



MIB REFERENCE GUIDE

PTP 820 and PTP 850 System Release

Release 13.3



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.

© 2026 Cambium Networks Limited. All rights reserved

Contents

Contents	3
Private MIB reference	5
Standard MIB support	7
RFC-1213 (MIB II)	7
System parameters	7
Interfaces	8
ifTable	8
Other parameters and tables	14
Multiple Spanning Tree Protocol (MSTP)	14
Trap ID	14
Trap Var-Bind	15
Common tasks	18
Software management	18
Downloading a software version	18
Configuration file management	21
System configuration FTP settings	21
Creating and uploading backup configuration archives	22
Backup and Export status	23
Enabling and configuring traps	23
Enabling trap administration	23
Managing a trap	23
Viewing current alarms	24
Alarm date and time	24
Alarm severity	25
Alarm description	25
Probable cause	25
Corrective actions	25
Viewing event log	26
Event date and time	26
Event severity	26
Event description	26

Event state	27
Performance monitoring and counters	27
Clearing all performance counter data	27
Managing radio configuration	27
Setting the radio threshold	27
Setting the traffic PM thresholds	28
MIB Revision History	29
MIB error table (Reserved for future use)	30
Alarms	31
Cambium Networks	123

Private MIB reference

The following table lists and describes the MIB files and file versions supported by System Release 13.3.

Table 1 *MIB File Names and Versions*

MIB File Name	MIB File Version	Description
MWRM-NETWORK-MIB	1.13.3.1	Networking related OIDs, including Ethernet switch configuration, forwarding, quality of service (QoS), policing, control protocols, and management.
MWRM-PM-MIB	1.13.3.1	Performance Monitoring OIDs for Ethernet and radio.
MWRM-RADIO-MIB	1.13.1.1	Radio related OIDs, including RFU and radio management, MRMC, radio group management (HSB, ABC), header de-duplication, and frame cut-through.
MWRM-TRAPS-MIB	1.12.3.1	Describes the System Release device-specific traps.
MWRM-UNIT-MIB	1.13.1.1	General platform-related OIDs, including alarm and event services, NTP, license, software version management, configuration management, and security and access control.
MWRM-DEFS.MIB		OID for microwave-radio (formerly in MMRM-RADIO-MIB).

You can display a list of entities in the private MIB from the Web EMS of any System Release device:

1. From the Web EMS main menu, select **Utilities > MIB Reference Guide**. The MIB Reference Table opens.

Table 2 MIB Reference Table in Web EMS

#	MIB OID	MIB Name	Type	MIB Type	MIB Access	Description
1	1.3.6.1.2.1.1.1	sysDescr	Scalar	OCTET STRING	read-only	A short description of the system
2	1.3.6.1.2.1.1.2	sysObjectID	Scalar	OCTET STRING	read-only	System object ID
3	1.3.6.1.2.1.1.3	sysUpTime	Scalar	INTEGER	read-only	The time (in hundredths of a second) since the system was last re-initialized
4	1.3.6.1.2.1.1.4	sysContact	Scalar	OCTET STRING	read-write	The required contact person for the system
5	1.3.6.1.2.1.1.5	sysName	Scalar	OCTET STRING	read-write	The name of the system
6	1.3.6.1.2.1.1.6	sysLocation	Scalar	OCTET STRING	read-write	The location of the system
7	1.3.6.1.2.1.2.2	ifTable	Table		not-accessible	This table contains a list of configuration information about the user managed interfaces
8	1.3.6.1.2.1.2.2.1.1	ifIndex	Column	INTEGER	read-only	Interface location
9	1.3.6.1.2.1.2.2.1.2	ifDescr	Column	OCTET STRING	read-only	A textual string containing information about the interface
10	1.3.6.1.2.1.2.2.1.3	ifType	Column	INTEGER (1..-1)	read-only	The type of the interface
11	1.3.6.1.2.1.2.2.1.4	ifHtu	Column	INTEGER (1..10000)	read-only	Maximum Transmission Unit. "The size of the largest datagram which can be sent/receive on the interface, specified in octets"
12	1.3.6.1.2.1.2.2.1.5	ifSpeed	Column	INTEGER	read-only	An estimate of the interface's bandwidth in bits per second
13	1.3.6.1.2.1.2.2.1.6	ifPhysAddress	Column	OCTET STRING	read-only	The MAC (Media Access Control) address of the interface
14	1.3.6.1.2.1.2.2.1.7	ifAdminStatus	Column	INTEGER (1..2)	read-write	The desired state of the interface
15	1.3.6.1.2.1.2.2.1.8	ifOperStatus	Column	INTEGER (1..7)	read-only	The current operational state of the interface
16	1.3.6.1.2.1.2.2.1.9	ifLastChange	Column	INTEGER (1..-1)	read-only	The value of system up time at the time the interface has entered its current operational-state
17	1.3.6.1.2.1.2.2.1.10	ifInOctets	Column	Counter32	read-only	The total number of octets received on the interface

2. The MIB Reference Table is customized to the type of device you are using. There are several separate versions of the MIB Reference Table:

- PTP 820C, PTP 820C-HP, PTP 820S
- PTP 820N and PTP 820A with TCC-U
- PTP 820N and PTP 820A with other TCC models
- PTP 850C and PTP 850E
- PTP 850CX, PTP 850EX, PTP 850EX-P, and PTP 850EXA
- PTP 850GP and PTP 850GPX



Note:

Even though the MIB Reference Table is customized to these product groups, some of the entities listed in the Table may not be relevant to the particular device you are using. This may occur because of activation key restrictions, minor differences between hardware types, or simply because a certain feature is not used in a particular configuration.

3. 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.
4. To save the MIB Reference Table as a .csv file, click **Save to File**.

Standard MIB support

This chapter details the public MIB standards supported by the System Release MIB.

RFC-1213 (MIB II)

This section details the implementation of each area of the RFC-1213 standard within the context of the System Release MIB.

System parameters

The table below details the legal values for each system parameter within RFC-1213 from implementation within the System Release MIB.

Table 3 *System Parameters*

Parameter	Access	Description
sysDescr	Read only	A description of the network element.
sysUpTime	Read only	The time (in hundredths of a second) since the network management portion of the system was last re-initialized
sysContact	Read write	The name of the contact person for this network element
sysName	Read write	An administratively assigned name for the network element. By convention, this is the node's fully qualified domain name
sysLocation	Read write	The physical location of the network element of this node

The table below details the System Object IDs (sysObjectID) within the System Release MIB. The sysObjectID is a unique identifier for the product type.

Table 4 *System Object IDs*

Product	System Object ID
PTP 820 Products	1.3.6.1.4.1.2281.1.20
PTP 820 Indoor Units	1.3.6.1.4.1.2281.1.20.1
PTP 820N 1RU	1.3.6.1.4.1.2281.1.20.1.1
PTP 820A 1RU	1.3.6.1.4.1.2281.1.20.1.1.2
PTP 820N 2RU	1.3.6.1.4.1.2281.1.20.1.2
PTP 820A 2RU	1.3.6.1.4.1.2281.1.20.1.2.2
PTP 820C	1.3.6.1.4.1.2281.1.20.2.2

Product	System Object ID
PTP 820C-HP	1.3.6.1.4.1.2281.1.20.2.2.8
PTP 820S	1.3.6.1.4.1.2281.1.20.2.2.2
PTP 820V	1.3.6.1.4.1.2281.1.20.2.4.1
PTP 850C	1.3.6.1.4.1.2281.1.20.2.2.12
PTP 850CX	1.3.6.1.4.1.2281.1.20.2.2.16
PTP 850E	1.3.6.1.4.1.2281.1.20.2.2.10
PTP 850EX	1.3.6.1.4.1.2281.1.20.2.2.15
PTP 850EX-P	1.3.6.1.4.1.2281.1.20.2.2.17
PTP 850EXA	1.3.6.1.4.1.2281.1.20.2.2.18
PTP 850GP	1.3.6.1.4.1.2281.1.20.1.5.1
PTP 850GPX	1.3.6.1.4.1.2281.1.20.1.5.2

Interfaces

ifNumber - The number of network interfaces (regardless of their current state) present on this system.

ifTable

The ifTable provides a list of all available interfaces to the application developer.

ifTable column supported

This section details ifTable support within the System Release MIB.

Table 5 *Supported IfTables*

MIB Name	OID	Notes
Ifindex	1.3.6.1.2.1.2.2.1.1	
Ifdescr	1.3.6.1.2.1.2.2.1.2	
Iftype	1.3.6.1.2.1.2.2.1.3	
Ifspeed	1.3.6.1.2.1.2.2.1.5	
Ifadminstatus	1.3.6.1.2.1.2.2.1.7	
Ifoperstatus	1.3.6.1.2.1.2.2.1.8	
Iflastchange	1.3.6.1.2.1.2.2.1.9	

MIB Name	OID	Notes
IfIndiscards	1.3.6.1.2.1.2.2.1.13	
IfInErrors	1.3.6.1.2.1.2.2.1.14	
IfOutdiscards	1.3.6.1.2.1.2.2.1.19	
IfOuterrors	1.3.6.1.2.1.2.2.1.20	

IfXTable

Table 6 *Standard IfXtable support*

MIB Name	OID	Notes
ifName	1.3.6.1.2.1.31.1.1.1.1	
ifInMulticastPkts	1.3.6.1.2.1.31.1.1.1.2	
ifInBroadcastPkts	1.3.6.1.2.1.31.1.1.1.3	
ifOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.4	
ifOutBroadcastPkts	1.3.6.1.2.1.31.1.1.1.5	
ifHCInOctets	1.3.6.1.2.1.31.1.1.1.6	
ifHCOctets	1.3.6.1.2.1.31.1.1.1.10	
ifHighSpeed	1.3.6.1.2.1.31.1.1.1.15	
ifAlias	1.3.6.1.2.1.31.1.1.1.18	

RMON – etherStatsTable

MIB Name	OID	Notes
etherStatsIndex	1.3.6.1.2.1.16.1.1.1.1	
etherStatsOctets	1.3.6.1.2.1.16.1.1.1.4	
etherStatsPkts	1.3.6.1.2.1.16.1.1.1.5	
etherStatsBroadcastPkts	1.3.6.1.2.1.16.1.1.1.6	
etherStatsMulticastPkts	1.3.6.1.2.1.16.1.1.1.7	
etherStatsCRCAlignPkts	1.3.6.1.2.1.16.1.1.1.8	
etherStatsUndersizePkts	1.3.6.1.2.1.16.1.1.1.9	
etherStatsOversizePkts	1.3.6.1.2.1.16.1.1.1.10	
etherStatsFragments	1.3.6.1.2.1.16.1.1.1.11	

MIB Name	OID	Notes
etherStatsJabbers	1.3.6.1.2.1.16.1.1.1.12	
etherStatsPkts64Octest	1.3.6.1.2.1.16.1.1.1.14	
etherStatsPkts64Octest	1.3.6.1.2.1.16.1.1.1.15	
etherStatsPkts65to127Octest	1.3.6.1.2.1.16.1.1.1.16	
etherStatsPkts127to511Octest	1.3.6.1.2.1.16.1.1.1.17	
etherStatsPkts512to1023Octest	1.3.6.1.2.1.16.1.1.1.18	
etherStatsPkts1024to1518Octest	1.3.6.1.2.1.16.1.1.1.19	

RMON – etherStatsHighCapacityTable

MIB Name	OID	Notes
EtherStatsHighCapacityOctets	1.3.6.1.2.1.16.1.7.1.4	

ifIndex

The IfIndex has the following structure:

Table 7 IfIndex Structure

Bit #	IfIndex (32 bit)					
	31 (MSB)	30..28	27..0 (LSB)			
Function	Reserved = 0	Format	Format dependent structures			
Bit Width	1 bit	3 bits	28 bits			

Table 8 IfIndex “Format” Field Optional Values

Format Value	7..4	3	2	1	0
Function	Reserved	NG Service Format	Reserved	NG Interface Format	Legacy

NG Interface Format

Table 9 NG Interface Format IfIndex Structure

	IfIndex (32 bit)						
Bit #	31 (MSB)	30...28	27...26	25...17	16...13	12...6	5...0 (LSB)
Function	Reserved = 0	Format	Interface Functional	Instance/Service Bundle ID	Interface Functional	Slot	Port

			Type (MSB)		Type (LSB)		
Bit Width	1 bit	3 bits = 001	2 bits	9 bits	4 bits	7 bits	6 bits

Table 10 *IfIndex "Interface Functional Type" Field Optional Values*

Interface Functional Type (6-bit)	
Functional Type Value	Function
0	N/A
1	Ethernet
2	Radio
3	Mng
4	Synch
5	PWE
6	TDM
7	STM-1/OC-3
8	PDC
9	FAN
10	Radio Unit (RFU) Interface
11	RFU-Based ABC Group
12	Enhanced ABC (Multiband)
13	MIMO
14	External Alarm
15	Group
16	Extension Port
17	Advanced Space Diversity
18	Space Diversity
19	XPIC
20	CPRI
21	XPIC State Diversity
22	Link Bonding
23-63	Reserved

Table 11 IfIndex “Slot” Field Optional Values

Slot (7-bit)		
	Slot Value	Function
Physical Slots	0	Chassis
	1	Slot-1
	2	Slot-2
	...	...
	50	PDC-1
	51	PDC-2
	55	Fan
	62	Slot-62
	63	Slot-63
Virtual Slots	64	LAG
	65	MR
	66	CMR/ABC
	67	XPIC
	68	Radio Protection
	69	PWE Protection
	70	MIMO
	71	Enhanced MC-ABC
	72-126	Reserved
	127	IVM

Table 12 IfIndex “Port/Group” Field Optional Values

Port Value	63	62		2	1	0
Function	Port-63	Port-62		Port-2	Port-1	N/A

NG Service Format

Table 13 NG Service Format Ifindex Structure

Ifindex (32 bit)

Bit #	31 (MSB)	30..28	27..24	23..12	11..7	6..4 (LSB)	3..0 (LSB)
-------	----------	--------	--------	--------	-------	------------	------------

Function	Reserved = 0	Format=3	Service type=1	Service Id	Service Point id	MEG Level	Reserved=0
Bit Width	1 bit	3 bits = 011	4 bit	12 bits	5 bits	3bits	4 bits

Table 14 *Service Type*

Service Type Value	15..2	1	0
Function	Reserved	Soam MEP	N/A

- Service Id – Value from 1 to 4096
- Service Point id – Value from 1 to 32
- MEG level – Value from 1 to 7



Note:

The instance is used according to the selected “Interface Functional Type”. For example, if the “Interface Functional Type” is TDM STM-1, the instances can be VC-12 (1..63) or VC-11 (1..84). If the “Interface Functional Type” is TDM E1, the instances can be TS (time slots) 0..31.

Calculation of IfIndex

The IfIndex for NG (Format = 1) is calculated as follows:

- IfIndex (decimal) = 268435456 + (Instance * 131072) + (Interface-Functional-Type * 8192) + (Slot * 64) + Port
- IfIndex (hex) = 0x10000000 + (Instance * 0x20000) (Interface-Functional-Type * 0x2000) + (Slot * 0x40) + Port

Given NG IfIndex (Format = 1), the following will be calculated out of it:

- Instance = (IfIndex >> 16) and 0x7FF
- Interface-Functional-Type = (IfIndex >> 12) and 0xF
- Slot = (IfIndex >> 5) and 0x7F
- **Port** = IfIndex and 0x3F

IfIndex Examples

Table 15 *IfIndex Examples*

Functional Type	Instance	Slot/Port	IfIndex (decimal)	IfIndex (Hex)
Ethernet	0	1/1	268443713	0x10002041
Ethernet	0	1/2	268443714	0x10002042
Group	0	LAG/1	268447745	0x10003001

Functional Type	Instance	Slot/Port	IfIndex (decimal)	IfIndex (Hex)
Group	0	MR/1	268456001	0x10005041
Group	0	MR/2	268456002	0x10005042
Management	0	1/1	268460097	0x10006041
Radio	0	1/1	268451905	0x10004041
TDM	VC27	2/1	272023681	0x1036C081

Other parameters and tables

The following parameters and tables are answered by the CPU interface of the network element.

Table 16 *Other Supported Networking Parameters*

Parameters	Supported by System Release MIB
AT (atTable)	Supported
IP	Supported (also defined in RFC 2011)
ICMP	Supported
TCP	Supported (also defined in RFC 2012)
UDP	Supported (also defined in RFC 2013)

Multiple Spanning Tree Protocol (MSTP)

System Release products support the following standard MIBs for Multiple Spanning Tree Protocol (MSTP):

- IEEE8021-MSTP-MIB-201103230000Z
- IEEE8021-SPANNING-TREE-MIB-200810150000Z

These MIBs are derived from IETF BRIDGE_MIB (RFC-4188).

There are two additional MSTP related MIBs which are part of the private MIB, since they are not defined as part of the standard MSTP MIB:

- genEquipProtocolsMstpGeneralAttributesTable
- genEquipProtocolsMstpCountersTable

For more details, refer to the MIB Reference Table. See [Private MIB reference](#).

Trap ID

The following table describes the Trap ID definition in NETWORK-MIB.

SNMP Version	Trap type	Name	ID
V.1	Alarm / Event	SNMPv1 Trap	2281.2000
V.1	heartbeat	SNMPv1 Trap	2281.2001
V.2/3	Alarm / Event	generalNGV3Trap	2281.11.2000
V.2/3	heartbeat	heartbeatNGV3Trap	2281.11.2001

Trap Var-Bind

Table 17 *Trap Var-Bind Parameters*

SNMP Version	Trap type	Name	OID	Comments
V.2/3	Alarm / Event	sysUpTime	1.3.6.1.2.1.1.3	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.
V.2/3	Alarm / Event	snmpTrapOID	1.3.6.1.6.3.1.1.4.1	The authoritative identification of the notification currently being sent (Trap ID).
V.1/2/3	Alarm / Event / heartbeat	genEquipCurrentAlarmCounter	1.3.6.1.4.1.2281.10.3.1.2.1.1	Contains the information of a RAISED trap.
V.1/2/3	Alarm / Event	genEquipCurrentAlarmRaisedTime T	1.3.6.1.4.1.2281.10.3.1.2.1.2	Time the alarm was raised.
V.1/2/3	Alarm / Event	genEquipNetworkAgentIp	1.3.6.1.4.1.2281.10.2.3	Agent IP address (IP V4)
V.1/2/3	Alarm /	genEquipCurrentAlarmId	1.3.6.1.4.1.2281.10.3.1.2.1.3	Alarm ID.

SNMP Version	Trap type	Name	OID	Comments
	Event			For a complete list of Alarm IDs, see Alarms .
V.1/2/3	Alarm / Event	genEquipCurrentAlarmDesc	1.3.6.1.4.1.2281.10.3.1.2.1.9	Description of the alarm. For a complete list of alarms and their descriptions, see Alarms .
V.1/2/3	Alarm / Event	genEquipCurrentAlarmIfIndex	1.3.6.1.4.1.2281.10.3.1.2.1.7	Interface index that indicates where the alarm occurred.
V.1/2/3	Alarm / Event	genEquipCurrentAlarmInstance	1.3.6.1.4.1.2281.10.3.1.2.1.5	Alarm Instance. For most alarms, this parameter is not used because this information is reflected in the ifindex.
V.1/2/3	Alarm / Event	genEquipCurrentAlarmSeverity	1.3.6.1.4.1.2281.10.3.1.2.1.6	Severity of the current alarm. Possible values are: - Indeterminate (0) - Critical (1) - Major (2) - Minor (3) - Warning (4)

SNMP Version	Trap type	Name	OID	Comments
				- Cleared (5)
V.1/2/3	Alarm / Event	genEquipCurrentAlarmState	1.3.6.1.4.1.2281.10.3.1.2.1.12	Indicates whether the alarm is raised or cleared. Possible values are: - Alarm cleared (0) - Alarm raised (1) - Event (2)
V.1/2/3	Alarm / Event	genEquipCurrentAlarmUserText	1.3.6.1.4.1.2281.10.3.1.2.1.15	User-defined alarm text. Does not need to contain a value.
V.1/2/3	Alarm / Event / heartbeat	genEquipTrapCfgMgrCLLI	1.3.6.1.4.1.2281.10.3.2.1.1.9	Configures the Common Language Location Identifier (CLLI). Does not need to contain a value.
V.1/2/3	Alarm / Event	genEquipNetworkAgentIpV6	1.3.6.1.4.1.2281.10.2.7	Agent IP address (IP V6)
V.1/2/3	Alarm / Event	genEquipInventorySerialNumber	1.3.6.1.4.1.2281.10.1.2.10.1.1.6	The serial number of the interface with the alarm.
V.1/2/3	Alarm / Event	genEquipCurrentAlarmModule	1.3.6.1.4.1.2281.10.3.1.2.1.8	The module of the interface with the alarm.

Common tasks

The task descriptions in this chapter are presented from a functional perspective and represent how the commands and parameters would be used according to a common workflow.

Each task description contains a step by step procedure that explains how to use the MIB objects to perform that task.

Software management

Downloading a software version

Software download procedural overview

This section describes the required procedure to download the software package for the System Release device.

To download and install a new software version:

1. Configure the FTP parameters using table `genEquipMngSwFileTransferTable`.
2. Download the desired software files with `genEquipMngSwOperationOperation` command using `download` parameter. The new software files are added to the library.
3. Verify the download status in the `genEquipMngSwFileTransferStatusResult` object, until status is download success.

The progress of the process (in percentage) can also be tracked using `genEquipMngSwFileTransferPercentageDone`.

4. Install the `genEquipMngSwOperationOperation` command using `install` parameter. The software is installed in the system.
5. Verify the installation status in the `genEquipMngSwInstallStatusResult` object, until status is installation success.

The progress of the process (in percentage) can also be tracked using `genEquipMngSwInstallPercentageDone`.

- The System Release device automatically resets and applies the changes to all modules.

Verify that the unit is using the downloaded version. The version numbers are located in the `genEquipMngSwIDUVersionsTabletable`.

Configuring FTP parameters

The new software versions are located on a remote FTP server. In order to download a new software version, you must configure the parameters of this server.

Table 18 *MIB Objects for Configuring FTP Parameters*

Parameter	Function	OID
genEquipMngSwFileTransferProtocol	Chooses the protocol to be used (FTP, SFTP)	1.3.6.1.4.1.2281.10.4.1.18.1.2
genEquipMngSwFileTransferUserName	User name for access to the configuration file location.	1.3.6.1.4.1.2281.10.4.1.18.1.3
genEquipMngSwFileTransferPassword	Password for the remote software update server.	1.3.6.1.4.1.2281.10.4.1.18.1.4
genEquipMngSwFileTransferAddress	IP address of the external server where from which software version files are to be taken.	1.3.6.1.4.1.2281.10.4.1.18.1.5
genEquipMngSwFileTransferPath	Location of the files in the external server.	1.3.6.1.4.1.2281.10.4.1.18.1.6

Managing software

There are two commands that help you control the software versions: Download and install.

The genEquipMngSwOperationOperation MIB object has four values which execute four different commands:

- No action (0)
- Download (1) – download packages from the remote server.
- Install (2) –install the downloaded packages.
- Update backup (3) –Not supported
- Swap boot section (4) – Not supported
- Abort timer (5) – Not supported

Table 19 *Managing software versions MIB object*

Parameter	Function	OID
genEquipMngSwOperationOperation	Commands that can be executed to manage software versions: No action (0) Download (1) – download packages from the remote server. install (2) –install the downloaded packages. update backup (3) – Not supported	1.3.6.1.4.1.2281.10.4.1.21.1

Parameter	Function	OID
	Swap boot section (4) – Not supported	
	Abort timer (5) – Not supported	

Checking software status

You can check the status of the most recent software download and installation.

The genEquipMngSwFileTransferStatusTable displays the following values to indicate the file transfer status:

- Ready (0)
- download-started (1)
- verifying-download-files (2)
- Download-in-progress (3)
- download-success (4)
- download-failure (5)
- all-components-exist (6)
- version-incompatible-with-system (7)
- incomplete-file-set (8)
- component-unsupported-by-hw (9)
- corrupt-sw-files (10)
- missing-dependencies (11)
- download-cancelled (12)

The genEquipMngSwInstallStatusTable displays the following values to indicate the software status:

- ready (0)
- installation-started (1)
- verifying-installation-files (2)
- installation-in-progress (3)
- installation-success (4)
- installation-partial-success (5)
- installation-failure (6)
- incomplete-sw-version (7)
- cancelled-timed-installation (8)

Table 20 MIB objects for Checking IDU Software Status

Parameter	Function	OID
genEquipMngSwFileTransferStatusResult	Displays the status of the most recent software download.	1.3.6.1.4.1.2281.10.4.1.19.1.2
genEquipMngSwFileTransferPercentageDone	Displays the progress of the file transfer operation, in percentage	1.3.6.1.4.1.2281.10.4.1.19.1.3
genEquipMngSwInstallStatusResult	Displays the status of the most recent software installation.	1.3.6.1.4.1.2281.10.4.1.20.1.2
genEquipMngSwInstallPercentageDone	Displays the progress of the installation operation, in percentage.	1.3.6.1.4.1.2281.10.4.1.20.1.3

Configuration file management

The System Release MIB file enables you to view the current configuration of the System Release device. It also allows you to create backup files of the system configuration and upload them to a FTP server. You can then download the archived backup file for later use.

System configuration FTP settings

The archived system configurations are stored on a FTP server. The server saves the file that contains the existing configuration. You can download the system configuration file and install it on the desired system when necessary.

The FTP settings must be set in the MIB file before you can use the FTP server.

Software download FTP parameters are located in *genEquipMngCfgFileTransferTable*.

Table 21 MIB objects for configuring FTP settings

Parameter	Function	OID
genEquipMngCfgFileTransferProtocol	Configures the protocol to be used (FTP, SFTP, HTTP, HTTPS)	1.3.6.1.4.1.2281.10.4.2.11.1.2
genEquipMngCfgFileTransferUserName	Configures the required user name for the FTP server.	1.3.6.1.4.1.2281.10.4.2.11.1.3
genEquipMngCfgFileTransferPassword	Configures the required password for the FTP server.	1.3.6.1.4.1.2281.10.4.2.11.1.4
genEquipMngCfgFileTransferAddress	Configures the host IP address of the FTP server.	1.3.6.1.4.1.2281.10.4.2.11.1.5

Parameter	Function	OID
genEquipMngCfgFileTransferPath	Configures the path of the host directory on the FTP server.	1.3.6.1.4.1.2281.10.4.2.11.1.6
genEquipMngCfgFileTransferFileName	Configures the filename to be used in the server.	1.3.6.1.4.1.2281.10.4.2.11.1.7

Creating and uploading backup configuration archives

To create a backup file which contains all the details of the current configuration, use `genEquipMngCfgOperationOperation` with a value of (1) Backup.

Table 22 *Creating Configuration Archive MIB Object*

Parameter	Function	OID
genEquipMngCfgOperationOperation	Executes the Backup system configuration commands: - Invalid-operation (0) - Backup (1)	1.3.6.1.4.1.2281.10.4.2.13.1.2

Procedural overview of uploading a system configuration

This section describes the required procedure to save the current system configuration of the System Release device and export it to an FTP server.

To save and upload the current system configuration:

1. Verify the FTP settings.
2. Create the archive files of the current system configuration. The `genEquipMngCfgOperationOperation` with Backup (1) command creates an archive file. Up to three files can be stored, each identified by parameter `genEquipMngCfgOperationFileNumber`.
3. Verify that the configuration file generation has succeeded in the `genEquipMngCfgBackupStatus` object. The status should be download-success (3).
4. Upload the archive files to the FTP server with the `genEquipMngCfgOperationOperation` with export (5) command.5 Verify that the upload to the FTP server has succeeded in the `genEquipMngCfgFileTransferStatus` object. The status should be download success (4).

Exporting an archived configuration

To export an archived configuration of the PTP 850 unit to an FTP server use `genEquipMngCfgOperationOperation` with a value of (5) export.

Table 23 *Uploading Archived Configuration MIB Object*

Parameter	Function	OID
genEquipMngCfgOperation Operation	Executes the Backup system configuration commands: • Export (1)	1.3.6.1.4.1.2281.10.4.2.13.1.2

Backup and Export status

The genEquipMngCfgFileTransferStatus and genEquipMngCfgUploadStatus objects display that backup and upload status of the system configuration.

Table 24 *Backup and Upload Status MIB Object*

Parameter	Function	OID
genEquipMngCfgBackupStatus	Status of the configuration backup file to the unit.	1.3.6.1.4.1.2281.10.4.2.1
genEquipMngCfgFileTransferStatus	Status of uploading the configuration backup file to the FTP server.	1.3.6.1.4.1.2281.10.4.2.21

Enabling and configuring traps

Enabling trap administration

To change the setup for a trap, you must enable the administrative state for the specific trap manager.

Table 25 *Enabling Trap Administration*

Index: genEquipTrapCfgMgrId

Parameter	Function	OID
genEquipTrapCfgMgrAdmin	Set to Enable (2) in order to configure a specific trap manager.	1.3.6.1.4.1.2281.10.3.2.1.1.2

Managing a trap

Trap manager configuration:

- Trap manager IP address to which the traps are sent.
- Port number that sends the trap.
- Name of the trap manager.

- Community name to trap forwarding.
- Period (in minutes) of the heartbeat trap.

CLLI (Common Language Location Identifier) free text that is sent with the trap.

Table 26 *Managing a trap*

Index: genEquipTrapCfgMgrId

Parameter	Function	OID
genEquipTrapCfgMgrId	The ID of the trap manager. User can define up to 4 independent trap managers	1.3.6.1.4.1.2281.10.3.2.1.1.1
genEquipTrapCfgMgrIP	Configures the trap manager's IP address.	1.3.6.1.4.1.2281.10.3.2.1.1.3
genEquipTrapCfgMgrPort	Configures the port that sends the trap for each manager.	1.3.6.1.4.1.2281.10.3.2.1.1.4
genEquipTrapCfgMgrName	Configures the name of the manager that receives the traps.	1.3.6.1.4.1.2281.10.3.2.1.1.5
genEquipTrapCfgMgrCommunity	Configures the name of the manager community that receives the traps.	1.3.6.1.4.1.2281.10.3.2.1.1.6
genEquipTrapCfgMgrCLLI	Configures the Common Language Location Identifier (CLLI).	1.3.6.1.4.1.2281.10.3.2.1.1.9
genEquipTrapCfgMgrHeartbeatPeriod	Configures the minute interval between each heartbeat.	1.3.6.1.4.1.2281.10.3.2.1.1.10

Viewing current alarms

Alarm date and time

You can view the date and time that an alarm was raised. There are two objects that can be used for this parameter.

Table 27 *Alarm date and time MIB object*

Parameter	Function	OID
genEquipCurrentAlarmRaisedTimeT	Time the alarm was raised, in seconds since January 1, 1970 00:00 UTC	1.3.6.1.4.1.2281.10.3.1.2.1.2
genEquipCurrentAlarmRaisedDateAndTime	Time the alarm was raised, in DateAndTime standard	1.3.6.1.4.1.2281.10.3.1.2.1.16

Parameter	Function	OID
	format.	

Alarm severity

You can view the alarm severity.

Table 28 Alarm severity MIB object

Parameter	Function	OID
genEquipCurrentAlarmSeverity	Severity of the current alarm: - Indeterminate (0) - Critical (1) - Major (2) - Minor (3) - Warning (4) - Cleared (5)	1.3.6.1.4.1.2281.10.3.1.2.1.6

Alarm description

You can view the description of the alarm.

Table 29 Alarm Description MIB Object

Parameter	Function	OID
genEquipCurrentAlarmDesc	Description of the alarm.	1.3.6.1.4.1.2281.10.3.1.2.1.9

Probable cause

You can view the probable cause for the alarm.

Table 30 Probable Alarm Cause MIB Object

Parameter	Function	OID
genEquipCurrentAlarmProbableCause	Probable cause of the alarm.	1.3.6.1.4.1.2281.10.3.1.2.1.10

Corrective actions

You can view the recommended corrective actions to solve the problem that caused the alarm.

Table 31 *Corrective Actions MIB Object*

Parameter	Function	OID
genEquipCurrentAlarmCorrectiveActions	Corrective actions that should be taken	1.3.6.1.4.1.2281.10.3.1.2.1.11

Viewing event log

Event date and time

You can view the date and time that an alarm or event was raised or cleared. There are two objects that can be used for this parameter.

Table 32 *Event date and time MIB objects*

Parameter	Function	OID
genEquipEventLogRaisedTimeT	Time the item was added to the Event Log. This is given in seconds since January 1, 1970 00:00 UTC	1.3.6.1.4.1.2281.10.3.3.1.1.2
genEquipEventLogRaisedDateAndTime	Time the item was added to the Event Log, in DateAndTime standard format.	1.3.6.1.4.1.2281.10.3.3.1.1.13

Event severity

You can view the event severity.

Table 33 *Event severity MIB object*

Parameter	Function	OID
genEquipEventLogSeverity	Severity of the current alarm or event: • Indeterminate (0) • Critical (1) • Major (2) • Minor (3) • Warning (4) • Cleared (5)	1.3.6.1.4.1.2281.10.3.3.1.1.3

Event description

You can view the description of the alarm or event.

Table 34 *Event Description MIB Object*

Parameter	Function	OID
genEquipEventLogDesc	Description of the alarm or event.	1.3.6.1.4.1.2281.10.3.3.1.1.5

Event state

You can view the current state of the alarm or event (raised or cleared).

Table 35 *Event Current State MIB Object*

Parameter	Function	OID
genEquipEventLogState	Current state of the alarm or event. • In case of alarm, 'cleard' or 'raised'. • In case of event, 'event'.	1.3.6.1.4.1.2281.10.3.3.1.1.6

Performance monitoring and counters

You can use the MIB file to configure and retrieve the performance monitoring data of the System Release device.

Clearing all performance counter data

You can use the genEquipPmClear command to clears the values for all of the performance monitoring tables.

The Object ID is: 1.3.6.1.4.1.2281.10.6.3.1.

Managing radio configuration

You can use the MIB file to manage the radio configuration data of the unit.

Setting the radio threshold

This section explains how to set the Radio thresholds. After the thresholds are set, the system records the number of seconds that each of them was exceeded.

Table 36 *Setting RSL Threshold*

Parameter	Function	OID
genEquipPmRadioThresholdMSE	Configures which PM table is accessed.	1.3.6.1.4.1.2281.10.6.3.4.5.1.1

Parameter	Function	OID
genEquipPmRadioThresholdRSL1	Configures which interface or port is monitored.	1.3.6.1.4.1.2281.10.6.3.4.5.1.2
genEquipPmRadioThresholdRSL2	Configures the time interval of the PM.	1.3.6.1.4.1.2281.10.6.3.4.5.1.3
GenEquipPmRadioThresholdTSL	Percentage of received frames that contained errors.	1.3.6.1.4.1.2281.10.6.3.4.5.1.5
genEquipPmRadioThresholdXPI	Maximum Ethernet throughput measured during the last interval.	1.3.6.1.4.1.2281.10.6.3.4.3.1.1.4

Setting the traffic PM thresholds

This section explains how to set radio capacity, throughput, and utilization PM thresholds. After the thresholds are set, the system records the number of seconds that each of them was exceeded.

Table 37 *Setting Traffic PM Thresholds*

Parameter	Function	OID
genEquipRadioCompNGCfGCapacityPmThreshold	Configures the threshold for capacity PMs, in Mbps. The range of values is 0 to 4294967295. The default value for is 1000.	1.3.6.1.4.1.2281.10.7.5.4.1.1.6
enEquipRadioCompNGCfGThroughputPmThreshold	Configures the threshold for throughput PMs, in Mbps. The range of values is 0 to 4294967295. The default value for is 1000.	1.3.6.1.4.1.2281.10.7.5.4.1.1.7
genEquipRadioCompNGCfGUtilizationPmThreshold	Configures the radio capacity utilization threshold, in % (1-100). The default value for is 100.	1.3.6.1.4.1.2281.10.7.5.4.1.1.8

MIB Revision History

The following HTML file is included in a ZIP file with this MIB Reference:

- MIB_13.1_to_13.3_DIFF_PTP 820N_PTP 820A.htm
- MIB_13.1_to_13.3_DIFF_PTP 820N_PTP 820A_TCC-U.htm
- MIB_13.1_to_13.3_DIFF_PTP 820C_PTP 820S.htm
- MIB_13.1_to_13.3_DIFF_PTP 850C_PTP 850E.htm
- MIB_13.1_to_13.3_DIFF_PTP 850CX_PTP 850EX.htm
- MIB_13.1.6_to_13.3_DIFF_PTP 850GP.htm

These files list the MIB objects that were changed, added, or deleted from System Release 13.1 to System Release 13.3.



Note:

For PTP 850GP, the file lists the MIB objects that were changed, added, or deleted from System Release 13.1.6 to System Release 13.3.

In these DIFF files, the column on the left displays the 13.1 (or 13.1.6) version of the object and the column on the right displays the 13.3 version of the object.

For rows in which the left column is empty, the object was added in System Release 13.3.

For rows in which the right column is empty, the object was removed in System Release 13.3.

MIB error table (Reserved for future use)

If there are any errors related to the System Release device, an errno is generated. Check the errno description in the following table to find a textual description of the error.

The table contains two columns:

- Errno Fault Number – genEquipFaultErrno (OID 1.3.6.1.4.1.2281.10.3.4)
- Errno Description – genEquipFaultErrDescr (OID 1.3.6.1.4.1.2281.10.3.5)

Alarms

The following table lists all alarms used in System Release devices.

Table 38 *Alarms*

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
10	radio-digital-loopback	Alarm	Equipment	Framer digital loopback is enabled	Warning	User enabled framer digital loopback.	Disable the framer digital loopback.
11	ntp-local	Alarm	Communications	NTP locked on local clock	Warning	The configured and enabled NTP servers are all unreachable or providing insufficient quality.	Configure or enable another NTP server, one that is reachable with sufficient quality.
15	ntp-locked	Event	Communications	NTP locked on server	Indeterminate		
25 See Note 1	main-board-extreme-temperature-alarm	Alarm		Unit Temperature is out of system specified limits.	Warning		
26	main-board-low-voltage-alarm	Alarm	N/A	Unit input voltage is too low.	Warning	1. Power supply output is too low. 2. Power cable to the unit is defective. 3. Threshold value is not set correctly.	1. Check/replace the power supply connected to the RFU. 2. Check/replace the power cable connected to the RFU. 3. Set the threshold

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							correctly.
27	main-board-high-voltage-alarm	Alarm	N/A	Unit input voltage is too high.	Warning	1. Power Supply output is too high. 2. Threshold value not set correctly.	1. Make sure the power supply voltage is within the specification range. 2. Adjust the threshold value.
28	main-board-warm-reset	Event		Unit warm reset.	Indeterminate		
30	main-board-poe-low-voltage-alarm	Alarm		POE input voltage is too low	Warning	1. PoE supply output is too low. 2. PoE cable to the unit is defective.	Make sure the PoE voltage is within the specification range.
31		Event		Change Remote request was sent	Major		
32		Event		Protection switchover due to remote request	Major		
33	protection-mimo-misconfiguration-alarm	Alarm			Major	Unit Redundancy and MIMO 4x4 cannot operate simultaneously.	
100	lag-degraded	Alarm	Equipment	LAG is not fully functional - LAG	Major	1. At least one interface is not	1. Check the physical connections.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				Degraded.		connected or configured to admin down. 2. If one of the members is radio it might be in operational state down due to channel fading	2. Verify that the Admin state of all the LAG members is up. 3. Verify the operational state of all radio members in the LAG.
101	lag-down	Alarm	Equipment	LAG operational state is down	Critical	The LAG group is not operational.	1. Check the physical connections and administrative status on both sides of the link of all interfaces that are members of the LAG Group. 2. Check the physical connections of all interfaces that are members of the LAG Group.
102	ethernet-loopback-	Alarm	Equipment	Loopback is active	Major	Ethernet loopback is	Wait for expiration of

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
	active-alarm					active.	the loopback timeout or disable the loopback.
103	port-mirroring-is-active	Alarm	Equipment	Slot X port XX is mirrored to slot Y port YY	Minor	Mirroring is enabled by user configuration.	Disable mirroring.
104	qos-mode-mismatch	Alarm	Processing	System reset is required after QoS mode has been changed	Major	QoS mode has been changed by user	Reset the system
105 See Note 2	tm-reset-alarm	Alarm	Processing	System reset is required after priority profile has been changed	Major	Priority profile has been changed by the user	Reset the system
110	lbg-degraded-alarm	Alarm	Equipment	Link Bonding Group is not fully functional - LBG degraded	Major	Radio or Ethernet port associated with the LBG member is down	Check the operational status of Radio or Ethernet ports
111	lbg-down-alarm	Alarm	Equipment	Link Bonding Group operational state is Down	Critical	Radio or Ethernet ports associated with the LBG are down	Check the operational status of Radio or Ethernet ports
112	lbg-chassis-reset-required-alarm	Alarm	Equipment	Chassis reset is required	Warning	1. Link Bonding Group was deleted.	Reset the unit

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				after Link Bonding group configuration was modified		2. Link Bonding Group max bandwidth was changed.	
120	port-speed-mismatch-alarm	Alarm	Equipment	Port speed mismatch	Major	System reset is required after the port speed was changed.	Change the port speed to its previous value
130	jumbo-or-cut-through-change-alarm	Alarm	Equipment	System reset is required after Jumbo mode or Cut Through mode has been changed	Major	Jumbo mode or Cut Through mode has been changed by user	Reset the system
150	auto-state-propagation-interface-down-alarm	Alarm	Communications	Auto-state-propagation is triggered	Major	Failure of the radio/remote radio interface which is monitored for automatic state propagation causes automatic shutdown of the controlled interface.	Check adjacent local/remote radio interface for failure conditions that cause automatic state propagation.
200	protection-communication-down-alarm	Alarm	Equipment	Protection communication is down	Major	1. Mate unit is absent/failure. 2. Protection cable is disconnected.	1. Verify that the mate unit is up and running. 2. Check the state of the

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						3. Unit failure. 4. In FIPS mode or IPsec mode, a mismatch between the IPsec pre-shared keys configured on the two units.	protection cable connection. 3. Reset the mate unit. 4. Replace the mate unit. 5. If IPsec/FIPS is enabled, verify the same pre-shared key is configured on both units.
201	protection-lockout-alarm	Alarm	Equipment	Protection in Lockout State	Major		
202	protection-switch-command	Event	Equipment	Protection switchover due to local failure	Major		1. Check the unit. 2. Look for current alarms.
203	protection-mate-not-present-alarm	Alarm	Equipment	Mate does not exist	Major	Mate does not exist or cable unplugged.	1. Verify that the mate unit is up and running. 2. Verify that the protection cable is properly connected between the units.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
204	protection-hsb-insufficient-alarm	Alarm	Equipment	HSB insufficient configuration	Critical	External Protection configured together with 1+1 HSB.	Remove External Protection or 1+1 HSB configuration.
205	protection-revertive-primary-insufficient-alarm	Alarm	Equipment	Protection revertive mode - insufficient configuration	warning	Identical configuration for the revertive-primary parameter.	Ensure one (and only one) unit is configured as the primary unit.
307	tdm-link-up	Event	Equipment	TDM interface is up	Warning		
308	tdm-link-down	Event	Equipment	TDM interface is down	Warning		
401	TrafficPhyLocAlarm	Alarm	Equipment	Loss of Carrier	Major	1. Cable disconnected. 2. Defective cable. 3. External equipment failure.	At both ends of the cable: 1. Check the cable connection. 2. Check the Admin state of the port. 3. Replace the cable. 4. Check external equipment.
402	eth-auto-neg-mismatch-alarm	Alarm	Communications	Ethernet interface speed is lower than the configured	Minor	1. A faulty or incompatible cable. 2. Connected device problem or	1. Verify Ethernet cable is compatible and isn't faulty.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				speed.		speed limitation.	2. Verify Ethernet interface on the opposite device is configured correctly and isn't faulty.
403	eth-electrical-sfp-invalid-config-alarm	Alarm	Communications	The configurations applied on the electrical SFP are invalid.	Major	1. The port speed of the electrical SFP was set to an illegal value. 2. The electrical SFP does not support SyncE.	1. Verify the port speed of the electrical SFP. The supported value for the electrical SFP is up to 1G. 2. Disable SyncE on the electrical SFP interface.
404	eth-sfp-invalid-speed-alarm	Alarm	Communications	The speed configurations applied on the SFP are invalid.	Major	The port speed of the SFP was set to an illegal value.	Verify the port speed of the SFP.
407	ethernet-link-up	Event	Equipment	Ethernet interface is up	Warning	Ethernet interface is back to being operational.	Notification. Corrective action is not required.
408	ethernet-link-down	Event	Equipment	Ethernet interface is down	Warning	1. User commanded the interface to admin	1. Set the Ethernet interface admin State to

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						down. 2. Ethernet cable is disconnected. 3. Ethernet card is initializing. 4. External equipment failure.	Up. 2. Reconnect the Ethernet cable 3. Wait 30 seconds to allow the Ethernet card to complete its init. 4. Check external equipment.
500	e-stabilizer-disconnection-alarm	Alarm	Communications	Connection to E-Stabilizer antenna is down.	Major	1. Cable Disconnection. 2. Service or Service Point is not configured correctly. 3. Incorrect IP and subnet configuration. 4. Loss of power to antenna. 5. Antenna malfunction.	1. Verify Antenna Service is correctly defined. 2. Verify antenna and antenna internal interface IPs and Subnets are defined correctly. 3. Perform SW reset to antenna. 4. Verify cable connection between

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							antenna and system. 5. Verify power to antenna.
501	e-stabilizer-position-alarm	Alarm	Communications	E-Stabilizer position error.	Major	Antenna malfunction.	Perform SW reset to antenna.
502	e-stabilizer-deviation-alarm	Alarm	Communications	E-Stabilizer deviation from initial position.	Minor	Antenna or Pole have shifted from initial position.	1. Save current position into Initial position via "Save initial position". 2. Re-align the antenna with field technician.
503	e-stabilizer-high-temperature-alarm	Alarm	Communications	E-Stabilizer internal temperature reach high temperature threshold	Minor	1. Extreme installation conditions. 2. Antenna malfunction.	1. Correct the installation conditions. 2. Replace the unit.
504	e-stabilizer-hpf-init-alarm	Alarm	Communications	E-Stabilizer internal Gyroscope High Pass Filter initialization has failed	Minor		Reset the antenna
505	Alignment mode active	Alarm	Communications	Alignment mode is used for	Major	Alignment mode was activated	To enable data communication, disable alignment

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				antenna alignment only, no data communications to or management of remote unit is possible in alignment mode. Also radio configuration is not possible in this mode.			mode
601	radio-excessive-ber	Alarm	Communications	Radio excessive BER	Major	1. Fade in the link. 2. Defective IF cable. 3. Fault in RFU. 4. Fault in RMC (Radio Modem Card). 5. Interference on the link.	1. Check link performance via the Web EMS Radio PM and Statistics page and take corrective action accordingly. 2. Check IF cable and replace if required. 3. Replace RFU. 4. Replace RMC (Radio Modem Card).

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							5. Remove source of interference or change link frequency.
602	remote-link-id-mismatch	Alarm	Equipment	Link ID mismatch	Major	1. Link ID is not the same at both sides of link. 2. Radio has synched on the wrong peer radio.	1. Configure same Link ID for both sides of link via Web EMS Radio Parameters page. 2. Check if the radio is synched on the correct peer radio (check: channel frequency, antennae direction).
603	radio-lof	Alarm	Communications	Radio loss of frame	Critical	1. Fade in the link. 2. Defective IF cable. 3. Fault in RFU. 4. Fault in RMC (Radio Modem Card). 5. Different radio scripts at	1. Check link performance. 2. Check IF cable and replace if required. 3. Replace RFU. 4. Replace RMC (Radio Modem Card).

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						both ends of the link.	5. Make sure same script is loaded at both ends of the link.
604	radio-signal-degrade	Alarm	Communications	Radio signal degrade	Minor	1. Fade in the link. 2. Defective IF cable. 3. Fault in RFU. 4. Fault in RMC (Radio Modem Card).	1. Check link performance. 2. Check IF cable and replace if required. 3. Replace RFU. 4. Replace RMC (Radio Modem Card).
605	radio-link-up	Event	Equipment	Radio interface is up	Warning	The radio interface is back to being operational.	No action is required.
606	radio-link-down	Event	Equipment	Radio interface is down	Warning	Radio interface is not operational: 1. User configured the radio interface to admin Down. 2. Loss of Frame (LOF) alarm is raised. 3. Excessive BER alarm	1. If required, set the radio interface admin State to Up. 2. Check if there is a reason for LOF / Excessive BER alarms. 3. Wait 30 seconds

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						is raised. 4. Radio card has not completed its init.	until the radio card finishes its init.
607	rfu-frequency-scanner-in-process	Alarm	Equipment	Frequency scanner in progress	Warning	The frequency scanner activated.	If required, stop the frequency scanner process.
801	corrupted-file-card-failure	Alarm	Equipment	Corrupted inventory file	Critical	The inventory file is corrupted	1. Reset the card. 2. Reinstall the software. 3. Replace the unit.
802	file-not-found	Alarm	Equipment	Inventory file not found	Warning	The inventory file is missing	1. Reset the system. 2. Reinstall the software. 3. Replace the unit.
803	sfp-rx-power-level-low	Alarm	Equipment	SFP port RX power level is below the rx power level low threshold	Warning	1. Remote SFP port Tx laser power is too low. 2. Fiber length is too long or fiber type doesn't fit the installed SFP.	1. Verify remote SFP Tx laser power is within range. 2. Check fiber type and length fit the installed SFP. If not, replace it with an

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							appropriate one.
804	sfp-rx-power-level-high	Alarm	Equipment	SFP port RX power level is above the rx power level high threshold	Warning	Remote SFP Tx power is too high.	Add attenuator on Rx side.
805	sfp-tx-power-level-low	Alarm	Equipment	SFP port TX power level is below the tx power level low threshold	Warning	SFP transmit laser power is too low	Check laser Bias current. If it is too low, replace SFP.
806	sfp-tx-power-level-high	Alarm	Equipment	SFP port TX power level is above the tx power level high threshold	Warning	SFP laser Tx power is too high.	Check laser Bias current and laser temperature values. If either of them is too high, replace SFP.
807	recovered-inventory-on-boot-event	Event	Equipment	Default Activation Key activated due to failure	Critical	Corrupted Inventory	
808	recovered-inventory-on-running-event	Event	Equipment	Activation Key Configuration failed	Critical	Corrupted Inventory	
809	sfp-voltage-level-low	Alarm	Equipment	SFP port supply voltage is too low	Minor	Power supply malfunction.	Replace the unit.
810	sfp-voltage-level-high	Alarm	Equipment	SFP port supply	Minor	Power supply malfunction.	Replace the unit.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				voltage is too high			
811	sfp-rx-power-low-threshold-crossing	Alarm	Equipment	SFP Rx power low threshold crossing	Minor	1. Remote SFP transmit power is too low 2. Poor optical connection	1. Replace the remote SFP unit 2. Clean the optical connectors
812	sfp-rx-power-high-threshold-crossing	Alarm	Equipment	SFP Rx power high threshold crossing	Minor	Remote SFP transmit power is too high	Replace the remote SFP unit
901	demo-license-alarm	Alarm	Equipment	Demo mode is active	Warning	Demo mode has been activated by the user	Disable demo mode from the Activation Key Configuration page in the Web EMS.
902	license-demo-expired	Event	Equipment	Demo mode is expired	Warning		
903	license-demo-start-by-user	Event	Processing	Demo mode is started	Warning		
904	license-demo-stop-by-user	Event	Processing	Demo mode is stopped	Warning		
905	license-load-fail	Event	Equipment	Activation key loading failure	Major		
906	license-load-successful	Event	Equipment	Activation key loaded successfully	Warning		
907	license-	Alarm	Equipment	Activation	Critical	The current	1. Go to the

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
	violation-alarm	m		key violation		configuration does not match the activation-key-enabled feature set. 48 hours after an "activation-key-violation" alarm is raised, sanction mode is activated in which all alarms except the activation key violation alarm are cleared and no new alarms are raised.	“Activation Key Overview” page in the Web EMS to display a list of features and their activation key violation status. 2. Install a new activation key that enables all features and capacities that you require.
908	demo-license-about-to-expire-alarm	Alarm	Equipment	Demo mode is about to expire	Major	Demo mode allowed period is about to end within 10 days	Disable demo mode and install a new valid activation key in the “Activation Key Configuration” page of the Web EMS.
910	license-signature-failed-alarm	Alarm	Equipment	Activation key signature failure	Major	Activation key validation has failed due to invalid product serial number or activation key that does not match.	Make sure that the activation key matches the serial number of the unit.
911	license-	Eve	Equipment	Activation	Major		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
	violation-runtime-counter-expired	nt		key violation sanction is enforced			
913	license-bad-xml-file-alarm	Alarm	Equipment	Activation key components are missing or corrupted	Major	Essential internal activation key components are missing or corrupted.	Reinstall software
914	usagemode-general-write-fail	Event	Equipment	Write operation has failed	Indeterminate	Incorrect write operation.	Verify write operation is performed correctly by usage mode server.
915	usagemode-server-disconnection-alarm	Alarm	Equipment	Smart Activation Key: Keep alive process with usage mode server was not performed for 60 hours, device entered disconnection grace period	Warning	Device was unreachable by server	Ensure device is reachable by server
916	usagemode-server-violation-status-set-to-grace	Alarm	Equipment	Device is in server violation: Grace state	Warning	1. License expiration. 2. Lack of credits. 3. Database tampering.	Perform corrective actions at usage mode server
917	usagemode-	Alarm	Equipment	Device is in	Critical	1. License	Perform

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
	server-violation-status-set-to-sanction	m		server violation: Violation state.		expiration. 2. Lack of credits. 3. Database tampering.	corrective actions at usage mode server
1002	radio-protection-configuration-mismatch	Alarm	Equipment	Radio protection configuration mismatch	Major	The configuration between the radio protection members is not aligned	Apply a copy-to-mate command to copy the configuration from the active radio to the standby radio.
1006	radio-protection-switchover-event	Event	Equipment	Radio protection switchover - reason	Warning	Protection decision machine initiated switchover due to local failure or user command	Check the system for local failures.
1007	radio-protection-no-mate	Alarm	Equipment	Radio protection no mate	Major	Radio protection function is missing radio module, module defected or disabled	1. Insert the radio module. 2. Replace a defective existing radio module. 3. Make sure all radio interfaces are enabled.
1008	radio-protection-remote-switch-request	Event	Equipment	Remote switchover request	Warning		
1009	radio-	Alarm	Equipment	Radio	Major	The user has	Clear the

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
	protection-lockout			protection lockout command is on		issued a lockout command	lockout command
1010	ethernet-protection-switchover	Event	Equipment	Ethernet Interface Group protection switchover	Warning	1. LOC event on an Ethernet interface. 2. Protection group member was disabled or pulled out of the shelf.	1. Check the system for local failures. 2. Check external equipment.
1011	interface-protection-lockout	Alarm	Equipment	Interface protection lockout is on	Major	3. The user has issued a lockout command	3. If required, clear the lockout.
1012	interface-protection-no-mate	Alarm	Equipment	Interface protection no mate: mate interface is missing or disabled	Major	Interface protection function is missing an interface module, module is defective or disabled.	1. Insert the interface module. 2. Replace a defective existing interface. 3. Make sure all interfaces are enabled.
1102	software-installation-status	Event	Processing	Software installation status:	Warning		
1105	software-new-version-installed	Event	Processing	New version installed	Warning	A software version has been installed but system has not been reset.	

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1111	software-user-confirmation-for-version	Event	Processing	User approved download of software version file	Warning		
1112	software-download-status	Event	Processing	Software download status:	Warning		
1113	software-download-missing-components	Event	Processing	Missing SW components:	Warning		
1114	software-management-incomplete-bundle	Event	Processing	Incomplete file set; missing components	Warning	Software bundle is missing components.	Get a complete software bundle
1118	software-mate-download-status	Event	Processing	Mate software download status:	Warning		
1119	software-mate-installation-status	Event	Processing	Mate software installation status:	Warning		
1150	backup-started	Event	Processing	Configuration file backup generation started	Warning	User command	
1151	backup-succeeded	Event	Processing	Configuration file backup created	Warning	Backup file creation finished successfully	
1152	backup-failure	Event	Processing	Failure in configuration file backup generation	Warning	System failed in attempt to create backup configuration file	

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1153	restore-succeeded	Event	Processing	Configuration successfully restored from file backup	Warning	Configuration restore finished successfully	
1154	restore-failure	Event	Processing	Failure in configuration restoring from backup file	Warning	System failed in attempt to restore configuration from backup file	1. Configuration file system type mismatch 2. Invalid or corrupted configuration file
1155	restore-canceled	Event	Processing	Configuration restore operation cancelled	Warning	Restore operation cancelled because of user command or execution of another configuration management operation	Try again
1156	file-transfer-issued	Event	Processing	User issued command for transfer of configuration file	Warning	User command	
1157	file-transfer-succeeded	Event	Processing	Configuration file transfer successful	Warning	Configuration file transfer successful	
1158	file-transfer-failure	Event	Processing	Configuration file transfer failure	Warning	1. Communications failure. 2. File not found in	1. Mark sure protocol details are properly configured.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						server	2. Make sure file exists.
1159	file-transfer-in-progress	Event	Processing	Configuration file transfer in progress	Warning	File transfer started	
1163	cli-script-activation-started	Event	Processing	CLI configuration script activation started	Warning	User command	
1164	cli-script-activation-succeeded	Event	Processing	CLI Configuration script executed successfully	Warning		
1165	cli-script-activation-failure	Event	Processing	CLI Configuration script failed	Warning	1. Syntax Error. 2. Error returned by system during runtime	Verify script in the relevant line, and run again. Note that script may assume pre-existing configuration.
1166	unit-info-file-transfer-status-changed	Event	Processing	Unit info file transfer status:	Warning		
1167	unit-info-file-creation-status-changed	Event	Processing	Unit info file creation status:	Warning		
1169	restore-started	Event	Processing	Configuration restore operation started	Warning	Restore operation started because of user command	
1201	file-missed	Alarm	Equipment	Modem firmware file not	Critical	Modem file is missing	1. Download software package.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				found			2. Reset the system.
1202	load-failed	Alarm	Equipment	Modem firmware was not loaded successfully	Critical	1. Modem firmware file is corrupted. 2. System failure.	1. Download software package. 2. Reset the system.
1203	modem-wd-reset	Event	Equipment	Modem watch-dog reset event	Warning		
1204	remote-syslog-tls-failure-alarm	Alarm	Equipment	Unable to connect remote syslog server	Minor	TLS version mismatch or cipher-suite mismatch	Upgrade Syslog server TLS
1301	fpga-file-corrupt-alarm	Alarm	Equipment	Radio MRMC script LUT file is corrupted	Critical	Damaged radio MRMC script LUT file	Download the specific radio MRMC script LUT file
1302	fpga-file-not-found-alarm	Alarm	Equipment	Radio MRMC script LUT file is not found	Critical	Missing radio MRMC script LUT file	Download the specific radio MRMC script LUT file
1304	modem-script-file-corrupt-alarm	Alarm	Equipment	Radio MRMC script modem file is corrupted	Critical	Damaged radio MRMC script modem file	Download the specific radio MRMC script modem file
1305	modem-script-file-not-found-alarm	Alarm	Equipment	Radio MRMC script modem file is not found	Critical	Missing radio MRMC script modem file	Download the specific radio MRMC script modem file
1306	mrmc-configuration-	Alarm	Equipment	The MRMC script	Critical	MRMC script doesn't match	Configure an MRMC script

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
	mismatch			doesn't match radio configuration		configuration (MIMO or digital loopback)	that match the current configuration
1308	rfu-file-corrupt-alarm	Alarm	Equipment	Radio MRMC file is corrupted	Critical	Damaged Radio MRMC script LUT file	Download the specific radio MRMC RFU file
1309	rfu-file-not-found-alarm	Alarm	Equipment	Radio MRMC RFU file is not found	Major	Missing radio MRMC RFU file	Download the specific radio MRMC RFU file
1312	script-loading-failed	Alarm	Equipment	Radio error! MRMC script loading failed	Major	Damaged hardware module	Replace the radio hardware module
1313	mrhc-profile-below-thresh1	Alarm	Equipment	MRMC RX profile below threshold 1	Major		
1314	mrhc-profile-below-thresh2	Alarm	Equipment	MRMC RX profile below threshold 2	Critical		
1315	rfu-logger-start	Event	Equipment	RFU logger start	Warning	RFU logger started by user	Stop the RFU logger
1316	rfu-logger-stop	Event	Equipment	RFU logger stop	Warning	RFU logger stopped by user	Stop the RFU logger
1401	incompatible-rfu-tx-calibration	Alarm	Equipment	Incompatible RFU TX calibration	Major	RFU calibration tables require SW upgrade	Upgrade IDU SW
1501	remote-communication-failure	Alarm	Equipment	Remote communication failure	Critical	Fade in the link	Check the link performance
1502	remote-timed-	Alarm	Equipment	Remote	Warning		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
	mute-alarm	m		RFU TX mute with timeout			
1601	if-loopback	Alarm	Equipment	IF loopback	Warning	User enabled IF loopback	Disable IF loopback
1602	lock-detect	Alarm	Equipment	IF synthesizer is unlocked.	Critical	1. Extreme temperature condition. 2. HW failure.	1. Check installation. 2. Reset the RMC (Radio Modem Card) module. 3. Replace the RMC (Radio Modem Card).
1610	rsl-degradation-threshold-out-of-range	Alarm	Equipment	Radio Receive Signal Level is below the configured threshold	Warning	RSL is very low due to: 1. Weather conditions, obstruction in antenna line of sight, antennae alignment. 2. Configured threshold needs to be adjusted.	1. Check for obstruction in link path. 2. Check the antennae alignment and link planning. 3. Recalculate the Path Loss and set the threshold accordingly. 4. Check link settings - Tx Power and Tx Frequency

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							y. 5. Check for a hardware problem.
1651	atpc-override	Alarm	Communications	ATPC overridden: Tx level has been equal to the Max Tx level for a longer time than allowed	Warning	Actual transmitted signal level has been at its maximum value for longer than allowed. This is probably caused by a configuration error or link planning error.	Correct the transmission levels. The alarm will be cleared only upon manual clearing.
1697	radio-unit-extreme-temperature	Alarm	Equipment	Radio unit extreme temperature	Warning	1. Installation conditions. 2. Defective RFU.	1. Correct the installation conditions. 2. Verify that the product is operating according to specifications. 3. Replace the RFU.
1698	radio-unit-low-voltage	Alarm	Equipment	Radio unit input voltage is too low	Warning	1. Power supply output is too low. 2. Power cable to RFU is defective.	1. Check/replace the power supply connected to the RFU.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							2. Check/replace the power cable connected to the RFU.
1699	radio-unit-high-voltage	Alarm	Equipment	Radio unit input voltage is too high	Warning	Power Supply output too high.	3. Check power supply.
1700	fw-download-failure	Alarm	Communications	Radio unit not aligned to IDU	Critical	1. FW alignment interrupted, power disruption, ODU cable malfunction. 2. Damaged ODU.	1. Reinitiate the FW download by disabling and then enabling the corresponding RFU port. 2. Replace the RFU.
1701	cable-open	Alarm	Equipment	Cable open	Major	Cable is not connected to the radio card or the RFU.	1. Check cables and connectors. 2. Verify that the N-Type connector inner pin is not spliced. 3. Replace the radio card. 4. Replace the RFU.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1702	cable-short	Alarm	Equipment	Cable short	Major	Physical short at the IF cable	1. Check cables and connectors. 2. Verify that the N-Type connector inner pin is not spliced. 3. Replace the radio card. 4. Replace the RFU.
1703	communication-failure	Alarm	Equipment	RFU communication failure	Warning	3. Defective IF cable. 4. IF cable not connected properly. 5. Defective RMC (Radio Modem Card). 6. Defective RFU. 7. RFU software download in progress.	1. Verify RFU software download completed. 2. Check IF cable and connector. 3. Verify that N-Type connector inner pin is not spliced. 4. Replace RMC. 5. Replace RFU. For a high power RF Unit: 1. Check BMA connector

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							- on OCB 2. Check BMA connector on RFU.
1704	delay-calibration-failure-1	Alarm	Equipment	RFU delay calibration failure 1	Warning	Defective RFU	1. Reset the RMC (Radio Modem Card) / RFU. 2. Replace RFU.
1705	delay-calibration-failure-2	Alarm	Equipment	RFU delay calibration failure 2	Warning	Calibration cannot be completed due to notch detection	Enter delay calibration value manually.
1706	extreme-temp-cond	Alarm	Equipment	RFU extreme temperature	Warning	1. Installation conditions. 2. Defective RFU.	1. Verify that the product is operating according to specifications. 2. Correct the installation conditions. 3. Replace the RFU.
1707	radio-unit-abc-incompatible-rfu	Alarm	Equipment	RFU is incompatible with ABC configuration	Warning	The RFU type does not support the type of Multi-Carrier ABC the user has configured.	Replace the RFU with an RFU type that supports the configured Multi-Carrier ABC type.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1708	freq-set-automatically	Event	Equipment	RFU frequency was set automatically	Warning	Defective RFU	1. Check if problem repeats and if errors/alarms reported. 2. Replace RFU.
1709	hardware-failure-1	Alarm	Equipment	RFU hardware failure 1	Critical	Defective RFU.	Replace RFU.
1710	hardware-failure-2	Alarm	Equipment	RFU hardware failure 2	Critical	Defective RFU.	Replace RFU.
1711	low-if-signal-to-rfu	Alarm	Equipment	Low IF signal to RFU	Major	1. IF cable connection. 2. Defective RFU. 3. Defective RMC (Radio Modem Card).	1. Check IF cable connectors. 2. Verify that N-Type connector inner pin is not spliced. 3. Replace RMC (Radio Modem Card). 4. Replace RFU.
1712	no-signal-from-rfu	Alarm	Equipment	Low IF signal from RFU	Warning	Low RX IF signal (140 MHz) from RFU.	1. Check IF cable and connectors. 2. Verify that N-Type connector inner pin is

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							not spliced. 3. Replace RMC (Radio Modem Card). 4. Replace RFU.
1713	pa-extreme-temp-cond	Alarm	Equipment	RFU PA extreme temperature	Warning	1. Installation conditions. 2. Defective RFU.	1. Check installation conditions. 2. Replace RFU.
1714	power-failure-12v	Alarm	Equipment	RFU power failure (12v)	Major	1. Defective IF cable/connector. 2. Defective RFU. 3. Defective IDU.	1. Replace IF cable/connector. 2. Replace RFU. 3. Replace IDU.
1715	power-failure-1point5	Alarm	Equipment	RFU power failure (1.5v)	Major	1. Defective IF cable/connector. 2. Defective RFU. 3. Defective IDU.	1. Replace IF cable/connector. 2. Replace RFU. 3. Replace IDU.
1716	power-failure-24v	Alarm	Equipment	RFU power failure (24v)	Major	1. Defective IF cable/connector. 2. Defective RFU. 3. Defective	1. Replace IF cable/connector. 2. Replace RFU. 3. Replace IDU.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						IDU.	
1717	power-failure-6v	Alarm	Equipment	RFU power failure (6v pro)	Major	1. Defective IF cable/connector. 2. Defective RFU. 3. Defective IDU.	1. Replace IF cable/connector. 2. Replace RFU. 3. Replace IDU.
1718	power-failure-6v-sw	Alarm	Equipment	RFU power failure (6v SW)	Major	1. Defective IF cable/connector. 2. Defective RFU. 3. Defective IDU.	1. Replace IF cable/connector. 2. Replace RFU. 3. Replace IDU.
1719	power-failure-minus-5v	Alarm	Equipment	RFU power failure (-5v)	Major	1. Defective IF cable/connector. 2. Defective RFU. 3. Defective IDU.	1. Replace IF cable/connector. 2. Replace RFU. 3. Replace IDU.
1720	power-failure-vd	Alarm	Equipment	RFU power failure (Vd)	Major	1. Defective IF cable/connector. 2. Defective RFU. 3. Defective IDU.	1. Replace IF cable/connector. 2. Replace RFU. 3. Replace IDU.
1721	reset-occurred	Event	Equipment	RFU reset	Major		
1722	rfu-loopback-active	Alarm	Equipment	RFU loopback is	Major	User has activated RFU	Disable RFU loopback.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				active		loopback.	
1723	rfu-mode-changed-to-combined	Event	Equipment	RFU mode changed to Combined	Indeterminate		
1724	rfu-mode-changed-to-diversity	Event	Equipment	RFU mode changed to Diversity	Indeterminate		
1725	rfu-mode-changed-to-main	Event	Equipment	RFU mode changed to Main	Indeterminate		
1726	rfu-power-supply-failure	Alarm	Equipment	RFU power supply failure	Major	At least one of the RFU's power supply voltages is too low.	1. Check the RFU cable connection. 2. Replace the RFU.
1727	rx-level-out-of-range	Alarm	Equipment	RFU RX level out of range	Warning	RSL is very low, link is down.	1. Check antenna alignment & link planning. 2. Check link settings (TX power, TX frequency). 3. Check antenna connections. 4. Replace local/remote RFU.
1728	rx-level-path1-out-of-range	Alarm	Equipment	RFU RX level path1 out of range	Warning	1. Improper installation. 2. Fading event.	1. Check that the fault is not due to rain/multi-path

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						3. Defective RFU.	fading or lack of LOS. 2. Check link settings (TX power, TX frequency). 3. Check antenna alignment. 4. Check antenna connections. 5. Replace local/remote RFU.
1729	rx-level-path2-out-of-range	Alarm	Equipment	RFU RX level path2 out of range	Warning	1. Improper installation. 2. Fading event. 3. Defective RFU.	1. Check that the fault is not due to rain/multi-path fading or lack of LOS. 2. Check link settings (TX power, TX frequency). 3. Check antenna alignment. 4. Check antenna connections.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							5. Replace local/remote RFU.
1730	radio-unit-communication-failure	Alarm	Equipment	Radio unit communication failure	Critical	1. Defective RFU cable. 2. RFU cable not connected properly. 3. Defective RIC (Radio Interface Card). 4. Defective RFU. 5. RFU initialization in progress. 6. RFU powered off.	1. Check RFU power supply. 2. Check RFU cable and connectors. 3. Replace RIC (Radio Interface Card). 4. Replace RFU.
1731	power-supply-radio-unit-cable-open	Alarm	Equipment	Power supply cable open	Major	Power is enabled but consumption is lower than threshold.	1. Check RFU cable and connectors. 2. If internal power supply is not in use, disable the power supply.
1732	power-supply-radio-unit-cable-short	Alarm	Equipment	Power supply cable short	Major	1. Power is enabled but consumption reached	1. Check RFU cable and connectors.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						the threshold. 2. Physical short at the ETH cable.	2. Disconnect and reconnect the RFU cable. 3. Extract the RIC-D and re-insert it. 4. Restart the IDU. 5. Replace the RIC-D card or the IDU.
1733	synthesizer-unlocked	Alarm	Equipment	RFU synthesizer unlocked	Major	At least one of the RFU synthesizers is unlocked	1. Replace RFU. 2. In XPIC mode, replace mate RFU as well.
1734	tx-level-out-of-range	Alarm	Equipment	RFU TX level out of range	Minor	Defective RFU (the RFU cannot transmit the requested TX power)	1. Replace RFU. 2. Intermediate solution - reduce TX power.
1735	tx-mute	Alarm	Equipment	RFU TX Mute	Warning	RFU Transmitter muted by user	Unmute the RFU transmitter
1736	unknown-rfu-type	Alarm	Equipment	IDU SW does not support this type of RFU	Major	IDC SW does not support the RFU	Upgrade IDC SW
1737	card-extracted-from-slot	Event	Equipment	Card was extracted from slot	Warning	Card was extracted from slot	NA

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1738	card-failure	Alarm	Equipment	Card is in Failure state	Major	Card is down as a result of card failure	1. Reset Card. 2. Check if slot was disabled.
1739	card-fpga-fw-not-found	Alarm	Equipment	FPGA Firmware file not found	Critical	There is no FPGA file found on the Main Board for the card on the slot	NA
1740	card-fw-load-fail	Alarm	Equipment	Download card firmware has failed	Major	Firmware download was unsuccessful.	1. Reset Card. 2. Download software package. 3. Try to insert another Card.
1741	card-inserted-to-slot	Event	Equipment	Card was inserted to slot	Warning	Card was inserted to slot	NA
1742	card-intermediate-channel-failure	Alarm	Equipment	Card is in interconnection failure state	Major	Card is down as a result of card interconnection failure	1. Reset Card. 2. Check if the slot was disabled.
1743	card-missing	Alarm	Equipment	Expected Card is missing in slot	Major	1. Card is missing. 2. Expected Card Type configured on empty slot.	1. Insert Expected Card. 2. Clear Expected Card Type.
1744	card-not-supported-for-slot	Alarm	Equipment	This Card type is not supported	Major	The card is not on the Allowed Card Types list	1. Reset. 2. Insert

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				in this slot		for this slot.	Card belongs to Allowed Card Types list.
1745	card-state-is-down	Event	Equipment	Card operational state is Down	Indeterminate	Card state was change to Down state	NA
1746	card-state-is-up	Event	Equipment	Card operational state is Up	Indeterminate	Card state was change to Up state	NA
1747	card-state-is-up-with-alarms	Event	Equipment	Card operational state is Up with Alarms	Indeterminate	Card state was change to Up state but with Alarms indication	NA
1748	card-unexpected	Alarm	Equipment	Unexpected Card Type in slot	Minor	Expected card type is different than the actual card type	1. Insert Expected Card. 2. Change Expected Card Type.
1749	slot-disabled	Event	Equipment	Slot was Disabled	Indeterminate	The user Disabled slot	NA
1750	slot-enabled	Event	Equipment	Slot was Enabled	Indeterminate	The user Enabled slot	NA
1751	slot-reseted	Event	Equipment	Card on slot was Reset	Indeterminate	The user Reset slot	NA
1752	fan-card-extraction-event	Event	Equipment	FAN Card was extracted from slot	Warning	FAN Card was extracted from slot	
1753	fan-card-failure-event	Event	Equipment	FAN failure	Major		
1754	fan-card-	Event	Equipment	FAN Card	Warning	FAN Card was	

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
	insertion-event	nt		was inserted to slot		inserted to slot	
1755	fan-card-missing	Alarm	Equipment	FAN Card is missing in slot	Critical	1. FAN Card is missing. 2. Slot enabled when empty.	1. Insert FAN Card. 2. Disable slot.
1756 See Note 3	fan-extreme-temperature	Alarm	Equipment	System Temperature not in allowed range.	Major	1. Installation conditions. 2. Defective unit. 3. Defective fan.	1. Correct the installation conditions. 2. Verify that the product is operating according to specifications. 3. Replace the fan card. 4. Replace the unit.
1757	fan-failure	Alarm	Equipment	FAN Card is in Failure state	Major	FAN Card is in Failure state	Change FAN Card
1758	pdc-card-extraction-event	Event	Equipment	Power Supply was extracted from slot	Warning	Power Supply was extracted from slot	Re-Insert the power supply back into the slot.
1759	pdc-card-insertion-event	Event	Equipment	Power Supply was inserted to slot	Warning	Power Supply was inserted to slot.	
1760	pdc-card-	Alarm	Equipment	Power	Major	1. Power	Insert Power

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
	missing	m		Supply is missing in slot		Supply is missing. 2. Slot enabled when empty.	Supply.
1761	pdc-over-voltage	Alarm	Equipment	Over voltage	Major	1. System power supply voltage is higher than allowed. 2. Threshold value is too low.	1. Make sure the power supply voltage is within the specification range. 2. Check the value of the threshold.
1762	pdc-under-voltage	Alarm	Equipment	Under voltage	Major	1. System power supply voltage is lower than allowed. 2. Threshold value is too high.	1. Make sure the power supply voltage is within the specification range. 2. Check the value of the threshold.
1763	TCC-fpga-fw-not-found	Alarm	Equipment	The Main board firmware is not found	Warning		
1764	TCC-fw-load-fail	Alarm	Equipment	Download Main Board firmware has failed	Major	Firmware download was unsuccessful.	1. Reset board. 2. Download software package. 3. Try to insert another

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							board.
1766	upload-software-failed	Event	Equipment	RFU installation failure	Warning	1. Unsupported RFU type. 2. IDU-RFU communications problem. 3. RFU failure.	1. Make sure RFU is supported by SW version. 2. Check IDU-RFU cable. 3. Replace RFU.
1767	upload-software-started	Event	Equipment	RFU installation in progress	Warning	User command	
1768	upload-software-succeeded-event	Event	Equipment	RFU installation successfully completed	Warning	User command	
1770	cable-lof-rfu	Event	Equipment	Unit performing power-up.	Major		
1771	cable-error-rfu	Alarm	Equipment	RFU cable error.	Major	Errors in signal from IDU to XCVR.	1. Check the IF cable and connectors. 2. Verify that the N-Type/TNC connector inner pin is not spliced. 3. Replace RMC. 4. Replace XCVR.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1772	xpic-data-los	Alarm	Equipment	Radio XPIC sync loss	Major	Signalling between RMCs (Radio Modem Cards) for XPIC functionality has failed	1. Check that the RMCs are in allowed slots. 2. Populate the RMCs in different allowed location in the chassis. 3. Replace RMC/s. 4. Replace chassis.
1773	early-warning	Alarm	Communications	Radio early warning.	Warning	The estimated radio BER (Bit Error Rate) is above 10E-12.	5. Check link performance. 6. Check IF cable, and replace if required. 7. Replace XCVR. 8. Replace RMC.
1774	sw-download-incompatible-rfu	Alarm	Equipment	RFU software download cannot be initiated.	Critical	The hardware of the XCVR is OK, but is it running with METRO radio application.	1. Upgrade the XCVR software application via XPAND-IP and then reinitiate software download..
1775	hw-incompatible-	Alarm	Equipment	RFU software	Critical	Wrong type of XCVR, the	Replace the XCVR

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
	rfu			download is not possible.		XCVR hardware is METRO.	
1776	pll-rmc	Alarm	Equipment	RMC hardware failure.	Major	RMC hardware failure of the clock distributor.	Replace the RMC.
1777	rfu-mute-with-timeout	Event	Equipment	RFU TX Mute with timeout	Warning	RFU Transmitter muted by user.	Unmute the RFU transmitter or wait for expiration of the timeout.
1778	rfu-power-decreased-due-to-pa-temp	Alarm	Equipment	RFU power decreased due to PA temperature	Major	Defective RFU (the RFU cannot transmit the requested TX power).	1. Replace RFU. 2. Intermediate solution - reduce TX power.
1779	rfu-reset-communication-recalibration	Event	Equipment	RFU reset due to communication recalibration	Warning	1. External link interference. 2. Faulty HW: Cable, RIC-D, or RFU.	1. Check the link performance. 2. Check the installation. 3. Replace the RFU cable. 4. Replace the RIC-D. 5. Replace the RFU.
1780	mrnc-running-script-deleted	Event	Equipment	MRMC running script is deleted	Warning	New installed software package does not include the running MRMC	6. Make sure the required software package

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						radio script	include the running MRMC radio script. 7. Download and install the correct software package.
1781	mrmc-running-script-updated	Event	Equipment	MRMC running script is updated	Warning	New installed software package does has an updated version of the running MRMC radio script	Reset the radio carrier to reacquire the new updated MRMC radio script
1782	radio-2_5gbps-mismatch-configuration	Alarm	Equipment	2.5Gbps mismatch configuration	Warning	The card can not function outside of an ABC group in 2.5Gbps mode.	Add the card to an ABC group, or change the Slot Section to 1Gbps.
1783	remote-fault-indication	Alarm	Communication	Radio remote fault indication (RFI)	Minor		
1784	rfu-pmin-atpc-disable	Event	Equipment	ATPC was disabled due to Tx level below 6 dBm	Warning	Tx level below 6 dBm	Set Tx level over 5dBWm and reenable ATPC
1785	rfu-pmin-atpc-enabled	Event	Equipment	To enable ATPC, Tx level should be 6 dBm or higher	Warning	Tx level below 6 dBm	Set Tx level over 5dBWm and reenable ATPC
1790	np-hw-failure	Alarm	Equipment	Hardware	Critical	An internal	Replace the

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
		m		failure		hardware failure has been detected by the system.	card or unit reporting the hardware failure.
1794	interface-not-functional-until-reset	Alarm	equipment	Interface is not operational until chassis reset	Warning	Changes were made to platform due to user configuration	Reset chassis
1800	t3-loc-alarm	Alarm	Equipment	T3 sync interface Loss of Carrier	Major	1. Cable disconnected. 2. Defective cable.	1. Check connection of the cable. 2. Disable the interface in the Interface Manager.
1975	radio-fan-failure	Alarm	Equipment	RFU fan failure	Major	1. RFU fan is disconnected. 2. RFU fan HW failure. 3. RFU fan jammed.	1. Check fan cable connection to the RFU. 2. Check/replace the fan. 3. Clear/clean the fan.
1976	second-bbi-hw-support-failure	Alarm	Equipment	RFU2 in the RIC-D cannot be used in the selected slot with the current TCC-U HW version	Major	User is trying to set Interface Type to "Extension" but the TCC-U model does not support using RFU2 in Slot 7 or Slot 8.	1. Replace the TCC-U card with a model that supports RFU2 in slots 7 and 8. 2. Set the

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							Interface Type to "Ethernet" or "RFU" to use TCC-U port 7 or 8 as a traffic port instead of RFU2 on the RIC-D. 3. Disable the Radio-Unit admin.
1977	unsupported-configuration-for-rfu-type	Alarm	Equipment	Unsupported configuration for RFU type	Warning	1. No radio support for TX mute to be configured to Off. 2. No radio support for a member of a TCC-based ABC group. 3. No radio support for a member of a radio protection group.	1. Configure TX mute to On. 2. Remove radio from TCC-based ABC group. 3. Remove the radio from the radio protection group.
1978	xpic-mismatch-alarm	Alarm	Equipment	XPIC insufficient condition - not supported configuration for RFU	Warning	No Radio Support for member in XPIC group	Remove radio port from XPIC group

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				type			
2001	pwe3-pwc-s-card-reset	Alarm	Equipment	TDM-LIC has rebooted and is not in service now	Major	1. Recent TDM-LIC card reset; 2. System malfunction.	1. Wait for card to reboot. 2. Reset the TDM-LIC card. 3. Replace card.
2002	pwe3-pwc-s-config-mismatch	Alarm	Equipment	TDM-LIC configuration mismatch	Major	System malfunction.	Power cycle the TDM-LIC.
2003	pwe3-pwc-s-front-panel-clock-los	Alarm	Equipment	Loss of Signal (LOS) on TDM-LIC's front panel clock port	Major	1. Cable is not properly connected. 2. External equipment is faulty.	1. Reconnect the cable. 2. Check line cables. 3. Check external equipment. 4. Reset the TDM-LIC.
2004	pwe3-pwc-s-host-pw-lic-comm-disrupt	Alarm	Equipment	Communication with TDM-LIC is disrupted in Host-Card direction	Minor	System malfunction	1. Reset the TDM-LIC. 2. Replace card.
2005	pwe3-pwc-s-hw-failure	Alarm	Equipment	TDM-LIC hardware failure	Major	System malfunction	1. Reset the TDM-LIC. 2. Replace card.
2006	pwe3-pwc-s-pw-lic-host-comm-disrupt	Alarm	Equipment	No communication with TDM-LIC	Major	TDM-LIC to Host communication failure.	1. Reset the TDM-LIC. 2. Reset the whole device.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							3. Replace card.
2007	pwe3-pws-s-jitter-buffer-overflow	Alarm	Equipment	Jitter-buffer-overflow alarm on TDM service	Major	TDM service synchronization failure.	1. Check TDM service configuration. 2. Check the loop timing/clock recovery configuration.
2008	pwe3-pws-s-late-frame	Alarm	Equipment	Late-frame alarm on TDM service	Warning	TDM service failure or device synchronization problem.	Check TDM service configuration across the network.
2009	pwe3-pws-s-loss-of-frames	Alarm	Equipment	Loss-of-frames alarm on TDM service	Major	Failure along the network path of TDM service	Check network or configuration for errors in the network transport side of the service
2010	pwe3-pws-s-malformed-frames	Alarm	Equipment	Malformed-frames alarm on TDM service	Major	1. Payload size does not correspond to the defined value. 2. Mismatch in PT value in RTP header (if used)	Check TDM service configuration
2011	pwe3-pws-s-	Alarm	Equipment	Misconnect	Major	Stray packets	Check TDM

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
	misconnection	m		ion alarm on TDM service		with wrong RTP configurations are received and dropped.	service configuration
2012	pwe3-tdm-ports-ais	Alarm	Equipment	Alarm Indication Signal (AIS) on TDM-LIC TDM port	Major	1. Cable is not properly connected. 2. External equipment is faulty. 3. External equipment is not properly configured.	1. Check the cable connectivity at both local and peer interfaces. 2. Check external equipment. 3. Check configuration of the external equipment.
2013	pwe3-tdm-ports-lof	Alarm	Equipment	Loss Of Frame (LOF) on TDM-LIC TDM port	Major	1. Line is not properly connected. 2. External equipment is faulty. 3. Configuration problem.	1. Check the line interface connectivity 2. Correct the TDM configuration. 3. Check the equipment that feeds the system
2014	pwe3-tdm-ports-lomf	Alarm	Equipment	Loss Of Multi-Frame (LOMF) on TDM-LIC TDM port	Major	1. Line is not properly connected. 2. External	1. Check the line interface connectivity

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						equipment is faulty. 3. Configuration problem.	2. Correct the TDM configuration. 1. Check the equipment that feeds the system
2015	pwe3-tdm-ports-loopback-alarm	Alarm	Equipment	Loopback on TDM-LIC TDM port	Warning	Loopback enabled.	Disable loopback.
2016	pwe3-tdm-ports-los	Alarm	Equipment	Loss Of Signal (LOS) on TDM-LIC TDM port	Major	1. Cable is not properly connected. 2. Cable is faulty; 3. External equipment is faulty; 4. Defective TDM-LIC.	1. Check the cable connectivity at both local and peer interfaces. 2. Check external equipment.
2017	pwe3-tdm-ports-rai	Alarm	Equipment	Remote Alarm Indication (RAI) on TDM-LIC TDM port	Minor	1. Cable is not properly connected. 2. External equipment is faulty.	1. Check the cable connectivity at both local and peer interfaces. 2. Check external equipment.
2018	pwe3-tdm-ports-unexpected-signal-alarm	Alarm	Equipment	E1/DS1 Unexpected signal on TDM-LIC TDM port	Warning	1. Port is disabled. 2. Line is connected to a	1. Enable relevant port. 2. Disconnect cable

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						disabled port.	from relevant port.
2021	pwe3-pwc-ssm-rx-changed	Event	Equipment	SSM received pattern change was discovered	Warning		No action is required.
2022	pwe3-stm1oc3-s-excessive-ber-alarm	Alarm	Equipment	Excessive BER on TDM-LIC STM1/OC3 port	Major	1. Line is not properly connected. 2. External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment. 4. Power cycle the TDM-LIC.
2023	pwe3-stm1oc3-s-lof-alarm	Alarm	Equipment	Loss Of Frame (LOF) on TDM-LIC STM1/OC3 port	Major	1. Cable is not properly connected. 2. External equipment is faulty. 3. Wrong TDM configuration.	1. Check the cable connectivity at both local and peer interfaces. 2. Check external equipment. 3. Reset the TDM-LIC.
2024	pwe3-stm1oc3-s-loopback-alarm	Alarm	Equipment	Loopback on TDM-LIC STM1/OC3 port	Warning	STM1/OC3 loopback enabled.	Disable STM1/OC3 loopback.
2025	pwe3-stm1oc3-s-loss-alarm	Alarm	Equipment	Loss Of Signal	Critical	1. Cable is not	1. Reconnect cable.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				(LOS) on TDM-LIC STM1/OC3 port		- properly connected. - External equipment is faulty. - Peer Equipment Configuration problem.	2. Check line cables. 3. Check external equipment. 4. Reset the TDM-LIC.
2026	pwe3-stm1oc3-s-mute-override-alarm	Alarm	Equipment	SFP is muted on TDM-LIC STM1/OC3 port	Warning	The SFP interface has been muted.	Set the interface to mute OFF.
2027	pwe3-stm1oc3-s-sfp-absent-alarm	Alarm	Equipment	SFP absent in TDM-LIC STM1/OC3 port	Critical	SFP is not inserted properly.	Insert the SFP.
2028	pwe3-stm1oc3-s-sfp-failure-alarm	Alarm	Equipment	SFP failure on TDM-LIC STM1/OC3 port	Critical	1. SFP is not inserted properly. 2. Card is faulty.	1. Insert the SFP. 2. Replace the SFP. 3. Replace the card.
2029	pwe3-stm1oc3-s-sfp-tx-fail-alarm	Alarm	Equipment	SFP transmit failure on TDM-LIC STM1/OC3 port	Critical	1. SFP is not inserted properly. 2. Card is faulty.	1. Insert the SFP. 2. Replace the SFP. 3. Replace the card.
2030	pwe3-stm1oc3-s-signal-degrade-alarm	Alarm	Equipment	Signal Degrade on TDM-LIC STM1/OC3 port	Minor	1. Line is not properly connected. 2. SFP is not properly	1. Install SFP properly. 2. Reconnect line. 3. Check line cables.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						installed. 3. SFP is faulty. 4. External equipment is faulty	4. Check external equipment. 5. Change Signal Degrade Threshold.
2031	pwe3-stm1oc3-s-slm-alarm	Alarm	Equipment	J0 Trace Identifier Mismatch on TDM-LIC STM1/OC3 port	Minor	1. J0 misconfiguration. 2. Line is not properly connected. 3. SFP is not properly installed. 4. External equipment is faulty.	1. Make sure expected and received J0 identifiers match. 2. Connect line cables properly. 3. Install SFP properly.
2032	pwe3-stm1oc3-s-ssm-rx-changed	Event	Equipment	SSM pattern received on TDM-LIC STM1/OC3 port changed	Warning		
2033	pwe3-vc12vt15-s-ais-alarm	Alarm	Equipment	Alarm Indication Signal (AIS) on TDM-LIC VC12/VT1.5	Minor	1. Cable is not properly connected. 2. Local/Peer Configuration is incorrect.	1. Check the cable connectivity at both local and peer interfaces. 2. Check/Correct the configuration at the local/peer.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2034	pwe3-vc12vt15-s-excessive-ber-alarm	Alarm	Equipment	Excessive BER on TDM-LIC VC12/VT1.5	Minor	1. Line is not properly connected. 2. External equipment is faulty.	1. Check the line cables. 2. Fix the problem at the peer. 3. Change the Excessive BER threshold.
2035	pwe3-vc12vt15-s-loopback-alarm	Alarm	Equipment	Loopback on TDM-LIC VC12/VT1.5	Warning	Loopback enabled on TDM-LIC VC12/VC11.	Disable loopback on TDM-LIC VC12/VC11.
2036	pwe3-vc12vt15-s-rcv-plm-alarm	Alarm	Equipment	Payload Mismatch Path (PLM) received on TDM-LIC VC12/VT1.5	Minor	Incorrect VC12/VC11 configuration	Check/Correct the configuration at the local/peer.
2037	pwe3-vc12vt15-s-rcv-rdi-alarm	Alarm	Equipment	Remote Defect Indication (RDI) received on TDM-LIC VC12/VT1.5	Minor	1. Alarm exists along the Trail. 2. Cable is not properly connected.	1. Fix the problem along the trail. 2. Check the cable connectivity at both local and peer interfaces.
2038	pwe3-vc12vt15-s-rcv-slm-alarm	Alarm	Equipment	Signal Label Mismatch (SLM) received on TDM-LIC VC12/VT1.5	Minor	1. J2 misconfiguration. 2. Line is not properly connected. 3. External	1. Make sure expected and receive J2 match. 2. Reconnect line. 3. Check line

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						equipment is faulty.	cables. 4. Check external equipment. 5. Reset the TDM-LIC.
2039	pwe3-vc12vt15-s-signal-degrade-alarm	Alarm	Equipment	Signal Degrade on TDM-LIC VC12/VT1.5	Minor	1. Line is not properly connected. 2. External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment. 4. Reset the TDM-LIC.
2040	pwe3-vc12vt15-s-unequipped-alarm	Alarm	Equipment	Unequipped on TDM-LIC VC12/VT1.5	Minor	1. Incorrect line is connected. 2. External equipment is faulty or misconfigured.	1. Reconnect line. 2. Check line cables. 3. Check external equipment. 4. Reset the TDM-LIC.
2041	pwe3-card-group-s-config-mismatch	Alarm	Equipment	TDM-LIC card protection configuration mismatch	Major	The configuration between the TDM-LIC card protection members is not aligned	Apply a copy-to-mate command to copy the configuration from the required TDM-LIC to the other one
2042	pwe3-card-group-s-lockout	Alarm	Equipment	TDM-LIC card	Minor	The user has issued a	Clear the lockout command

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				protection group lockout command is on		lockout command	
2043	pwe3-card-group-s-no-mate	Alarm	Equipment	A member of TDM-LIC card protection group is missing	Minor	TDM-LIC card is not installed in the shelf	Install the missing TDM-LIC card
2044	pwe3-card-group-s-protection-switch-evt	Event	Equipment	TDM-LIC card protection switch over, priority	Warning	1. LOS alarm on a STM1 interface of the TDM-LIC card protection group member; 2. A TDM-LIC card protection group member was disabled or pulled out of the shelf	1. Check line cables. 2. Enable the TDM-LIC card protection group member or insert the missing card into the shelf..
2045	pwe3-vc12vt15-s-lop-alarm	Alarm	Equipment	Loss Of Pointer (LOP) received on TDM-LIC VC12/VT1.5	Minor	1. Timing not configured correctly. 2. End-to-end timing is not synchronized. 3. External Equipment is faulty.	1. Correct the timing configuration. 2. Correct the end-to-end timing problem. 3. Check the external

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						4. Network service connectivity problem. 5. Lower layer problem.	equipment. 4. Fix the network service problem. 5. Fix the interface and card problem.
2046	pwe3-tunnel-groups-s-protection-switch	Event	Equipment	Path protection switch on TDM service	Minor	1. Failure along service primary path. 2. User command.	1. Check errors along primary path 2. Check local service configuration.
2047	pwe3-tunnel-groups-s-revertive-switch	Event	Equipment	Path protection revertive switch on TDM service	Minor	Primary path has been operational for the duration of the defined WTR time	-
2100	STM-1-OC-3-IN-LOS	Alarm	Equipment	Loss of Signal on Line Interface (LOS) on STM-1/OC-3 port.	Critical	1. Line is not properly connected. 2. External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment.
2101	STM-1-OC-3-IN-LOF	Alarm	Equipment	Loss of Frame on Line Interface (LOF) on STM-1/OC-	Major	1. Line is not properly connected. 2. External	1. Reconnect line. 2. Check line cables. 3. Check

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				3 port.		equipment is faulty.	external equipment.
2102	STM-1-OC-3-IN-MSAIS	Alarm	Equipment	Alarm Indication Signal on Line Interface (MS-AIS/AIS-L) received.	Minor	1. Line is not properly connected. 2. External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment.
2103	STM-1-OC-3-IN-MSRDI	Alarm	Equipment	Remote Defect Indication on Line Interface (MS-RDI/RDI-L) received.	Minor	External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment.
2104	STM-1-OC-3-RX-LOS	Alarm	Equipment	Loss of STM-1/OC-3 Frame on Radio Interface.	Major	1. All channels in Multi Carrier ABC group are down. 2. Incorrect configuration on remote side.	1. Check link performance. 2. Check radio alarms for channel. 3. Check configuration.
2105	STM-1-OC-3-RX-MSAIS	Alarm	Equipment	MS-AIS/AIS-L on Radio Interface detected.	Minor	1. Remote STM-1/OC-3 signal is missing (LOS/LOF/MS-AIS/AIS-L on remote STM-1/OC-3)	Check remote equipment.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						interface). 2. STM-1/OC-3 Channel removed due to reduced radio capacity on remote side.	
2106	STM-1-OC-3-RX-RDI	Alarm	Equipment	MS-RDI/RDI-L on Radio Interface detected.	Minor	External equipment is faulty.	Check remote equipment.
2107	STM-1-OC-3-LOOPBACK	Alarm	Equipment	STM-1/OC-3 Loopback	Warning	Looping.	Remove looping.
2108	STM-1/OC-3-CHANNEL-1-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading	1. Check link performance. 2. Check radio alarms for channel.
2109	STM-1-OC-3-PBRS-INSERTION	Alarm	Equipment	PRBS insertion.	Warning	PRBS insertion on STM-1/OC-3 card.	Remove PRBS insertion.
2110	STM-1-OC-3-SFP-NOT-DETECTED	Alarm	Equipment	SFP absent in STM-1/OC-3 port.	Critical	1. SFP is not properly installed. 2. SFP is faulty.	1. Install SFP properly. 2. Replace the card.
2111	STM-1-OC-3-SFP-TX-FAILURE	Alarm	Equipment	SFP Transmit Failure on STM-1/OC-3 port.	Critical	1. SFP is faulty.	1. Replace SFP or insert SFP if it is not inserted correctly. 2. Replace

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							the card.
2112	STM-1/OC-3-SFP-TX-MUTED	Alarm	Equipment	SFP is muted on STM-1/OC-3 port.	Warning	SFP is muted by configuration.	Remove muting.
2113	STM-1/OC-3-CHANNEL-2-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for channel.
2114	STM-1/OC-3-CHANNEL-3-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for channel.
2115	STM-1/OC-3-CHANNEL-4-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for channel.
2116	STM-1/OC-3-CHANNEL-5-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for channel.
2117	STM-1/OC-3-CHANNEL-6-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				capacity).			channel.
2118	STM-1/OC-3-CHANNEL-7-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for channel.
2119	STM-1/OC-3-CHANNEL-8-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for channel.
2120	STM1-OC3-GROUP-ACTIVITY-CHANGED	Event	Equipment	STM-1/OC-3 Group protection switchover	Warning	1. LOS alarm on an STM-1/OC-3 interface. 2. STM1-OC3 Group protection group member was disabled or pulled out of the shelf.	1. Check line cables. 2. Check external equipment.
2200	MC-ABC-Local-LOF	Alarm	Communications	Multi Carrier ABC LOF.	Critical	All channels in Multi Carrier ABC group are down.	1. Check link performance on all radio channels in Multi Carrier ABC group. 2. Check

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							radio alarms for channels in Multi Carrier ABC group. 3. Check configuration of Multi Carrier ABC group.
2201	MC-ABC-local-cap-below	Alarm		Multi Carrier ABC bandwidth is below the threshold	Major	1. One of the radio channels in the Multi Carrier ABC group has a lower capacity than expected 2. Minimum bandwidth threshold configuration is wrong	1. Check link performance on all radio channels in Multi Carrier ABC group 2. Check radio alarms for channels in Multi Carrier ABC group 3. Check configuration of Multi Carrier ABC group Minimum bandwidth threshold
2203	MC-ABC-Lvds-Error-SI2	Alarm	Equipment	LVDS RX Error Slot 2.	Major	Hardware failure	1. Replace RMC/RIC.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						between RMC/RIC and TCC cards.	2. Replace TCC. 3. Replace chassis.
2204	MC-ABC-Lvds-Error-SI3	Alarm	Equipment	LVDS RX Error Slot 3.	Major	Hardware failure between RMC/RIC and TCC cards.	1. Replace RMC/RIC. 2. Replace TCC. 3. Replace chassis.
2205	MC-ABC-Lvds-Error-SI4	Alarm	Equipment	LVDS RX Error Slot 4.	Major	Hardware failure between RMC/RIC and TCC cards.	1. Replace RMC/RIC. 2. Replace TCC. 3. Replace chassis.
2206	MC-ABC-Lvds-Error-SI5	Alarm	Equipment	LVDS RX Error Slot 5.	Major	Hardware failure between RMC/RIC and TCC cards.	1. Replace RMC/RIC. 2. Replace TCC. 3. Replace chassis.
2207	MC-ABC-Lvds-Error-SI6	Alarm	Equipment	LVDS RX Error Slot 6.	Major	Hardware failure between RMC/RIC and TCC cards.	1. Replace RMC/RIC. 2. Replace TCC. 3. Replace chassis.
2208	MC-ABC-Lvds-Error-SI7	Alarm	Equipment	LVDS RX Error Slot 7.	Major	Hardware failure between RMC/RIC and TCC cards.	1. Replace RMC/RIC. 2. Replace TCC. 3. Replace chassis.
2209	MC-ABC-Lvds-Error-SI8	Alarm	Equipment	LVDS RX Error Slot 8.	Major	Hardware failure	1. Replace RMC/RIC.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						between RMC/RIC and TCC cards.	2. Replace TCC. 3. Replace chassis.
2210	MC-ABC-Lvds-Error-SI9	Alarm	Equipment	LVDS RX Error Slot 9.	Major	Hardware failure between RMC/RIC and TCC cards.	1. Replace RMC/RIC. 2. Replace TCC. 3. Replace chassis.
2211	MC-ABC-Lvds-Error-SI10	Alarm	Equipment	LVDS RX Error Slot 10.	Major	Hardware failure between RMC/RIC and TCC cards.	1. Replace RMC/RIC. 2. Replace TCC. 3. Replace chassis.
2212	MC-ABC-Lvds-Error-SI12	Alarm	Equipment	LVDS RX Error Slot 12.	Major	Hardware failure between RMC/RIC and TCC cards.	1. Replace RMC/RIC. 2. Replace TCC. 3. Replace chassis.
2213	MC-ABC-robustness-member-disabled	Alarm	Equipment	MC-ABC member has been disabled due to robustness reason	Major	The corresponding MC-ABC member has been temporarily disabled within the group. It was caused by consecutive RFU HW failures	Verify the proper functioning and connectivity of the cable and RF unit.
2219	MC-ABC-Ch-Id-Mismatch-Ch1	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch	Warning	Configuration failure.	Compare Channel ID configuration with remote

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				Ch1.			side.
2220	MC-ABC-Ch-Id-Mismatch-Ch2	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch2.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.
2221	MC-ABC-Ch-Id-Mismatch-Ch3	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch3.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.
2222	MC-ABC-Ch-Id-Mismatch-Ch4	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch4.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.
2223	MC-ABC-Ch-Id-Mismatch-Ch5	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch5.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.
2224	MC-ABC-Ch-Id-Mismatch-Ch6	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch6.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.
2225	MC-ABC-Ch-Id-Mismatch-Ch7	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch7.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.
2226	MC-ABC-Ch-Id-Mismatch-Ch8	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch8.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.
2227	MC-ABC-Ch-Id-Mismatch-Ch9	Alarm	Equipment	Multi Carrier ABC Channel Id	Warning	Configuration failure.	Compare Channel ID configuration

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				Mismatch Ch9.			with remote side.
2228	MC-ABC-Ch-Id-Mismatch-Ch10	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch10.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.
2235	MC-ABC-Ch-Id-Disabled-Ch1	Alarm	Equipment	Multi Carrier ABC Channel Id Manual Disabled Ch1.	Warning	Admin state for channel is down.	Enable admin state for channel.
2236	MC-ABC-Ch-Id-Disabled-Ch2	Alarm	Equipment	Multi Carrier ABC Channel Id Manual Disabled Ch2.	Warning	Admin state for channel is down.	Enable admin state for channel.
2237	MC-ABC-Ch-Id-Disabled-Ch3	Alarm	Equipment	Multi Carrier ABC Channel Id Manual Disabled Ch3.	Warning	Admin state for channel is down.	Enable admin state for channel.
2238	MC-ABC-Ch-Id-Disabled-Ch4	Alarm	Equipment	Multi Carrier ABC Channel Id Manual Disabled Ch4.	Warning	Admin state for channel is down.	Enable admin state for channel.
2239	MC-ABC-Ch-Id-Disabled-Ch5	Alarm	Equipment	Multi Carrier ABC Channel Id Manual Disabled Ch5.	Warning	Admin state for channel is down.	Enable admin state for channel.
2240	MC-ABC-Ch-Id-Disabled-Ch6	Alarm	Equipment	Multi Carrier ABC Channel Id	Warning	Admin state for channel is down.	Enable admin state for channel.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				Manual Disabled Ch6.			
2241	MC-ABC-Ch-Id-Disabled-Ch7	Alarm	Equipment	Multi Carrier ABC Channel Id Manual Disabled Ch7.	Warning	Admin state for channel is down.	Enable admin state for channel.
2242	MC-ABC-Ch-Id-Disabled-Ch8	Alarm	Equipment	Multi Carrier ABC Channel Id Manual Disabled Ch8.	Warning	Admin state for channel is down.	Enable admin state for channel.
2250	CRB-Group-Entity	Alarm	communications	Enhanced Multi Carrier ABC LOF	Critical	All channels in Enhanced Multi Carrier ABC group are down	1. Check link performance on all channels in Enhanced Multi Carrier ABC group. 2. Check alarms for channels in Enhanced Multi Carrier ABC group. 3. Check configuration of Enhanced Multi Carrier ABC

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							group.
2300	protection-configuration-mismatch	Alarm	Equipment	Protection configuration mismatch!	Major	The configuration between the protected devices is not aligned.	Apply copy-to-mate command to copy the configuration from the required device to the other one.
2301	protection-copytomate-started	Event	Processing	Copy to mate started	Indeterminate	The copy-to-mate command has just begun!	This is a notification
2302	protection-copytomate-completed	Event	Processing	Copy to mate completed	Indeterminate	The copy-to-mate command was completed.	This is a notification
2303	protection-version-mismatch-alarm	Alarm	Equipment	Protection version mismatch	Major	The protected devices run different software versions or have different hardware capabilities.	1. Install the same software version on the protected devices. 2. Ensure the protected devices are identical in terms of supported features by hardware inventory.
2400	cpri-optical-rx-loss	Alarm	Equipment	Loss of CPRI optical signal - based on	Critical	1. No SFP is connected. 2. Issue with the Fiber	Check Fiber connection

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				RX level lower than a predefined threshold		link.	
2401	cpri-los	Alarm	Equipment	CPRI LOS caused by at least 16 8B/10B violation events in a whole hyperframe	Major	1. Input signal is not in a CPRI format. 2. CPRI format is different than the configured one. 3. Errors in the CPRI link that feeds the system.	1. Check CPRI format. 2. Check CPRI link/cable.
2402	cpri-clock-unit-unlock	Alarm	Equipment	CPRI clock unit is not locked	Warning	1. The recovered clock of the CPRI module is not locked.	Check the clock source of the CPRI module.
3001	10gbps-mode-front-panel-ports-unavailable	Alarm	Equipment	Reset chassis to activate front panel Ethernet ports	Warning	Front panel Ethernet ports cannot work when slot 12 is configured in 10Gbps mode.	Reset chassis.
3002	slot-mode-front-panel-ports-not-functional	Alarm	Equipment	Front panel Ethernet port cannot function in current configured capacity	Warning	Front panel Ethernet port cannot work in a mode other than 1Gbps.	Configure the relevant capacity mode to 1 Gbps mode.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				mode			
3003	abc-mode-not-functional	Alarm	Equipment	Multi Carrier ABC group is not functional in current configured capacity mode	Warning	Multi Carrier ABC group does not support the configured capacity mode.	Configure the relevant capacity mode to 1 Gbps mode.
3004	abc-mode-not-functional-until-reset	Alarm	Equipment	Multi Carrier ABC group is not functional in current configured capacity mode until chassis is reset	Warning	Multi Carrier ABC group capacity mode is different than the configured capacity mode.	Reset chassis.
4000	hw-failure	Alarm	Equipment	Card has one or more HW failures	Critical	One or more HW faults.	Replace card.
4001	slotsection-2_5gbps-compatibility	Alarm	Equipment	Card can not function in 2.5Gbps mode.	Warning	The user set an expected card that does not support 2.5Gbps.	Change the Slot Section to 1Gbps.
4002	slot-slotsection-10gbps-card-not-functional	Alarm	Equipment	Card is not functional until chassis is reset	Warning	Slot is not in 10Gbps mode.	Reset chassis.
5000	failure-login-event	Event	Equipment	User blocked due to consecutive failure login	Indeterminate	User blocked due to consecutive failure login	The user should wait few minutes until it account will be unblock
5001	g8032-	Alarm	Processing	ERPI is	Minor	Either link	Fix the broken

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
	protection-switching-alarm	m		either in protection state or forced protection state		failure happened in the ring or force/manual command is active.	link in the ring or release the force/manual command.
5002	g8032-failure-of-protocol-pm-alarm	Alarm	Processing	More than a single RPL is configured in a ring	Warning	RPL configuration is wrong.	Reconfigure the RPL.
5003	lldp-topology-change	Event	Processing	LLDP topology change	Warning	New neighbor	None
5004	security-log-upload-started-event	Event	Equipment	Security log upload started	Indeterminate	Security log upload started	
5005	security-log-upload-failed-event	Event	Equipment	Security log upload failed	Indeterminate	Security log upload failed	
5006	security-log-upload-succeeded-event	Event	Equipment	Security log upload succeeded	Indeterminate	Security log upload succeeded	
5010	force-mode-alarm	Alarm	Equipment	System is in sync force mode state	Warning	User command	
5011	sync-quality-change-event	Event	Equipment	The sync-source quality level was changed	Major		
5012	system-clock-in-holdover-mode	Alarm	Equipment	System Synchronization Reference in Holdover Mode	Critical	Active Sync Source Failure and the clock unit enters holdover mode	1. Fix the Sync Source Failure. 2. Provide an alternative sync

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							source.
5013	sync-T0-quality-change-event	Event	Equipment	System sync reference T0 quality has changed	Major		
5014	sync-pipe-invalid-interface-clock-source	Alarm	Equipment	The pipe interface clock-source in signal-interface table is not system-clock	Major	For interfaces of a Pipe, the outgoing clock source type must be "System Clock".	Set the outgoing clock source type to System Clock in the Outgoing Clock Table via Outgoing Clock view in the Web EMS or the platform sync interface config command in the CLI.
5015	sync-pipe-missing-edge	Alarm	Equipment	The pipe is missing an edge interface	Major	Pipe Regenerator contains less than 2 interfaces.	Configure a second interface for the Pipe Regenerator.
5016	sync-pipe-interface-op-state-down	Alarm	Equipment	Pipe interface operational state is down	Major	One or both of the Regenerator Interfaces status is down.	1. Check both interfaces of the pipe regenerator - admin and operational statuses. 2. Check Ethernet cable communication

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							ation. 3. Make sure Radio Link is up.
5017	sync-pipe-invalid-pipe	Alarm	Equipment	Pipe is invalid	Major	Pipe Regenerator configuration is invalid or interface operational failure.	1. Fix the Pipe Regenerator configuration. 2. Ensure both interfaces are operational.
5018	sync-1588-tc-not-operational	Alarm	Equipment	1588TC is not operational	Major	System Failure	Reboot the unit
5019	sync-1588-tc-not-calibrated	Alarm	Sync	1588TC over the radio is not calibrated	Major	1588TC over the radio is enabled but could not be calibrated	Check that the radio link configuration have: 1. TC enabled on both sides 2. Frequency lock UP on both sides 3. TC downstream at one side and upstream on the other side
5020	sync-T3-remote-loopback	Alarm	Equipment	T3 interface at loopback mode	Warning	T3 Interface is configured in loopback.	If required, disable the loopback.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5021	sync-T4-analog-loopback	Alarm	Equipment	T4 interface at loopback mode	Warning	T4 Interface is configured in loopback.	If required, disable the loopback.
5022	security-rsa-download-success-event	Event	Equipment	Security RSA key download succeeded	Indeterminate	Security RSA key download succeeded	
5023	security-rsa-download-failed-event	Event	Equipment	Security RSA key download failed	Indeterminate	Security RSA key download failed	
5024	security-rsa-download-started-event	Event	Equipment	Security RSA key download started	Indeterminate	Security RSA key download started	
5025	security-rsa-install-success-event	Event	Equipment	Security RSA key install succeeded	Indeterminate	Security RSA key download succeeded	
5026	security-rsa-install-failed-event	Event	Equipment	Security RSA key install failed	Indeterminate	Security RSA key install failed	
5027	security-rsa-install-started-event	Event	Equipment	Security RSA key install started	Indeterminate	Security RSA key install started	
5028	remote-authentication-server-connected	Event	Equipment	Remote Authentication Server is connected	Indeterminate	Remote Authentication Server is connected	
5029	remote-authentication-server-failed-to-connect	Event	Equipment	Remote Authentication Server failed to connect	Indeterminate	Remote Authentication Server failed to connect	
5030	soam-connectivity-failure	Alarm	Processing	A connectivity failure in	Minor	Wrong link configurations.	Check the link in the traffic path

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				MA/MEG			
5031	soam-def-error-failure	Alarm	Processing	Error CCM received	Major	1. Invalid CCMs has been received. 2. MEP Id does not exist or a wrong interval was received in the CCM.	1. Check the links along the traffic path. 2. Check the configuration of the MEPs.
5032	soam-def-mac-failure	Alarm	Processing	Remote mep MAC status not up	Minor	Remote MEP's associated MAC is reporting an error status.	Check remote port interface status.
5033	soam-def-rdi-failure	Alarm	Processing	Mep Rdi received	Minor	Remote Defect indication has been received from remote MEP	1. Check the SOAM configurations. 2. Check that all local MEPs are configured correctly and enabled. 3. Check the service connectivity.
5034	soam-remote-ccm-failure	Alarm	Processing	Remote mep CCMs are not received	Major	The MEP is not receiving CCMs from at least one of the remote MEPs	1. Check all the remote SOAM configurations. 2. Check that

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							all remote MEPs are configured correctly and enabled. 3. Check the service connectivity.
5035	soam-def-xcon-failure	Alarm	Processing	Cross Connect CCM received	Major	CCM from another MAID or lower MEG level have been received	Check MA/MEG and MEP configurations
5036	ptp-stream-state-change	Event	Processing	1588-BC port state changed	Warning		
5037	ptp-bmca-update	Event	Processing	1588-BC BMCA has been updated.	Warning		
5038	ptp-output-squelch	Event	Processing	1588-BC outputs are squelched.	Warning		
5039	ptp-parent-data-set-change	Event	Processing	1588-BC parent dataset has changed.	Warning		
5040	ptp-utc-offset-change	Event	Processing	1588-BC UTC offset value changed.	Warning		
5041	ptp-leap-seconds-flag-change	Event	Processing	1588-BC one of the leap seconds flags have changed.	Warning		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5042	ptp-message-interval-change	Event	Processing	1588-BC message interval change detected.	Warning		
5043	ptp-message-rate-announce	Alarm	Processing	1588-BC announce message rate is below expected.	Major	Misconfiguration of the peer system.	Check the message rate configuration of the peer system.
5044	ptp-message-rate-sync	Alarm	Processing	1588-BC sync message rate is below expected.	Major	Misconfiguration of the peer system.	Check the message rate configuration of the peer system.
5045	ptp-message-rate-delay-req	Alarm	Processing	1588-BC delay request message rate is below expected.	Major	Misconfiguration of the peer system.	Check the message rate configuration of the peer system.
5046	ptp-no-syncE	Alarm	Processing	1588-BC performance is degraded due to loss of system clock reference.	Critical	Loss of system clock reference.	Restore the system clock synchronization to a PRC-traceable source.
5047	soam-csf-rdi-alarm	Alarm	Processing	Auto-state-propagation indication received	Major	Remote system triggered auto-state-propagation	Resolve the problem on the attached system.
5048	lACP-port-out-of-sync-alarm	Alarm	Processing	LACP port out of collecting-distributing	Major	LACP port was not selected by the aggregator or partner is out of sync	Resolve the problem on the attached system

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5049	ptp-bc-is-not-operational	Alarm	Processing	1588-BC is not operational	Major	No GM available in the network	Check the GM status
5051	admin-password-change-required-alarm	Alarm	Equipment	'Admin' user password needs to be changed	Warning	'Admin' user default password has not been changed	Change 'admin' user password
5100	mkey-mismatch	Alarm	Equipment	Master key mismatch cross over the link	Critical	Master Key was not set correctly.	Verify the Master Key.
5101	mkey-no-exist	Alarm	Equipment	No Master Key set, default value used	Warning	Crypto module has been enabled, but no Master Key has been loaded.	Set the Master Key.
5102	general-encryption-failure	Alarm	Equipment	Payload Encryption failure	Critical	1. Radio LOF on Tx/Rx direction. 2. The session key does not match across the link. 3. The AES admin setting does not match across the link.	1. Validate the MSE on both sides of the link. 2. Validate the session key on both sides of the link. 3. Validate the AES admin setting on both sides of the link.
5104	kep-initiated	Event	Equipment	Key Exchange Protocol in progress, Traffic has	Indeterminate		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				been blocked			
5105	kep-remote-initiated	Event	Equipment	Key Exchange Protocol initiated by remote side	Indeterminate		
5107	bypass-self-test-alarm	Alarm	Equipment	FIPS Bypass Self-Test failed	Critical	Disk failure	
5108	post-fail-alarm	Alarm	Equipment	Power On Self-Test Failed	Critical	System failure	1. Reboot the unit. 2. Check for faults. 3. Replace unit.
5109	main-board-non-fips-alarm	Alarm	Equipment	Main Board is not FIPS certified	Critical	Main Board used is not FIPS certified	Use a FIPS-certified TCC.
5110	radio-non-fips-alarm	Alarm	Equipment	Radio card is not FIPS certified	Major	Radio Card used is not FIPS certified	Use a FIPS-certified RMC.
5111	aes-self-test-fail-alarm	Alarm	Equipment	Radio crypto module fail	Critical	FIPS Radio Encryption Self-Test failed	Use different FIPS supported radio card
5112	hw-not-supported-alarm	Alarm	Equipment	Radio Encryption not supported	Major	No Payload Encryption Activation Key inserted	Insert suitable Activation Key and reboot the unit
5113	ipsec-pre-shared-key-alarm	Alarm	Equipment	IPSec Pre-Shared Key has the default value	Major	IPSec Pre-Shared Key was not configured	Configure the IPSec Pre-Shared Key to a different value than the default
5114	aes-admin-change-reset-	Alarm	Equipment	Chassis reset is	Warning	1. Payload Encryption	Reset the unit.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
	required-alarm			required after changing Payload Encryption Admin State		was enabled 2. Payload Encryption was disabled	
5132	security-certificate-download-success-event	Event	Security	Security certificate download succeeded	Indeterminate	Security certificate download succeeded	N/A
5133	security-certificate-download-failed-event	Event	Security	Security certificate download failed	Indeterminate	Security certificate download failed	N/A
5134	security-certificate-download-started-event	Event	Security	Security certificate download started	Indeterminate	Security certificate download started	N/A
5222	security-csr-upload-success-event	Event	Security	Security CSR upload succeeded	Indeterminate	Security csr upload succeeded	N/A
5223	security-csr-upload-failed-event	Event	Security	Security CSR upload failed	Indeterminate	Security csr upload failed	N/A
5224	security-csr-upload-started-event	Event	Security	Security CSR upload started	Indeterminate	Security csr upload started	N/A
5225	storage-integrity-invalid-alarm	Alarm	Equipment	Storage integrity check failed	Warning	Possible hardware failure or storage corruption	1. Remove the unit from the network 2. Contact customer support
20100	ext-in-alarm	Alarm	Equipment				
300	Clock-source-	Event	Equipment	Clock	Critical	1. Faulty	1. Try re-

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
07	sharing-failure-event	nt		source sharing failure		coaxial cable between master and slave RFUs. 2. Hardware failure in Master RFU. 3. Hardware failure in Slave RFU.	initiation of MIMO. If still fails: 2. Replace faulty coaxial cable and reset Master RFU. 3. Replace faulty RFU.
31000	Insufficient-conditions-for-MIMO-alarm	Alarm	Equipment	Insufficient conditions for MIMO	Critical	1. Insufficient conditions for MIMO. 2. Hardware failure. 3. In FIPS mode or IPsec mode, a mismatch between the IPsec pre-shared keys configured on the two units.	1. Make sure all cables between master and slave are connected (MIMO 4x4 only). 2. Replace faulty units and check that cables are plugged. 3. If IPsec/FIPS is enabled, verify the same pre-shared key is configured on both units.
31003	Unsuitable-hardware-for-MIMO-alarm	Alarm	Communications	Unsuitable hardware for MIMO	Critical	1. Unsuitable hardware for MIMO	Make sure both RFUs are compatible for

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						operation requirements. 2. Dual carrier RFUs (MIMO 2x2 and 4x4). 3. RFUs with MIMO bus interface (MIMO 4x4). 4. Clock source sharing capability (MIMO 4x4).	MIMO operation.
31004	Unsuitable-software-configuration-for-MIMO-alarm	Alarm	Communications	Unsuitable software configuration for MIMO	Critical	1. Not all MIMO carriers are set to same radio script or script is not compatible for MIMO. 2. Radio TX and RX frequency is not identical on all MIMO carriers. 3. XPIC or Multi radio	1. Load same MIMO compatible radio script to all MIMO carriers. 2. Set same TX and RX frequency on all MIMO carriers. 3. Disable XPIC, Multi radio and ATPC on all MIMO carriers.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						or ATPC features are enabled.	
31005	Clock-source-sharing-failure-alarm	Alarm	Equipment	Clock source sharing cable unplugged	Critical	1. Faulty coaxial cable between master and slave RFUs 2. Mate does not exist	1. Replace faulty coaxial cable and reset Master RFU. 2. Replace faulty RFU.
31006	Master-slave-configuration-mismatch-alarm	Alarm	Equipment	Master slave configuration mismatch	Critical	Incorrect master slave configuration, master/master or slave/slave	Reconfigure master slave configuration
31100	AMCC-Incompatible-radio-script-alarm	Alarm	Communications	Radio script is incompatible to AMCC	Critical	MRMC Script selected does not support AMCC Group type/subtype	Set AFR Script in both Agg1 & Agg2 carriers
31101	AMCC-Inconsistent-MRMC-Script-alarm	Alarm	Communications	Inconsistent MRMC script between members	Critical	All members of a group must be configured to the same MRMC Script	Set the members to the appropriate MRMC script
31102	AMCC-Inconsistent-radio-frequency-alarm	Alarm	Communications	Inconsistent radio frequency	Critical	Radio TX/RX frequency is not identical on all AMCC carriers	Set same radio TX/RX frequency on all AMCC carriers
31103	AMCC-Failed-To-Load-Alarm	Alarm	Communications	Agg 1 failed Bring-up procedure	Critical	Agg1 did not complete Bring-up successfully	Drop both Agg1 & Agg2 into single carrier mode (Pre-Init)
31104	AMCC-Invalid-	Alarm	Communications	Invalid	Critical	AMCC member have been set	Set AMCC

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
	ACM-Configuration-alarm			ACM configuration		to fixed profile	member to adaptive ACM profiles
31105	AMCC-Mimo-not-supported-alarm	Alarm	Equipment	AMCC/MIMO insufficient condition – configuration is not supported	Critical	1. MIMO script is not enabled on any radio member. 2. Different TX/RX frequency. 3. ATPC enabled. 4. XPIC enabled. 5. ACM mode (adaptive/Fixed) is not the same. 6. Unit Redundancy enabled. 7. Platform not supported.	1. Align MIMO script on all radio members. 2. Align same frequency on all radio members. 3. Disable ATPC. 4. Disable XPIC. 5. Align ACM mode. 6. Disable Unit Redundancy. 7. Replace unit.
31106	AMCC-Master-failure-alarm	Alarm	Equipment	AMCC insufficient condition – Master unit failure.	Critical	Master unit failure.	1. Verify Master unit power. 2. Replace hardware.
31107	AMCC-Slave-failure-alarm	Alarm	Equipment	AMCC insufficient condition –	Critical	Slave unit failure.	1. Verify Slave unit power.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
				Slave unit failure.			2. Replace hardware.
31108	AMCC-Data-Sharing-cable-disconnected-alarm	Alarm	Equipment	AMCC insufficient condition – Data sharing cable failure.	Critical	Data sharing cable failure.	1. Verify Data sharing cable connected. 2. Replace Data sharing cable.
31109	AMCC-Port-cable-disconnected-alarm	Alarm	Equipment	MIMO insufficient condition – Mate communication cable failure.	Critical	1. Mate communication cable failure. 2. In FIPS mode or IPsec mode, a mismatch between the IPsec pre-shared keys configured on the two units.	1. Verify Mate communication cable connected. 2. Replace Mate communication cable. 3. If IPsec/FIPS is enabled, verify the same pre-shared key is configured on both units.
31110	AMCC-Source-Sharing-cable-disconnected-alarm	Alarm	Equipment	MIMO insufficient condition – Source sharing cable failure.	Critical	Source sharing cable failure.	1. Verify Source sharing cable connected.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							2. Replace Source sharing cable.
3111	AMCC-Master-Slave-config-mismatch-alarm	Alarm	Equipment	MIMO insufficient condition - Master/Slave configuration mismatch	Critical	Master/Slave configuration mismatch due to: 1. Different TX/RX frequency. 2. Different MIMO script ID. 3. Different ACM mode (adaptive/Fixed).	Align Master/Slave configuration.
3112	AMCC-Remote-failure-alarm	Alarm	Equipment	AMCC insufficient condition – Remote failure	Critical	AMCC remote failure.	Handle AMCC remote failure.
3113 See Note 4	AMCC-Asd-not-supported-alarm	Alarm	Radio	AMCC/ASD insufficient condition - configuration is not supported	Critical	1. ASD script is not enabled on any radio member. 2. Different TX/RX frequency. 3. ATPC enabled. 4. XPIC enabled. 5. ACM mode is	1. Align ASD script on all radio members. 2. Align same frequency on all radio members. 3. Disable ATPC. 4. Disable XPIC. 5. Set ACM

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						not adaptive on any radio member. 6. Unit Redundancy enabled. 7. Platform not supported.	mode to adaptive on all radio members. 6. Disable Unit Redundancy. 7. Replace platform.
31114	AMCC-SD-not-supported-alarm	Alarm	Radio	AMCC/SD insufficient condition - configuration is not supported	Critical	1. SD script is not enabled on any radio member. 2. Different TX/RX frequency. 3. ATPC enabled. 4. XPIC enabled. 5. ACM mode (adaptive/Fixed) is not the same. 6. RFU not supported.	1. Align SD script on all radio members. 2. Align same frequency on all radio members. 3. Disable ATPC. 4. Disable XPIC. 5. Align ACM mode. 6. Replace RFU.
31115	AMCC-Data-Sharing-failure-alarm	alarm	Radio	AMCC insufficient condition - Units alignment failure.	Critical	Units alignment failure.	1. Verify Source sharing cable connected.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							2. Replace Source sharing cable. 3. Verify Data sharing cable connected. 4. Replace Data sharing cable. Verify using correct SFPs.
31118	AMCC-XPIC-not-supported-alarm	alarm	Radio	XPIC configuration is not supported	Critical	1. XPIC MRMC script is not configured 2. Different TX/RX frequency. 3. ACM mode (adaptive/fixed) is not configured the same.	1. Set XPIC MRMC script 2. Align same frequency on all radio members. 3. Align same ACM mode.
31119	AMCC-XPIC-remote-failure-alarm	alarm	Radio	XPIC configuration failure in remote	Warning	XPIC remote failure	Handle XPIC remote failure
31120	AMCC-XPIC-mate-communication-failure-alarm	Alarm	Communications	XPIC communication with mate unit is interrupted	Warning	1. The mate unit is unreachable. 2. In FIPS or	1. Check the cable between the two units.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
						IPSec mode, possible mismatch between the IPSec pre-shared keys configured on the two units.	2. In FIPS or IPSec mode, make sure that the same IPSec pre-shared key is configured on the two units.
31121	AMCC-Radio-unit-failure-alarm	Alarm	Communications	AMCC insufficient condition - Radio unit failure.	Critical	Radio Unit failure.	1. Verify radio unit power. 2. Replace HW.
31122 See Note 5	AMCC-Asd-split-not-supported-alarm	Alarm	Equipment	AMCC/ASD insufficient condition - configuration is not supported	Critical	1. ASD script is not enabled on any radio member. 2. Different TX/RX frequency. 3. XPIC enabled. 4. ACM mode is not adaptive on any radio member. 5. Platform not supported.	1. Align ASD script on all radio members. 2. Align same frequency on all radio members. 3. Disable XPIC. 4. Set ACM mode to adaptive on all radio members. 5. Disable the adaptive power on all radio members.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
							6. Replace platform.
32000	unit-mgr-undervoltage-alarm	Alarm	Equipment	Under voltage	Major	System Power Voltage lower than allowed.	
32001	unit-mgr-overvoltage-alarm	Alarm	Equipment	Over voltage	Major	System Power Voltage higher than allowed.	
32002	unit-mgr-extremeTemperature-alarm	Alarm	Equipment	System Temperature not in allowed range.	Major		
32003	unit-mgr-unit-reset-event	Event	Management	Unit is resetting.	Warning	The unit is about to perform a system reset	Wait until the reset cycle has ended and the system is up and running
32004	unit-mgr-power-up-event	Event	Equipment	Unit has performed power up	Warning		
32005	line-redundancy-state-is-changed-evt-log	Event	Equipment	Unit state is changed	Major		
32006	reset-system-entity	Event	Equipment	Unit is resetting due to configuration change	Warning	The user performed a configuration change that causes the system to be reset.	Wait until the reset cycle has ended and the system is up and running.
32007	reset-system-entity	Event	Equipment	Unit is resetting due to user command	Warning	The user performed a command to reset the unit.	Wait until the reset cycle has ended and the system is up and running.
330	anti-theft-	Event	Management	Anti-Theft	Indetermini		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
01	enabled-event	nt	nt	Procedures have been enabled	nate		
33002	anti-theft-temporary-disabled-event	Event	Management	Anti-Theft Procedures have been temporary disabled	Indeterminate		
33003	anti-theft-sanction-timer-countdown-alarm	Alarm	Management	Anti-Theft Sanction Mode 24 hours window has been triggered	Critical	Watchdog timer countdown	Return the equipment to the network
33004	anti-theft-sanction-mode-entered-alarm	Alarm	Management	Anti-Theft Sanction Mode is Active	Critical	Equipment has been stolen	Return the equipment to the network
37704	iptables-rollback-timer-expired-event	Event	Equipment	ACL rollback performed	Warning		



Note:

1. This alarm is only relevant for PTP 820 all-outdoor products.
2. This alarm is only relevant for PTP 850EX and PTP 850CX. For those products, changes in scheduling priority profiles are not applied until the next device reboot. This alarm informs the user that a change in a scheduling priority profile has been made and will not be applied until the next reboot.
3. This alarm is only relevant for PTP 820 split-mount products.
4. This alarm is only relevant for PTP 820 all-outdoor products.
5. This alarm is only relevant for PTP 820N and PTP 820A. For ASD with PTP 820C and PTP 820C-HP, the equivalent alarm is 31113.

Cambium Networks

Cambium Networks delivers wireless communications that work for businesses, communities, and cities worldwide. Millions of our radios are deployed to connect people, places, and things with a unified wireless fabric that spans multiple standards and frequencies of fixed wireless and Wi-Fi, all managed centrally via the cloud. Our multi-gigabit wireless fabric offers a compelling value proposition over traditional fiber and alternative wireless solutions. We work with our Cambium certified Connected Partners to deliver purpose built networks for service provider, enterprise, industrial, and government connectivity solutions in urban, suburban, and rural environments, with wireless that just works.

Support website	https://support.cambiumnetworks.com
Support enquiries	
Technical training	https://learning.cambiumnetworks.com/learn
Main website	https://www.cambiumnetworks.com
Sales enquiries	solutions@cambiumnetworks.com
Warranty	https://www.cambiumnetworks.com/support/standard-warranty/
Telephone number list	https://www.cambiumnetworks.com/contact-us/
User Guides	https://www.cambiumnetworks.com/guides
Address	Cambium Networks Limited, Unit B2, Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP United Kingdom



www.cambiumnetworks.com

Cambium Networks and the stylized circular logo are trademarks of Cambium Networks, Ltd. All other trademarks are the property of their respective owners.

Copyright © 2026 Cambium Networks, Ltd. All rights reserved.