. Permitted values are: 0 – 25000000
shaper-profile-name	Text String	Up to 20 characters.	A description of the profile.
cbs	Number	1 – 4096	The Committed Burst Size (CBS) for the shaper, in KBytes. The default value is 4096.

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

Only Service Bundle 1 is supported.

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 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
```

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
```

The following command assigns Service Bundle Shaper Profile 5 to Ethernet port 1 and enables shaping on this interface and 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 from 5 to 4:

```
eth type eth [1/1]> service-bundle-shaper edit service-bundle-id 1 admin-
state enable profile-id 4
```

Configuring Scheduling (CLI)

This section includes:

- Configuring Queue Priority (CLI)
- Configuring Interface Priority Profiles (CLI)
- Attaching a Priority Profile to an Interface (CLI)
- Configuring Weighted Fair Queuing (WFQ) (CLI)

> **Note**
>
> For a description of Scheduling, see Scheduling Overview.

Configuring Queue Priority (CLI)

A priority profile defines the exact order for serving the eight priority queues in a single service bundle.

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 188 *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 Service 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.

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 189 *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 priority for the CoS 0 queue, from 4 (highest) to 1 (lowest). This priority is applied to frames with CoS 0 egressing the service bundle to which the profile is assigned.

Parameter	Input Type	Permitted Values	Description
description	Text String	Up to 20 characters.	A description of the priority level.
cos1-priority	Number	1 – 4	The priority for the CoS 1 queue, from 4 (highest) to 1 (lowest). This priority is applied to frames with CoS 1 egressing the service bundle to which the profile is assigned.
cos2-priority	Number	1 – 4	The priority for the CoS 2 queue, from 4 (highest) to 1 (lowest). This priority is applied to frames with CoS 2 egressing the service bundle to which the profile is assigned.
cos3-priority	Number	1 – 4	The priority for the CoS 3 queue, from 4 (highest) to 1 (lowest). This priority is applied to frames with CoS 3 egressing the service bundle to which the profile is assigned.
cos4-priority	Number	1 – 4	The priority for the CoS 4 queue, from 4 (highest) to 1 (lowest). This priority is applied to frames with CoS 4 egressing the service bundle to which the profile is assigned.
cos5-priority	Number	1 – 4	The priority for the CoS 5 queue, from 4 (highest) to 1 (lowest). This priority is applied to frames with CoS 5 egressing the service bundle to which the profile is assigned.
cos6-priority	Number	1 – 4	The priority for the CoS 6 queue, from 4 (highest) to 1 (lowest). This priority is applied to frames with CoS 6 egressing the service bundle to which the profile is assigned.
cos7-priority	Number	1 – 4	The priority for the CoS 7 queue, from 4 (highest) to 1 (lowest). This priority is applied to frames with CoS 7 egressing the service bundle to which the profile is assigned.

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 190 *Interface Priority Sample Profile Parameters*

CoS	Priority (user defined)	Description
0	1	c0_p1
1	1	c1_p1
2	1	c2_p1
3	2	c3_p2

CoS	Priority (user defined)	Description
4	2	c4_p2
5	3	c5_p3
6	4	c6_p4
7	4	c7_p4

The following command edits the profile you created in the previous command so that CoS 6 queues have a 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
```

Attaching a Priority Profile to an Interface (CLI)

Note

When a profile is assigned to an interface or when a profile that is already assigned to an interface is modified, the device must be reset before the change is applied. Until the device is reset, an alarm is raised. This alarm has Alarm ID 105, *System reset is required after priority profile has been changed*. This alarm is also raised if the default profile (Profile 9) is modified, even if the profile is not assigned to an interface.

To attach a priority profile to an interface, go to interface view for the interface and enter the following command:

```
eth type eth [1/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 [1/x]> port-priority show profile-id
```

Table 191 *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.

The following command attaches Interface Priority Profile 3 to Eth 3:

```
eth type eth [1/3]> priority set profile-id 3
```

The following is a sample output from the port-priority show profile-id command:

```
eth type eth [1/3]>port-priority show profile-id
Profile ID: 9
```

CoS	Priority (When queue is green)	Priority (When queue is yellow)	Description
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 [1/3]>
```

Configuring Weighted Fair Queuing (WFQ) (CLI)

This section includes:

- Configuring a WFQ Profile (CLI)
- Attaching a WFQ Profile to an Interface (CLI)

Note

For an overview of WFQ, see WFQ Overview.

Configuring a WFQ Profile (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>
```

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>
```

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
```

This profile has the parameters listed in the following table.

Table 192 *WFQ Sample Profile Parameters*

CoS	Queue Weight
0	15
1	15
2	15
3	15
4	15
5	15
6	15
7	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 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
```

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 [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 193 *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.

The following command assigns WFQ Profile 3 to Eth 3:

```
eth type eth [1/3]> port-wfq set profile-id 3
```

The following is a sample display for the port-wfq show profile-id command:

```
eth type eth [1/3]>port-wfq show profile-id
```

Profile ID: 1

CoS	Queue Weight
0	20
1	20
2	20
3	20
4	20
5	20
6	20
7	20

```
eth type eth [1/3]>
```

Displaying Egress PMs and Statistics (CLI)

PTP 850 collects egress PMs and statistics at the queue level and the service bundle level.

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)
- Dropped Green Packets (64 bits counter)
- Dropped Green Bytes (64 bits counter)
- Transmitted Yellow Packets (64 bits counter)
- Transmitted Yellow Bytes (64 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 [1/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 [1/x]> tm-queue clear statistics service-bundle-id <service-
bundle-id>
```

Table 194 *Egress Queue Level PMs CLI Parameters*

Parameter	Input Type	Permitted Values	Description
service-bundle-id	Number	1	Only Service Bundle ID 1 is supported.
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 Eth 3. The PMs are cleared after they are displayed:

```
eth type eth [1/3]> 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 Eth 3:

```
eth type eth [1/3]> tm-queue clear statistics service-bundle-id 1
```

Configuring and Displaying Queue-Level PMs (CLI)

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 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 [1/3]>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 module, muting of a radio interface, and an operational status of Down.

Ethernet Protocols (CLI)

This section includes:

Related Topics:

- Configuring Service OAM (SOAM) Fault Management (FM) (CLI)

Configuring G.8032 (CLI)

This section includes:

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.

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 195 *G.8032 Destination MAC Address CLI Parameters*

Parameter	Input Type	Permitted Values	Description
MAC address	Six groups of two hexadecimal digits	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.

> **Note**
>
> 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 type can be used.

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 <east-sp> level
<level> version <version>
```

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> east-sp <east-sp> level
<level> version <version>
```

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 <level> version <version>
```

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 196 *G.8032 ERPI Configuration CLI Parameters*

Parameter	Input Type	Permitted Values	Description
erpi-id	Number	1-64	A unique ID that identifies the ERPI.
erpi-service-id	Number	1-4095	The ID of the Ethernet service to which the ERPI belongs.
west-sp	Number	1-32	The first endpoint for the ERPI. This can be any service point that has been configured for the service.
east-sp	Number	1-32	The second endpoint for the ERPI. This can be any service point that has been configured for the service.
sub-ring-sp	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 service.
level	Number	0-7	Optional. The Maintenance Entity Group (MEG) level used for R-APS messages sent in the ERPI.
version	Number	1-2	Optional. The ERPI (G.8032) protocol version currently being used in the unit.
erpi-name	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 service_x
```

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
root> ethernet g8032 set-erpi-name erpi-id 1 erpi-name Sub_ring
```

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
root> ethernet g8032 set-erpi-name erpi-id 1 erpi-name RSRi
```

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 197 *G.8032 RPL Owner CLI Parameters*

Parameter	Input Type	Permitted Values	Description
erpi-id	Number	1-64	The ID of the ERPI for which you want to set or delete the RPL owner.
SP	Number or Variable	east west sub-ring	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:

```
root> ethernet g8032 remove-rpl-owner erpi-id 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.

Note

The Guard Time is used to prevent Ethernet ring nodes from acting upon outdated R-APS messages and prevents the possibility of forming a closed loop.

- **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 198 *G.8032 Timer Configuration CLI Parameters*

Parameter	Input Type	Permitted Values	Description
erpi-id	Number	1-64	The ID of the ERPI for which you want to set a timer.
wtr	Number	1-12	The minimum time (in minutes) the system waits after signal failure is recovered before reverting to idle state.
guard-time	Number	10-2000, in multiples of 10	The minimum time (in msec) the system waits after recovery from a signal failure before accepting new R-APS messages.
holdoff-time	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 199 *G.8032 Switching and Reversion CLI Parameters*

Parameter	Input Type	Permitted Values	Description
erpi-id	Number	1-64	The ID of the ERPI on which you want to perform or clear the switch or initiate convergence.
SP	Number or Variable	east west sub-ring	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-id> SP <SP>
tx-raps <tx-raps>
```

Table 200 *G.8032 Switching and Reversion CLI Parameters*

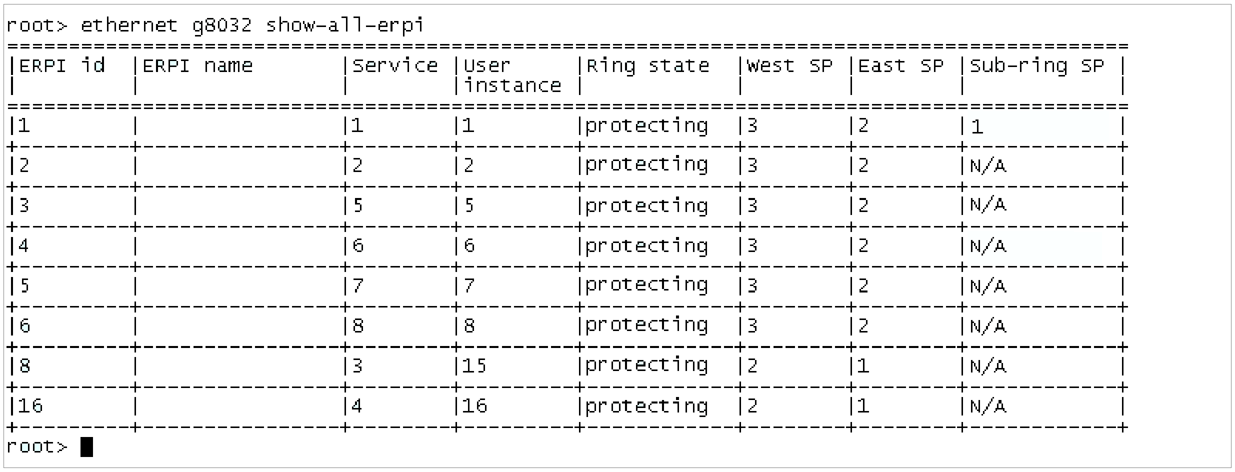
Parameter	Input Type	Permitted Values	Description
erpi-id	Number	1-64	The ID of the ERPI on which you want to perform or clear the switch or initiate convergence.
SP	Variable	east west sub-ring	Specifies the service point on which to clear the manual or forced switch or to implement convergence.
tx-raps	Variable	true false	**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>
```

To display all ERPIs that include a service point on a Multiband or Multi-Carrier ABC group, enter the following command in root view:

```
root> ethernet g8032 show-all-port-erpi group-on-slot enhanced-abc slot 1
group-id <1-4>
```

The following command displays all ERPIs with a service point on LAG group 1:

```
root> ethernet g8032 show-all-port-erpi group lag1
```

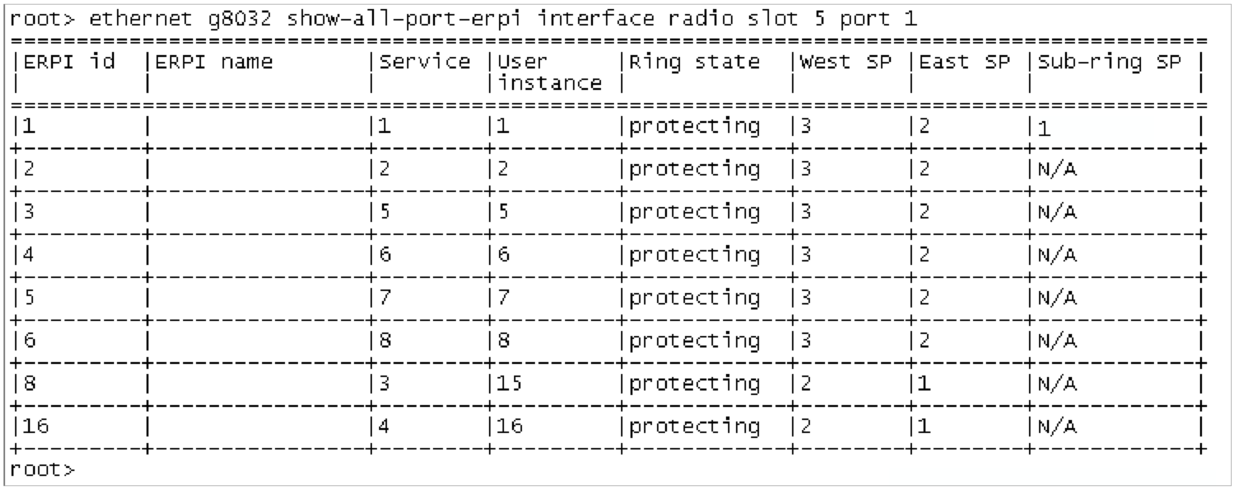
The following command displays all ERPIs with a service point on HSB protection group 2:

```
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-on-slot enhanced-abc slot 1
group-id 1
```

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>
```

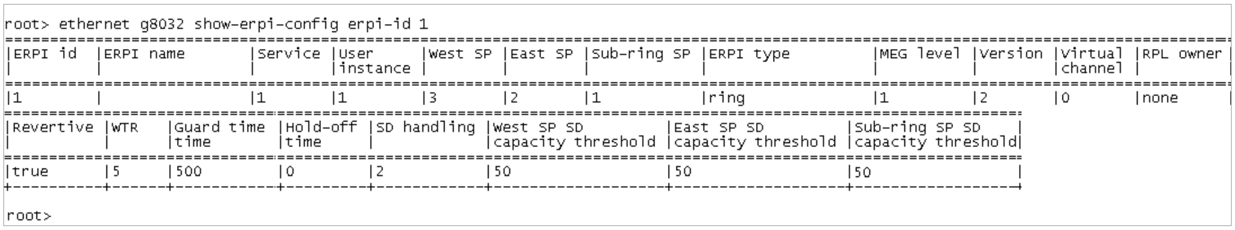
To display detailed information about a specific ERPI, enter the following command in root view:

```
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>
```

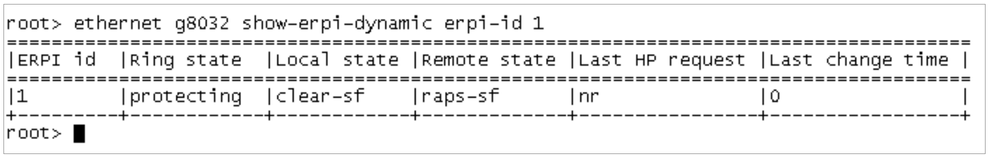
To display state information about a specific ERPI, enter the following command in root view:

```
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 201 *G.8032 ERPI Display Command Input Parameters*

Parameter	Input Type	Permitted Values	Description
interface	Variable	eth radio	Enter the type of interface:

Parameter	Input Type	Permitted Values	Description
			eth – Ethernet radio – Radio
slot	Number	Ethernet: 1 Radio: 1	
port	Number	Ethernet: • PTP 850EX: 2-4 Radio: • PTP 850EX: 1	The port number of the interface.
group	Variable	lb1 lb2 lb3 lb4 lag1 lag2 lag3 lag4	To enter interface view for a Link Bonding group (lb1 – lb4) or a LAG (lag1 - lag4), enter the group.
erpi-id	Number	1-64	The ID of the ERPI for which you want to perform or clear the switch, initiate convergence, or display information.

Table 202 *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.
Ring State	Indicates the current ERPI state. Possible values are: Initializing Idle Pending Protecting

Parameter	Description
	FS (Forced Switch) MS (Manual Switch)
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 Threshold	Reserved for future use.
East SP SD Capacity Threshold	Reserved for future use.
Sub-Ring SP SD Capacity Threshold	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.

Parameter	Description
Last HP Request	The last high priority request.
Last Change Time	The time of the last ring state transition.

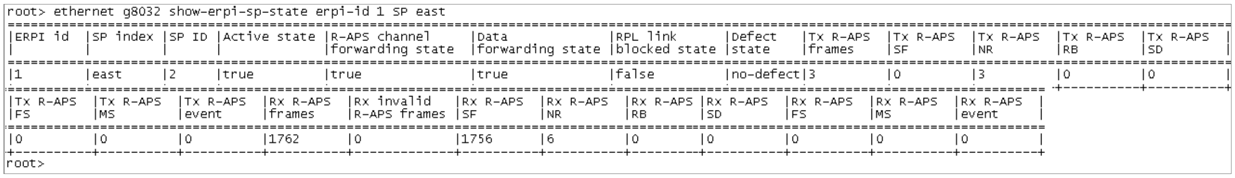
To display the state of a specific service point, enter the following command in root view:

```
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  |Tx R-APS  |
|          |          |      |              |forwarding state  |forwarding state  |blocked state |state    |frames    |SF        |NR        |RB        |SD        |
=======================================================================================================================================================================
|1         |east      |2     |true          |true              |true              |false         |no-defect|3         |0         |3         |0         |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  |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 203 *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 point is in blocked state.
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.

Parameter	Description
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.
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.

Configuring MSTP (CLI)

This section includes:

- Configuring the MSTP Bridge Parameters (CLI)
- Configuring the MSTP Port Parameters (CLI)

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.

Configuring the MSTP Bridge Parameters (CLI)

This section includes:

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.

Note

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 850 supports 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>
```

Note

Changing the number of MSTIs causes the MSTP stack to reset.

To display the number of MSTIs on the unit, enter the following command in root view:

```
root> ethernet mstp show-number-of-instances
```

Table 204 *Defining Number of MSTIs CLI Parameters*

Parameter	Input Type	Permitted Values	Description
MSTI	Number	2-16	The number of MSTIs on the unit. This number does not include the Common and Internal Spanning Tree (CIST).

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-mac>
```

Table 205 *BPDU Destination MAC Address CLI Parameters*

Parameter	Input Type	Permitted Values	Description
bpdu-destination-mac	Variable	customer provider	**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.

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.

Note

This feature is planned for future release.

To determine how SD failures are treated, enter the following command in root view:

```
root> ethernet mstp set sd-handling <sd-handling>
```

Table 206 *MSTP Signal Degrade Failure CLI Parameters*

Parameter	Input Type	Permitted Values	Description
sd-handling	Variable	ignored same-as-SF	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 207 *MSTP Configuration ID CLI Parameters*

Parameter	Input Type	Permitted Values	Description
configuration-name	Text String		The IEEE 802.1Q Configuration Name. The Configuration Name is part of the bridge configuration Identifier.
revision-level	Number	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.

Note

All mapping of Ethernet services to MSTP instances (MSTIs) should be performed *before* enabling MSTP.

To assign a service to another MSTI, enter the following command in root view:

```
root> ethernet generalcfg instance-to-service-mapping set service sid
<sid> instance-id <instance-id>
```

To assign a range of services to another MSTI, enter the following command in root view:

```
root> ethernet generalcfg instance-to-service-mapping set service sid
<sid> to <sid> instance-id <instance-id>
```

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 service sid
<sid>
```

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 service sid
<sid> to <sid>
```

Table 208 *MSTP Service to MSTI Mapping CLI Parameters*

Parameter	Input Type	Permitted Values	Description
sid	Number or Range	Any Ethernet service or range of services configured in the unit.	The service ID.
instance-id	Number	1-16, 4095	The MSTI to which you want to map the service.

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 209 *MSTP Bridge Level Spanning Tree CLI Parameters*

Parameter	Input Type	Permitted Values	Description
cist-bridge-priority	Number	0-61440, in steps of 4096.	Enter a value as the writeable portion of the Bridge ID. This value constitutes the first two octets of the Bridge ID.
cist-bridge-hold-time	Number	10-100	Enter a value (in cs) as the interval length during which no more than two configuration bridge PDUs will be transmitted by this node.
cist-bridge-max-age	Number	600-4000	Enter 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.
cist-bridge-forward-delay	Number	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 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.
cist-bridge-hello-time	Number	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 determines how often the switch broadcasts its hello message to other switches, and is the same for all MSTIs.
cist-bridge-max-hops	Number	6-40	Enter 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.

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 210 *Bridge Level MSTI CLI Parameters*

Parameter	Input Type	Permitted Values	Description
instance	Number	1-16	Enter the MSTI ID of the MSTI you want to configure.
msti-bridge-priority	Number	0-61440, in steps of 4096.	The MSTI writeable portion of the Bridge ID.
interface	Variable	eth radio	Enter the type of interface: eth – Ethernet radio – Radio
slot	Number	Ethernet: 1 Radio: 1	
port	Number	Ethernet: • PTP 850EX: 2-4 Radio: • PTP 850EX: 1	The port number of the interface.
group	Variable	lag1 lag2 lag3 lag4	To enter interface view for a LAG group (lag1 - lag4), enter the group.

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>
```

Table 211 *CIST Port CLI Parameters*

Parameter	Input Type	Permitted Values	Description
interface	Variable	eth radio	Enter the type of interface: eth – Ethernet radio – Radio
slot	Number	Ethernet: 1 Radio: 1	
port	Number	Ethernet: • PTP 850EX: 2-4 Radio: • PTP 850EX: 1	The port number of the interface.
group	Variable	lag1 lag2 lag3 lag4	To enter interface view for a LAG group (lag1 - lag4), enter the group.
cist-port-priority	Number	0-240, in multiples of 16.	The priority contained in the first octet of the two-octet Port ID.
cist-port-path-cost	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:** Changing the value of this parameter is considered to be a topology change by the MSTP mechanism.
cist-port-edge-port	Variable	true false	true – The port is considered an edge port in the CIST. false – The port is considered a non-edge port in the CIST.
cist-port-mac-enabled	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

Parameter	Input Type	Permitted Values	Description
			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 False if the MAC is connected to a non-point-to-point and half-duplex LAN.

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 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 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-port-priority>
```

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-port-
priority <msti-port-priority>
```

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-port-path-cost>
```

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-port-path-
cost <msti-port-path-cost>
```

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 212 *MSTI Port CLI Parameters*

Parameter	Input Type	Permitted Values	Description
instance	Number	1-16	Enter the MSTI ID of the MSTI you want to configure.
interface	Variable	eth radio	Enter the type of interface: eth – Ethernet radio – Radio
slot	Number	Ethernet: 1 Radio: 1	
port	Number	Ethernet: • PTP 850EX: 2-4 Radio: • PTP 850EX: 1	The port number of the interface.
group	Variable	lag1 lag2 lag3 lag4	To enter interface view for a LAG group (lag1 - lag4), enter the group.
msti-port-priority	Number	0-240, in multiples of 16.	The priority contained in the first octet of the two-octet Port ID.
msti-port-path-cost	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 should be affected.

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 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 213 *Port BPDU Counters CLI Parameters*

Parameter	Input Type	Permitted Values	Description
interface	Variable	eth radio	Enter the type of interface: eth – Ethernet radio – Radio
slot	Number	Ethernet: 1 Radio: 1	
port	Number	Ethernet: • PTP 850EX: 2-4 Radio: • PTP 850EX: 1	The port number of the interface.
group	Variable	lag1 lag2 lag3 lag4	To enter interface view for a LAG group (lag1 - lag4), enter the group.

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

Notes

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 in which the Monitored and Control interfaces are both single interfaces, 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 create an ETH-BN entity in which the Monitored interface is a Multi-Carrier ABC group and the Control interface is a single Ethernet interface, enter the following command in root view:

```
root> ethernet ebn ebn-entity-create ebn-name <eb-name> monitored-group-
on-slot enhanced-abc monitored-slot 1 monitored-port 1 control-interface
<control-interface> control-slot <control-slot> vlan <vlan>
```

To create an ETH-BN entity in which the Monitored interface is an individual radio interface and the Control interface is a LAG, 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-group <control-group> 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 for ETH-BN must be set to a value greater than the MEG level of the CFM MEP. Otherwise, the BNM frames will be dropped. – this is a correct behavior.

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>
```

Note

If the *holdoff-time* is set to 0, then if the bandwidth drops below the nominal value, a BNM frame is transmitted immediately.

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. For Link Bonding configurations, it is recommended to leave the default value of 0 so that BNM frames will be sent immediately to the Link Bonding group on the main unit.

```
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 214 *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	

Parameter	Input Type	Permitted Values	Description
monitored-port	Number		
monitored-group	Variable	lag1 lag2 lag3 lag4 mc-abc1 mc-abc2 mc-abc3 mc-abc4	To configure a Multi-Carrier ABC group or a LAG (lag1-4) as the monitored interface, use this parameter instead of the interface, slot, and port parameters to identify the group.
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	PTP 850EX: 2-4	The specific Ethernet interface to which messages are transmitted when bandwidth in the monitored interface degrades below the nominal value.
control-group	Variable	lag1 lag2 lag3 lag4	To configure a LAG group as the control interface, use this parameter instead of the interface, slot, and port parameters to identify the group.
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: • **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

Parameter	Input Type	Permitted Values	Description
			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.
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 2
- 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, with no holdoff time.
- 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 2 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 0
root>
```

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 – 2009 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 215 *General LLDP CLI Parameters*

Parameter	Input Type	Permitted Values	Description
tx-interval	Number	5-3600	The interval, in seconds, at which LLDP frames are transmitted. The default value is 30.
hold-multiplier	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.
notif-interval	Number	5-3600	The interval, in seconds, between transmission of LLDP notifications during normal transmission periods. The default

Parameter	Input Type	Permitted Values	Description
			value is 30.

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 216 *LLDP Port CLI Parameters*

Parameter	Input Type	Permitted Values	Description
slot	Number	1	The slot in which the card resides.
port	Number	PTP 850EX: 2-4	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-notif-enable	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:

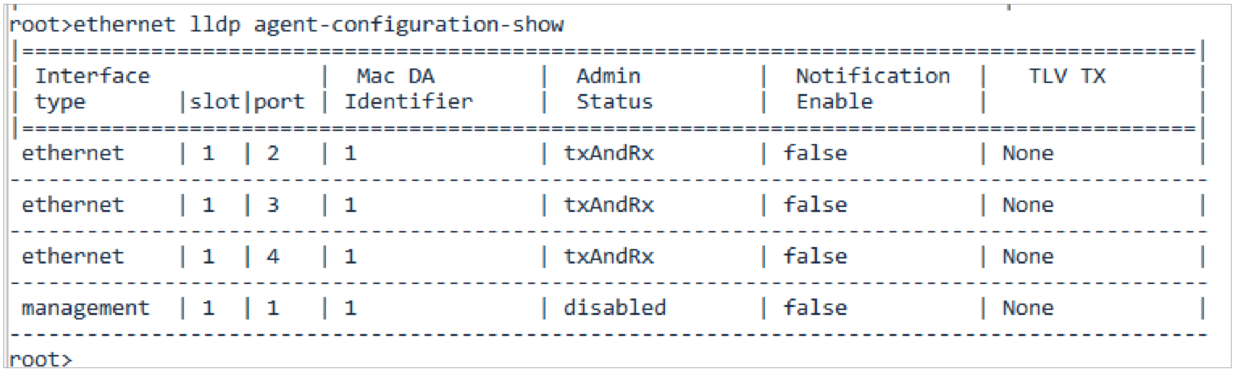
```
root> ethernet lldp agent-admin-set interface eth slot 1 port 3 agent-
admin txAndRx
root> ethernet lldp agent-notif-enable interface eth slot 1 port 3 agent-
notif-enable true
```

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   | 2    | 1                | txAndRx          | false           | None             |
--------------------------------------------------------------------------------------------
 ethernet      | 1   | 3    | 1                | txAndRx          | false           | None             |
--------------------------------------------------------------------------------------------
 ethernet      | 1   | 4    | 1                | txAndRx          | false           | None             |
--------------------------------------------------------------------------------------------
 management    | 1   | 1    | 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)

> **Note**
>
> 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 217 *LLDP Remote Unit CLI Parameters*

Parameter	Input Type	Permitted Values	Description
slot	Number	1	The slot in which the card resides.
port	Number	PTP 850EX: 2-4	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 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.

  Note: The Rem Port Description, Rem System Name, and Rem System Description fields are not used in the current version.
- **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 218 *LLDP Remote Management Data Per Port CLI Parameters*

Parameter	Input Type	Permitted Values	Description
slot	Number	1	
port	Number	PTP 850EX: 2-4	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 - 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. 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.

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)
- Configuring 1588 Boundary Clock (CLI)
- Disabling 1588 PTP Clock (CLI)

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.

The following command changes the ETSI/ANSI mode from the default value of ETSI to ANSI mode:

```
root> platform management set tdm-interfaces-standard ansi
```

To display the current ETSI/ANSI mode, enter the following command in root view:

```
root> platform management show tdm-interfaces-standard
```

Changing the ETSI/ANSI mode does *not* require unit reset.

Configuring the Sync Source (CLI)

> **Note**
>
> To configure a sync source on which the sync source Quality parameter is set according to ANSI specifications, you must change the ETSI/ANSI mode to ANSI before configuring the sync source. See Changing the ETSI/ANSI Mode (CLI).
>
> An interface with an electrical SFP module cannot be used as a Sync source.

The 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. 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 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)

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 Interfaces (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	PTP 850EX: 2-4	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 • stratum-3e • stratum-3 • smc • g813.8262 • unknown	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).

The following command configures Eth 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
```

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 1 port <1-2> radio-
channel 0 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 1 port <1-2> radio-
channel 0 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 1 port <1-2> radio-
channel 0
```

Table 220 *Sync Source Radio CLI Parameters*

Parameter	Input Type	Permitted Values	Description
slot	Number	1	
port	Number	PTP 850EX: 1	
radio-channel	Number	0	
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 • stratum-3e • stratum-3	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
		• smc • g813.8262 • unknown	

The following command changes the priority of a synchronization source on the radio interface to 14:

```
root> platform sync source edit radio-interface slot 1 port 1 radio-
channel 0 priority 14
```

The following command removes this synchronization source:

```
root> platform sync source remove radio-interface slot 1 port 1 radio-
channel 0
```

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 <slot> port
<port> 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 1 port <port>
source <source>
```

Note

To configure the interface clock on an Ethernet interface, the Media Type of the interface must be sfp, *not* auto-type. To view and configure the Media Type of an Ethernet interface, see Configuring an Interface's Media Type (CLI).

Table 221 *Outgoing Clock CLI Parameters*

Parameter	Input Type	Permitted Values	Description
slot	Number	Ethernet: 1 Radio: 1	

Parameter	Input Type	Permitted Values	Description
port	Number	Ethernet: - PTP 850EX: 2-4 Radio: - PTP 850EX: 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 Eth 3 to the system clock:

```
root> platform sync interface-clock set eth-interface slot 1 port 3 source
system-clock
```

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
```

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
```

Configuring SSM Messages (CLI)

In order to provide topological resiliency for synchronization transfer, PTP 850 implements the passing of SSM messages over the Ethernet and radio interfaces. SSM timing in PTP 850 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 the radio interface, enter the following command in root view:

```
root> platform sync ssm admin radio-interface slot 1 port 1 admin on
```

To disable SSM on the radio interface, enter the following command in root view:

```
root> platform sync ssm admin radio-interface slot 1 port 1 admin off
```

To enable SSM on an Ethernet interface, enter the following command in root view:

```
root> platform sync ssm admin eth-interface slot 1 port <2-4> admin on
```

To disable SSM on an Ethernet interface, enter the following command in root view:

```
root> platform sync ssm admin eth-interface slot 1 port <2-4> admin off
```

The following command enables SSM on Ethernet port 3:

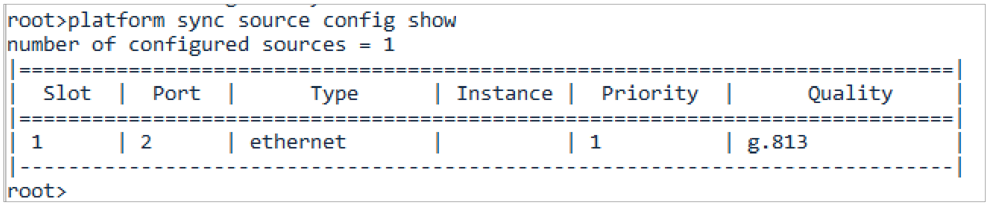
```
root> platform sync ssm admin eth-interface slot 1 port 3 admin on
```

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:

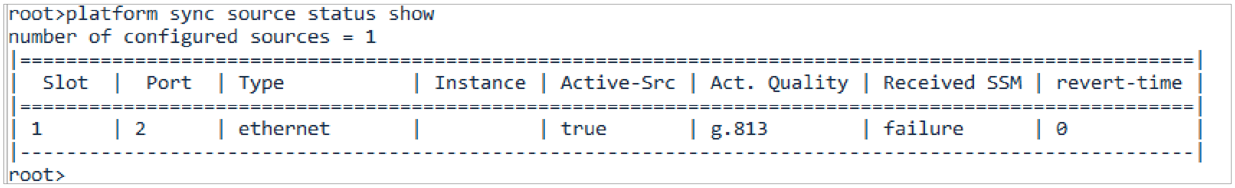


```
root>platform sync source config show
number of configured sources = 1
|=============================================================================|
|  Slot  |  Port  |      Type      | Instance |  Priority  |      Quality      |
|=============================================================================|
| 1      | 2      | ethernet       |          | 1          | g.813             |
|-----------------------------------------------------------------------------|
root>
```

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 status show
number of configured sources = 1
|=============================================================================================|
|  Slot  |  Port  | Type            | Instance | Active-Src | Act. Quality | Received SSM | revert-time |
|=============================================================================================|
| 1      | 2      | ethernet        |          | true       | g.813        | failure      | 0           |
|---------------------------------------------------------------------------------------------|
root>
```

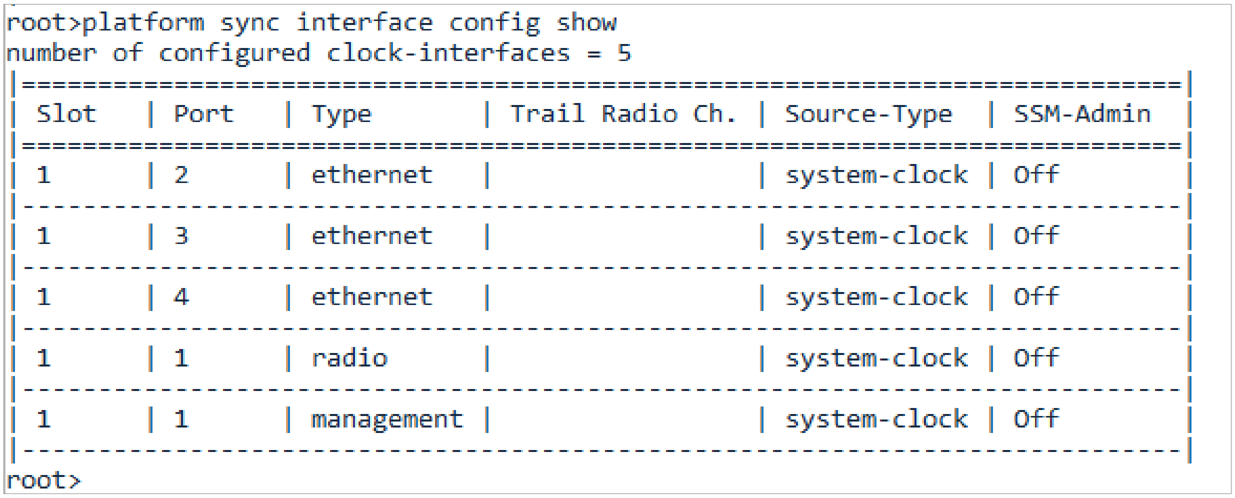
To display the current system reference clock quality, enter the following command in root view:

```
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 for PTP 850EX:



```
root>platform sync interface config show
number of configured clock-interfaces = 5
|=======================================================================|
| Slot    | Port    | Type        | Trail Radio Ch. | Source-Type  | SSM-Admin |
|=======================================================================|
| 1       | 2       | ethernet    |                 | system-clock | Off       |
|-----------------------------------------------------------------------|
| 1       | 3       | ethernet    |                 | system-clock | Off       |
|-----------------------------------------------------------------------|
| 1       | 4       | ethernet    |                 | system-clock | Off       |
|-----------------------------------------------------------------------|
| 1       | 1       | radio       |                 | system-clock | Off       |
|-----------------------------------------------------------------------|
| 1       | 1       | management  |                 | 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

Configuring 1588 Transparent Clock (CLI)

PTP 850 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

1588 TC is not supported when Master-Slave communication is using the IPv6 transport layer.

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.

PTP phase alignment relies on symmetric delay between the timestamping units. Therefore, to ensure the best results, it is recommended to use the same port speed (e.g., 10 Gbps), media type (e.g., RJ-45 or SFP) and equipment type (e.g., PTP 850EX) on both sides of the link.

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. See Displaying Synchronization Status and Parameters (CLI).

6. Enter the following command in root view to enable Transparent Clock:

```
root> platform sync ptp-tc set admin enable
```

7. Verify that Transparent Clock is enabled on the interface by entering the following command:

```
root> platform sync ptp-tc show status
```

8. If Transparent Clock is not enabled on the interface, enter the following command to enable it:

```
root> platform sync ptp-tc set radio slot 1 port <port> admin enable
```

Note

For instructions on disabling Transparent Clock for the device or an individual interface, see Disabling 1588 PTP Clock (CLI). Disabling 1588 PTP can drastically affect time synchronization performance in the entire network.

9. 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 <1-2> port <port> direction
<upstream|downstream>
```

For Multi-Carrier ABC groups, use the following command:

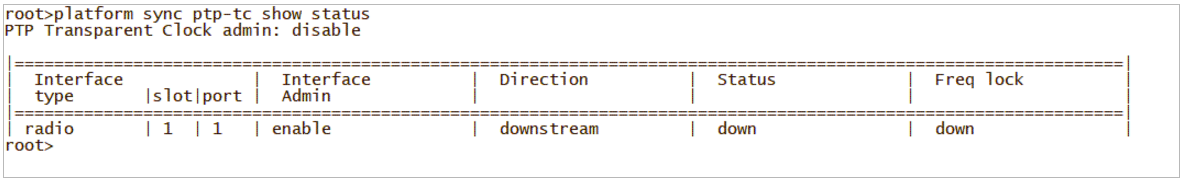
```
root> platform sync ptp-tc set group-on-slot type enhanced-abc slot 1
group-number <group-number> direction <upstream|downstream>
```

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
```

For example:



```
root>platform sync ptp-tc show status
PTP Transparent Clock admin: disable

|==========================================================================================================|
|  Interface              |  Interface            |  Direction            |  Status               |  Freq lock            |
|  type       |slot|port  |  Admin                |                       |                       |                       |
|==========================================================================================================|
| radio       | 1  | 1    | enable                |  downstream           |  down                 |  down                 |
root>
```

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
```

10. 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
    ```

11. 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.

Configuring 1588 Boundary Clock (CLI)

Boundary Clock complies with ITU-T Telecom Profile G.8275.1. This enables PTP 850, with Boundary Clock, to meet the rigorous synchronization requirements of 5G networks.

The Boundary Clock in PTP 850 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 850 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 850 node.

- 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)

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, as well as Multi-Carrier ABC groups.

For each interface, use the following commands to enable and define Boundary Clock.To enable Boundary Clock on an individual 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, 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.

For individual interfaces:

```
root> platform sync ptp-bc interfaces set interface-type <interface-type>
slot <slot> port <port> local-priority <local-priority>
```

For Multi-Carrier ABC groups:

```
root> platform sync ptp-bc interfaces set groups-on-slot set interface-
type enhanced-abc slot 1 port 1 local-priority <local-priority>
```

Use the following command to set a MAC address for multicast re-transmission of PTP packets.

For individual interfaces:

```
root> platform sync ptp-bc interfaces set interface-type <interface-type>
slot <slot> port <port> dest-mac <dest-mac>
```

For Multi-Carrier ABC groups:

```
root> platform sync ptp-bc interfaces set groups-on-slot set interface-
type enhanced-abc slot 1 port 1 dest-mac <dest-mac>
```

Table 223 *Boundary Clock Configuration CLI Parameters*

Parameter	Input Type	Permitted Values	Description
interface-type	Variable	ethernet radio	

Parameter	Input Type	Permitted Values	Description
slot	Number	Ethernet: 1 Radio: 1	
port	Number	Ethernet: - PTP 850EX: 2-4 Radio: - PTP 850EX: 1	Ethernet: 1
admin	Variable	enable disable	Enables or disables Boundary 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 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 850 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 frame.

The following commands set up a Boundary Clock node that includes Ethernet interfaces Eth 2 and Eth 3 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 2 admin enable
root> platform sync ptp-bc interfaces set interface-type ethernet slot 1
port 2 master-only no

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 radio slot 1 port
1 admin enable
root> platform sync ptp-bc interfaces set interface-type radio slot 1 port
1 master-only yes
```

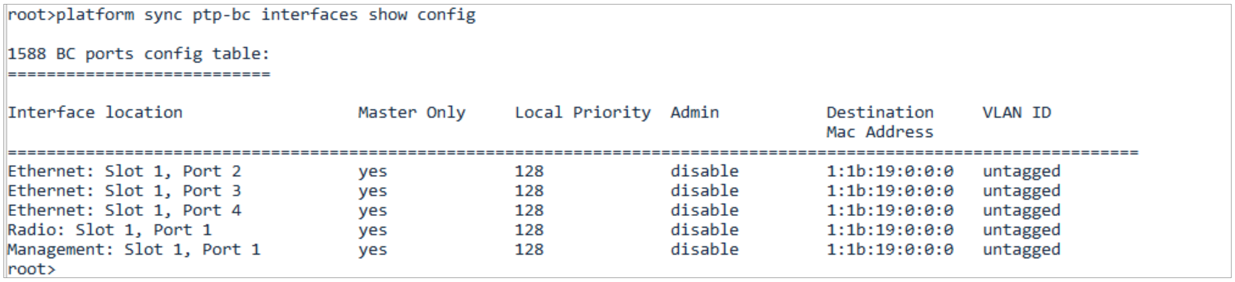
In addition, you must perform the following steps to properly configure the Boundary Clock node:

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 371 *1588 Boundary Clock – Current Configuration Sample Display (PTP 850EX)*



```
root>platform sync ptp-bc interfaces show config

1588 BC ports config table:
===========================

Interface location                  Master Only     Local Priority  Admin           Destination     VLAN ID
                                                                                    Mac Address
===================================================================================================================
Ethernet: Slot 1, Port 2            yes             128             disable         1:1b:19:0:0:0   untagged
Ethernet: Slot 1, Port 3            yes             128             disable         1:1b:19:0:0:0   untagged
Ethernet: Slot 1, Port 4            yes             128             disable         1:1b:19:0:0:0   untagged
Radio: Slot 1, Port 1               yes             128             disable         1:1b:19:0:0:0   untagged
Management: Slot 1, Port 1          yes             128             disable         1:1b:19:0:0:0   untagged
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 850'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 850 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>
```

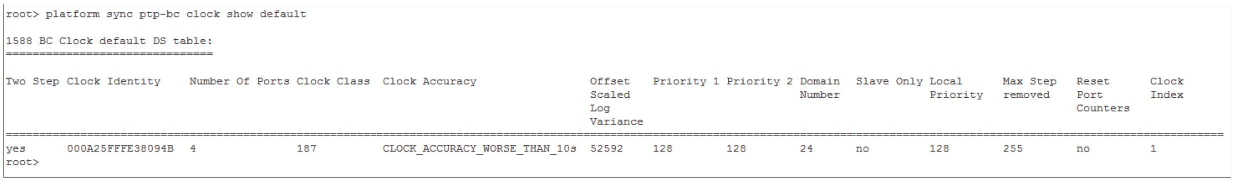
Table 224 *Boundary Clock Default Settings – CLI Parameters*

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 372 *1588 Boundary Clock – Default Parameters Sample Display (CLI)*



```
root> platform sync ptp-bc clock show default

1588 BC Clock default DS table:
===============================

Two Step Clock Identity    Number Of Ports Clock Class  Clock Accuracy                 Offset    Priority 1 Priority 2 Domain  Slave Only Local      Max Step   Reset      Clock
                                                                                       Scaled                            Number             Priority   removed    Port       Index
                                                                                       Log                                                                        Counters
                                                                                       Variance
======================================================================================================================================================================================
yes      000A25FFFE38094B  4               187          CLOCK_ACCURACY_WORSE_THAN_10s  52592     128        128        24      no         128        255        no         1
root>
```

Boundary Clock Default Parameters lists and describes the Boundary Clock default parameters.

Table 225 *Boundary Clock Default Parameters*

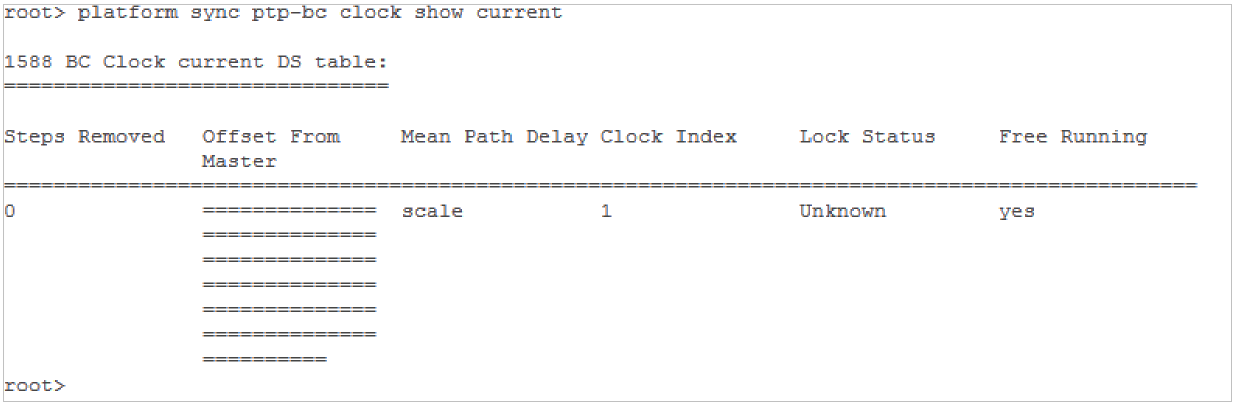
Parameter	Definition
Two Step (read only)	Indicates whether the Boundary Clock node is operating in two-step mode. For PTP 850E, Two Step is always set to No.
Clock Identity (read only)	Identifies the system clock.
Number of Ports (read only)	Displays the number of ports on the unit on which Boundary Clock is enabled. The maximum is 16 per PTP 850 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 850'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 850, 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 850 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 850, this is always set to no.
Clock Index	In PTP 850, 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 advanced parameters.

```
root> platform sync ptp-bc clock show current
```

Figure 373 *1588 Boundary Clock – Advanced (General) Parameters Sample Display (CLI)*

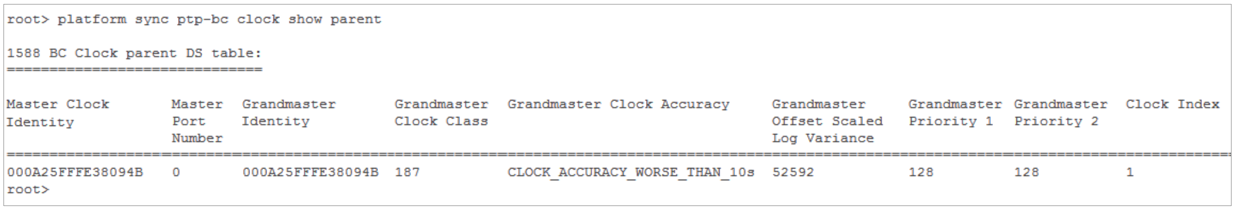


```
root> platform sync ptp-bc clock show current

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 current master and grandmaster being used by the Boundary Clock node.

```
root> platform sync ptp-bc clock show parent
```

Figure 374 *1588 Boundary Clock – Parent Clock Parameters Sample Display (CLI)*

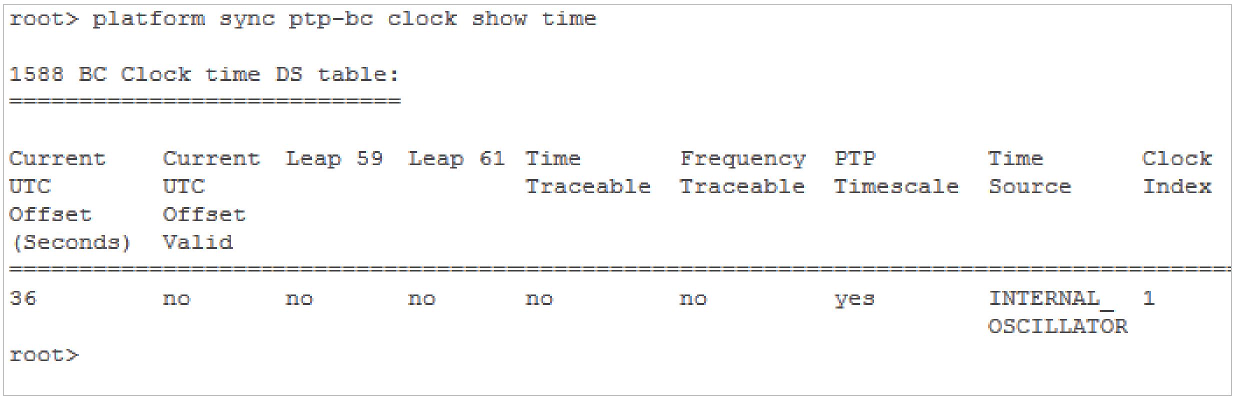


```
root> platform sync ptp-bc clock show parent

1588 BC Clock parent DS table:
==============================

Master Clock        Master   Grandmaster        Grandmaster  Grandmaster Clock Accuracy      Grandmaster     Grandmaster  Grandmaster  Clock Index
Identity            Port     Identity           Clock Class                                  Offset Scaled   Priority 1   Priority 2
                    Number                                                                   Log Variance
==========================================================================================================================================================
000A25FFFE38094B    0        000A25FFFE38094B   187          CLOCK_ACCURACY_WORSE_THAN_10s   52592           128          128          1
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 375 *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. Boundary Clock Advanced Parameters (CLI) 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 850 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.
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.

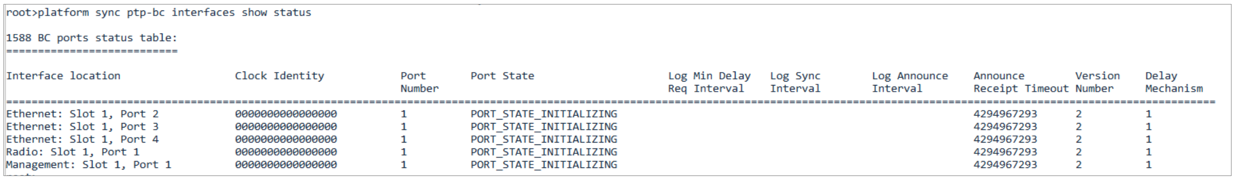
Parameter	Definition
Leap 61	Indicates that the last minute of the current UTC day contains 61 seconds.
Time Traceable	Traceability to the primary time reference.
Frequency Traceable	Traceability to the primary frequency reference.
PTP Timescale	Indicates whether the clock time scale of the grandmaster 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 376 *1588 Boundary Clock Port Parameters*



```
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 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
Radio: Slot 1, Port 1               0000000000000000          1          PORT_STATE_INITIALIZING                                                        4294967293      2          1
Management: Slot 1, Port 1          0000000000000000          1          PORT_STATE_INITIALIZING                                                        4294967293      2          1
```

Boundary Clock Port Parameters (CLI) lists and describes the Boundary Clock port parameters.

Table 227 *Boundary Clock Port Parameters (CLI)*

Parameter	Definition
Clock Identity	The PTP 850 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>
```

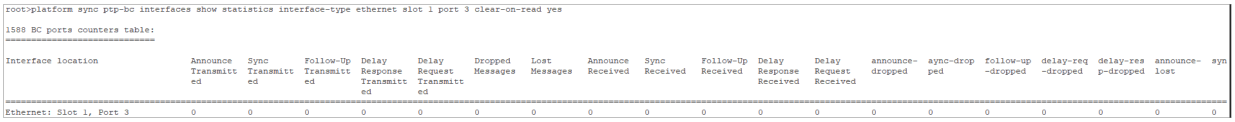
Table 228 *Boundary Clock Configuration CLI Parameters*

Parameter	Input Type	Permitted Values	Description
interface-type	Variable	ethernet radio	
port	Number	Ethernet: • PTP 850EX: 2-4 Radio: • PTP 850EX: 1	The port number.
clear-on-read	Boolean	yes no	If yes is selected, the interface statistics are cleared after the command is executed.

The following command displays statistics for Eth 3, 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
```

Table 229 *1588 Boundary Clock Statistics (CLI)*



```
root>platform sync ptp-bc interfaces show statistics interface-type ethernet slot 1 port 3 clear-on-read yes

1588 BC ports counters table:
=============================

Interface location                  Announce   Sync       Follow-Up  Delay      Delay      Dropped    Lost       Announce   Sync       Follow-Up  Delay      Delay      announce-  aync-drop  follow-up  delay-req  delay-res  announce-  syn
                                    Transmitt  Transmitt  Transmitt  Response   Request    Messages   Messages   Received   Received   Received   Response   Request    dropped    ped        -dropped   -dropped   p-dropped  lost
                                    ed         ed         ed         Transmitt  Transmitt                                                        Received   Received
                                                                     ed         ed
=============================================================================================================================================================================================================================================
Ethernet: Slot 1, Port 3            0          0          0          0          0          0          0          0          0          0          0          0          0          0          0          0          0          0          0
```

Boundary Clock Port Statistics (CLI) lists and describes the Boundary Clock port statistics.

Table 230 *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 Transmitted	The number of Delay Response messages that have been transmitted from the port.

Parameter	Definition
Delay Request Transmitted	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.
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.

Disabling 1588 PTP Clock (CLI)

Use the following command to disable each Boundary Clock interface on the device. 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 without disabling it on the device. You can do this by disabling Transparent Clock on the interface, as follows.

To disable Clock on the radio interface, enter the following command in root view:

```
root> platform sync ptp-tc set radio slot 1 port 1 admin disable
```

Access Management and Security (CLI)

This section includes:

Related Topics:

- Logging On (CLI)

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)

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 231 *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
```

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 232 *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
```

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
```

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 block-failure-login period to expire. See Configuring Blocking Upon Login Failure (CLI).

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 233 *Blocking Unused Accounts CLI Parameters*

Parameter	Input Type	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
```

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)
- Configuring Password Reuse Limit (CLI)
- Displaying the System Password Settings (CLI)

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 234 *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.

The following command sets the password aging time to 60 days:

```
root> platform security access-control password aging set 60
```

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 235 *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.

Parameter	Input Type	Permitted Values	Description
			- 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*.

The following command enables password strength enforcement:

```
root> platform security access-control password enforce-strength set yes
```

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 236 *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.

Configuring Password Reuse Limit (CLI)

To configure the number of previous passwords that cannot be reused, enter the following command in root view:

```
root> platform security access-control password history <history>
```

Table 237 *Password Reuse Limit CLI Parameters*

Parameter	Input Type	Permitted Values	Description
history	Number	0-10	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.

Displaying the System Password Settings (CLI)

Use the following command to display the system password settings:

```
root> platform security access-control password show-all
```

Configuring Users (CLI)

This section includes:

- Configuring User Profiles (CLI)
- Configuring User Accounts (CLI)

Related topics:

- Logging On (CLI)

Note

For an overview of user configuration, see User Configuration Overview.

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.

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 238 *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.

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 239 *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.
profile-name	Text String	Up to 49 characters	The name of the user profile.
channel-type	Variable	Serial Web	The access channel type allowed or disallowed by the command for users with this user profile.

Parameter	Input Type	Permitted Values	Description
		NMS Telnet SSH	
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.

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
```

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>
```

Use the following command to edit a user account:

```
root> platform security access-control user-account edit user-name <user-
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.
- 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*.

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>
```

> **Note**
>
> The latest date that can be configured is 30-12-2037.

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 240 *User Accounts CLI Parameters*

Parameter	Input Type	Permitted Values	Description
user-name	Text String	Up to 32 characters. User names cannot include special 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 To configure the user with no expiration date, enter unlimited.	The date on which the user account will expire. When this date occurs, the user automatically becomes inactive.
block	Variable	yes no	yes - blocks the account. no - unblocks the account.

The following command creates a user account named Tom_Jones, with user profile “operator”. This user’s account expires on February 1, 2024.

```
root> platform security access-control user-account add user-name Tom_
Jones profile-name operator expired-date 2024-02-01
```

The following command creates a user account named Sam_Wilson, with user profile “operator” and no expiration date.

```
root> platform security access-control user-account add user-name Sam_
Wilson profile-name operator expired-date unlimited
```

Configuring RADIUS (CLI)

This section includes:

- Activating RADIUS Authentication (CLI)
- Configuring the RADIUS Server Attributes (CLI)

Note

For instructions on configuring a RADIUS server, see Configuring a RADIUS Server. For an overview of RADIUS, see RADIUS Overview.

Activating RADIUS Authentication (CLI)

To enable or disable Radius access control, enter the following command:

```
root> platform security radius-admin set <admin>
```

Table 241 *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 242 *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.

Parameter	Input Type	Permitted Values	Description
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
```

Configuring TACACS+ (CLI)

Notes

For an overview of TACACS+, see TACACS+ Overview.

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 entering the *admin = enable* command below, all active sessions are terminated and you must log in again via TACACS+.

To enable or disable TACACS+ access control, enter the following command in root view:

```
root>platform security tacacs-plus set admin <enable|disable>
```

To define a timeout (in seconds), enter the following command in root view:

```
root>platform security tacacs-plus set timeout <1-60>
```

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.

To define the number of retries, enter the following command in root view:

```
root> platform security tacacs-plus set retry <1-5>
```

This sets 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.

To set the TACACS+ server attributes, enter one of the following commands, depending on whether you want to configure the TACACS+ server's IP address in IPv4 or IPv6 format. You can configure up to four TACACS+ servers. When authenticating a user, the device contacts attempts to contact the TACACS+ servers in the order of the Server IDs you assign to each server. If no response is received from Server 1 within the user-defined timeout period, the device attempts to contact Server 2, then Server 3, then Server 4. If no response is received from any of the servers, the device performs user authentication locally.

Note

You cannot enter both an IPV4 and an IPV6 address. Whichever format you enter, the other field must be left blank.

To determine the authentication type for TACACS+, enter the following command in root view:

```
root> platform security tacacs-plus set authentication type
<ascii|pap|chap>
```

To configure a TACACS+ server with an IPv4 IP address, enter the following command in root view:

```
root> platform security tacacs-plus set ipv4 server-id <1-4> ip-address
<IPv4-address> port <port> shared-secret <shared-secret>
```

To configure a TACACS+ server with an IPv6 IP address, enter the following command in root view:

```
root>platform security tacacs-plus set ipv6 server-id <1-4> ip-address
<IPv6-address> port < port > shared-secret <shared-secret>
```

To delete a TACACS+ server, enter the following command in root view:

```
root>platform security tacacs-plus delete server-id <1-4>
```

Table 243 *TACACS+ CLI Parameters*

Parameter	Input Type	Permitted Values	Description
server-id	Number	1-4	Sets the priority of the server.
IPv4-address	Dotted decimal format	Any valid IPV4 address.	The IP address of the TACACS+ server.
IPv6-address	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The IP address of the TACACS+ server.
port	Number	0-65535	The port ID of the TACACS+ server. The default value is 49.
shared-secret	String	Between 6-63 characters	The shared secret of the TACACS+ server. **Note**This field should not be left empty unless necessary for debugging.

To display the current TACACS+ configuration and status for the device, enter the following command in root view:

```
root>platform security tacacs-plus show
```

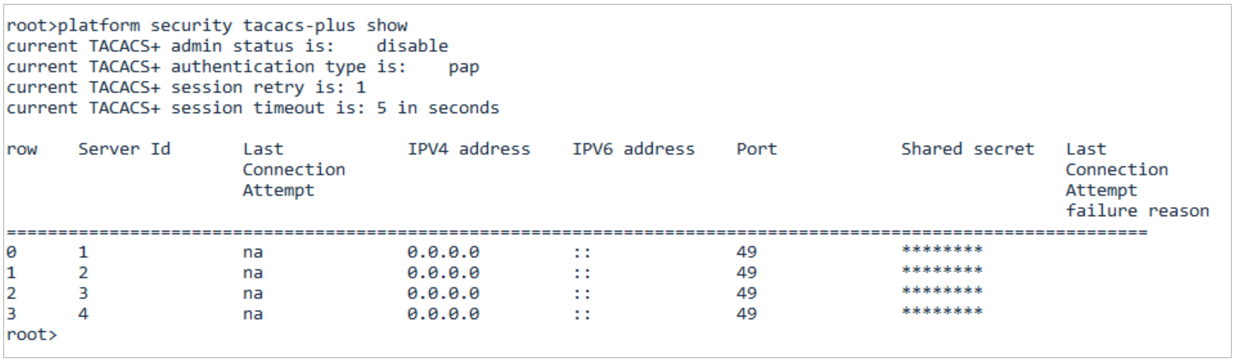
The following is a sample output. In addition to the configurable parameters described above, the command output displays the following for each server:

- **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, the reason for the failure is displayed in the **Last Connection Attempt failure reason** column of the command output:

    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.



```
root>platform security tacacs-plus show
current TACACS+ admin status is:    disable
current TACACS+ authentication type is:    pap
current TACACS+ session retry is: 1
current TACACS+ session timeout is: 5 in seconds

row    Server Id       Last            IPV4 address    IPV6 address    Port            Shared secret   Last
                       Connection                                                                      Connection
                       Attempt                                                                         Attempt
                                                                                                       failure reason
===============================================================================================================
0      1               na              0.0.0.0         ::              49              ********
1      2               na              0.0.0.0         ::              49              ********
2      3               na              0.0.0.0         ::              49              ********
3      4               na              0.0.0.0         ::              49              ********
root>
```

Displaying Remote Access Users

You can view remote access user connectivity and permissions information for all RADIUS or TACACS+ 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, Normal, or Advanced.
- **Security Func Group Write level** – The Write access level in the Security functional group: None, Normal, or Advanced.

- **Management Func Group Read level** – The Read access level in the Management functional group: None, Normal, or Advanced.
- **Management Func Group Write level** – The Write access level in the Management functional group: None, Normal, or Advanced.
- **Radio Func Group Read level** – The Read access level in the Radio functional group: None, Normal, or Advanced.
- **Radio Func Group Write level** – The Write access level in the Radio functional group: None, Normal, or Advanced.
- **TDM Func Group Read level** – The Read access level in the TDM functional group: None, Normal, or Advanced.
- **TDM Func Group Write level** – The Write access level in the TDM functional group: None, Normal, or Advanced.
- **Eth Func Group Read level** – The Read access level in the Eth functional group: None, Normal, or Advanced.
- **Eth Func Group Write level** – The Write access level in the Eth functional group: None, Normal, or Advanced.
- **Sync Func Group Read level** – The Read access level in the Sync functional group: None, Normal, or Advanced.
- **Sync Func Group Write level** – The Write access level in the Sync functional group: None, Normal, or Advanced.

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)

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 (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 244 *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)
state	String		The state, province, or region in which the organization is located. Do not abbreviate.

Parameter	Input Type	Permitted Values	Description
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.
password	Text String		The password for the SFTP session. To configure the SFTP settings without a password, simply omit this parameter.

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 245 *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.
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.

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 http
```

To display which protocol is currently enabled, enter the following command in root view:

```
root> platform security url-protocol-show
```

If you change the protocol to HTTPS, you can also block Port 80 and redirect traffic to Port 443. By default, Port 80 is not blocked. To change this setting, enter the following command in root view:

```
root> platform security protocols-control http redirect-to-https set
<no|yes>
```

The following command blocks Port 80:

```
root> platform security protocols-control http redirect-to-https set no
```

The following command unblocks Port 80:

```
root> platform security protocols-control http redirect-to-https set yes
```

To display the current setting for Port 80 blocking, enter the following command in root view:

```
root> platform security protocols-control http redirect-to-https-show
```

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+7jRmt27yF4xDh5Pc8w4ikvXUu32BI
0eOyELmeUBnEeIHbCOXD3upi8+ZnH51Q+8hzgoSqXgEYFgZMoF/sXCrO2yf62UJ5ohj3zadhx/7585zoG
wHtYz1S62hsa4+cdAl/i1Vbc6CoUBh5642XYje+Q+q1XJtObed884eaQcXUFLlBipYKvVx2kuelymansE91WJ
U+UjFlc3aiQG8qsSgW5Ar6wet0pXkP2Vdemo//QAXXjcTqqMBuizrlhlcvi+OKYFl9kSh21ZqSgjvK3cfAssCJ
BlY5d6t6bVkX9p2gjo/lPnErjAv7W6lZoemotb5KAeSHeR1sYTw17/xlpM7AgMBAAECggEAAwliLKQMOq4k

h/UXD/OPAlPDXyp1jjaTw8dBm811OG5wttzXGrxJ+OIFX5Rn79DbHnbayCiJL8tMe2dx5yhY+hA247roX3ua
0w57cuPxnp21izc+S0fC7H/TTM1jpRCbATparuTRMlitinZshJGA73Lsod3v36GEXxm/6dHnz/drCs2F4NdHW
pjMAAG/1CiBwut8jNkJUwa78Ivk3JF+XRoZ0txN2mIybQxxzjuNXqZbNO6H3Ua2u1iYyD+McfgOWCCUfSns
tGRhFg0OsQuqj6d74qKVQWaukEH91SVZHEoqX6DgpKy4INZBxORZmlTNmadwNhw5O7rvFxZ205u4gQ
KBgQDT5bXvc0Ok+Ypm2xnIbu2GFjxNYwYhR3TvHPy14NIO5Q9I/uDqwrSL1igzalr6EbZyLu8cDXa4aybrz
CyBfPeG89Qq+a6J3JR/RwJndLyjV4h5CT8Zy4O/wjgTrP3Rhq7LAbWgLjSarafLgruHTcnOifhkK7MK7Fr+xi2
lJfOKQQKBgQDmq1eYNzlMPlATESlsfbkcL49jSsu70kYg0g5Iol6+bVPo9K7mopICtWC/fwdNlUAfO+vr/231
YUfSo7YNEDNNRoT/NwvqqtAYxZaIUdIQxhMywF9jjYBBuq6+f/7+dwDfNBtMb2q7hceTdk6yZ8/MehCkvS
wOBmP+lq0FwTmmewKBgQClxmj31G1ve+rTXUZmkKly7OJwiLAbCRRqnXr3r9Om43151i2QfJNTc1AwKVz
Tl1ftLNrUT5Q541qnzyxigaoFYmzy0jPCl1d128/9sE6EW87hImLDg3ynYQMOIaDRc1T8bXHyxzNQb9t+U+Dy
keD4POifNbD1MsRd3h1xDn/iAQKBgHmKpukJkCNgYgjp7g3AYR084izLaHZa4aDBjc0v4QQtzxzccJwN5S
mQMJ42bL6wecz7YeBEAshcrd+La42Oj7mUAtgHRTwtLOEgm6TQmANGmy8OtjRahs4bc5/lCZNDWS5C
4m9v9alBYFuO5wCSOqffWY20L9Zj/6RR+HEj0yCpAoGAHwrbRqPVZtZptFuNsCq130dtmqI7HFQAlqrc5D
wP7YSsznE6biHfLUw891xu0vmevALrCaoeOMaidugohgiorSJO4qk7I3XN3pUJhPYqbhtdCVnBI2Fm9pr3V
/SHGvrl1NW92cXObeQ2UEBiKPOyQKfOBlbac707u0HqaTu+/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 246 *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 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 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 “”..

Enabling Telnet Access (CLI)

You can enable or disable telnet access to the unit. By default, telnet access is disabled.

To enable telnet access, enter the following command:

```
root> platform security protocols-control telnet admin set enable
```

To disable telnet access, enter the following command:

```
root> platform security protocols-control telnet admin set disable
```

To display whether telnet is currently enabled or disabled, enter the following command:

```
root> platform security protocols-control telnet show
```

Note

When you disable telnet after it has been enabled, any current telnet sessions are immediately disconnected.

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 drop
```

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 247 *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

Parameter	Input Type	Permitted Values	Description
			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.
ip-address	Dotted decimal format.	Any valid IP address.	The IP address of the FTP server.
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.

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
```

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 248 *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. 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. For example: UnitInfo.zip 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	ftp sftp	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

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 ftp
```

The following command exports the configuration log to the external server location:

```
root> platform security configuration-log upload
```

Enabling NETCONF (CLI)

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.

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
```

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

Alarm Management and Troubleshooting (CLI)

This section includes:

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
```

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
```

Note

You can save the event log to a CSV file from the Web EMS. See Viewing and Saving the Event Log.

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)

Displaying Alarm Information (CLI)

To display a list of all alarm types, their severity levels, descriptions, and admin status (enabled or disabled), enter the following command in root view:

```
root> platform status alarm-management show alarm-id all
```

To display the attributes of a specific alarm, enter the following command in root view:

```
root> platform status alarm-management show alarm-id <alarm-id> attributes
```

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 249 *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.

The following command changes the severity level of alarm type 401 (Loss of Carrier) to minor:

```
root> platform status alarm-management set alarm-id 401 severity-level
minor
```

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
```

The following command restores alarm type 401 (Loss of Carrier) to its default severity level:

```
root> platform status alarm-management set alarm-id 401 restore default
```

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.

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
```

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.

Note

All alarms are enabled by default except the Auto Negotiation Speed alarm (Alarm ID 402). See Enabling the Auto Negotiation Speed Alarm (CLI).

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 except Alarm ID 402, enter the following command in root view:

```
root> platform status alarm-management set all admin default
```

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. See Enabling the Auto Negotiation Speed Alarm (CLI).

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.

Enabling the Auto Negotiation Speed Alarm (CLI)

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, enter the following command:

```
root> platform status alarm-management set alarm-id 402 admin enable
```

Configuring Voltage Alarm Thresholds and Displaying Voltage PMs (CLI)

You can configure undervoltage and overvoltage alarm thresholds.

The default thresholds for PTP 850EX devices 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>
```

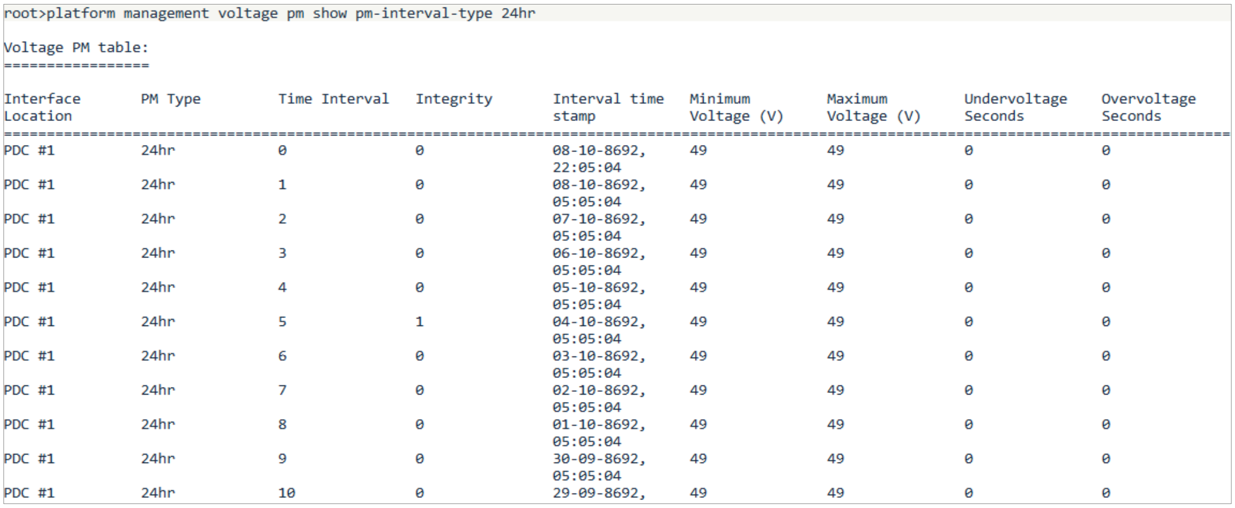
You can display voltage PMs that indicate, per 15-minute and 24-hour periods:

- 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               0               08-10-8692,     49              49              0               0
                                                                22:05:04
PDC #1          24hr            1               0               08-10-8692,     49              49              0               0
                                                                05:05:04
PDC #1          24hr            2               0               07-10-8692,     49              49              0               0
                                                                05:05:04
PDC #1          24hr            3               0               06-10-8692,     49              49              0               0
                                                                05:05:04
PDC #1          24hr            4               0               05-10-8692,     49              49              0               0
                                                                05:05:04
PDC #1          24hr            5               1               04-10-8692,     49              49              0               0
                                                                05:05:04
PDC #1          24hr            6               0               03-10-8692,     49              49              0               0
                                                                05:05:04
PDC #1          24hr            7               0               02-10-8692,     49              49              0               0
                                                                05:05:04
PDC #1          24hr            8               0               01-10-8692,     49              49              0               0
                                                                05:05:04
PDC #1          24hr            9               0               30-09-8692,     49              49              0               0
                                                                05:05:04
PDC #1          24hr            10              0               29-09-8692,     49              49              0               0
```

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.

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 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.

In order to export a unit information file, you must install an FTP or SFTP server on the laptop or PC to which you are performing the export. PTP 850 works with any standard FTP or SFTP server. For details, see Installing and Configuring an FTP or SFTP Server.

Note

You can also use HTTP or HTTPS to upload the Unit Information file. HTTP or HTTPS upload must be performed via the Web EMS. See Uploading Unit Info.

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 root> platform management ip set ip-address-family <IPv4|IPv6> 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 250 *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 "//".
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.

Parameter	Input Type	Permitted Values	Description
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
```

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
```

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 Cambium’s 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. See Uploading Unit Info (CLI).

> **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>.
```

Note

Whenever you activate the Radio Logger, any previous Radio Logger results are deleted.

Configuring Port Mirroring (CLI)

Note

Port Mirroring is planned for future release.

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
```

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, see Syslog Overview.

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.

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>
```

Performing Diagnostics (CLI)

This section includes:

- Performing Radio Loopback (CLI)
- Configuring Service OAM (SOAM) Fault Management (FM) (CLI)

Performing Radio Loopback (CLI)

Notes

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.

Setting radio loopback, either RF or IF, will cause full loss of the end-to-end traffic and in-band management to remote units. 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.

You can perform loopback on a radio.

To set the timeout for a radio loopback, enter the following command in radio view:

```
radio[1/x]> radio loopbacks-timeout set duration <duration>
```

To display the radio loopback timeout, enter the following command in radio view:

```
radio[1/x]>radio loopbacks-timeout show
```

To activate an RF loopback, enter the following command in radio view:

```
radio[1/x]>rf loopback-rf set admin <admin>
```

Table 251 *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.

The following commands initiate an RF loopback with a timeout of two minutes:

```
radio[1/x]> radio loopbacks-timeout set duration 2
radio[1/x]>rf loopback-rf set admin on
```

The following command cancels an RF loopback:

```
radio[1/x]>rf loopback-rf set admin off
```

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)

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
- Loopback

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.

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 252 *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.
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.

Configuring MA/MEGs (CLI)

You can configure up to 256 MEGs per network element. MEGs are classified as Fast MEGs or Slow MEGs according to the CCM interval (see SOAM MEG CLI Configuration Parameters):

- 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 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
<defMHFdefault|defMHFexplicit>
```

For example, 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 253 *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.
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

Parameter	Input Type	Permitted Values	Description
			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.
ccm	Variable	interval100ms interval1s interval10s interval1min interval10min	interval100ms - 100 ms 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

Parameter	Input Type	Permitted Values	Description
			domain is encompassed by another domain. defMHFdefer – No MIPs are created.

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).

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>
```

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>
```

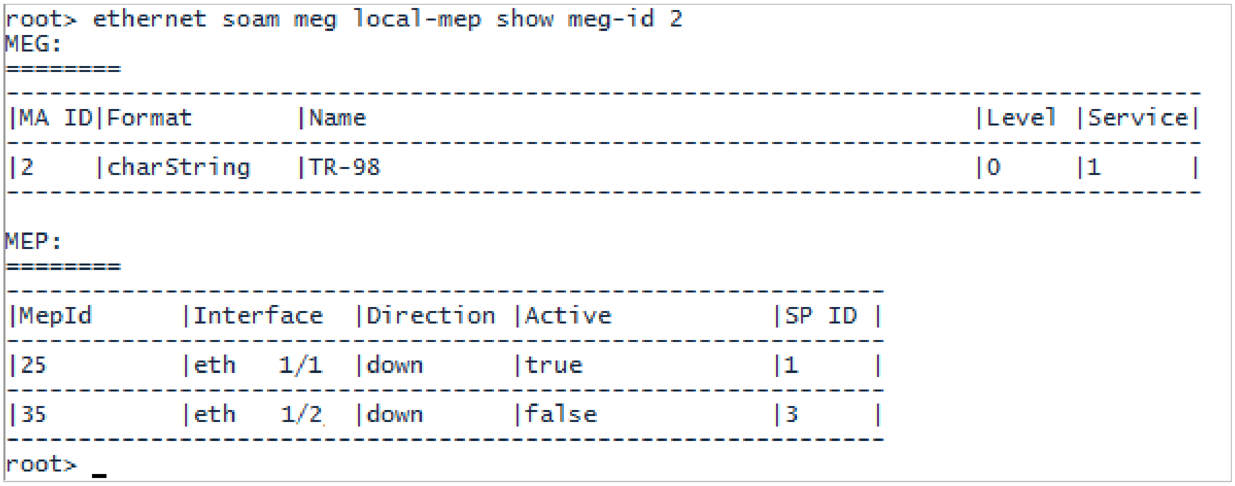
The following command changes MEP 35 from a local to a remote MEP.

```
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> _
```

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 254 *MEP CLI Configuration Parameters*

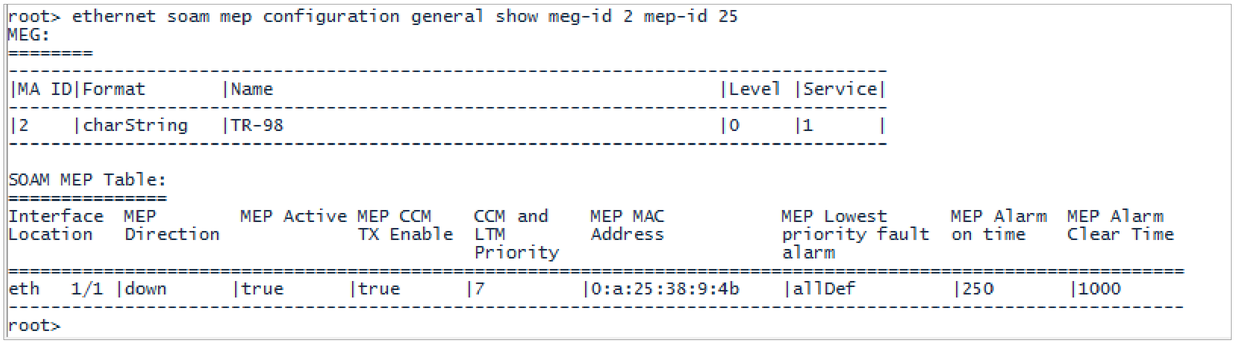
Parameter	Input Type	Permitted Values	Description
meg-id	Number	1-4294967295	Enter an ID for the MEG.
mep-id	Number	1-8191	A name to identify the MEG.
sp-id	Number	0-32	The Service Point ID of the service point to which you want to assign the MEP.
mep-dir	Variable	up down	The MEP direction.
ccm-enabled	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.

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:

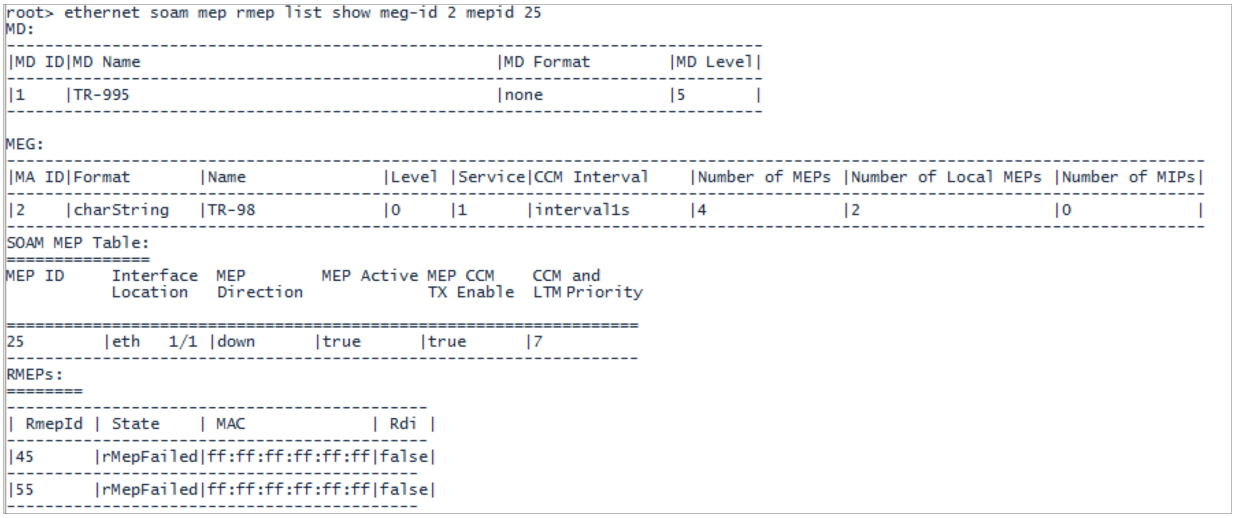


```
root> ethernet soam mep configuration general show meg-id 2 mep-id 25
MEG:
========
----------------------------------------------------------------------------------
|MA ID|Format       |Name                                              |Level |Service|
----------------------------------------------------------------------------------
|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:

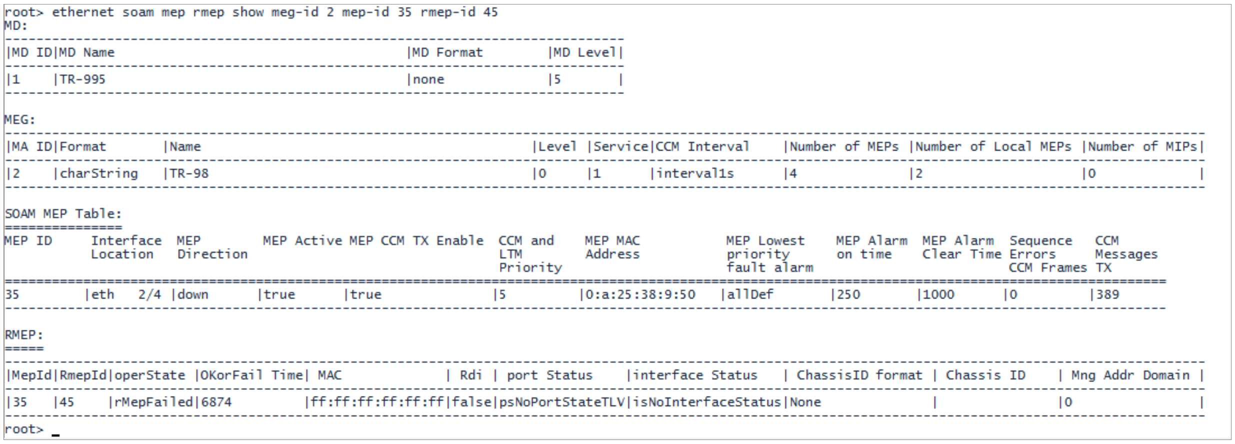


```
root> ethernet soam mep rmep list show meg-id 2 mepid 25
MD:
---------------------------------------------------------------------------
|MD ID|MD Name                                         |MD Format        |MD Level|
---------------------------------------------------------------------------
|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 255 *MEP and Remote MEP Status Parameters (CLI)*

Parameter	Definition
MD Parameters	
MD ID	The MD ID.
MD Name	The MD name (44 characters).

Parameter	Definition
MD Format	The MD format (None).
MD Level	The maintenance level of the MD (0-7).
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).

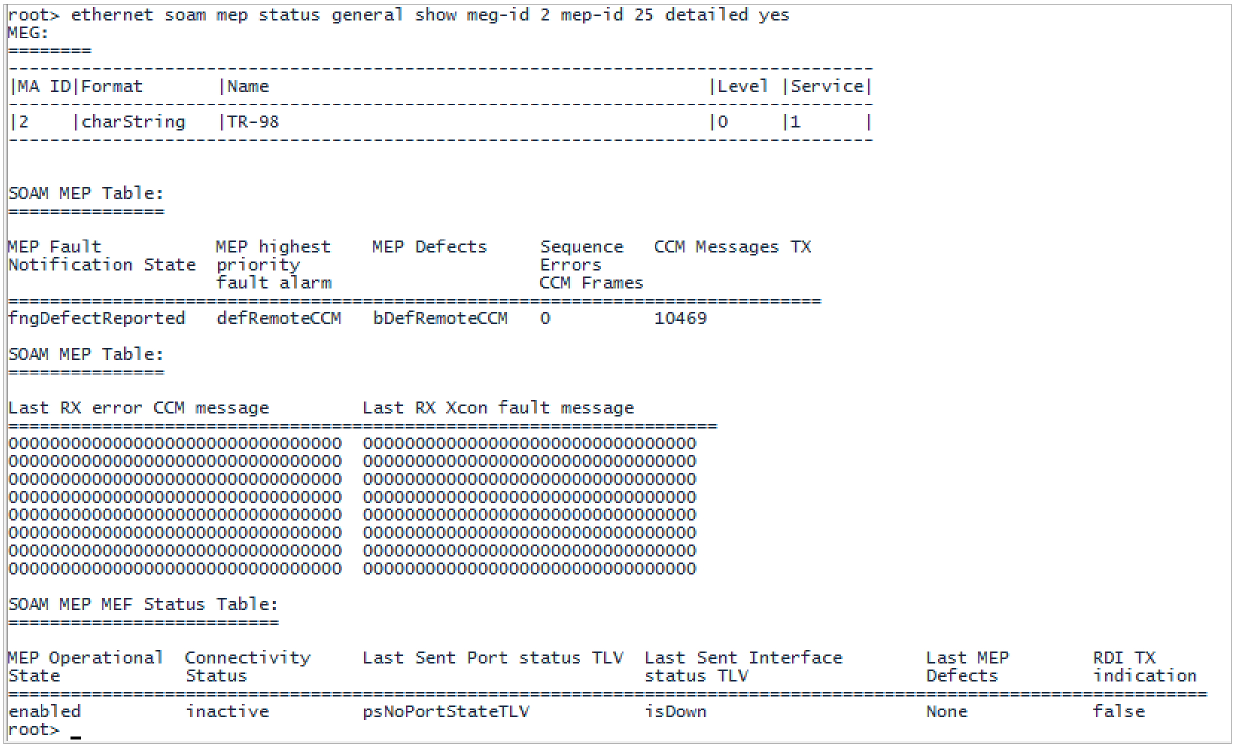
Parameter	Definition
MEP Alarm Clear Time	The amount of time that defects must be absent before an alarm is cleared, msec intervals (250-1000).
Sequence errors CCM Frames	The number of out-of-sequence CCM messages received.
CCM Messages TX	The number of transmitted CCM messages.
RMEP Parameters	
MepId	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).

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.

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
```

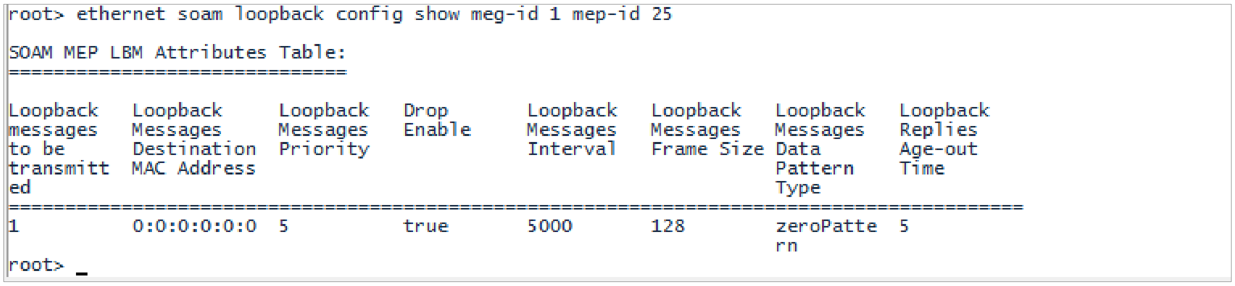
Note:

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>
```

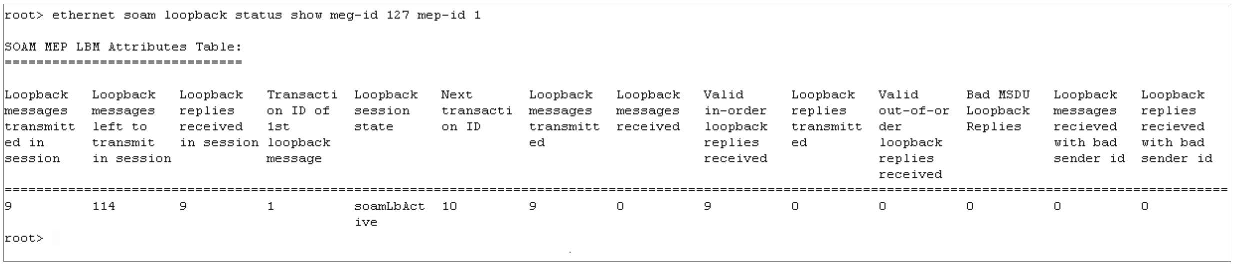
Table 256 *Loopback CLI Parameters*

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.
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

Parameter	Input Type	Permitted Values	Description
			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   Loopback
messages   messages   replies    on ID of   session    transacti  messages   messages   in-order   replies    out-of-or  Loopback   messages   replies
transmitt  left to    received   1st        state      on ID      transmitt  received   loopback   transmitt  der        Replies    recieved   recieved
ed in      transmit   in session loopback                         ed                    replies    ed         loopback              with bad   with bad
session    in session            message                                                received              replies                          sender id  sender id
                                                                                                              received
=======================================================================================================================================================
9          114        9          1          soamLbAct  10         9          0          9          0          0          0          0          0
                                            ive
root>
```

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 in radio view:

```
radio[1/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[1/x] modem tx-source set mode one-tone freq-shift <freq-shift>
```

To transmit two tones, enter the following command in radio view:

```
radio[1/x] modem tx-source set mode two-tone freq-shift <freq-shift> freq-
shift2 <freq-shift>
```

To exit CW mode, enter the following command in radio view:

```
radio[1/x] modem tx-source set admin disable
```

Table 257 *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 1 port 1
radio[1/1] modem tx-source set admin enable
radio[1/1] radio[1/1] modem tx-source set mode one-tone freq-shift 5050
radio[1/1] modem tx-source set admin disable
```

Maintenance

This section includes:

- Troubleshooting TipsTroubleshooting Tips
- Temperature Ranges
- PTP 850EX Interface Pin-outs and LEDS

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.

Temperature Ranges

To display the current unit temperature, see Configuring Unit Parameters.

Temperature Ranges – PTP 850EX

The following is the permissible unit temperature range for PTP 850EX devices:

- -40°C to 55C°/-40°F to +131°F

An extreme temperature alarm (32002) is raised if the unit's internal temperature reaches 90°C/194°F or -40°C/-40°.

The alarm is cleared when the temperature reaches within ±1° of the following values:

- High temperature: 79°C/174°F
- Low temperature: -34°C/-29°F.

The permissible humidity range is 5%RH to 100%RH.

PTP 850EX Interface Pin-outs and LEDS

PTP 850EX Interfaces

PTP 850EX has two optical SFP28 cages for traffic and one RJ-45 port for management and traffic. It also has one QSPF port which can be used as an XPIC/protection port or a 1 x 1GbE or 10GbE traffic port.

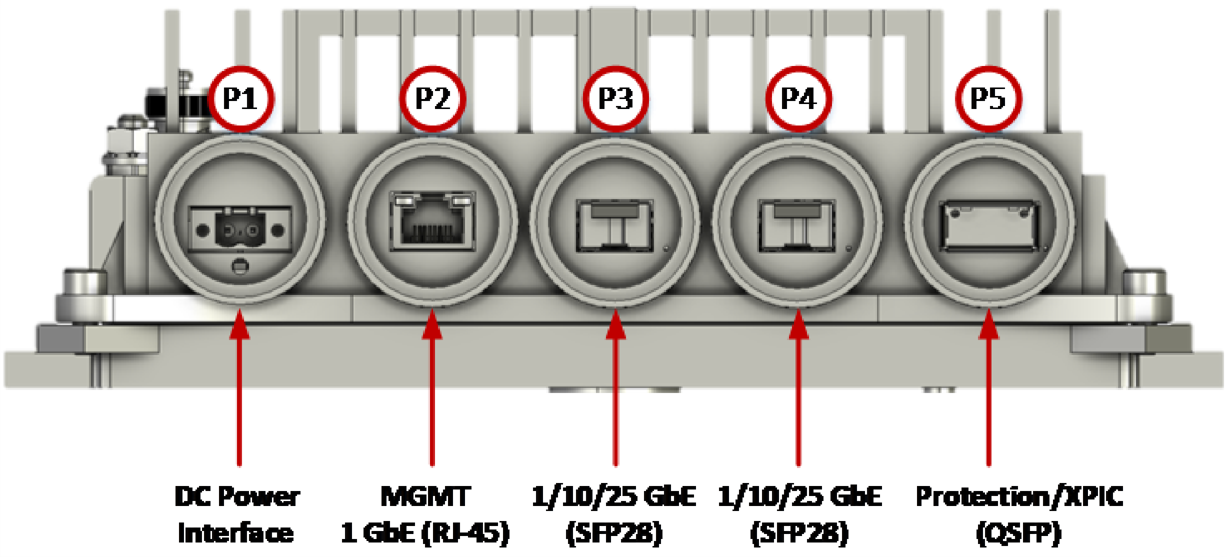
Note

XPIC and Unit Redundancy are planned for future release.

PTP 850EX also has an RJ-45 management port.

For power, the PTP 850EX has a DC power interface (-48V) (Port 1).

Figure 377 *PTP 850EX Interfaces*



- P1 – Power Interface (-48V)
- P2 (MNG 1/Eth 1):
  - Electric: 100/1000Base-T RJ-45
  - Management port (no traffic)
- P3 (Eth 2):
  - SFP cage which supports SFP28 standard
  - 1/10/25 GbE Eth traffic (user configurable)
- P4 (Eth 3):
  - SFP cage which supports SFP28 standard
  - 1/10/25 GbE Eth traffic (user configurable)
- P5 (Eth 4):
  - QSFP (internal) for Protection/XPIC
  - Option for SFP or SFP+ (1 x 1 or 10GbE) with adaptor (1+0 configurations only)
- RSL/Source Sharing interface – TNC connector
- Antenna Port – Cambium proprietary flange (flange compliant with UG385/U)
- Grounding screw

PTP 850EX Interface Pin-outs

P2 – Management Interface (RJ-45)

Table 258 *PTP 850EX Management 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)

P3 and P4 (Eth 2 and Eth 3) Optical Interfaces (SFP28)

P3 and P4 are SFP cages that support the SFP28 standard.

P5 (Eth 4) QSFP Optical Interface (QSFP)

P5 is a QSFP port designed to support Unit Redundancy and XPIC configurations.

Note

XPIC and Unit Redundancy are planned for future release.

It can also be used as a 1/10 Gbps traffic port, with an adaptor (QSFP-to-SFP Adaptor).

RSL Interface

RSL interface – A TNC interface is available to enable voltage measurements for RSL indication. You can use a BNC-to-DVM 6 mm jack cable to measure the RSL with this interface.

PTP 850EX LEDs

The PTP 850EX provides the following LEDs to indicate the status of the unit's interfaces, and the unit as a whole:

- P2 Management Interface (RJ-45) LEDs
- P3 and P4 Optical Interface (SFP28) LEDs
- P5 QSFP Optical Interface (QSFP) LEDs
- Status LED

P2 Management Interface (RJ-45) LEDs

There are two LEDs next to the MGT interface, on the upper left and upper right of the interface.

The LED on the left indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

- **Off** – The cable is disconnected.
- **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 on the right is for future use.

> **Note**
>
> The ability to use the Management interface for traffic is planned for future release.

P3 and P4 Optical Interface (SFP28) LEDs

There is one Green LED to the left of each interface. This LED indicates the status of 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 Blinking Green state is not supported in System Release 12.7.

P5 QSFP Optical Interface (QSFP) LEDs

There is one Green LED to the left of the interface. This LED indicates the status of 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 Blinking Green state is not supported in System Release 12.7.

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. In a Unit Redundancy configuration, Green (without blinking) also indicates that the unit is the Active unit.

- **Green Blinking -** The power is on, the unit is up, the radio is up, and no major or critical alarms are raised. In a Unit Redundancy configuration, the blinking indicates that the unit is the Standby unit in a 1+1 HSB configuration.

Note

Unit Redundancy is planned for future release.

Abbreviations

The following table lists the abbreviations used in this guide.

Table 259 *Abbreviations*

A	
AC	Alternating Current
ACAP	Adjacent Channel Alternate Polarization
ACCP	Adjacent Channel Co-Polarization
ACM	Adaptive Coding Modulation
ACMB	Adaptive Coding Modulation and Bandwidth
AIS	Alarm Indicating Signal
AMCC	Advanced Multi-Carrier Configuration
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ATPC	Automatic Transmit Power Control

B	
BBU	Baseband Unit
BER	Bit Error Rate

C	
CBS	Committed Burst Size
CCITT	Comité Consultatif International de Télégraph et des Télécommunications (ITU)
CCM	Continuity Check Message
CET	Carrier-Ethernet Transport
CFM	Connectivity Fault Management
CIR	Committed Information Rate
CLI	Command Line Interface
Clk	Clock
CoS	Class of Service

D	
DAD	Destination Address
DC	Direct Current
DDM	Digital Diagnostic Monitoring
DSCP	Differentiated Services Code Point
DST	Daylight Savings Time
DUID	DHCP Unique Identifier

E	
EBS	Excess Burst Size
EIR	Excess Information Rate
EMC	Electromagnetic Compatibility
ESD	Electrostatic Discharge
ETH-BN	Ethernet Bandwidth Notification
ETSI	European Telecommunications Standards Institute

F	
FCC	Federal Communications Commission
FTP	File Transfer Protocol

G	
GARP	Gratuitous ARP
GbE	Gigabit Ethernet

H	
HTTP	Hypertext Transfer Protocol
HTTPS	Secured Hypertext Transfer Protocol

I	
IDC	Indoor Controller
IF	Intermediate Frequency
IPSec	Internet Security Protocol
ISO	International Organization for Standardization
ITU	International Telecom. Union
ITU-R	International Telecom. Union (former CCIR)
ITU-T	International Telecom. Union (former CCITT)

L	
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LED	Light Emitting Diode
LOC	Loss of Carrier
LOF	Loss of Frame
LOS	Loss of Signal

M	
MAID	Maintenance Association Identifier
MPLS	Multi Protocol Label Switching

N	
NMS	Network Management System
NTP	Network Time Protocol

O	
OAM	Operation Administration & Maintenance (Protocols)
OCB	Outdoor Circulator Box

P	
PC	Personal Computer
PCB	Printed Circuit Board
PIR	Peak Information Rate
PM	Performance Monitoring
PROM	Programmable Read Only Memory
PWR	Power

Q	
QoS	Quality of Service

R	
RBAC	Role Based Access Control
RDI	Reverse Defect Indication
RF	Radio Frequency
RMON	Remote Network Monitoring
RRH	Remote Radio Head
RSA	Rivest–Shamir–Adleman public-key cryptosystem
RSL	Received Signal Level
RSTP	Rapid Spanning Tree Protocol

S	
SAP	Service Access Point
SFTP	Secure FTP
SLA	Service Level Agreements
SNMP	Simple Network Management Protocol
SNP	Service Network Point
SNTP	Simple Network Time Protocol
SOAM	Service OAM

SP	Service Point
SSH	Secured Shell (Protocol)
STP	Spanning Tree Protocol
SyncE	Synchronous Ethernet
Syslog	System Logging Protocol

T	
TACACS+	Terminal Access Controller Access-Control System Plus
TC	Traffic Class
TLS	Transport Layer Security

U	
UDP	User Datagram Protocol

V	
VC	Virtual Container

W	
Web EMS	Web-Based Element Management System
WFQ	Weighted Fair Queue
WRED	Weighted Random Early Detection
WRR	Weighted Round Robin

X	
XCVR	Transceiver (Transmitter/Receiver)
XO	Crystal Oscillator
XPIC	Cross Polarization Interference Cancellation