Cambium Networks™

User Guide

PTP 850E

System Release 11.5

Accuracy

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

Copyrights

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

Restrictions

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

License Agreements

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

High Risk Materials

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

Contents

List of Figures

List of Tables

About This User Guide

This document explains how to configure and operate PTP 850 devices. This document applies to System relase 11.3. For a full description of feature limitations per release, refer to the Release Notes for the System relase you are using.

What You Should Know

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

Target Audience

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

Related Documents

- PTP 850C Technical Description
- PTP 850E Technical Description
- PTP 850S Technical Description
- PTP 850C Installation Guide
- PTP 850E Installation Guide
- PTP 850S Installation Guide
- PTP 850 MIB Reference
- Release Notes for System relase 11.3, PTP 850 Products

This guide contains the following Chapters:

Contacting Cambium Networks

Support website:	https://support.cambiumnetworks.com
Main website:	http://www.cambiumnetworks.com
Sales enquiries:	solutions@cambiumnetworks.com
Support enquiries:	https://support.cambiumnetworks.com
Repair enquiries	https://support.cambiumnetworks.com
Telephone number list:	http://www.cambiumnetworks.com/support/contact-support
Address:	Cambium Networks Limited, Unit B2, Linhay Business Park, Eastern Road Ashburton, United Kingdom, TQ13 7UP

Purpose

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

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

Cross references

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

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

Feedback

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

Problems and warranty

Reporting problems

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

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

Repair and service

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

Hardware warranty

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

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

⚠	**Caution** Using non-Cambium parts for repair could damage the equipment or void warranty. Contact Cambium for service and repair instructions. Portions of Cambium equipment may be damaged from exposure to electrostatic discharge. Use precautions to prevent damage.

Security advice

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

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

Warnings, cautions, and notes

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

Warnings

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

Warning

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

Cautions

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

Caution

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

Notes

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

Note

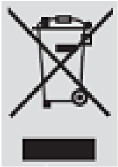
Note text.

Caring for the environment

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

In EU countries

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



Disposal of Cambium equipment

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

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

Disposal of surplus packaging

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

In non-EU countries

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

Chapter 1: Introduction

This section includes:

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

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

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

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

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

PTP 850C Overview

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

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

16 Gbps switching capacity, channel spacing of up to 224 MHz[1], and a wide range of modulations, from BPSK to 4096 QAM with ACM. These and other advanced capabilities are combined in PTP 850C with the full range of Cambium Networks's MultiCore technologies to produce an all-outdoor product that can be used throughout the microwave network, from small cells to massive aggregation sites.

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

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

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

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

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

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

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

PTP 850S Overview

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

PTP 850S operates over channels of 14 to 224 MHz[3], with modulations of BPSK to 4096 QAM, enabling it to provide capacity of up to 2 Gbps over a single carrier.

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

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

PTP 850E Overview

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

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

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

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

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

[4] Dualband configurations are planned for future release.

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

System Overview

Configuration Tips

This section describes common issues and how to avoid them.

Ethernet Port configuration

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

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

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

For instructions, see Configuring Ethernet Interfaces.

SyncE Interface Configuration

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

In-Band Management

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

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

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

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

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

Software Upgrade

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

Configuration Management and Backup Restoration

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

PTP 850E Overview

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

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

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

PoE Injector Overview

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

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

Note

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

Two models of the PoE Injector are available:

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

N000082L164APTP 820C INDOOR AC POE INJECTOR, 90W

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

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

The Web-Based Element Management System

This section includes:

Introduction to the Web EMS

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

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

Fault Monitoring – Enables you to view active alarms.

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

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

Security Configuration – Enables you to configure security features.

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

The Web EMS opens to a page that summarizes the key unit parameters. The next page, when scrolling down the Web EMS main menu, summarizes the key radio parameters. See Unit Summary Page and Radio Summary Page.

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

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

Note

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

Web EMS Page Layout

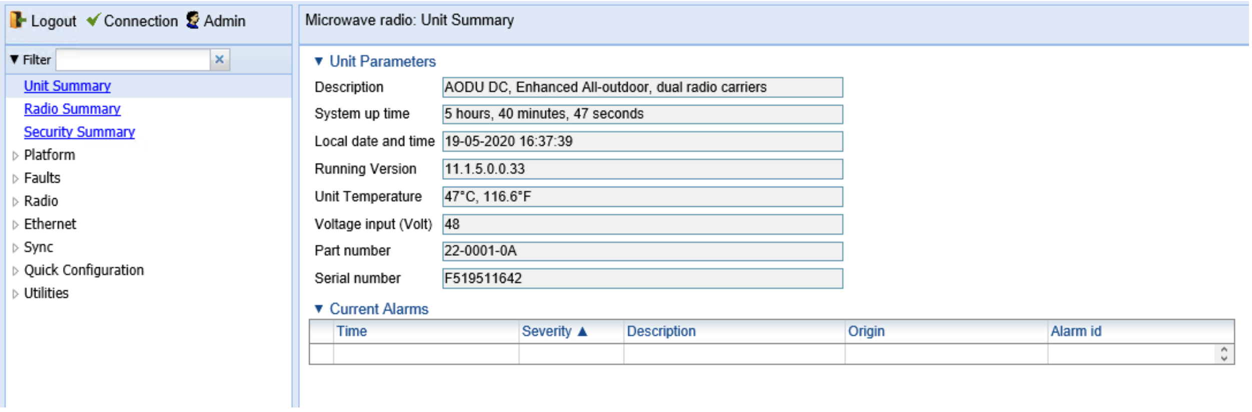
Each Web EMS page includes the following sections:

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

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

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

Figure 1 Main Web EMS Page PTP 850C



Microwave radio: Unit Summary

▼ Unit Parameters

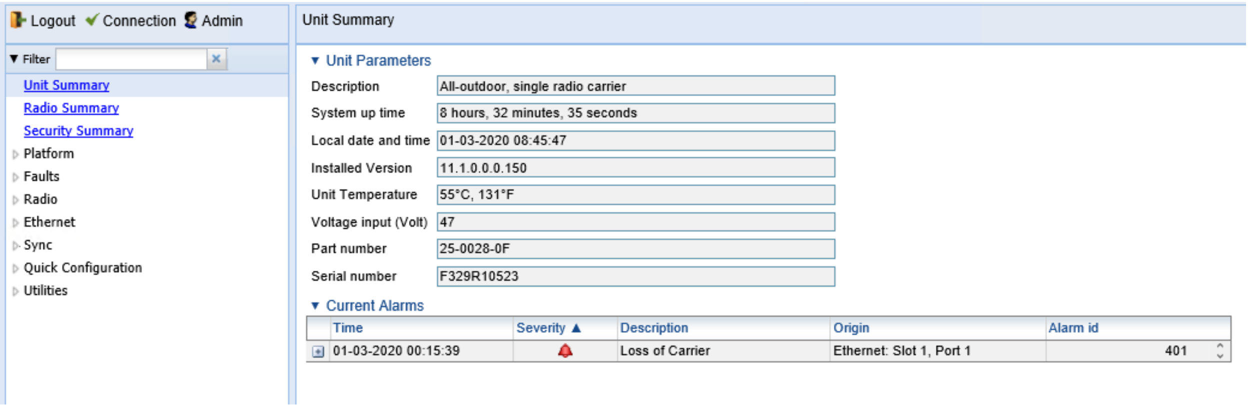
Description	AODU DC, Enhanced All-outdoor, dual radio carriers
System up time	5 hours, 40 minutes, 47 seconds
Local date and time	19-05-2020 16:37:39
Running Version	11.1.5.0.0.33
Unit Temperature	47°C, 116.6°F
Voltage input (Volt)	48
Part number	22-0001-0A
Serial number	F519511642

▼ Current Alarms

Time	Severity ▲	Description	Origin	Alarm id

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

Figure 2 Main Web EMS Page – PTP 850S



Unit Summary

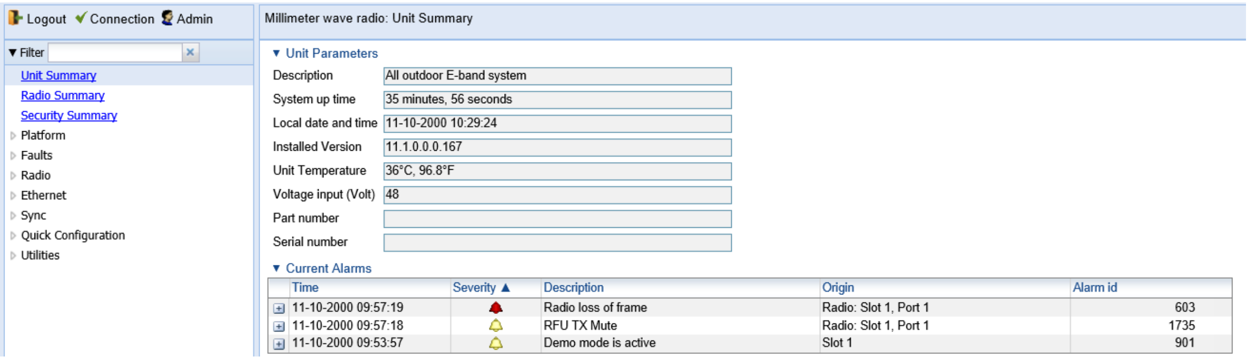
▼ Unit Parameters

Description	All-outdoor, single radio carrier
System up time	8 hours, 32 minutes, 35 seconds
Local date and time	01-03-2020 08:45:47
Installed Version	11.1.0.0.0.150
Unit Temperature	55°C, 131°F
Voltage input (Volt)	47
Part number	25-0028-0F
Serial number	F329R10523

▼ Current Alarms

Time	Severity ▲	Description	Origin	Alarm id
01-03-2020 00:15:39	🔔	Loss of Carrier	Ethernet: Slot 1, Port 1	401

Figure 3 Main Web EMS Page – PTP 850E



Millimeter wave radio: Unit Summary

▼ Unit Parameters

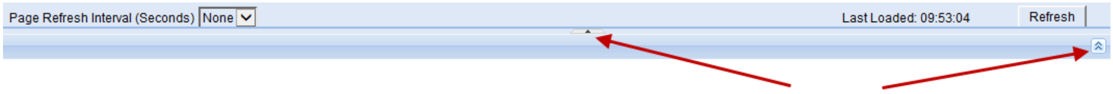
Description	All outdoor E-band system
System up time	35 minutes, 56 seconds
Local date and time	11-10-2000 10:29:24
Installed Version	11.1.0.0.0.167
Unit Temperature	36°C, 96.8°F
Voltage input (Volt)	48
Part number	
Serial number	

▼ Current Alarms

Time	Severity ▲	Description	Origin	Alarm id
11-10-2000 09:57:19	🔔	Radio loss of frame	Radio: Slot 1, Port 1	603
11-10-2000 09:57:18	🔔	RFU TX Mute	Radio: Slot 1, Port 1	1735
11-10-2000 09:53:57	🔔	Demo mode is active	Slot 1	901

Front Panel Representation

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

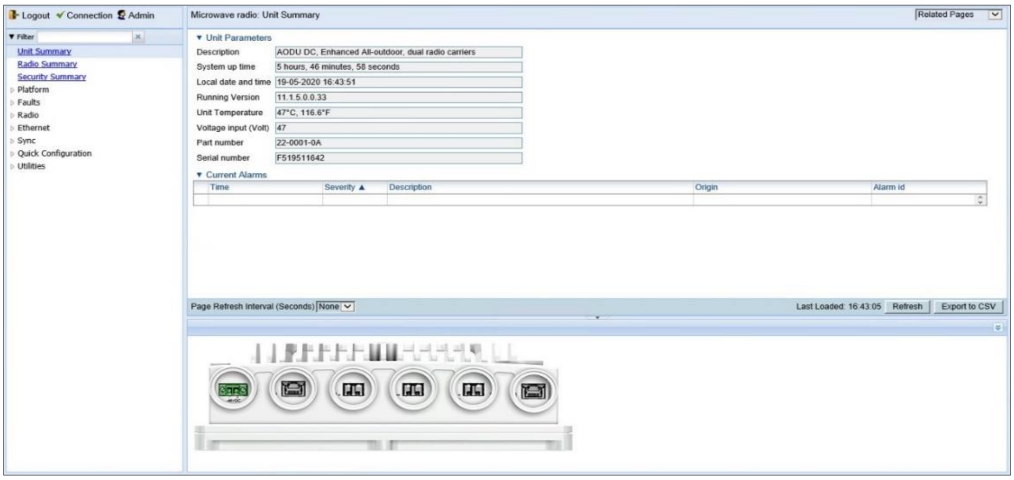


Page Refresh Interval (Seconds) None

Last Loaded: 09:53:04

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

Figure 4 Displaying a Representation of the Front Panel



Microwave radio: Unit Summary

Unit Parameters

Description AODU DC, Enhanced All-outdoor, dual radio carriers

System up time 5 hours, 46 minutes, 58 seconds

Local date and time 19-05-2020 16:43:51

Running Version 11.1.5.0.0.33

Unit Temperature 47°C, 116.6°F

Voltage input (Volt) 47

Part number 22-0001-0A

Serial number F519511642

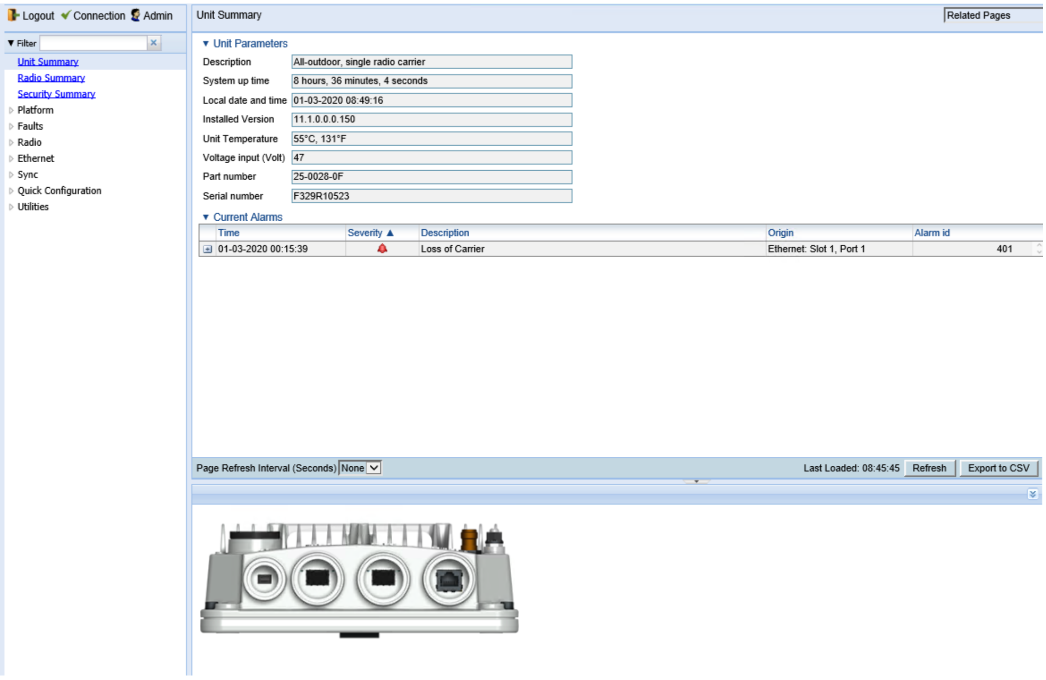
Current Alarms

Time	Severity ▲	Description	Origin	Alarm id

Page Refresh Interval (Seconds) None

Last Loaded: 16:43:05

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



Unit Summary

Unit Parameters

Description All-outdoor, single radio carrier

System up time 8 hours, 36 minutes, 4 seconds

Local date and time 01-03-2020 08:49:16

Installed Version 11.1.0.0.0.150

Unit Temperature 55°C, 131°F

Voltage input (Volt) 47

Part number 25-0028-0F

Serial number F329R10523

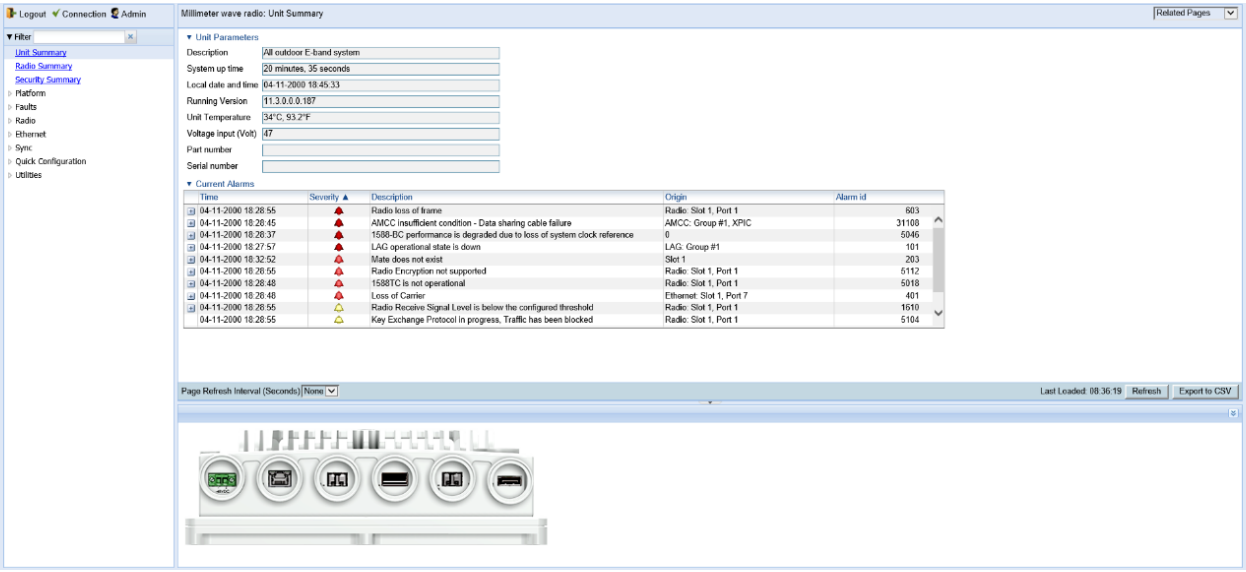
Current Alarms

Time	Severity ▲	Description	Origin	Alarm id
01-03-2020 00:15:39	▲	Loss of Carrier	Ethernet: Slot 1, Port 1	401

Page Refresh Interval (Seconds) None

Last Loaded: 08:45:45

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



Millimeter wave radio: Unit Summary

Unit Parameters

Description	All outdoor E-band system
System up time	20 minutes, 35 seconds
Local date and time	04-11-2000 18:45:33
Running Version	11.3.0.0.0.187
Unit Temperature	34°C, 93.2°F
Voltage input (Volt)	47
Part number	
Serial number	

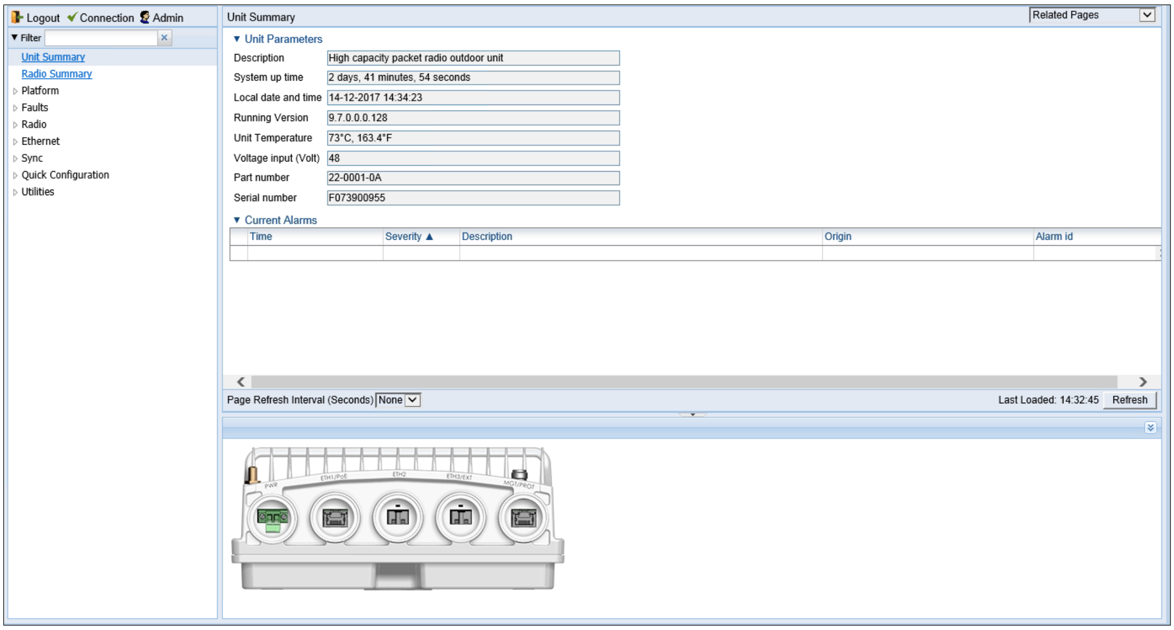
Current Alarms

Time	Severity ▲	Description	Origin	Alarm id
04-11-2000 18:28:55	🔔	Radio loss of frame	Radio: Slot 1, Port 1	603
04-11-2000 18:28:45	🔔	AMCC insufficient condition - Data sharing cable failure	AMCC: Group #1, XPIC	31108
04-11-2000 18:28:37	🔔	1588-BC performance is degraded due to loss of system clock reference	0	5046
04-11-2000 18:27:57	🔔	LAG operational state is down	LAG: Group #1	101
04-11-2000 18:32:52	🔔	Mate does not exist	Slot 1	203
04-11-2000 18:28:55	🔔	Radio Encryption not supported	Radio: Slot 1, Port 1	5112
04-11-2000 18:28:48	🔔	1588TC is not operational	Radio: Slot 1, Port 1	5018
04-11-2000 18:28:48	🔔	Loss of Carrier	Ethernet: Slot 1, Port 7	401
04-11-2000 18:28:55	🔔	Radio Receive Signal Level is below the configured threshold	Radio: Slot 1, Port 1	1610
04-11-2000 18:28:55	🔔	Key Exchange Protocol in progress, Traffic has been blocked	Radio: Slot 1, Port 1	5104

Page Refresh Interval (Seconds) None

Last Loaded: 08:36:19

Figure 7 Main Web EMS Page with Representation of Front Panel



Unit Summary

Unit Parameters

Description	High capacity packet radio outdoor unit
System up time	2 days, 41 minutes, 54 seconds
Local date and time	14-12-2017 14:34:23
Running Version	9.7.0.0.0.128
Unit Temperature	73°C, 163.4°F
Voltage input (Volt)	48
Part number	22-0001-0A
Serial number	F073900955

Current Alarms

Time	Severity ▲	Description	Origin	Alarm id

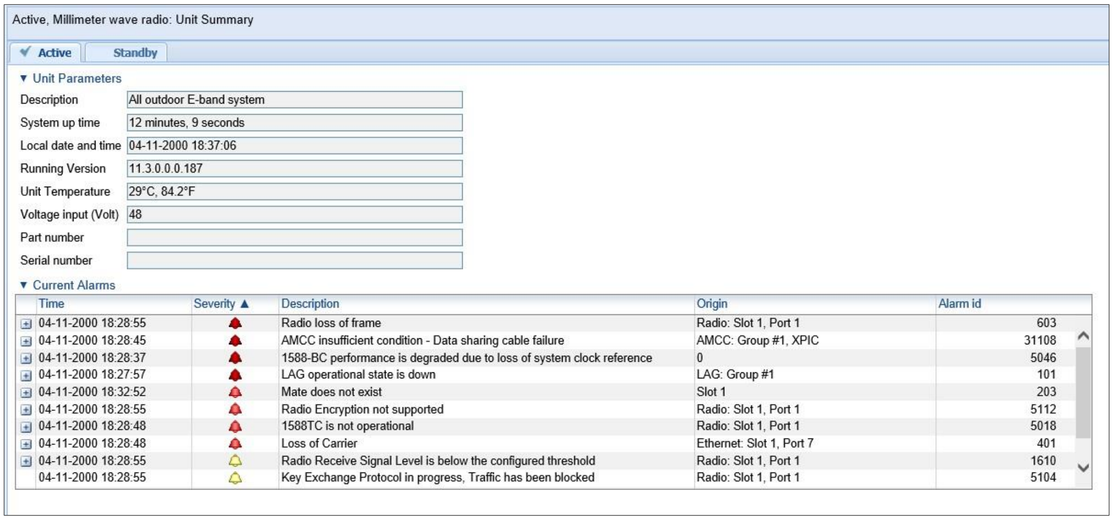
Page Refresh Interval (Seconds) None

Last Loaded: 14:32:45

Active and Standby Tabs

When HSB unit protection is enabled, two tabs appear on the top of the main section. These tabs are labeled *Active* and *Standby* and enable you to configure the Active and Standby units separately if necessary. The title above the main section indicates whether you are working with the Active or Standby unit. For details on configuring HSB unit protection, see *Configuring 1+1 HSB Unit Protection*.

Figure 8 Main Web EMS Page with Active and Standby Tabs



Active, Millimeter wave radio: Unit Summary

▼ Unit Parameters

Description	All outdoor E-band system
System up time	12 minutes, 9 seconds
Local date and time	04-11-2000 18:37:06
Running Version	11.3.0.0.0.187
Unit Temperature	29°C, 84.2°F
Voltage input (Volt)	48
Part number	
Serial number	

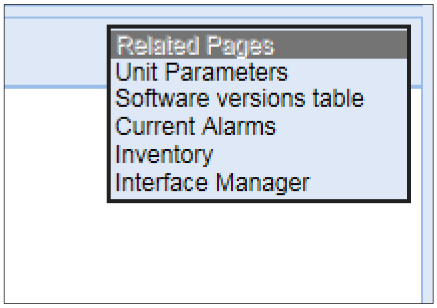
▼ Current Alarms

Time	Severity ▲	Description	Origin	Alarm id
04-11-2000 18:28:55	🔔	Radio loss of frame	Radio: Slot 1, Port 1	603
04-11-2000 18:28:45	🔔	AMCC insufficient condition - Data sharing cable failure	AMCC: Group #1, XPIC	31108
04-11-2000 18:28:37	🔔	1588-BC performance is degraded due to loss of system clock reference	0	5046
04-11-2000 18:27:57	🔔	LAG operational state is down	LAG: Group #1	101
04-11-2000 18:32:52	🔔	Mate does not exist	Slot 1	203
04-11-2000 18:28:55	🔔	Radio Encryption not supported	Radio: Slot 1, Port 1	5112
04-11-2000 18:28:48	🔔	1588TC is not operational	Radio: Slot 1, Port 1	5018
04-11-2000 18:28:48	🔔	Loss of Carrier	Ethernet: Slot 1, Port 7	401
04-11-2000 18:28:55	🔔	Radio Receive Signal Level is below the configured threshold	Radio: Slot 1, Port 1	1610
04-11-2000 18:28:55	🔔	Key Exchange Protocol in progress, Traffic has been blocked	Radio: Slot 1, Port 1	5104

Related Pages Drop-Down List

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

Figure 9 Related Pages Drop-Down List



Export to CSV Option

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

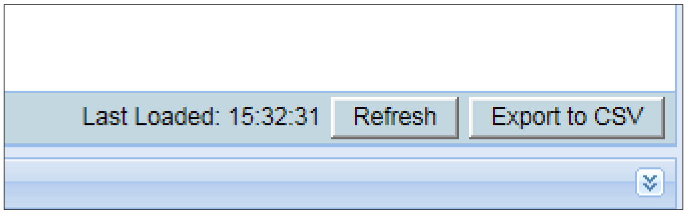
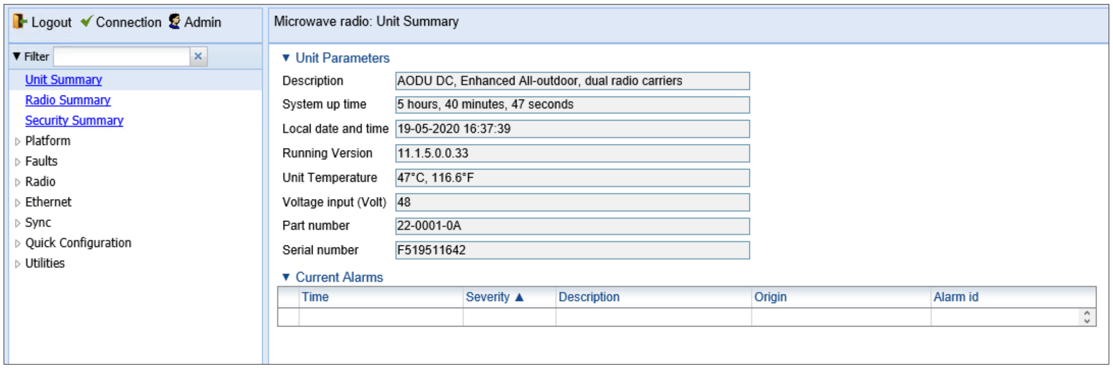


Figure 10 Related Pages Drop-Down List

Unit Summary Page

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

Figure 11 Unit Summary Page- PTP 850C



Microwave radio: Unit Summary

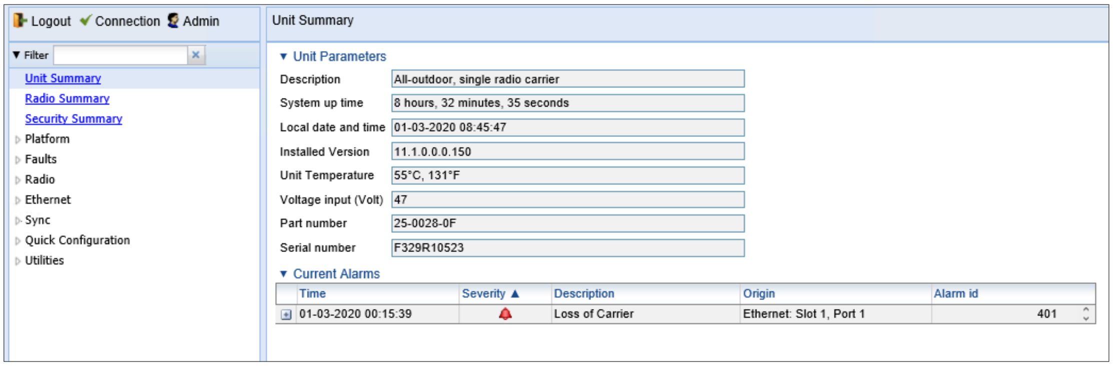
▼ Unit Parameters

Description	AODU DC, Enhanced All-outdoor, dual radio carriers
System up time	5 hours, 40 minutes, 47 seconds
Local date and time	19-05-2020 16:37:39
Running Version	11.1.5.0.0.33
Unit Temperature	47°C, 116.6°F
Voltage input (Volt)	48
Part number	22-0001-0A
Serial number	F519511642

▼ Current Alarms

Time	Severity ▲	Description	Origin	Alarm id

Figure 12 Unit Summary Page – PTP 850S



Unit Summary

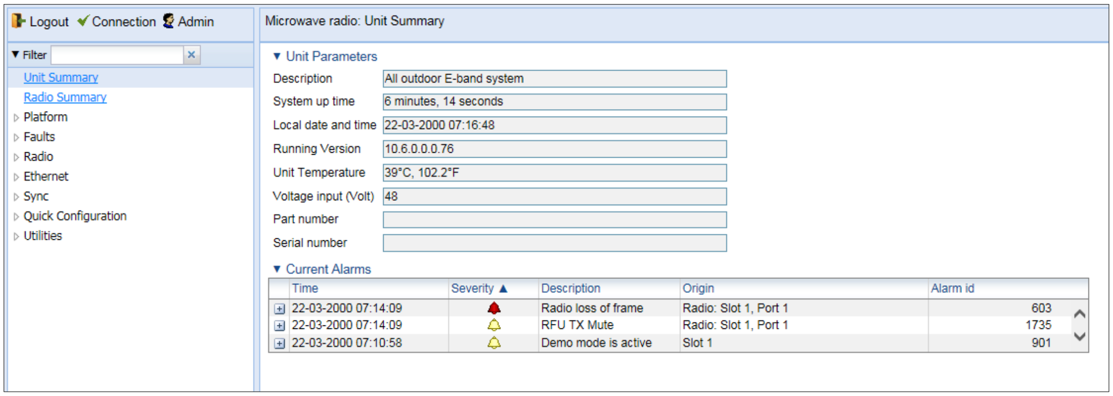
▼ Unit Parameters

Description	All-outdoor, single radio carrier
System up time	8 hours, 32 minutes, 35 seconds
Local date and time	01-03-2020 08:45:47
Installed Version	11.1.0.0.0.150
Unit Temperature	55°C, 131°F
Voltage input (Volt)	47
Part number	25-0028-0F
Serial number	F329R10523

▼ Current Alarms

Time	Severity ▲	Description	Origin	Alarm id
01-03-2020 00:15:39	🔔	Loss of Carrier	Ethernet: Slot 1, Port 1	401

Figure 13 Unit Summary Page – PTP 850E



Microwave radio: Unit Summary

▼ Unit Parameters

Description	All outdoor E-band system
System up time	6 minutes, 14 seconds
Local date and time	22-03-2000 07:16:48
Running Version	10.6.0.0.0.76
Unit Temperature	39°C, 102.2°F
Voltage input (Volt)	48
Part number	
Serial number	

▼ Current Alarms

Time	Severity ▲	Description	Origin	Alarm id
22-03-2000 07:14:09	🔔	Radio loss of frame	Radio: Slot 1, Port 1	603
22-03-2000 07:14:09	🔔	RFU TX Mute	Radio: Slot 1, Port 1	1735
22-03-2000 07:10:58	🔔	Demo mode is active	Slot 1	901

The Unit Summary page includes:

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

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

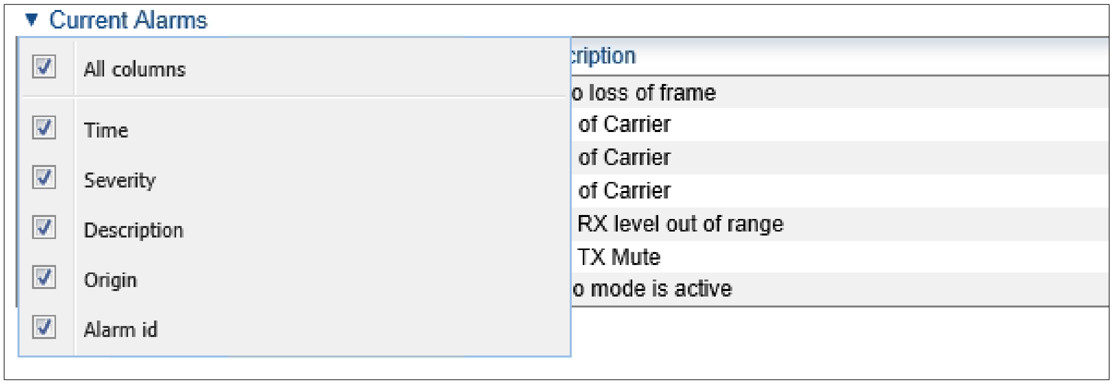
The Unit Summary page can be customized to include only specific columns and tables. This enables you to hide information you do not need in order to focus on the information that is most relevant.

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

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

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

Figure 14 Unit Summary Page – Customizing Columns



▼ Current Alarms

☑ All columns

☑ Time

☑ Severity

☑ Description

☑ Origin

☑ Alarm id

:ription

o loss of frame

of Carrier

of Carrier

of Carrier

RX level out of range

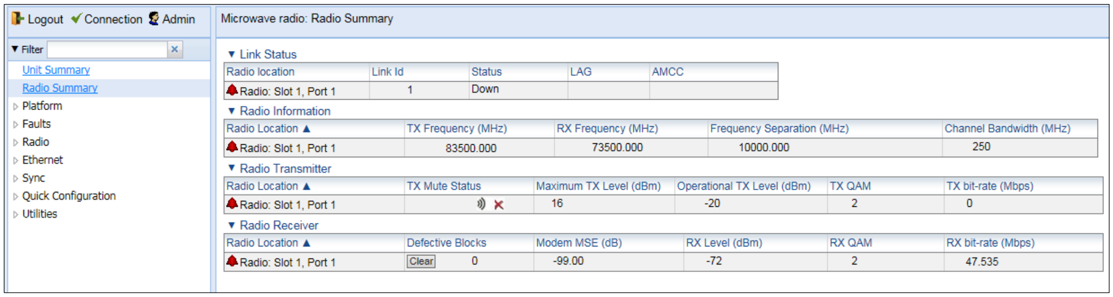
TX Mute

o mode is active

Radio Summary Page

The Radio Summary page gathers the key link and radio parameters on a single page for quick viewing. To display the Radio Summary page, select **Radio Summary** from the Web EMS main menu.

Figure 15 Radio Summary Page- PTP 850C



Microwave radio: Radio Summary

▼ Link Status

Radio location	Link Id	Status	LAG	AMCC
Radio: Slot 1, Port 1	1	Down		

▼ Radio Information

Radio Location ▲	TX Frequency (MHz)	RX Frequency (MHz)	Frequency Separation (MHz)	Channel Bandwidth (MHz)
Radio: Slot 1, Port 1	83500.000	73500.000	10000.000	250

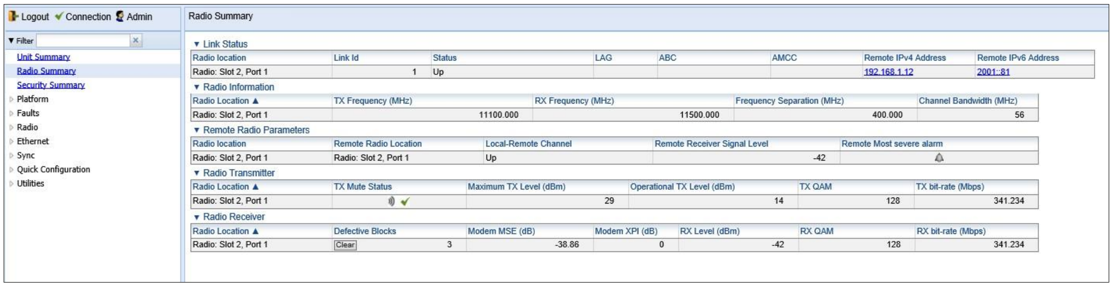
▼ Radio Transmitter

Radio Location ▲	TX Mute Status	Maximum TX Level (dBm)	Operational TX Level (dBm)	TX QAM	TX bit-rate (Mbps)
Radio: Slot 1, Port 1	✗	16	-20	2	0

▼ Radio Receiver

Radio Location ▲	Defective Blocks	Modem MSE (dB)	RX Level (dBm)	RX QAM	RX bit-rate (Mbps)
Radio: Slot 1, Port 1	Clear 0	-99.00	-72	2	47.535

Figure 16 Radio Summary Page – PTP 850S



Radio Summary

▼ Link Status

Radio location	Link Id	Status	LAG	ABC	AMCC	Remote IPv4 Address	Remote IPv6 Address
Radio: Slot 2, Port 1	1	Up				192.168.1.12	2001::81

▼ Radio Information

Radio Location ▲	TX Frequency (MHz)	RX Frequency (MHz)	Frequency Separation (MHz)	Channel Bandwidth (MHz)
Radio: Slot 2, Port 1	11100.000	11500.000	400.000	56

▼ Remote Radio Parameters

Radio location	Remote Radio Location	Local-Remote Channel	Remote Receiver Signal Level	Remote Most severe alarm
Radio: Slot 2, Port 1	Radio: Slot 2, Port 1	Up	-42	

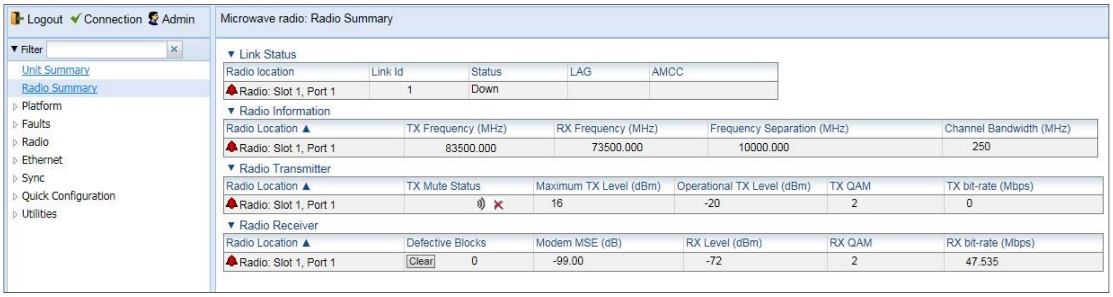
▼ Radio Transmitter

Radio Location ▲	TX Mute Status	Maximum TX Level (dBm)	Operational TX Level (dBm)	TX QAM	TX bit-rate (Mbps)
Radio: Slot 2, Port 1	✓	29	14	128	341.234

▼ Radio Receiver

Radio Location ▲	Defective Blocks	Modem MSE (dB)	Modem XPI (dB)	RX Level (dBm)	RX QAM	RX bit-rate (Mbps)
Radio: Slot 2, Port 1	Clear 3	-38.86	0	-42	128	341.234

Figure 17 Radio Summary Page – PTP 850E



Microwave radio: Radio Summary

▼ Link Status

Radio location	Link Id	Status	LAG	AMCC
Radio: Slot 1, Port 1	1	Down		

▼ Radio Information

Radio Location ▲	TX Frequency (MHz)	RX Frequency (MHz)	Frequency Separation (MHz)	Channel Bandwidth (MHz)
Radio: Slot 1, Port 1	83500.000	73500.000	10000.000	250

▼ Radio Transmitter

Radio Location ▲	TX Mute Status	Maximum TX Level (dBm)	Operational TX Level (dBm)	TX QAM	TX bit-rate (Mbps)
Radio: Slot 1, Port 1	✗	16	-20	2	0

▼ Radio Receiver

Radio Location ▲	Defective Blocks	Modem MSE (dB)	RX Level (dBm)	RX QAM	RX bit-rate (Mbps)
Radio: Slot 1, Port 1	Clear 0	-99.00	-72	2	47.535

The Radio Summary page includes:

Link Status – Link status per radio carrier, including whether or not the link is Up, groups to which the link is assigned (such as LAG, XPIC, protection, and/or Multi-Carrier ABC), and the IP address (both IPv4 and IPv6) of the remote carrier. For additional information, see **Error! Reference source n ot found.**.

Radio Information – The TX and RX frequencies, frequency separation, and channel bandwidth on which the link is operating. For additional information, see **Error! Reference source not found.**.

Remote Radio Parameters – Key information about the status of the remote carrier. For additional information, see Configuring the Remote Radio Parameters.

Radio Transmitter – Mute status, maximum and operational TX level, modulation, and bit rate. For additional information, see **Error! Reference source not found.**.

Radio Receiver – Receiver PMs and statistics, including defective blocks, modem MSE, and RX level, modulation, and bit rate. For additional information, see **Error! Reference source not found.** a nd Configuring the Radio (MRMC) Script(s).

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

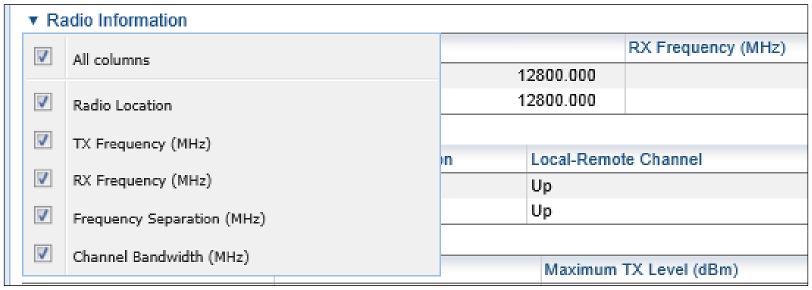
To hide a specific section of the Radio Summary page, click the section title. To display a section that has been hidden, click the section title again.

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

Note

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

Figure 18 Radio Summary Page- Customizing Columns



▼ Radio Information

- ☑ All columns
- ☑ Radio Location
- ☑ TX Frequency (MHz)
- ☑ RX Frequency (MHz)
- ☑ Frequency Separation (MHz)
- ☑ Channel Bandwidth (MHz)

	RX Frequency (MHz)
12800.000	
12800.000	

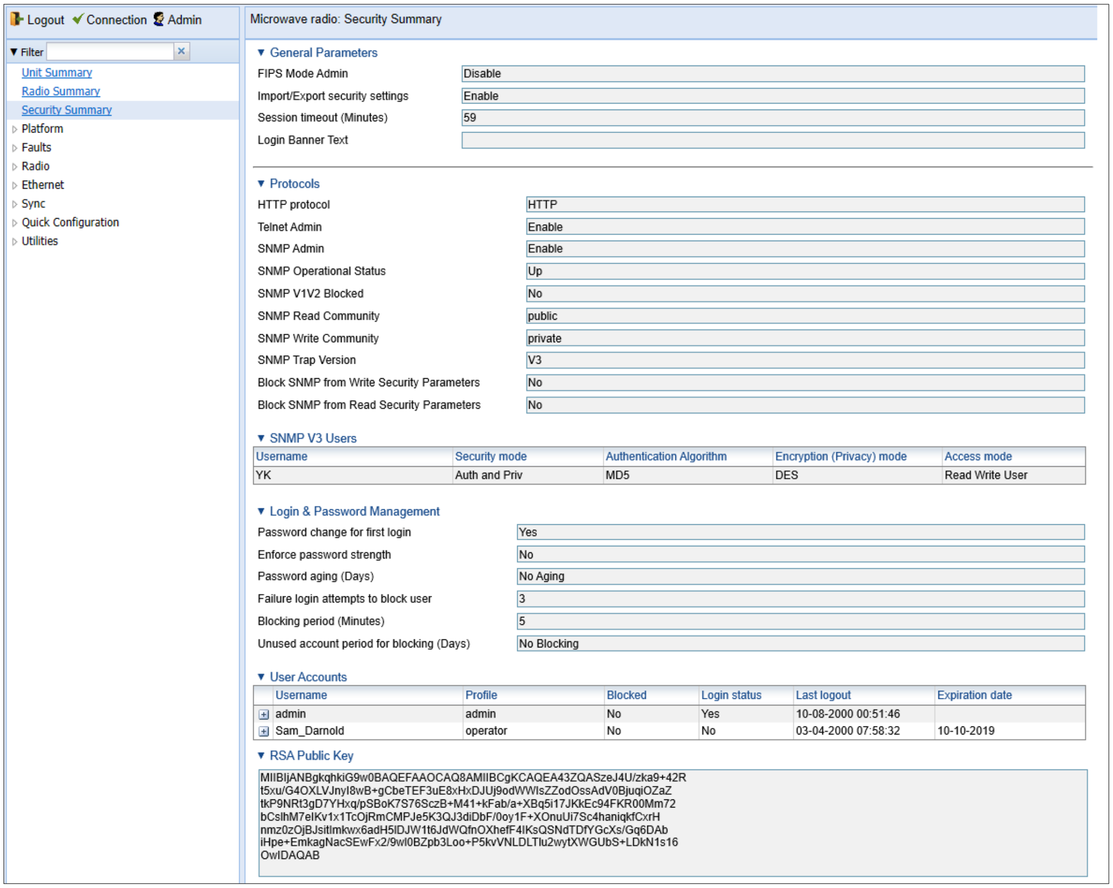
n	Local-Remote Channel
	Up
	Up

Maximum TX Level (dBm)

Security Summary Page

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

Figure 19 Security summary page



Microwave radio: Security Summary

▼ General Parameters

FIPS Mode Admin	Disable
Import/Export security settings	Enable
Session timeout (Minutes)	59
Login Banner Text	

▼ Protocols

HTTP protocol	HTTP
Telnet Admin	Enable
SNMP Admin	Enable
SNMP Operational Status	Up
SNMP V1V2 Blocked	No
SNMP Read Community	public
SNMP Write Community	private
SNMP Trap Version	V3
Block SNMP from Write Security Parameters	No
Block SNMP from Read Security Parameters	No

▼ SNMP V3 Users

Username	Security mode	Authentication Algorithm	Encryption (Privacy) mode	Access mode
YK	Auth and Priv	MD5	DES	Read Write User

▼ Login & Password Management

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

▼ User Accounts

	Username	Profile	Blocked	Login status	Last logout	Expiration date
⊞	admin	admin	No	Yes	10-08-2000 00:51:46	
⊞	Sam_Darnold	operator	No	No	03-04-2000 07:58:32	10-10-2019

▼ RSA Public Key

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA43ZQASzeJ4U/zka9+42R
t5xu/G4OXLVJnyI8wB+gCbeTEF3uE8xHxDJUj9odWWIsZZodOssAdV0BjuqiOZaZ
tkP9NRt3gD7YHxq/pSBoK7S76SczB+M41+kFab/a+XBq5i17JKkEc94FKR00Mm72
bCslhM7elKv1x1TcOjRmCMPJe5K3QJ3diDbF/0oy1F+XOnuUi7Sc4haniqkfCxrH
nmz0zOjBJsitlmkwx6adH5lDJW1t6JdWQfnOXhefF4lKsQSNdTDfYGcXs/Gq6DAb
iHpe+EmkagNacSEwFx2/9wl0BZpb3Loo+P5kvVNLDLTlu2wytXWGUbS+LDkN1s16
OwIDAQAB

The Security Summary page includes:

General Parameters – Includes the following fields:

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

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

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

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

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

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

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

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

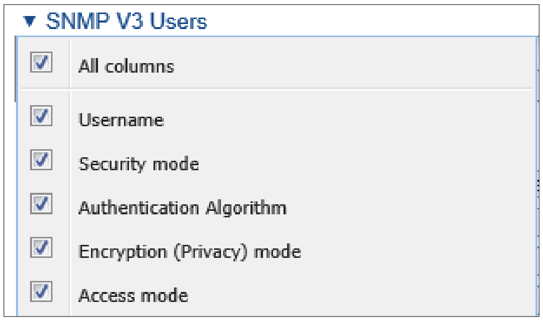
To hide a specific section of the Radio Summary page, click the section title. To display a section that has been hidden, click the section title again.

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

Note

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

Figure 20 Security Summary Page – Customizing Columns



▼ SNMP V3 Users

☑ All columns

☑ Username

☑ Security mode

☑ Authentication Algorithm

☑ Encryption (Privacy) mode

☑ Access mode

Reference Guide to Web EMS Menu Structure

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

Note

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

Table 1 Web EMS Menu Hierarchy – Platform Menu

Sub-Menus	For Further Information
Shelf Management > Chassis Configuration	Performing a Hard (Cold) Reset Setting the Unit to the Factory Default Configuration
Shelf Management > Unit Redundancy	Configuring 1+1 HSB Unit Protection
Interfaces > Interface Manager	Enabling the Interfaces (Interface Manager)
Interfaces > SFP	Planned for future release.
Management > Unit Parameters	Configuring Unit Parameters
Management > NTP Configuration	Configuring NTP
Management > Time Services	Setting the Time and Date (Optional)
Management > Inventory	Displaying Unit Inventory
Management > Unit Info	Uploading Unit Info
Management > Login Banner	Defining a Login Banner
Management > Networking > Local	Configuring In-Band Management Changing the Management IP Address Defining the IP Protocol Version for Initiating Communications
Management > Networking > Remote	Configuring the Remote Unit's IP Address
Management > SNMP > SNMP Parameters	Configuring SNMP
Management > SNMP > Trap Managers	Configuring Trap Managers
Management > SNMP > V3 Users	Configuring SNMP
Software > Versions	Viewing Current Software Versions
Software > Download & Install	Downloading and Installing Software Configuring a Timed Installation

Sub-Menus	For Further Information
Configuration > Timer Parameters	Planned for future release.
Configuration > Backup Files	Viewing Current Backup Files
Configuration > Configuration Management	Backing Up and Restoring Configurations
Activation Key > Activation Key Configuration	Configuring the Activation Key
Activation Key > Activation Key Overview	Displaying a List of Activation-Key-Enabled Features
Security > General > Configuration	Planned for future release.
Security > General > Security Log Upload	Uploading the Security Log
Security > General > Configuration Log Upload	The File transfer progress field displays the progress of any current security log upload operation. Uploading the Configuration Log
Security > X.509 Certificate > CSR	Configuring X.509 CSR Certificates
Security > X.509 Certificate > Download & Install	Configuring X.509 CSR Certificates
Security > Access Control > General	Configuring the General Access Control Parameters
Security > Access Control > User Profiles	Configuring User Profiles
Security > Access Control > User Accounts	Configuring Users
Security > Access Control > Password Management	Configuring the Password Security Parameters
Security > Access Control > Change Password	Changing Your Password
Security > Access Control > Radius > Radius Configuration	Planned for future release.
Security > Access Control > Radius > Radius Users	Planned for future release.
Security > Protocols Control	Configuring the Session Timeout Blocking Telnet Access
PM & Statistics > SFP	Planned for future release.
PM & Statistics > Voltage	Configuring Voltage Alarm Thresholds and Displaying Voltage PMs

Table 2 Web EMS Menu Hierarchy – Faults Menu

Sub-Menus	For Further Information
Current alarms	*Viewing Current Alarms*
Alarm Statistics	*Viewing Alarm Statistics*
Event Log	***Error! Reference source not found.***
Alarm Configuration	***Error! Reference source not found.***
Voltage Alarm Configuration	*Configuring Voltage Alarm Thresholds*

Table 3 Web EMS Menu Hierarchy – Radio Menu

Sub-Menus	For Further Information
Radio Parameters	**Error! Reference source not found.**
Frequency Scanner	Running the Frequency Scanner
Remote Radio Parameters	**Error! Reference source not found.**
Radio BER Thresholds	**Error! Reference source not found.**
Ethernet Interface > Counters	***Error! Reference source not found.***
MRMC > Symmetrical Scripts > ETSI	**Error! Reference source not found.**
MRMC > Symmetrical Scripts > FCC	**Error! Reference source not found.**
MRMC > MRMC Status	**Error! Reference source not found.**
PM & Statistics > Counters	Displaying and Clearing Defective Block Counters
PM & Statistics > Signal Level	Displaying Signal Level PMs
PM & Statistics > Aggregate	**Error! Reference source not found.**
PM & Statistics > MSE	Displaying MSE PMs
PM & Statistics > MRMC	Displaying MRMC PMs
PM & Statistics > Traffic > Capacity/Throughput	***Error! Reference source not found.***
PM & Statistics > Traffic > Utilization	***Error! Reference source not found.***
Diagnostics > Loopback	Performing Radio Loopback
Groups > Multi Carrier ABC	*Configuring* Multiband

Table 4 Web EMS Menu Hierarchy – Ethernet Menu

Sub-Menus	For Further Information
General Configuration	*Setting the MRU Size and the S-VLAN Ethertype*
Services	*Configuring Ethernet Service(s)*
Interfaces > Physical Interfaces	*Configuring Ethernet Interfaces*
Interfaces > Logical Interfaces	*Configuring Ingress Path Classification on a Logical Interface* *Assigning Policers to Interfaces* *Configuring the Ingress and Egress Byte Compensation* *Assigning WRED Profiles to Queues* *Assigning a Queue Shaper Profile to a Queue* *Assigning a Priority Profile to an Interface* *Assigning a WFQ Profile to an Interface* *Performing Ethernet Loopback*
Interfaces > ASP & LLF	Configuring Automatic State Propagation and Link Loss Forwarding
PM & Statistics > RMON	*RMON Statistics*
PM & Statistics > Port TX	*Port TX Statistics*
PM & Statistics > Port RX	*Port RX Statistics*
PM & Statistics > Egress CoS Statistics	*Egress CoS Statistics*
PM & Statistics > Egress CoS PM > Configuration	*Configuring and Displaying Queue-Level PMs*
PM & Statistics > Egress CoS PM > Egress CoS PM	*Configuring and Displaying Queue-Level PMs*
QoS > Classification > 802.1Q	*Modifying the C-VLAN 802.1Q UP and CFI Bit Classification Table*
QoS > Classification > 802.1AD	*Modifying the S-VLAN 802.1 UP and DEI Bit Classification Table*
QoS > Classification > DSCP	*Modifying the DSCP Classification Table*
QoS > Classification > MPLS	*Modifying the MPLS EXP Bit Classification Table*
QoS > Policer > Policer Profile	*Configuring Policer Profiles*
QoS > Marking > 802.1Q	*Modifying the 802.1Q Marking Table*
QoS > Marking > 802.1AD	*Modifying the 802.1AD Marking Table*
QoS > WRED > WRED Profile	*Configuring WRED*

Sub-Menus	For Further Information
QoS > Shaper > Queue Profiles	*Configuring Queue Shaper Profiles*
QoS > Scheduler > Priority Profiles	*Configuring Priority Profiles*
QoS > Scheduler > WFQ Profiles	*Configuring WFQ Profiles*
Protocols > Bandwidth Notification	*Planned for future release.*
Protocols > LLDP > Remote Management	*Planned for future release.*
Protocols > LLDP > Advanced > Configuration > Parameters	*Planned for future release.*
Protocols > LLDP > Advanced > Configuration > Port Configuration	*Planned for future release.*
Protocols > LLDP > Advanced > Configuration > Destination Address	*Planned for future release.*
Protocols > LLDP > Advanced > Configuration > Management TLV	*Planned for future release.*
Protocols > LLDP > Advanced > Remote System > Management	*Planned for future release.*
Protocols > LLDP > Advanced > Remote System > Remote Table	*Planned for future release.*
Protocols > LLDP > Advanced > Local System > Parameters	*Planned for future release.*
Protocols > LLDP > Advanced > Local System > Port	*Planned for future release.*
Protocols > LLDP > Advanced > Local System > Management	*Planned for future release.*
Protocols > LLDP > Advanced > Statistic > General	*Planned for future release.*
Protocols > LLDP > Advanced > Statistic > Port TX	*Planned for future release.*
Protocols > LLDP > Advanced > Statistic > Port RX	*Planned for future release.*
Protocols > SOAM > MD	*Configuring Service OAM (SOAM) Fault Management (FM)*
Protocols > SOAM > MA/MEG	*Configuring Service OAM (SOAM) Fault Management (FM)*
Protocols > SOAM > MEP	*Configuring Service OAM (SOAM) Fault Management (FM)*
Protocols > LACP > Aggregation	*Planned for future release.*
Protocols > LACP > Port > Status	*Planned for future release.*

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

Table 5 Web EMS Menu Hierarchy – Sync Menu

Sub-Menus	For Further Information
SyncE Regenerator	*Planned for future release.*
Sync Source	*Configuring the Sync Source*
Outgoing Clock	*Configuring the Outgoing Clock and SSM Messages*
1588 > General Configuration	***Error! Reference source not found.***
1588 > Transparent Clock	***Error! Reference source not found.***
1588 > Boundary Clock > Clock Parameters > Default	*Planned for future release.*
1588 > Boundary Clock > Clock Parameters > Advanced	*Planned for future release.*
1588 > Boundary Clock > Port Parameters	*Planned for future release.*
1588 > Boundary Clock > Port Statistics	*Planned for future release.*

Table 6 Web EMS Menu Hierarchy – Quick Configuration Menu

Sub-Menus	For Further Information
From Release Plan	*Planned for future release.*
Platform Setup	*Performing Quick Platform Setup*
Security > General Parameters	*Quick Security Configuration – General Parameters Page*
Security > Protocols	*Quick Security Configuration – Protocols Page*
Security > Access Control	*Quick Security Configuration – Access Control Page*
Security > RSA Key & Certificate	*Quick Security Configuration – RSA Key & Certificate Page*
PIPE > Single Carrier > 1 + 0	*Configuring a 1+0 Link Using the Quick Configuration Wizard*
PIPE > Multi Carrier ABC > Multiband	*Configuring a Multiband (Enhanced Multi-Carrier ABC) Link Using the Quick Configuration Wizard*

Table 7 Web EMS Menu Hierarchy – Utilities Menu

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

Chapter 2: Getting Started

This section includes:

- Assigning IP Addresses in the Network
- Establishing a Connection
- Logging on
- Changing Your Password
- Applying a Pre-Defined Configuration File
- Performing Quick Platform Setup
- Configuring In-Band Management
- Changing the Management IP Address
- Configuring the Activation Key
- Setting the Time and Date (Optional)
- Enabling the Interfaces (Interface Manager)
- Configuring the Radio (MRMC) Script(s)
- Running the Frequency Scanner
- Configuring the Radio Parameters
- Creating Service(s) for Traffic

Assigning IP Addresses in the Network

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

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

IP address: 192.168.1.1

Subnet mask: 255.255.255.0

Caution

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

Establishing a Connection

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

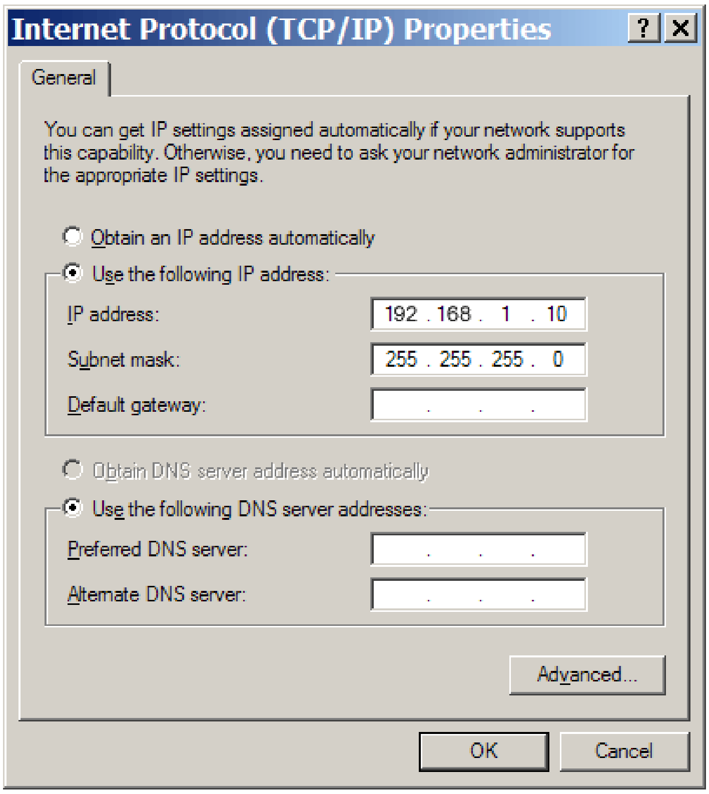
PC Setup

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

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

1. Select **Control Panel > All Control Panel Items > Network and Sharing Center**.
2. Click **Change the adapter settings.**
3. Select **Local Area Connection > Properties > Internet Protocol Version 4 (TCP/IP)**, and set the following parameters:
   - IP address: 192.168.1.10
   - Subnet mask 255.255.255.0
   - No default gateway
4. Click **OK** to apply the settings.

Figure 21 Internet Protocol Properties Window



Internet Protocol (TCP/IP) Properties

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

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 1 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

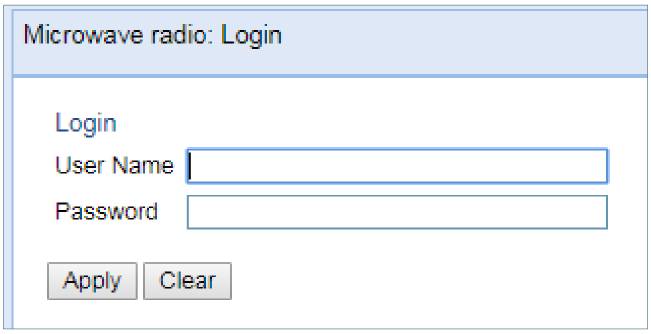
○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

Logging on

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

Figure 22 Login Page



Microwave radio: Login

Login

User Name

Password

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

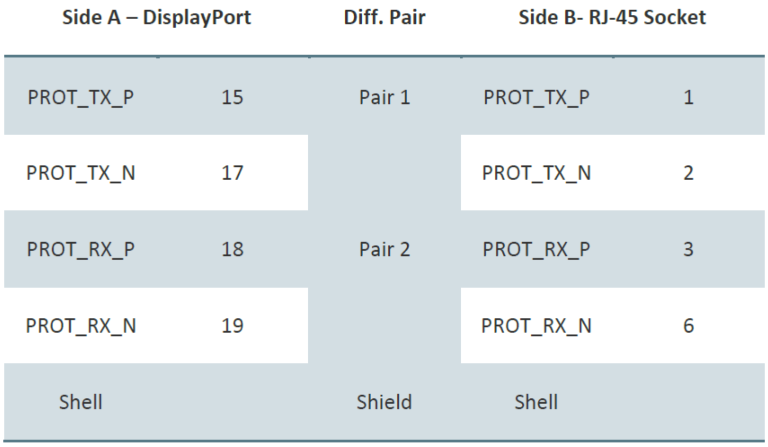
Logging in Without Knowing the IP Address

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

Table 9: Cable for Direct CPU Connection

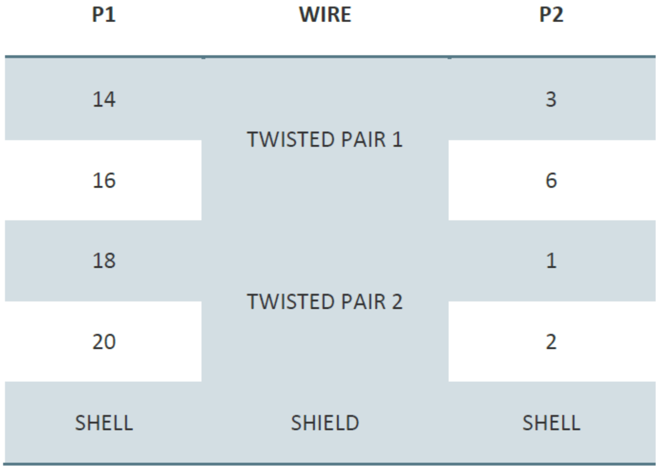
Product	Cable Marketing Model	Cable Description
PTP 850C	SPL-ETH-CBL	CABLE,RJ45 TO 2XRJ45F, 0.54M,CAT-5E,FOR ETH
PTP 850E	DP to RJ45 MNG CABLE	CABLE,DP TO RJ45F,0.2M,FOR FIELD DEBUG
PTP 850S	PTP 820_Mini-MNG-CBL_ESP	CABLE,MiniDP TO RJ45F,0.2M,FOR FIELD DEBUG. ESP

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



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

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



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

To log in using this cable:

1 Disconnect the management cable from the PTP 850E.

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

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

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

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

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

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

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

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

7 Click **Apply**.

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

Changing Your Password

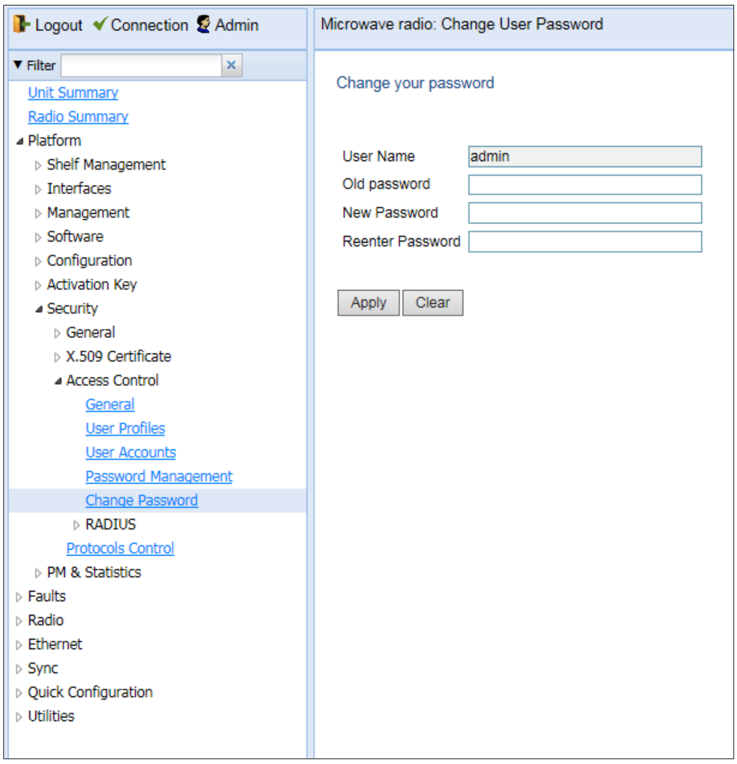
It is recommended to change your default Admin password as soon as you have logged into the system.

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

To change your password:

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

Figure 23 Change User Password Page



User Name: admin
Old password:
New Password:
Reenter Password:

2. In the **Old password** field, enter the current password. For example, upon initial login, enter the default password (**admin**).
3. In the **New password** field, enter a new password. If **Enforce Password Strength** is activated (see Configuring the Password Security Parameters), the password must meet the following criteria:
   - Password length must be at least eight characters.
   - Password must include characters of at least three of the following character types: lower case letters, upper case letters, digits, and special characters. For purposes of meeting this requirement, upper case letters at the beginning of the password and digits at the end of the password are not counted.
   - A password cannot be repeated within five changes of the password.
4. Click **Apply**.

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

Applying a Pre-Defined Configuration File

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

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

Platform parameters:

- ETSI to ANSI conversion
- General unit parameters, such as unit name, location, and contact person
- Activation Key (or Demo mode) configuration
- IP configuration (IPv4 and IPv6)
- NTP configuration
- Basic SNMP Parameters (Enable/Disable, Read and Write Communities)
- Time services configuration

Interface configuration:

- Radio
- Ethernet
- Radio protection

Advanced radio configuration

- XPIC

Services configuration

- Management
- Point-to-Point
- Multipoint

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

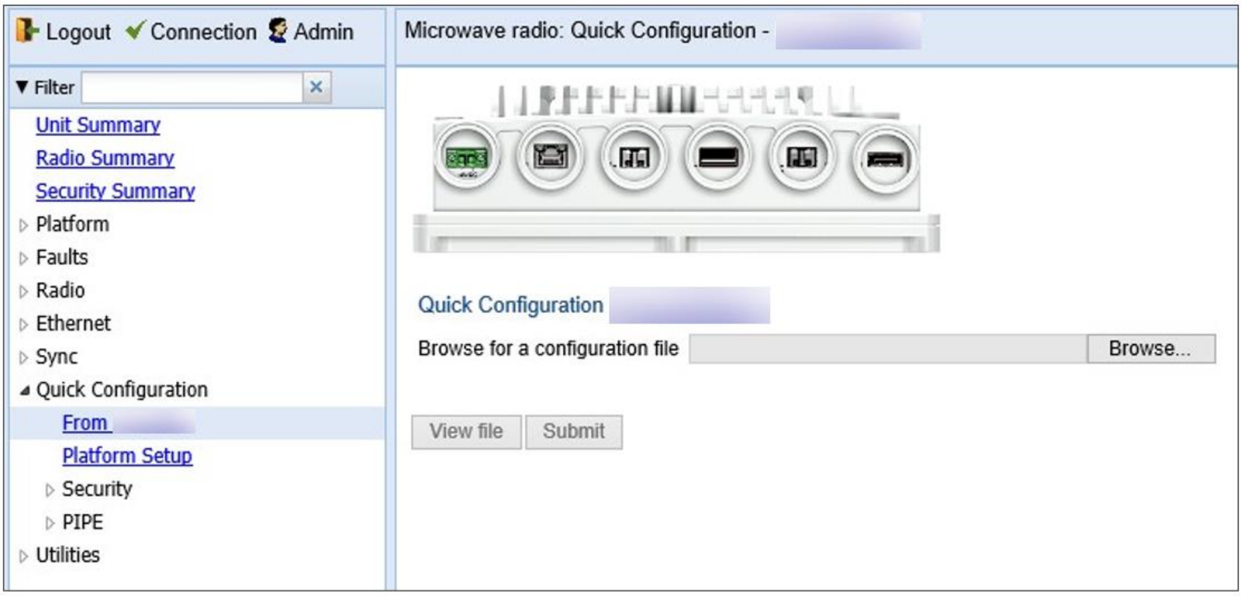
The pre-defined configuration file must be compatible with the System release version the PTP 850E device is running. Configuration files must also be compatible with the type of device. For example, a configuration file created for PTP 820E cannot be applied to an PTP 850E device.

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

To apply a pre-defined configuration file:

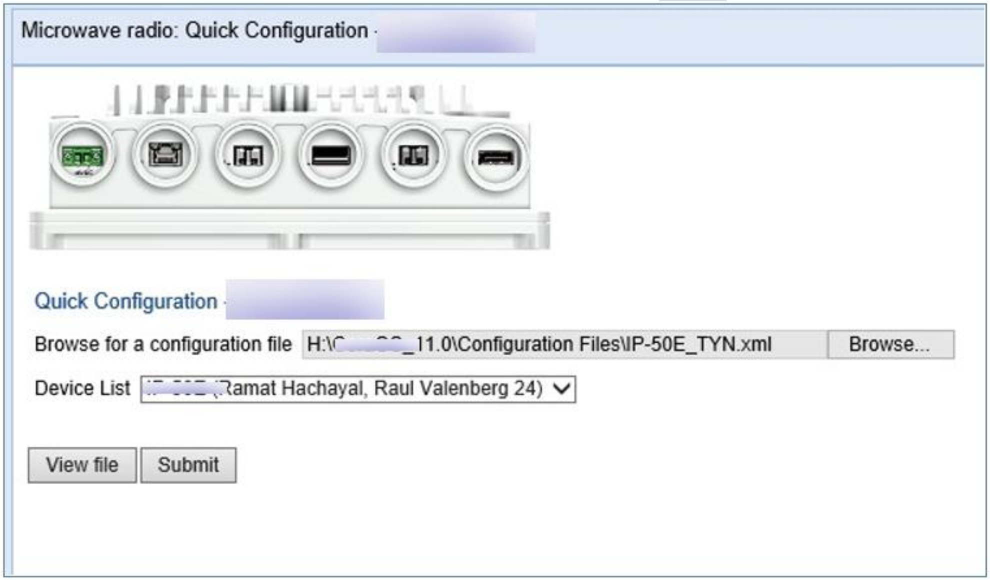
1 Select **Quick Configuration > From File**. The Quick Configuration – From File page opens.

Figure 24 Quick Configuration – From File Page



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

Figure 25 Quick Configuration – From File Page – Configuration File Loaded



Browse for a configuration file H:\C[redacted]_11.0\Configuration Files\IP-50E_TYN.xml

Device List [redacted] Ramat Hachayal, Raul Valenberg 24)

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

Note
Although the configuration file may contain parameters for multiple

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

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

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

When the configuration is complete, the unit reboots.

Note

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

Performing Quick Platform Setup

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

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

IPv4 Address, Subnet Mask, and Default Gateway

NTP Enable/Disable

Demo Activation Key Enable/Disable

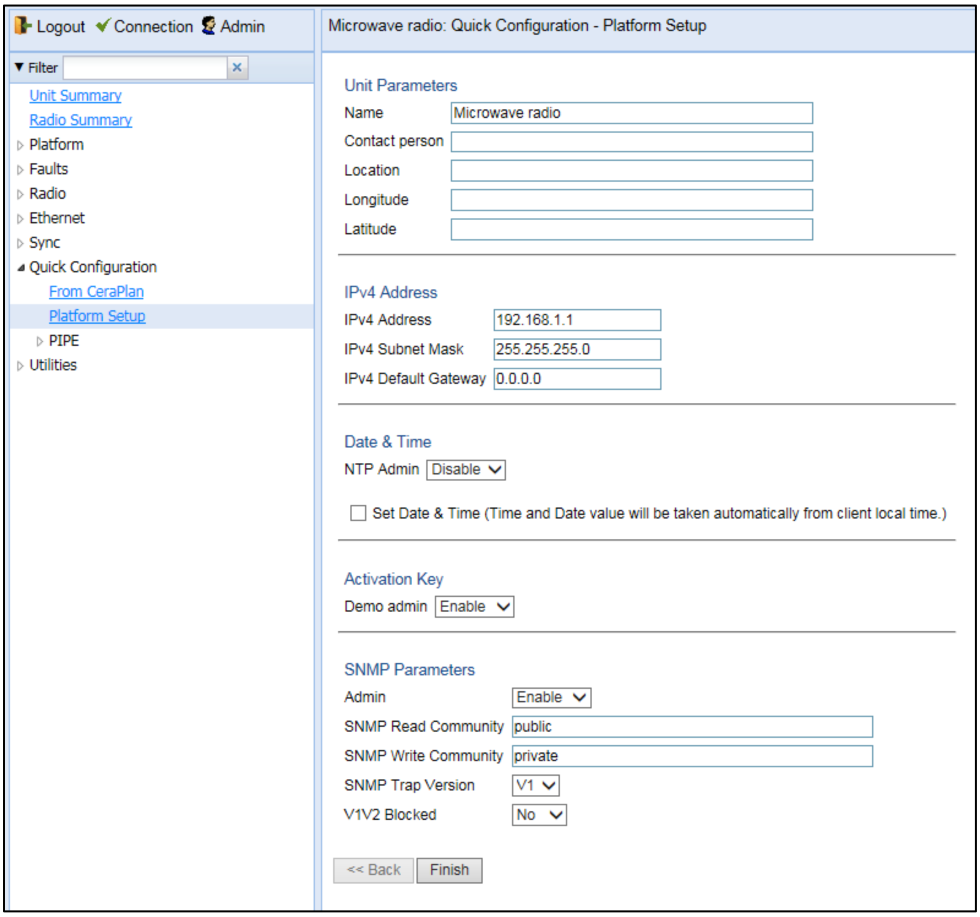
SNMP Parameters

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

To use the Platform Setup page:

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

Figure 26 Quick Configuration – Platform Setup Page



Microwave radio: Quick Configuration - Platform Setup

Unit Parameters

Name: Microwave radio
Contact person:
Location:
Longitude:
Latitude:

IPv4 Address

IPv4 Address: 192.168.1.1
IPv4 Subnet Mask: 255.255.255.0
IPv4 Default Gateway: 0.0.0.0

Date & Time

NTP Admin: Disable

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

Activation Key

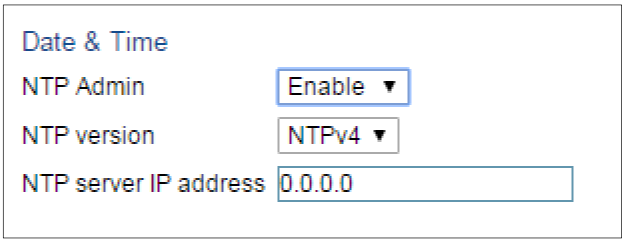
Demo admin: Enable

SNMP Parameters

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

1. The Unit Parameters section is optional. For details on each field, see Configuring Unit Parameters.

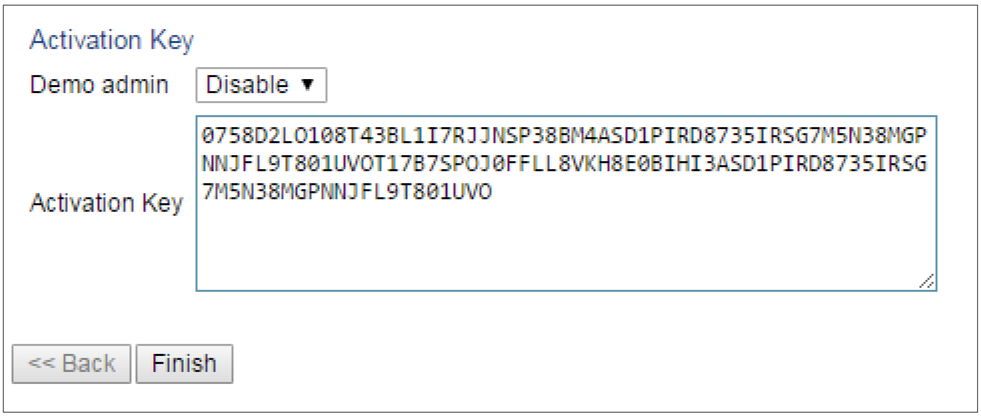
2. In the IPv4 Address section, configure the unit's management IP address, subnet mask, and, optionally, a default gateway. If you want to use an IPv6 address, see Changing the Management IP Address.
3. In the Date & Time section, you can enable Network Time Protocol (NTP). NTP distributes Coordinated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



Date & Time

NTP Admin	Enable ▼
NTP version	NTPv4 ▼
NTP server IP address	0.0.0.0

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



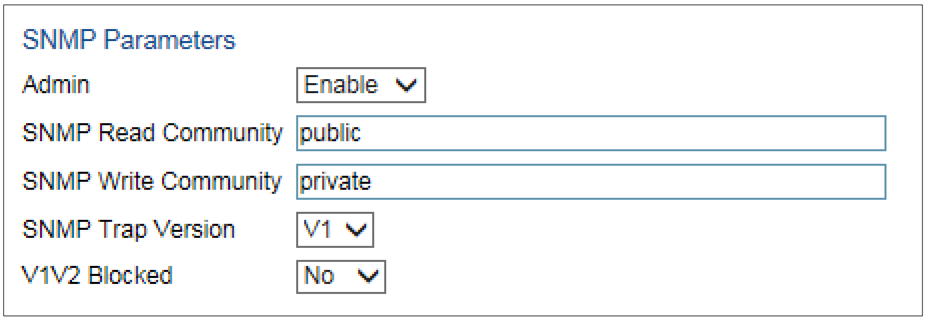
Activation Key

Demo admin: Disable ▼

Activation Key:

```
0758D2LO108T43BL1I7RJJNSP38BM4ASD1PIRD8735IRSG7M5N38MGP
NNJFL9T801UVOT17B7SPOJ0FFLL8VKH8E0BIHI3ASD1PIRD8735IRSG
7M5N38MGPNNJFL9T801UVO
```

5. In the SNMP Parameters section, you can set whether to enable or disable SNMP monitoring in the Admin field, and set the SNMP Read Community and SNMP Write Community. You can also configure the **SNMP Trap Version**. If you select **V3**, you can select **Yes** in the **V1V2 Blocked** field to block SNMPv1 and SNMPv2 access so that only SNMPv3 access will be enabled. For a full explanation of SNMP parameters, see Configuring SNMP.

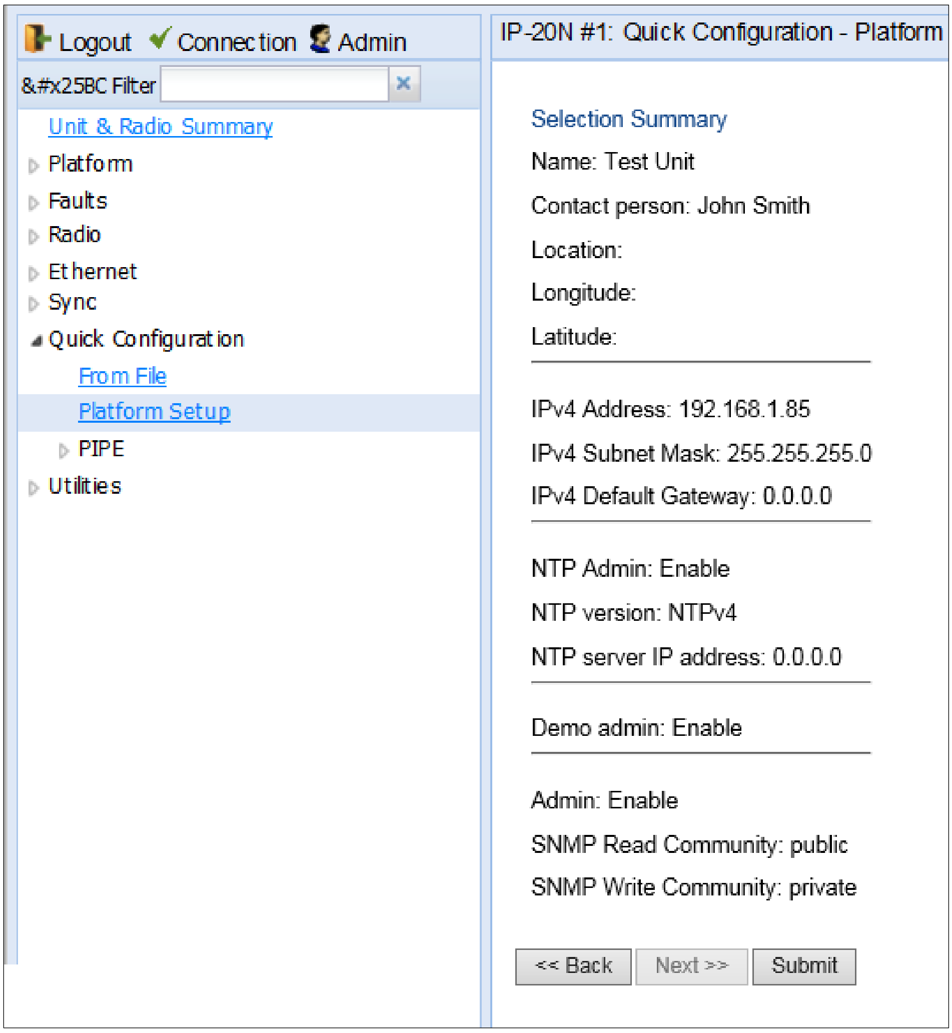


SNMP Parameters

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

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

Figure 27 Quick Configuration– Platform Setup Summary Page



Selection Summary

Name: Test Unit

Contact person: John Smith

Location:

Longitude:

Latitude:

IPv4 Address: 192.168.1.85

IPv4 Subnet Mask: 255.255.255.0

IPv4 Default Gateway: 0.0.0.0

NTP Admin: Enable

NTP version: NTPv4

NTP server IP address: 0.0.0.0

Demo admin: Enable

Admin: Enable

SNMP Read Community: public

SNMP Write Community: private

Configuring In-Band Management

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

> **Note**
>
> Before configuring in-band management, it is recommended to review the configuration recommendations for in-band management listed in*Error! Reference s ource not found.*.

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

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

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

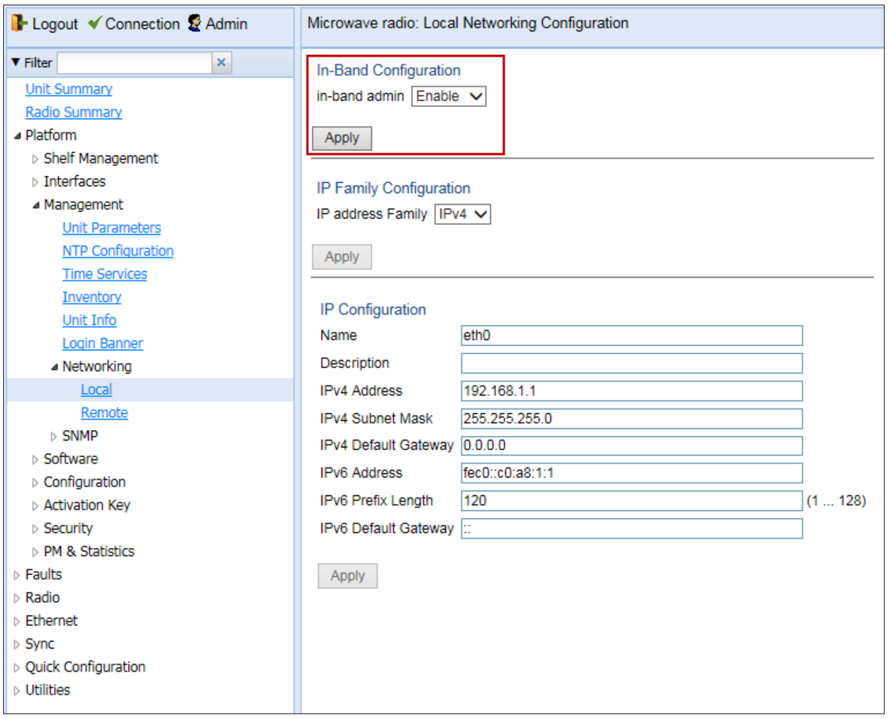
> **Note**
>
> In order to use in-band management, it must be supported on the external switch.

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

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

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

Figure 28 Local Networking Configuration Page – In-Band Management



Microwave radio: Local Networking Configuration

In-Band Configuration

in-band admin: Enable

IP Family Configuration

IP address Family: IPv4

IP Configuration

Name	eth0
Description	
IPv4 Address	192.168.1.1
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	0.0.0.0
IPv6 Address	fec0::c0:a8:1:1
IPv6 Prefix Length	120 (1 ... 128)
IPv6 Default Gateway	::

2. In the **In-Band Admin** field, select **Enable**.

3. Click **Apply** underneath the **In-Band Admin** field.

Changing the Management IP Address

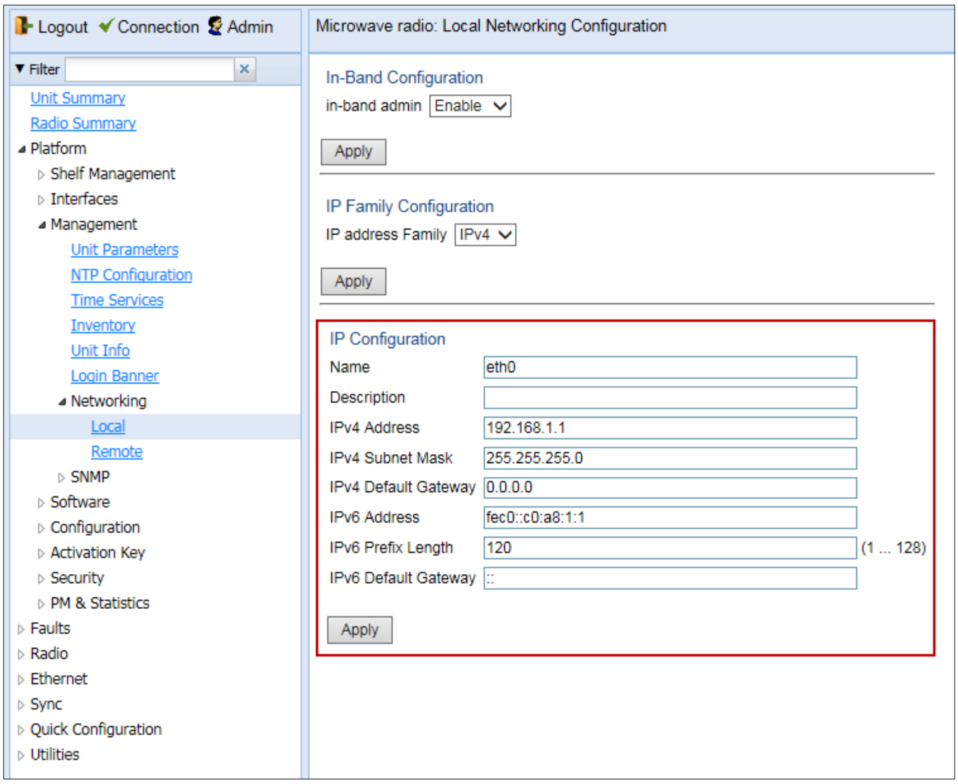
Related Topics:

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

To change the management IP address of the local unit:

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

Figure 29 Local Networking Configuration Page



Microwave radio: Local Networking Configuration

In-Band Configuration

in-band admin: Enable

Apply

IP Family Configuration

IP address Family: IPv4

Apply

IP Configuration

Name	eth0
Description	
IPv4 Address	192.168.1.1
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	0.0.0.0
IPv6 Address	fec0::c0:a8:1:1
IPv6 Prefix Length	120 (1 ... 128)
IPv6 Default Gateway	::

Apply

2. Optionally, in the **Name** field, enter a name for the unit.
3. Optionally, in the **Description** field, enter descriptive information about the unit.
4. In the **IPv4 address** field, enter an IP address for the unit. You can enter the address in IPv4 format in this field, and/or in IPv6 format in the **IPv6 Address** field. The unit will receive communications whether they are sent to its IPv4 address or its IPv6 address.
5. If you entered an IPv4 address, in the **IPv4 Subnet mask** field, enter the subnet mask.
6. Optionally, in the **IPv4 Default gateway** field, enter the default gateway address.
7. Optionally, in the **IPv6 Address** field, enter an IPv6 address for the unit. You can enter the address in IPv6 format in this field, and/or in IPv4 format in the **IPv4 IP Address** field. The unit will receive communications whether they are sent to its IPv4 address or its IPv6 address.
8. If you entered an IPv6 address, enter the IPv6 prefix length in the **IPv6 Prefix-Length** field.
9. Optionally, if you entered an IPv6 address, enter the default gateway in IPv6 format in the **IPv6 Default Gateway** field.

10. Click **Apply**.

Configuring the Activation Key

This section includes:

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

Displaying a List of Activation-Key-Enabled Features

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

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

Note

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

Activation Key Overview

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

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

Note

To obtain an activation key cipher, you may need to provide the unit's serial number. You can display the serial number in the Web EMS Inventory page. See ***Error! R eference source not found.***.

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

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

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

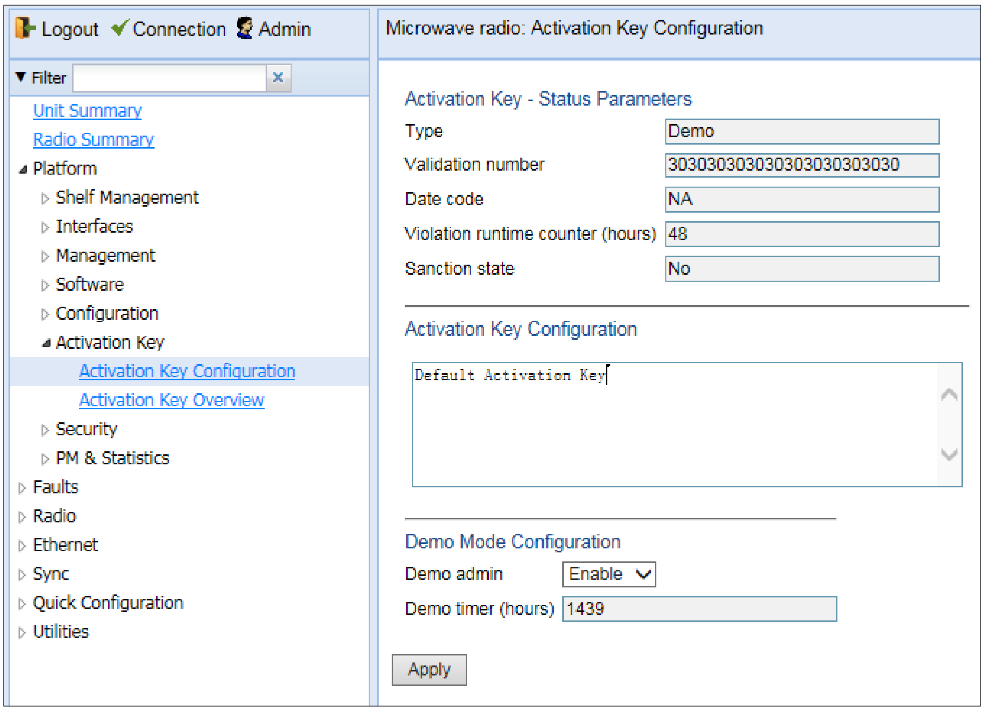
Demo mode is available, which enables all features for 60 days. When demo mode expires, the most recent valid activation key goes into effect. The 60-day period is only counted when the system is powered up. 10 days before demo mode expires, an alarm is raised indicating that demo mode is about to expire.

Viewing the Activation Key Status Parameters

To display the current activation key status parameters:

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

Figure 30 Activation Key Configuration Page



Microwave radio: Activation Key Configuration

Activation Key - Status Parameters

Type: Demo
Validation number: 30303030303030303030303030
Date code: NA
Violation runtime counter (hours): 48
Sanction state: No

Activation Key Configuration

Default Activation Key

Demo Mode Configuration

Demo admin: Enable
Demo timer (hours): 1439

Table 8 Activation Key Status Parameters

Parameter	Definition
Type	Displays the current activation key type.
Validation number	Displays a random, system-generated validation number.
Date code	Displays a date code used for validation of the current activation key cipher.
Violation runtime counter (hours)	In the event of an Activation Key Violation alarm, this field displays the number of hours remaining in the 48-hour activation key violation grace period.

Parameter	Definition
Sanction state	If an Activation Key Violation alarm has occurred, and the 48-hour activation key violation grace period has expired without the system having been brought into conformance with the activation-key-enabled capacity and feature set, Yes appears in this field to indicate that the system is in an Activation Key Violation sanction state. All other alarms are hidden until the capacity and features in use are brought within the activation-key-enabled capacity and feature set.

Entering the Activation Key

1. To enter a new activation key:
2. Select **Platform > Activation Key > Activation Key Configuration**. The Activation Key Configuration page opens (Figure 30).
3. Enter the activation key cipher you have received from the vendor in the Activation Key field. The activation key cipher is a string that enables all features and capacities that have been purchased for the unit.
4. Click **Apply**.

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

Activating a Demo Activation Key

To activate demo mode:

1. Select **Platform > Activation Key > Activation Key Configuration**. The Activation Key Configuration page opens (Figure 31).
2. In the **Demo admin** field, select **Enable**.
3. Click **Apply**.

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

Activation Key Reclaim

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

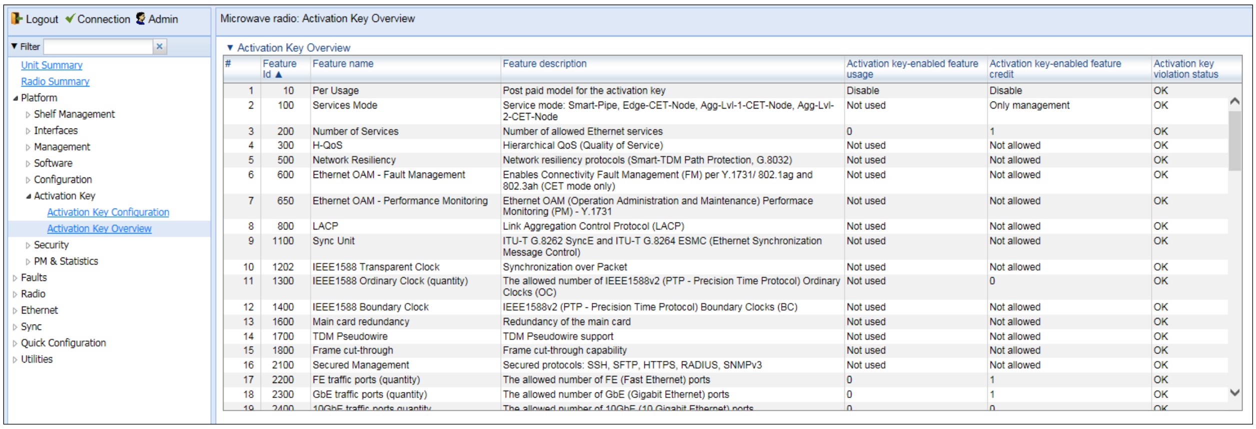
Where the customer has purchased upgrade activation keys, credit is given for the full feature or capacity, not for each individual upgrade. For example, if the customer purchased two capacity activation keys for 300M and later purchased one upgrade activation key to 350M, credit is given as if the customer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

Displaying a List of Activation-Key-Enabled Features

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

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

Figure 31 Activation Key Overview Page



Microwave radio: Activation Key Overview

▼ Activation Key Overview

#	Feature Id ▲	Feature name	Feature description	Activation key-enabled feature usage	Activation key-enabled feature credit	Activation key violation status
1	10	Per Usage	Post paid model for the activation key	Disable	Disable	OK
2	100	Services Mode	Service mode: Smart-Pipe, Edge-CET-Node, Agg-Lvl-1-CET-Node, Agg-Lvl-2-CET-Node	Not used	Only management	OK
3	200	Number of Services	Number of allowed Ethernet services	0	1	OK
4	300	H-QoS	Hierarchical QoS (Quality of Service)	Not used	Not allowed	OK
5	500	Network Resiliency	Network resiliency protocols (Smart-TDM Path Protection, G.8032)	Not used	Not allowed	OK
6	600	Ethernet OAM - Fault Management	Enables Connectivity Fault Management (FM) per Y.1731/ 802.1ag and 802.3ah (CET mode only)	Not used	Not allowed	OK
7	650	Ethernet OAM - Performance Monitoring	Ethernet OAM (Operation Administration and Maintenance) Performace Monitoring (PM) - Y.1731	Not used	Not allowed	OK
8	800	LACP	Link Aggregation Control Protocol (LACP)	Not used	Not allowed	OK
9	1100	Sync Unit	ITU-T G.8262 SyncE and ITU-T G.8264 ESMC (Ethernet Synchronization Message Control)	Not used	Not allowed	OK
10	1202	IEEE1588 Transparent Clock	Synchronization over Packet	Not used	Not allowed	OK
11	1300	IEEE1588 Ordinary Clock (quantity)	The allowed number of IEEE1588v2 (PTP - Precision Time Protocol) Ordinary Clocks (OC)	Not used	0	OK
12	1400	IEEE1588 Boundary Clock	IEEE1588v2 (PTP - Precision Time Protocol) Boundary Clocks (BC)	Not used	Not allowed	OK
13	1600	Main card redundancy	Redundancy of the main card	Not used	Not allowed	OK
14	1700	TDM Pseudowire	TDM Pseudowire support	Not used	Not allowed	OK
15	1800	Frame cut-through	Frame cut-through capability	Not used	Not allowed	OK
16	2100	Secured Management	Secured protocols: SSH, SFTP, HTTPS, RADIUS, SNMPv3	Not used	Not allowed	OK
17	2200	FE traffic ports (quantity)	The allowed number of FE (Fast Ethernet) ports	0	1	OK
18	2300	GbE traffic ports (quantity)	The allowed number of GbE (Gigabit Ethernet) ports	0	1	OK
19	2400	10GbE traffic ports quantity	The allowed number of 10GbE (10 Gigabit Ethernet) ports	0	0	OK

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

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

Table 9 Activation Key-Enabled-Features Table Parameters

Parameter	Definition
Feature ID	A unique ID that identifies the feature.
Feature name	The name of the feature.
Feature Description	A description of the feature.
Activation key-enabled feature usage	Indicates whether the activation-key-enabled feature is actually being used.
Activation key-enabled feature credit	Indicates whether the feature is allowed under the activation key that is currently installed in the unit.
Activation key violation status	Indicates whether the system configuration violates the currently installed activation key with respect to this feature.

Table 10 Activation Key-Enabled-Features Description

Activation Key Name	Description
Services Mode	Enables a number of Ethernet services, depending on the type of activation key: • Smart-Pipe –Smart Pipe (L1) services only (unlimited) and a single management service. • Edge-CET Node – Up to 8 services (all supported service types). • Agg-Lvl-1-CET-Node – Up to 64 services (all supported service types). • Agg-Lvl-2-CET-Node – Up to 1024 services (all supported service types). Any CET activation key also enables the following: • A GbE traffic port in addition to the port provided by the default activation key, for a total of 2 GbE traffic ports. • Full QoS for all services including basic queue buffer management (fixed queues buffer size limit, tail-drop only) and eight queues per port, no H-QoS.
Number of Services	Indicates how many services are allowed according to the Services Mode activation key, and how many are actually configured on the device.
H-QoS	Not relevant in the current release.
Network Resiliency	Not relevant for PTP 850.
Ethernet OAM – Fault Management	Enables Connectivity Fault Management (FM) per Y.1731 (CET mode only).
Ethernet OAM – Performance Monitoring	Not relevant in the current release.
LACP	Not relevant in the current release.
Sync Unit	Enables the G.8262 synchronization unit. This activation key is required in order to provide end-to-end synchronization distribution on the physical layer. This activation key is also required to use SyncE.
IEEE 1588 Transparent Clock	Enables IEEE-1588 Transparent Clock.
IEEE 1588 Ordinary Clock (quantity)	Not relevant in the current release.
IEEE 1588 Boundary Clock	Enables IEEE-1588 Boundary Clock.
Main Card Redundancy	Not relevant for PTP 850.
TDM Pseudowire	Not relevant for PTP 850.
Frame cut-through	Not relevant in the current release.
Secured Management	Enables secure management protocols (SSH, HTTPS, SFTP, SNMPv3, and RADIUS).
FE traffic ports (quantity)	Displays the number of FE traffic ports allowed under the current activation key.
GbE traffic ports (quantity)	Displays the number of GbE traffic ports allowed under the current activation key.

Activation Key Name	Description
10GbE traffic ports (quantity)	Displays the number of 10G traffic ports allowed under the current activation key.
ACM (quantity)	Displays the number of radio carriers that are allowed to use ACM under the current activation key.
Narrow CHBW 1.75MHz script (quantity)	Not relevant for PTP 850.
Header De-Duplication (quantity)	Displays the number of radio carriers that are allowed to use Header De-Duplication. Only relevant for PTP 850S.
XPIC (quantity)	Displays the number of radio carriers that are allowed to use XPIC. Each carrier in the XPIC pair requires an XPIC activation key.
Multi-Carrier ABC (quantity)	Not relevant for PTP 850.
MIMO	Not relevant for PTP 850.
SD	Not relevant for PTP 850.
ASD	Not relevant for PTP 850.
AFR 1+0 (quantity)	Not relevant for PTP 850.
ACMB Adaptive BW	Displays the number of radio carriers for which there is permission to use ACMB, which enables the use of radio profiles 1 and 2.
Payload Encryption AES-256 (quantity)	Displays the number of radio carriers that can use of AES-256 encryption Note that: • If no AES activation key is configured for the unit and the user attempts to enable AES on a radio carrier, in addition to an Activation Key Violation alarm the feature will remain inactive and no encryption will be performed. • After entering an AES activation key, the user must reset the unit before AES can be activated. Unit reset is only necessary for the first AES activation key. If AES activation keys are acquired later for additional radio carriers, unit reset is not necessary. Only relevant for PTP 850E.
Second core activation	Not relevant for PTP 850.
Second core activation for RFU-D	Not relevant for PTP 850.
Second core activation for HP	Not relevant for PTP 850.
Second modem activation	Not relevant for PTP 850.
RFU port activation key	Not relevant for PTP 850.
Radio capacity level 1	Displays the number of radio carriers for which there is permission to use up to 10 Mbps. This is the default level, so every radio carrier on the device has this capacity level.
Radio capacity level 2	Displays the number of radio carriers for which there is permission to use up to 50 Mbps.

Activation Key Name	Description
Radio capacity level 3	Displays the number of radio carriers for which there is permission to use up to 100 Mbps.
Radio capacity level 4	Displays the number of radio carriers for which there is permission to use up to 150 Mbps.
Radio capacity level 5	Displays the number of radio carriers for which there is permission to use up to 200 Mbps.
Radio capacity level 6	Displays the number of radio carriers for which there is permission to use up to 225 Mbps.
Radio capacity level 7	Displays the number of radio carriers for which there is permission to use up to 250 Mbps.
Radio capacity level 8	Displays the number of radio carriers for which there is permission to use up to 300 Mbps.
Radio capacity level 9	Displays the number of radio carriers for which there is permission to use up to 350 Mbps.
Radio capacity level 10	Displays the number of radio carriers for which there is permission to use up to 400 Mbps.
Radio capacity level 11	Displays the number of radio carriers for which there is permission to use up to 450 Mbps.
Radio capacity level 12	Displays the number of radio carriers for which there is permission to use up to 500 Mbps.
Radio capacity level 13	Displays the number of radio carriers for which there is permission to use up to 650 Mbps.
Radio capacity level 14	Displays the number of radio carriers for which there is permission to use up to 1000 Mbps.
Radio capacity level 15	Displays the number of radio carriers for which there is permission to use up to 1600 Mbps.
Radio capacity level 16	Displays the number of radio carriers for which there is permission to use up to 2000 Mbps.
Radio capacity level 17	Displays the number of radio carriers for which there is permission to use up to 2500 Mbps.
Radio capacity level 18	Displays the number of radio carriers for which there is permission to use up to 3000 Mbps.
Radio capacity level 19	Displays the number of radio carriers for which there is permission to use up to 4000 Mbps.
Radio capacity level 20	Displays the number of radio carriers for which there is permission to use up to 5000 Mbps.
Radio capacity level 21	Displays the number of radio carriers for which there is permission to use up to 6000 Mbps.
Radio capacity level 22	Displays the number of radio carriers for which there is permission to use up to 7000 Mbps.

Activation Key Name	Description
Radio capacity level 23	Displays the number of radio carriers for which there is permission to use up to 8000 Mbps.
Radio capacity level 24	Displays the number of radio carriers for which there is permission to use up to 9000 Mbps.
Radio capacity level 25	Displays the number of radio carriers for which there is permission to use up to 10000 Mbps.
Auto State Propagation and LLF	Enables the use of Link Loss Forwarding (LLF) with Automatic State Propagation (ASP). Without the activation key, only one LLF ID can be configured. This means that only one ASP pair can be configured per radio interface or radio group.
Enhanced Multi-Carrier ABC (quantity)	Enables the configuration and use of a Multiband (Enhanced Multi-Carrier ABC) link. Two activation keys are required per Multiband node, on the IP 50E. One of these activation keys is for the radio port, the other is for the Ethernet port carrying traffic to the unit paired with the PTP 850E. No activation key is required for the unit paired with the PTP 850E.

Setting the Time and Date (Optional)

Related Topics:

Configuring NTP

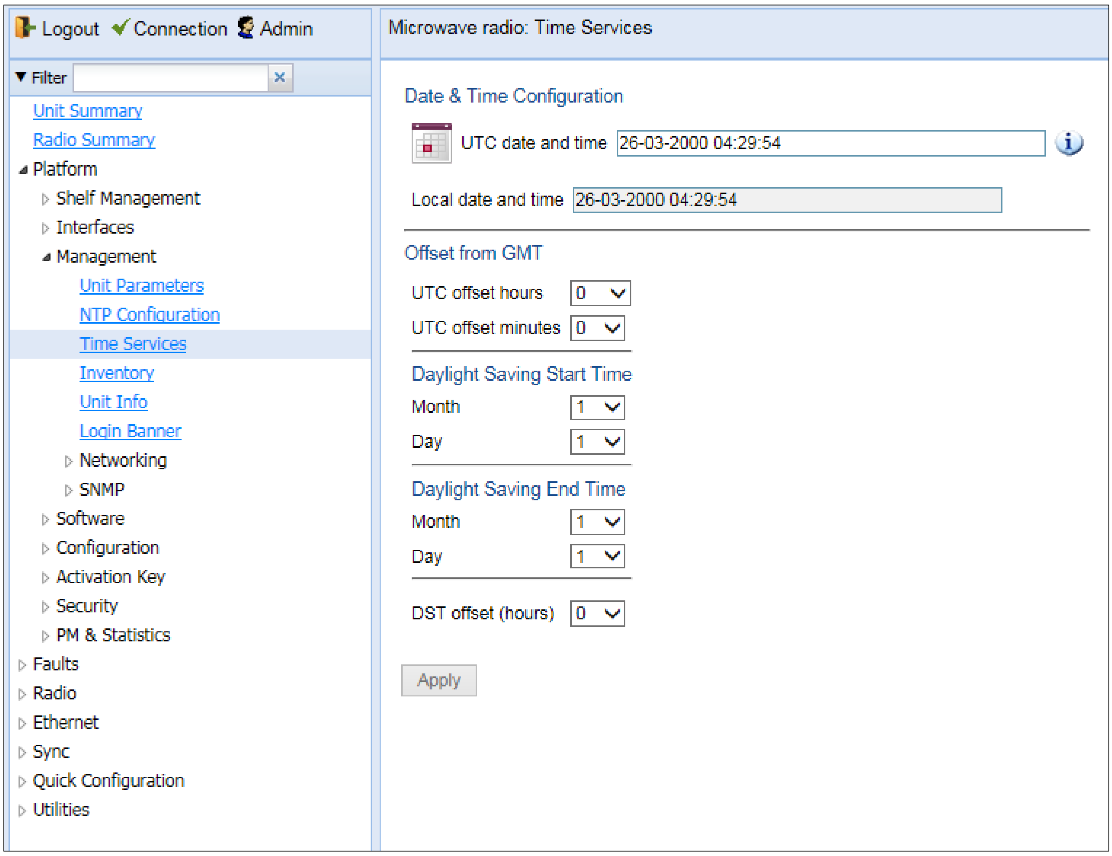
PTP 850 uses the Universal Time Coordinated (UTC) standard for time and date configuration. UTC is a more updated and accurate method of date coordination than the earlier date standard, Greenwich Mean Time (GMT).

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

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

To display and configure the UTC parameters:

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



Microwave radio: Time Services

Date & Time Configuration

UTC date and time: 26-03-2000 04:29:54

Local date and time: 26-03-2000 04:29:54

Offset from GMT

UTC offset hours: 0

UTC offset minutes: 0

Daylight Saving Start Time

Month: 1

Day: 1

Daylight Saving End Time

Month: 1

Day: 1

DST offset (hours): 0

Figure 32 Time Services Page

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

Table 11 Time Services Parameters

	Parameter	Definition
Date & Time Configuration	UTC Date and Time	The UTC date and time.
	Local Current Date and Time	Read-only. The calculated local date and time, based on the local clock, Universal Time Coordinated (UTC), and Daylight Savings Time (DST) configurations.
Offset from GMT	UTC Offset Hours	The required hours offset (positive or negative) relative to GMT. This is used to offset the clock relative to GMT, according to the global meridian location.
	UTC Offset Minutes	The required minutes offset (positive or negative) relative to GMT. This is used to offset the clock relative to GMT, according to the global meridian location.
Daylight Saving Start Time	Month	The month when Daylight Savings Time begins.
	Day	The date in the month when Daylight Savings Time begins.
Daylight Saving End Time	Month	The month when Daylight Savings Time ends.
	Day	The date in the month when Daylight Savings Time ends.
	DST Offset (Hours)	The required offset, in hours, for Daylight Savings Time. Only positive offset is supported.

Enabling the Interfaces (Interface Manager)

By default:

Ethernet traffic interfaces are disabled and must be manually enabled.

The Ethernet management interface is enabled.

Radio interfaces are enabled.

Note

In release 11.1, Ethernet Slot 1, Ports 2 through 7 are supported.

Port 2 can only be used in Multiband configurations to connect the PTP 850E with the paired unit.

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

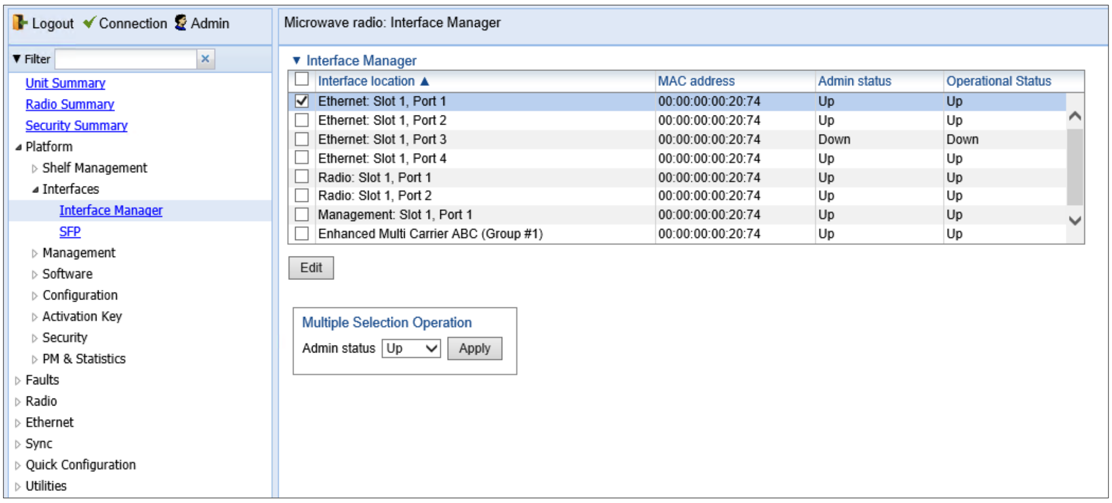
In a 4x1/10G configuration the QSFP port can provide four Ethernet interfaces: Ethernet Slot 1, Port 3, Ethernet Slot 1, Port 4, Ethernet Slot 1, Port 5, and Ethernet Slot 1, Port 6. In this configuration, a QSFP transceiver is attached to the QSFP port, and an MPO-MPO cable is connected between the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

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

To enable or disable interfaces:

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

Figure 33 Interface Manager Page-PTP 850C



Microwave radio: Interface Manager

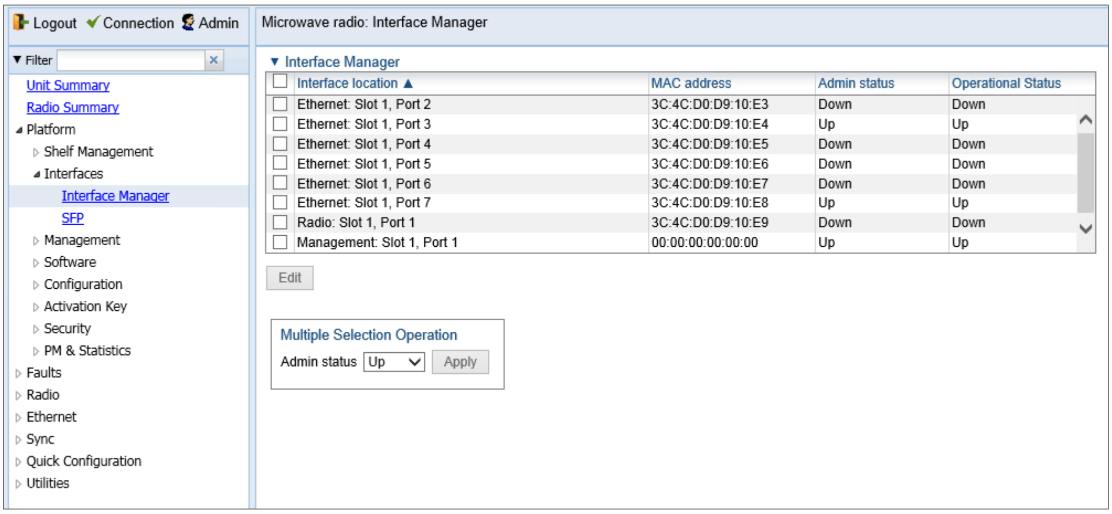
Interface Manager

□	Interface location ▲	MAC address	Admin status	Operational Status
☑	Ethernet: Slot 1, Port 1	00:00:00:00:20:74	Up	Up
□	Ethernet: Slot 1, Port 2	00:00:00:00:20:74	Up	Up
□	Ethernet: Slot 1, Port 3	00:00:00:00:20:74	Down	Down
□	Ethernet: Slot 1, Port 4	00:00:00:00:20:74	Up	Up
□	Radio: Slot 1, Port 1	00:00:00:00:20:74	Up	Up
□	Radio: Slot 1, Port 2	00:00:00:00:20:74	Up	Up
□	Management: Slot 1, Port 1	00:00:00:00:20:74	Up	Up
□	Enhanced Multi Carrier ABC (Group #1)	00:00:00:00:20:74	Up	Up

Multiple Selection Operation

Admin status: Up

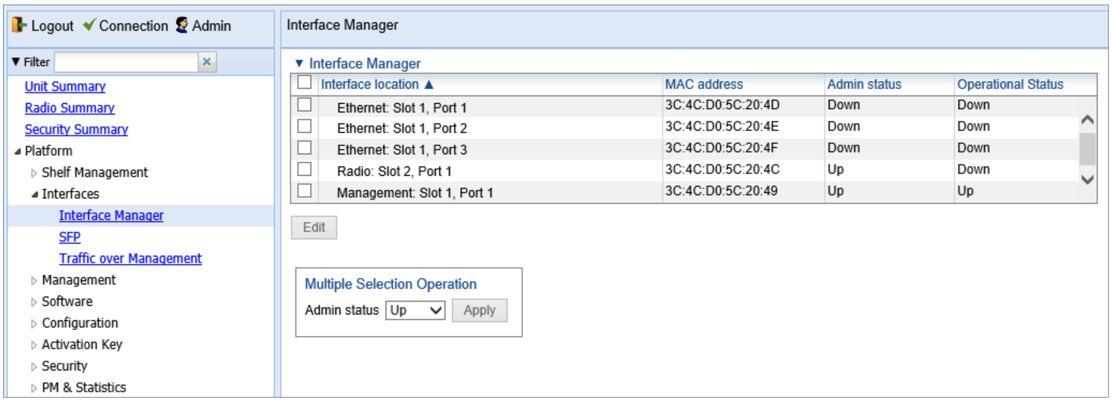
Figure 34 Interface Manager Page-PTP 850E



□	Interface location ▲	MAC address	Admin status	Operational Status
□	Ethernet: Slot 1, Port 2	3C:4C:D0:D9:10:E3	Down	Down
□	Ethernet: Slot 1, Port 3	3C:4C:D0:D9:10:E4	Up	Up
□	Ethernet: Slot 1, Port 4	3C:4C:D0:D9:10:E5	Down	Down
□	Ethernet: Slot 1, Port 5	3C:4C:D0:D9:10:E6	Down	Down
□	Ethernet: Slot 1, Port 6	3C:4C:D0:D9:10:E7	Down	Down
□	Ethernet: Slot 1, Port 7	3C:4C:D0:D9:10:E8	Up	Up
□	Radio: Slot 1, Port 1	3C:4C:D0:D9:10:E9	Down	Down
□	Management: Slot 1, Port 1	00:00:00:00:00:00	Up	Up

Admin status: Up

Figure 35 Interface Manager Page-PTP 850S



□	Interface location ▲	MAC address	Admin status	Operational Status
□	Ethernet: Slot 1, Port 1	3C:4C:D0:5C:20:4D	Down	Down
□	Ethernet: Slot 1, Port 2	3C:4C:D0:5C:20:4E	Down	Down
□	Ethernet: Slot 1, Port 3	3C:4C:D0:5C:20:4F	Down	Down
□	Radio: Slot 2, Port 1	3C:4C:D0:5C:20:4C	Up	Down
□	Management: Slot 1, Port 1	3C:4C:D0:5C:20:49	Up	Up

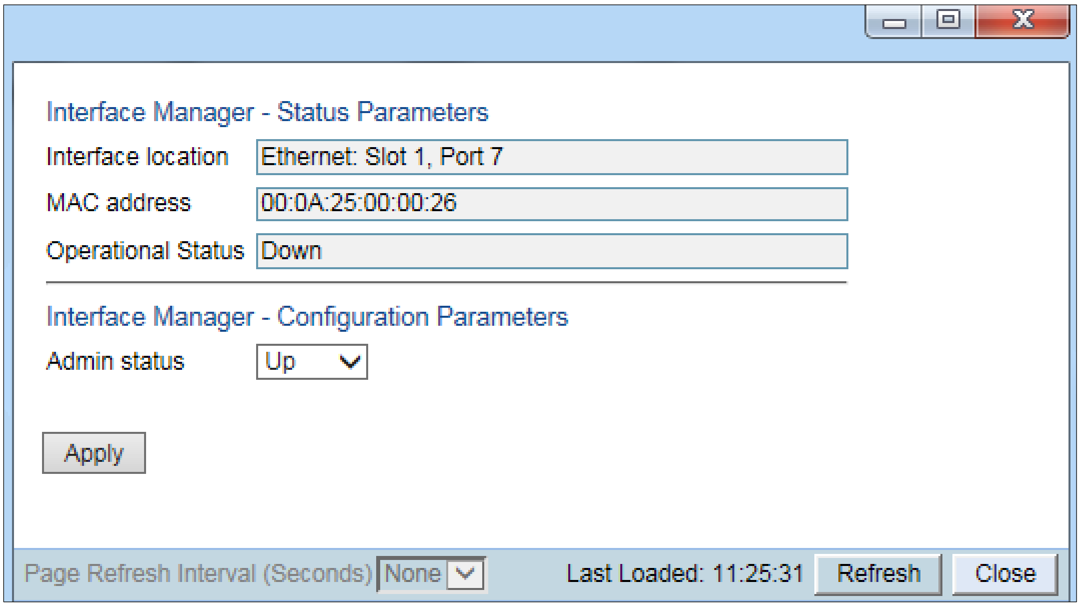
Admin status: Up

If an alarm is currently raised on an interface, an alarm icon appears to the left of the interface location. For example, in ***Error! Reference source not found.***, an alarm is raised on the Radio i nterface. To display details about the alarm or alarms in tooltip format, hover the mouse over the alarm icon.

To enable or disable an individual interface:

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

Figure 36 Interface Manager – Edit Page



Interface Manager - Status Parameters

Interface location: Ethernet: Slot 1, Port 7

MAC address: 00:0A:25:00:00:26

Operational Status: Down

Interface Manager - Configuration Parameters

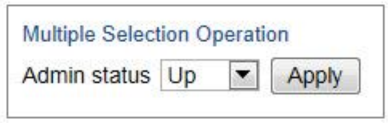
Admin status: Up

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

To enable or disable multiple interfaces:

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

Figure 37 Multiple Selection Operation Section (Interface Manager Page)



Multiple Selection Operation

Admin status: Up

3. Click **Apply**.

Note

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

PTP 850S Management Interface

The PTP 850S management port (Port 1) can be used for traffic as well as management and PoE. This increases the number of available Ethernet traffic ports and enables customers to configure setups in which a single cable is used to carry management, power, and traffic from the customer equipment to the PTP 850S device.

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

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

- Support for RMON

Because this interface is used for management, a management service (Service ID

257)) and service point (Service Point ID 1) are configured on the interface and cannot be removed.

A Policer (Policer ID 251) is attached to this service point and cannot be edited or removed.

In order to ensure that the port can be used for traffic services, the Attached Interface Type of the management service point can be modified from its default value of dot1q if it is the only service point on the interface. It can be changed to s-tag or QinQ, giving you the flexibility to configure services on the interface according to the expected user traffic. See *Editing a Service Point*.

The following limitations exist for this port:

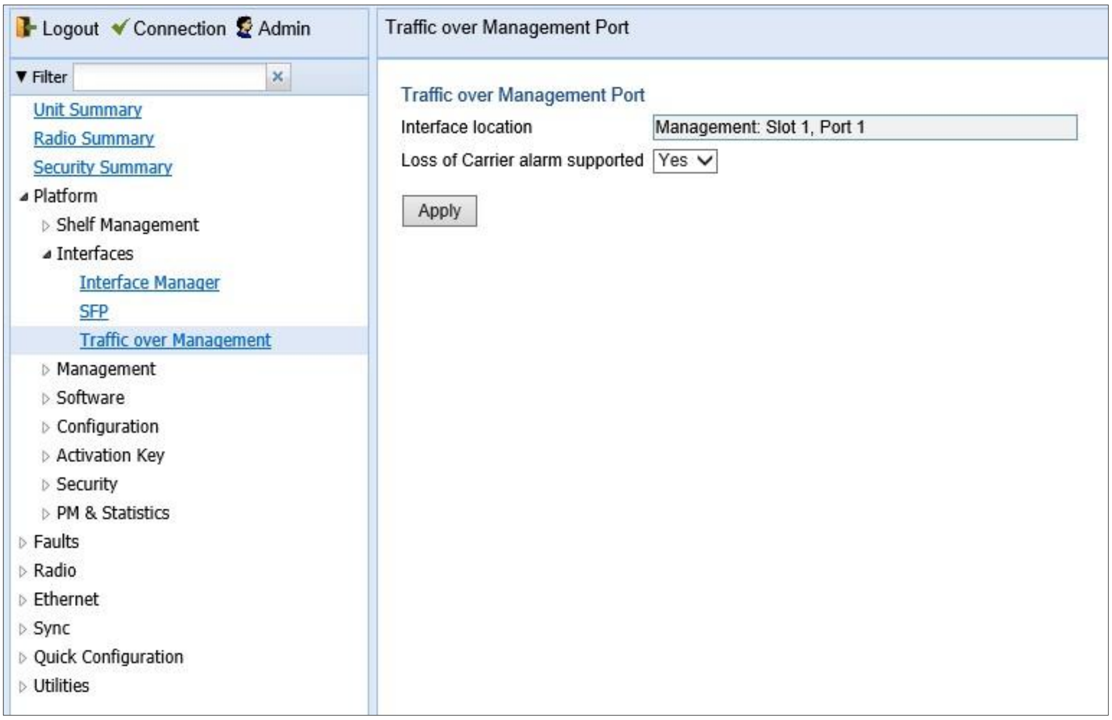
- Cannot belong to LAG groups
- Does not support MSTP and G.8032
- Automatic State Propagation can only be used in CSF mode

To use the PTP 850S management port for traffic, you should perform the following configurations:

- An egress Service Bundle Shaper (Shaper ID 256) is attached to this service point. This Shaper cannot be edited, but it can and must be either detached or disabled on the port in order for the port to support 1G traffic. See *Assigning a Service Bundle Shaper Profile to a Service Bundle*.
- Change the port speed from its default value of 100 Mbps to 1 Gbps. See *Configuring Ethernet Interfaces*.
- Enable the LOC alarm (Alarm ID 401) for the management port. By default, this alarm is disabled on the management port and must be manually enabled when using the port for traffic.

To enable the LOC alarm:

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



Traffic over Management Port

Traffic over Management Port

Interface location: Management: Slot 1, Port 1

Loss of Carrier alarm supported: Yes

Figure 38: Traffic over Management Page

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

3 Click **Apply**.

Configuring the Radio (MRMC) Script(s)

Related Topics:

Displaying MRMC Status

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

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

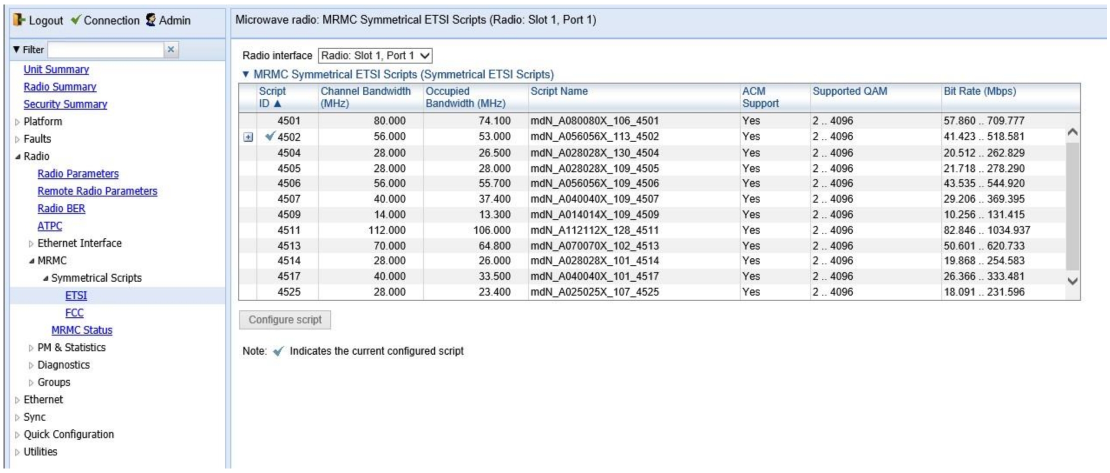
To display the MRMC scripts and their basic parameters and select a script:

1. Select one of the following, depending on the regulatory framework in which you are operating:
    - To display ETSI scripts, select **Radio > MRMC > Symmetrical Scripts > ETSI**.
    - To display ANSI (FCC) scripts, select **Radio > MRMC > Symmetrical Scripts > FCC.**

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

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

Figure 38 MRMC Symmetrical Scripts Page-PTP 850C



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

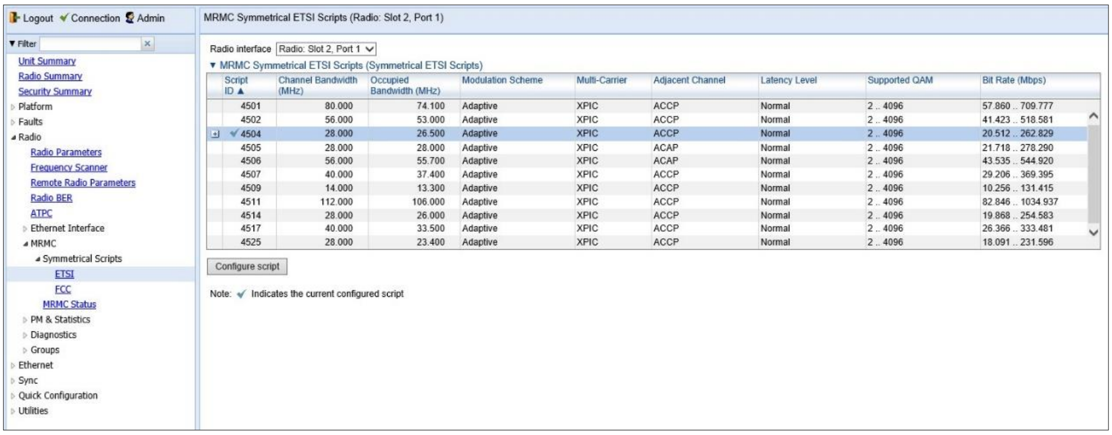
Radio interface: Radio: Slot 1, Port 1

▼ MRMC Symmetrical ETSI Scripts (Symmetrical ETSI Scripts)

	Script ID ▲	Channel Bandwidth (MHz)	Occupied Bandwidth (MHz)	Script Name	ACM Support	Supported QAM	Bit Rate (Mbps)
	4501	80.000	74.100	mdN_A080080X_106_4501	Yes	2 .. 4096	57.860 .. 709.777
⊞	✓ 4502	56.000	53.000	mdN_A056056X_113_4502	Yes	2 .. 4096	41.423 .. 518.581
	4504	28.000	26.500	mdN_A028028X_130_4504	Yes	2 .. 4096	20.512 .. 262.829
	4505	28.000	28.000	mdN_A028028X_109_4505	Yes	2 .. 4096	21.718 .. 278.290
	4506	56.000	55.700	mdN_A056056X_109_4506	Yes	2 .. 4096	43.535 .. 544.920
	4507	40.000	37.400	mdN_A040040X_109_4507	Yes	2 .. 4096	29.206 .. 369.395
	4509	14.000	13.300	mdN_A014014X_109_4509	Yes	2 .. 4096	10.256 .. 131.415
	4511	112.000	106.000	mdN_A112112X_128_4511	Yes	2 .. 4096	82.846 .. 1034.937
	4513	70.000	64.800	mdN_A070070X_102_4513	Yes	2 .. 4096	50.601 .. 620.733
	4514	28.000	26.000	mdN_A028028X_101_4514	Yes	2 .. 4096	19.868 .. 254.583
	4517	40.000	33.500	mdN_A040040X_101_4517	Yes	2 .. 4096	26.366 .. 333.481
	4525	28.000	23.400	mdN_A025025X_107_4525	Yes	2 .. 4096	18.091 .. 231.596

Note: ✓ Indicates the current configured script

Figure 39 MRMC Symmetrical Scripts Page-PTP 850S



MRMC Symmetrical ETSI Scripts (Radio: Slot 2, Port 1)

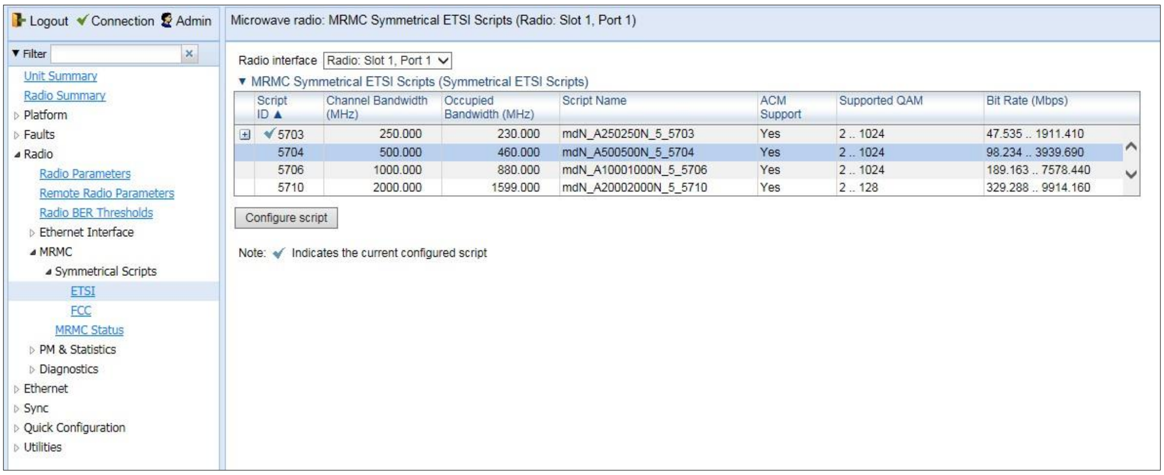
Radio interface: Radio: Slot 2, Port 1

▼ MRMC Symmetrical ETSI Scripts (Symmetrical ETSI Scripts)

Script ID ▲	Channel Bandwidth (MHz)	Occupied Bandwidth (MHz)	Modulation Scheme	Multi-Carrier	Adjacent Channel	Latency Level	Supported QAM	Bit Rate (Mbps)
4501	80.000	74.100	Adaptive	XPIC	ACCP	Normal	2 .. 4096	57.860 .. 709.777
4502	56.000	53.000	Adaptive	XPIC	ACCP	Normal	2 .. 4096	41.423 .. 518.581
✓ 4504	28.000	26.500	Adaptive	XPIC	ACCP	Normal	2 .. 4096	20.512 .. 262.829
4505	28.000	28.000	Adaptive	XPIC	ACAP	Normal	2 .. 4096	21.718 .. 278.290
4506	56.000	55.700	Adaptive	XPIC	ACAP	Normal	2 .. 4096	43.535 .. 544.920
4507	40.000	37.400	Adaptive	XPIC	ACCP	Normal	2 .. 4096	29.206 .. 369.395
4509	14.000	13.300	Adaptive	XPIC	ACCP	Normal	2 .. 4096	10.256 .. 131.415
4511	112.000	106.000	Adaptive	XPIC	ACCP	Normal	2 .. 4096	82.846 .. 1034.937
4514	28.000	26.000	Adaptive	XPIC	ACCP	Normal	2 .. 4096	19.868 .. 254.583
4517	40.000	33.500	Adaptive	XPIC	ACCP	Normal	2 .. 4096	26.366 .. 333.481
4525	28.000	23.400	Adaptive	XPIC	ACCP	Normal	2 .. 4096	18.091 .. 231.596

Note: ✓ Indicates the current configured script

Figure 40 MRMC Symmetrical Scripts Page-PTP 850E



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

Radio interface: Radio: Slot 1, Port 1

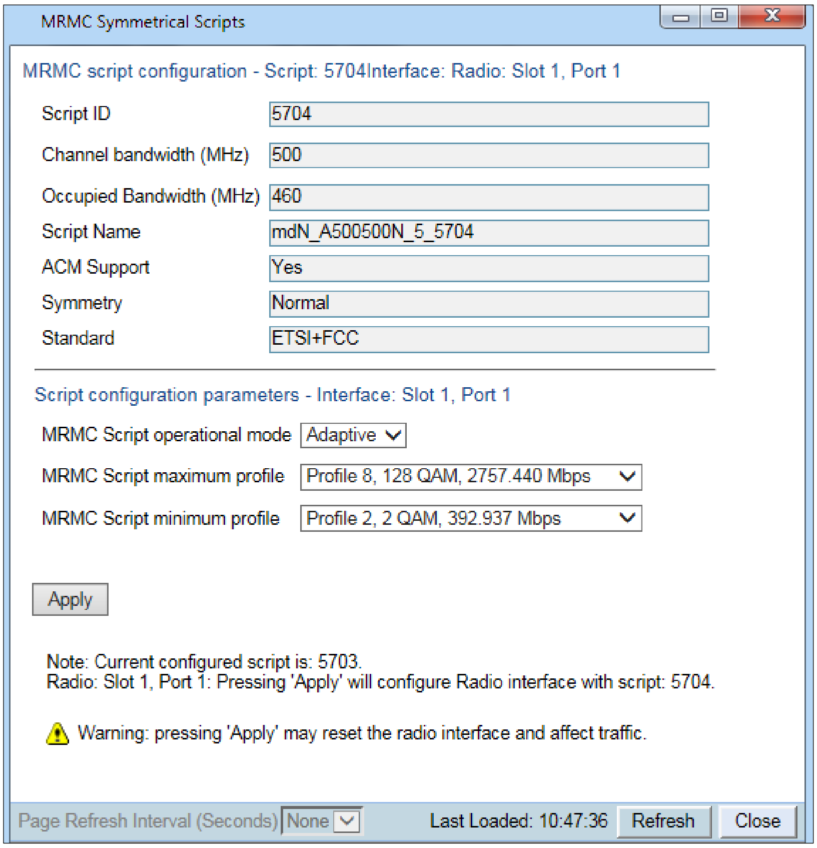
▼ MRMC Symmetrical ETSI Scripts (Symmetrical ETSI Scripts)

Script ID ▲	Channel Bandwidth (MHz)	Occupied Bandwidth (MHz)	Script Name	ACM Support	Supported QAM	Bit Rate (Mbps)
✓ 5703	250.000	230.000	mdN_A250250N_5_5703	Yes	2 .. 1024	47.535 .. 1911.410
5704	500.000	460.000	mdN_A500500N_5_5704	Yes	2 .. 1024	98.234 .. 3939.690
5706	1000.000	880.000	mdN_A10001000N_5_5706	Yes	2 .. 1024	189.163 .. 7578.440
5710	2000.000	1599.000	mdN_A20002000N_5_5710	Yes	2 .. 128	329.288 .. 9914.160

Note: ✓ Indicates the current configured script

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

Figure 41 **MRMC Symmetrical Scripts Page – Configuration**



MRMC script configuration - Script: 5704Interface: Radio: Slot 1, Port 1

Script ID	5704
Channel bandwidth (MHz)	500
Occupied Bandwidth (MHz)	460
Script Name	mdN_A500500N_5_5704
ACM Support	Yes
Symmetry	Normal
Standard	ETSI+FCC

Script configuration parameters - Interface: Slot 1, Port 1

MRMC Script operational mode: Adaptive

MRMC Script maximum profile: Profile 8, 128 QAM, 2757.440 Mbps

MRMC Script minimum profile: Profile 2, 2 QAM, 392.937 Mbps

Note: Current configured script is: 5703.
Radio: Slot 1, Port 1: Pressing 'Apply' will configure Radio interface with script: 5704.

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

Page Refresh Interval (Seconds): None

Last Loaded: 10:47:36

4. In the **MRMC Script operational mode** field, select the ACM mode: **Fixed** or **Adaptive**.
   - ○ Fixed ACM mode applies constant Tx and Rx rates. However, unlike regular scripts, with a Fixed ACM script you can specify a maximum profile to inhibit inefficient transmission levels.
   - ○ In Adaptive ACM mode, Tx and Rx rates are dynamic. An ACM-enabled radio system automatically chooses which profile to use according to the channel fading conditions. If you select **Adaptive**, two fields are displayed enabling you to select minimum and maximum ACM profiles.
5. Define the script profile or profiles
   - ○ If you selected **Fixed** ACM mode, select the ACM profile in the **MRMC Script profile** field.
   - ○ If you selected **Adaptive** ACM mode, select the maximum and minimum ACM profiles in the **MRMC Script maximum profile** and the **MRMC Script minimum profile** fields.
6. Click **Apply**.

Note

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

Table 12 MRMC Symmetrical Scripts Page Parameters

Parameter	Definition
Script ID	A unique ID assigned to the script in the system.
Channel Bandwidth (MHz)	The script's channel bandwidth (channel spacing).
Occupied Bandwidth (MHz)	The script's occupied bandwidth.
Script Name	The name of the script.
ACM Support	Indicates whether the script supports ACM. All PTP 850E scripts support ACM.
Supported QAMModulation Scheme	MRMC Symmetrical Scripts Main Page only: Displays the range of modulation levels, in QAM, supported by the script.PTP 850S only. Indicates whether the script supports Adaptive Coding Modulation (ACM). In ACM mode, a range of profiles determines Tx and Rx rates. This enables the radio to modify its transmit and receive levels in response to environmental conditions.
Bit Rate (Mbps)Multi-Carrier	MRMC Symmetrical Scripts Main PagePTP 850S only: Displays. Indicates the rangeMulti-Carrier status of bit rates, in Mbps, supported by the script. (XPIC, MIMO, or Single-Carrier).
Adjacent Channel	PTP 850C only. Displays the script’s adjacent channel polarization mode.
Latency Level	Always displays Normal.
Supported QAM	MRMC Symmetrical Scripts Main Page only: Displays the range of modulation levels, in QAM, supported by the script.
Bit Rate (Mbps)	MRMC Symmetrical Scripts Main Page only: Displays the range of bit rates, in Mbps, supported by the script.
Symmetry	MRMC Symmetrical Scripts Configuration Page only: Indicates that the script is symmetrical (Normal). Only symmetrical scripts are supported in the current release.
Standard	MRMC Symmetrical Scripts Configuration Page only: Indicates whether the script is compatible with ETSI or FCC (ANSI) standards, or both.
MRMC Script operational mode	MRMC Symmetrical Scripts Configuration Page only: The ACM mode: **Fixed** or **Adaptive**. • Fixed ACM mode applies constant TX and RX rates. However, unlike regular scripts, with a Fixed ACM script you can specify a maximum profile to inhibit inefficient transmission levels. • In Adaptive ACM mode, TX and RX rates are dynamic. An ACM-enabled radio system automatically chooses which profile to use according to the channel fading conditions.
MRMC Script profile	MRMC Symmetrical Scripts Configuration Page, Fixed ACM mode only: The profile in which the system will operate.
MRMC Script maximum profile	MRMC Symmetrical Scripts Configuration Page, Adaptive ACM mode only: The maximum profile for the script. For example, if you select a maximum profile of 5, the system will not climb above profile 5, even if channel fading conditions allow it.

Parameter	Definition
MRMC Script minimum profile	MRMC Symmetrical Scripts Configuration Page, Adaptive ACM mode only: The minimum profile for the script. For example, if you select a minimum profile of 3, the system will not go below profile 3 regardless of the channel fading conditions. The minimum profile cannot be greater than the maximum profile, but it can be equal to it. **Note:** The default minimum profile is 2.

Radio Profiles

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

Radio Profiles for PTP 850C and PTP 850S

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

Radio Profiles for PTP 850E

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

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

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

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

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

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

Profile	Modulation
Profile 0	BPSK ¼ channel spacing
Profile 1	BPSK ½ channel spacing
Profile 2	BPSK-full channel spacing
Profile 3	4 QAM
Profile 4	8 QAM
Profile 5	16 QAM
Profile 6	32 QAM
Profile 7	64 QAM
Profile 8	128 QAM
Profile 9	256 QAM
Profile 10	512 QAM

Running the Frequency Scanner

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

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

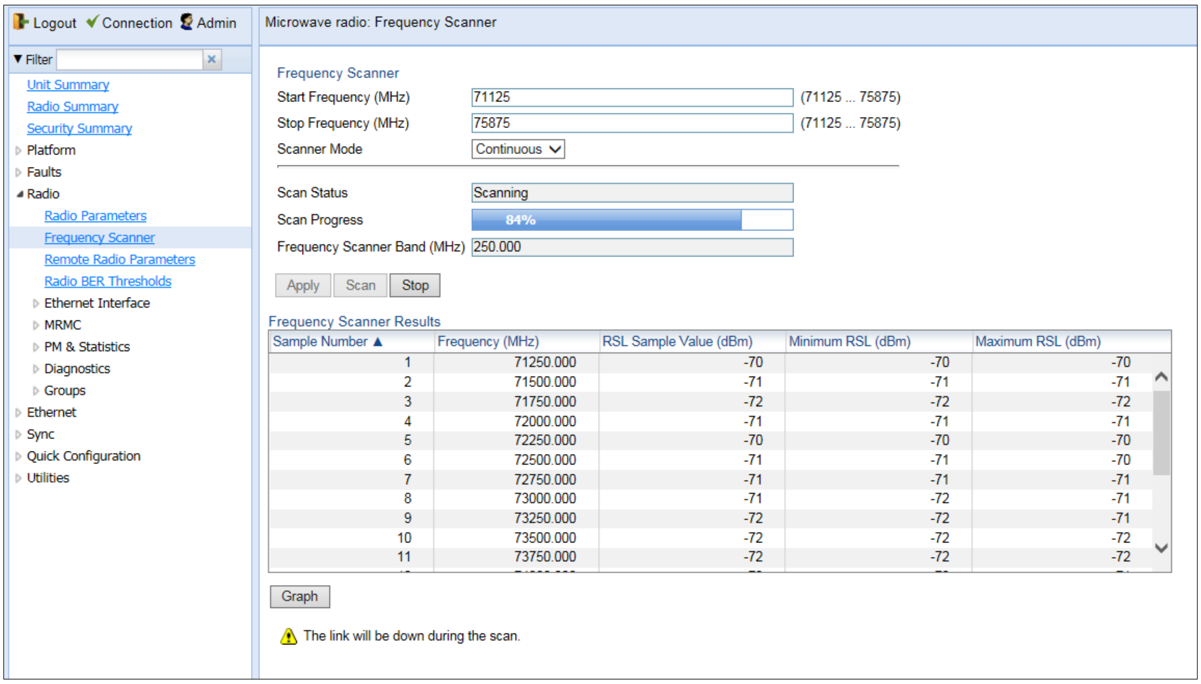
When the frequency scan begins, the unit stops receiving traffic until the scan is complete. This means the link is effectively down while the frequency scanner is operating. Once the frequency scan operation has been completed, either at the end of a Single Mode scan or by user action in the case of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

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

To perform a frequency scan:

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

Figure 42 Frequency Scanner Page – Continuous Mode



Microwave radio: Frequency Scanner

Frequency Scanner

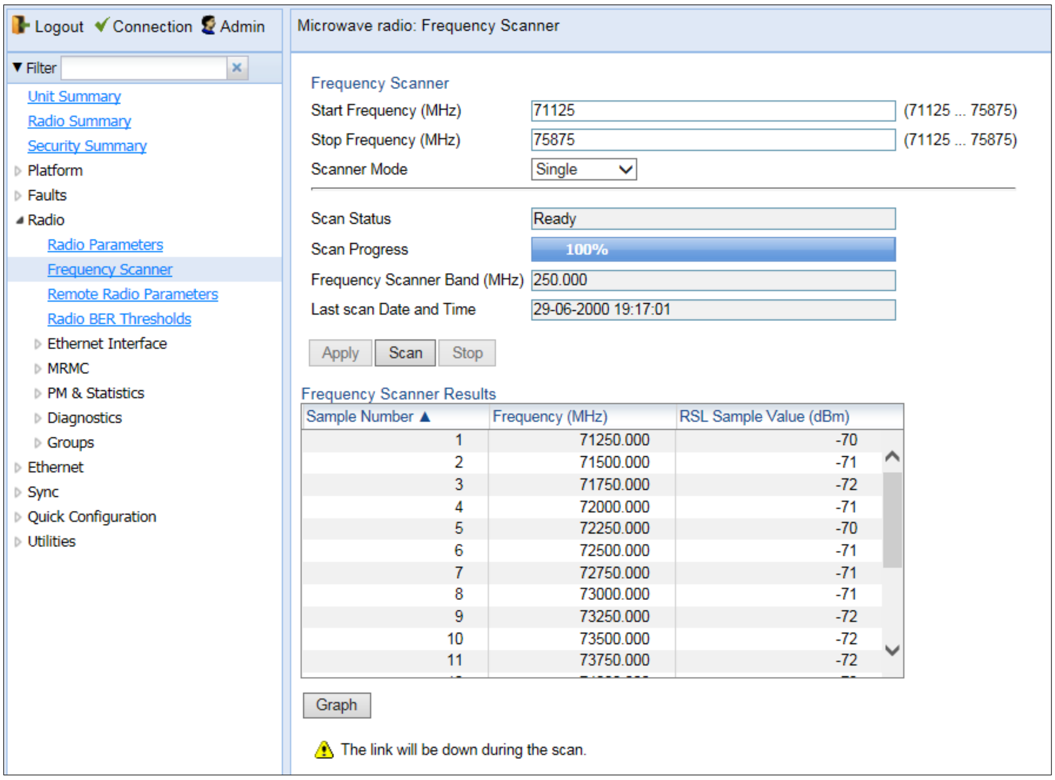
Start Frequency (MHz)	71125	(71125 ... 75875)
Stop Frequency (MHz)	75875	(71125 ... 75875)
Scanner Mode	Continuous	
Scan Status	Scanning	
Scan Progress	84%	
Frequency Scanner Band (MHz)	250.000	

Frequency Scanner Results

Sample Number ▲	Frequency (MHz)	RSL Sample Value (dBm)	Minimum RSL (dBm)	Maximum RSL (dBm)
1	71250.000	-70	-70	-70
2	71500.000	-71	-71	-71
3	71750.000	-72	-72	-72
4	72000.000	-71	-71	-71
5	72250.000	-70	-70	-70
6	72500.000	-71	-71	-70
7	72750.000	-71	-71	-71
8	73000.000	-71	-72	-71
9	73250.000	-72	-72	-71
10	73500.000	-72	-72	-72
11	73750.000	-72	-72	-72

⚠ The link will be down during the scan.

Figure 43 Frequency Scanner Page – Single Mode



Microwave radio: Frequency Scanner

Frequency Scanner

Start Frequency (MHz) 71125 (71125 ... 75875)

Stop Frequency (MHz) 75875 (71125 ... 75875)

Scanner Mode Single

Scan Status Ready

Scan Progress 100%

Frequency Scanner Band (MHz) 250.000

Last scan Date and Time 29-06-2000 19:17:01

Frequency Scanner Results

Sample Number ▲	Frequency (MHz)	RSL Sample Value (dBm)
1	71250.000	-70
2	71500.000	-71
3	71750.000	-72
4	72000.000	-71
5	72250.000	-70
6	72500.000	-71
7	72750.000	-71
8	73000.000	-71
9	73250.000	-72
10	73500.000	-72
11	73750.000	-72

⚠ The link will be down during the scan.

2 Enter a range for the scan (in MHz) by entering the lower frequency of the range in the **Start Frequency** field and the upper frequency of the range in the **Stop Frequency** field. The range of permissible values is 81000-86000 MHz on the high side and 71000-76000 MHz on the low side

3 In the **Scanner Mode** field, select from the following options:

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

Note

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

4 Click **Apply** to save the scan configuration.

5 Click **Scan**:

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

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

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

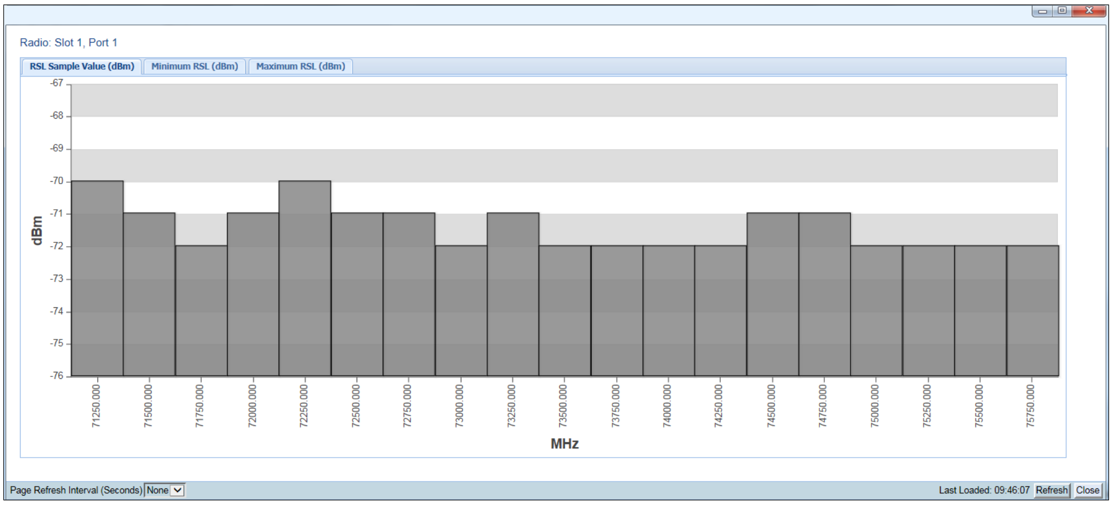
- Frequency (MHz) – The starting frequency in the scanned channel.
- RSL Sample Value (dBm) – In Single Mode, the RSL value measured for the scanned channel. In Continuous Mode, the latest RSL value measured for the scanned channel.
- Minimum RSL (dBm) – In Continuous Mode, the lowest RSL value measured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

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

The Graph page has the following tabs:

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

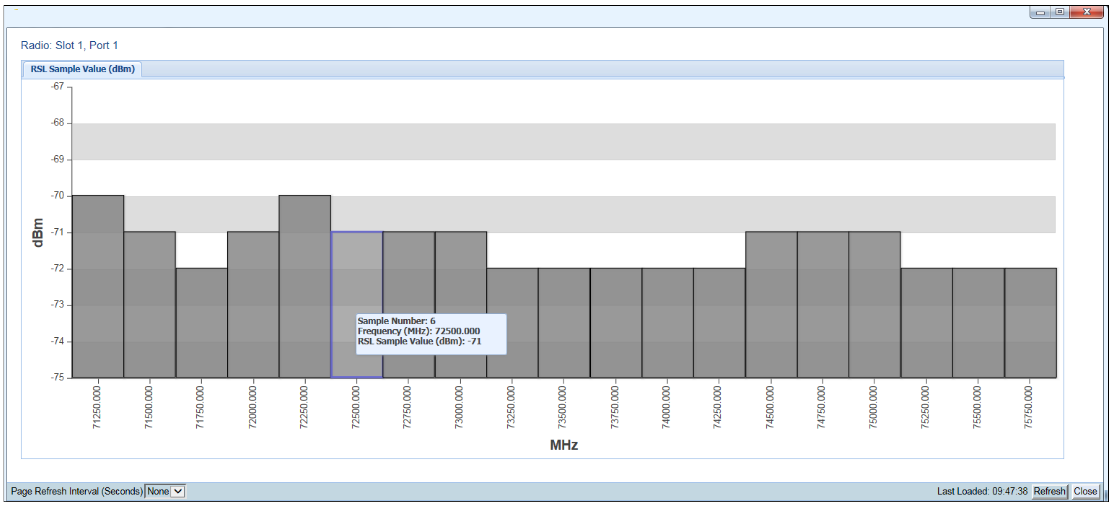
Figure 44 Frequency Scanner Results – Graph Format (Continuous Mode)


Radio: Slot 1, Port 1

Page Refresh Interval (Seconds) None

Last Loaded: 09:46:07

Figure 45 Frequency Scanner Results – Graph Format (Single Mode)


Radio: Slot 1, Port 1

Sample Number: 6
Frequency (MHz): 72500.000
RSL Sample Value (dBm): -71

Page Refresh Interval (Seconds) None

Last Loaded: 09:47:38

Configuring the Radio Parameters

In order to establish a radio link, you must:

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

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

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

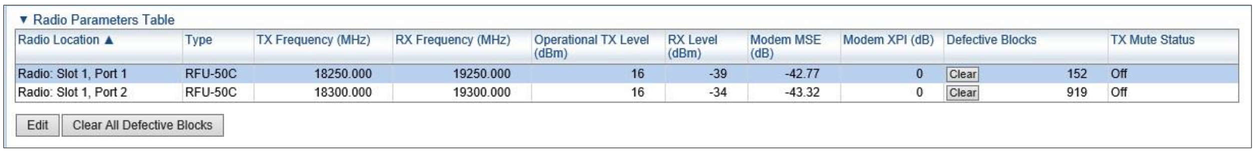
> **Note:**
>
> If you are using the default values and did not change any other parameters on the Radio Parameters page, the **Apply** button will be grayed out. To activate the **Apply** button, change any parameter on the page, then change it back to the desired value.

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

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

To configure the radio parameters:

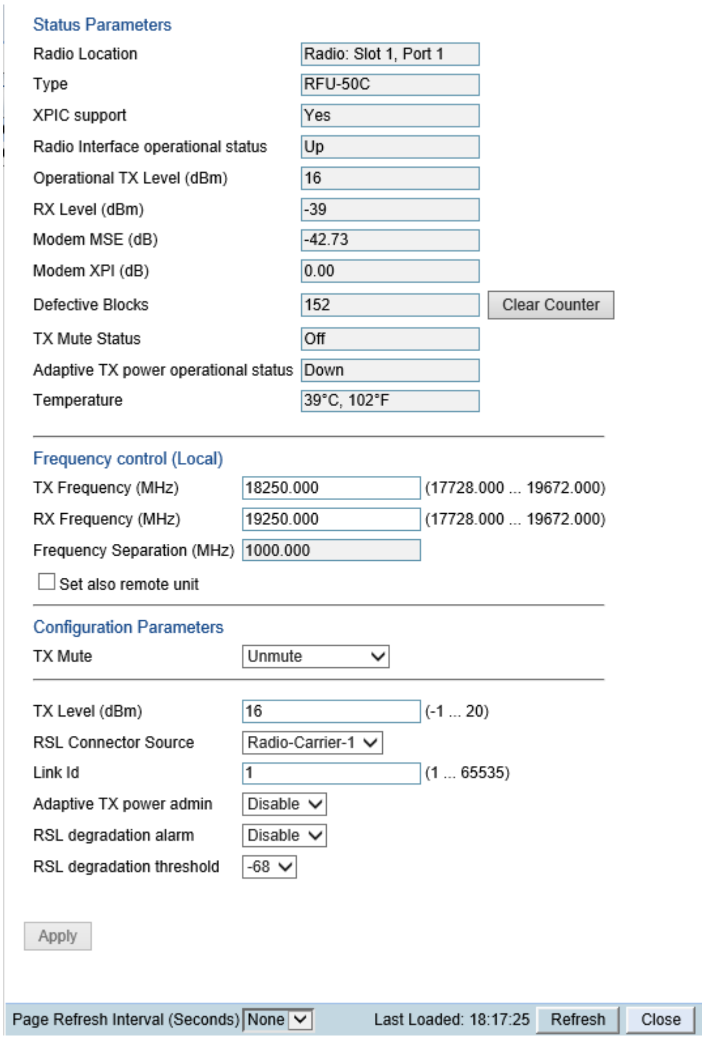
1. Select **Radio** > **Radio Parameters.** The Radio Parameters page opens.



▼ Radio Parameters Table

Radio Location ▲	Type	TX Frequency (MHz)	RX Frequency (MHz)	Operational TX Level (dBm)	RX Level (dBm)	Modem MSE (dB)	Modem XPI (dB)	Defective Blocks		TX Mute Status
Radio: Slot 1, Port 1	RFU-50C	18250.000	19250.000	16	-39	-42.77	0	Clear	152	Off
Radio: Slot 1, Port 2	RFU-50C	18300.000	19300.000	16	-34	-43.32	0	Clear	919	Off

Figure 46 Radio Parameters Page



Status Parameters

Radio Location: Radio: Slot 1, Port 1

Type: RFU-50C

XPIC support: Yes

Radio Interface operational status: Up

Operational TX Level (dBm): 16

RX Level (dBm): -39

Modem MSE (dB): -42.73

Modem XPI (dB): 0.00

Defective Blocks: 152 Clear Counter

TX Mute Status: Off

Adaptive TX power operational status: Down

Temperature: 39°C, 102°F

Frequency control (Local)

TX Frequency (MHz): 18250.000 (17728.000 ... 19672.000)

RX Frequency (MHz): 19250.000 (17728.000 ... 19672.000)

Frequency Separation (MHz): 1000.000

☐ Set also remote unit

Configuration Parameters

TX Mute: Unmute

TX Level (dBm): 16 (-1 ... 20)

RSL Connector Source: Radio-Carrier-1

Link Id: 1 (1 ... 65535)

Adaptive TX power admin: Disable

RSL degradation alarm: Disable

RSL degradation threshold: -68

Apply

Page Refresh Interval (Seconds): None Last Loaded: 18:17:25 Refresh Close

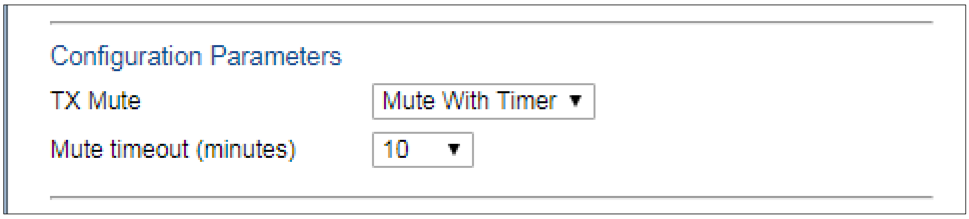
2. For multi-carrier units, select the carrier in the Radio table and click **Edit**. A separate Radio Parameters page opens.
   i. In the **TX Frequency (MHz)** field, set the transmission radio frequency in MHz.
   ii. i In the **RX Frequency (MHz)** field, set the received radio frequency in MHz.
   iii. ii Click **Apply**. The system automatically calculates and displays the frequency separation in the **Frequency Separation (MHz)** field, based on the configured TX and RX frequencies.
   iv. iii Optionally, select **Set also remote unit** to apply the frequency settings to the remote unit as well as the local unit.

Note:

Release 10.6 does not support the ability to configure the remote frequency settings.

3. Set the other radio parameters in the **Configuration parameters** section:
   i. i To mute the TX output of the radio carrier, select **Mute** in the **TX Mute** field. To unmute the TX output of the radio carrier, select **Unmute**. To configure a timed mute, select **Mute with Timer**.

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



Configuration Parameters

TX Mute: Mute With Timer

Mute timeout (minutes): 10

	Note: In contrast to an ordinary mute, a timed mute is not persistent. This means that if the unit is reset, the radio is not muted when the unit comes back online, even if the timer had not expired.

ii. In the **TX Level (dBm)** field, enter the desired TX signal level (TSL). The range of values depends on the frequency and RFU type. When **Adaptive TX power admin** is configured to **Enable**, this field determines the maximum TX level, as described below.

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

iv. The **Adaptive TX power admin** field enables or disables Adaptive TX Power. When Adaptive TX Power is enabled, the radio adjusts its TX power dynamically based on the current modulation. When the modulation is at a high level, the TX power is adjusted to the level required with the high modulation. If the modulation goes down to a lower level, the TX power increases to compensate for the lower modulation. The TX level configured in the **TX Level (dBm)** field determines the maximum TX level, but the actual TX level as shown in the **Operational TX Level (dBm)** field can be expected to be lower when the radio is operating at high modulations requiring less TX power.

To enable Adaptive TX power, select **Enable**. The **Adaptive TX power operational status** field should now indicate **Up** to indicate that the feature is fully functional.

	Note: Adaptive TX Power only operates when the MRMC script is configured to Adaptive mode. If the script is configured to Fixed mode (or Adaptive mode with the Minimum and Maximum Profile set to the same value), you can set **Adaptive TX Power** to **Enable**, but the **Adaptive TX power operational status** field will indicate **Down**. Adaptive TX Power is not supported with release 10.6.

v. In the **RSL degradation alarm** field, select **Enable** if you want the unit to generate an alarm in the event that the RSL falls beneath the threshold defined in the **RSL degradation threshold** field. The range of values is -99 to 0. By default, the alarm is disabled, with a default degradation threshold of -68 dBm. The RSL degradation alarm is alarm ID 1610, *Radio Receive Signal Level is below the configured threshold*.

The alarm is cleared when the RSL goes above the configured threshold. The alarm is masked if the radio interface is disabled, the radio does not exist, or a communication-failure alarm (Alarm ID #1703) is raised.

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

Creating Service(s) for Traffic

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

Configuring CPRI

Optionally, PTP 850E can be used with a CPRI module. The CPRI module is inserted in the PTP 850E’s QSFP port (P4), and provides up to 10 Gbps capacity for CPRI traffic. The CPRI module converts CPRI signals to Ethernet and Ethernet to CPRI in accordance with Radio over Ethernet (RoE) standard IEEE 1914.3 and CPRI specification v7.0. For more details, see the Technical Description for PTP 850E.

Note: Support for CPRI is planned for future release.

CPRI Configuration Overview

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

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

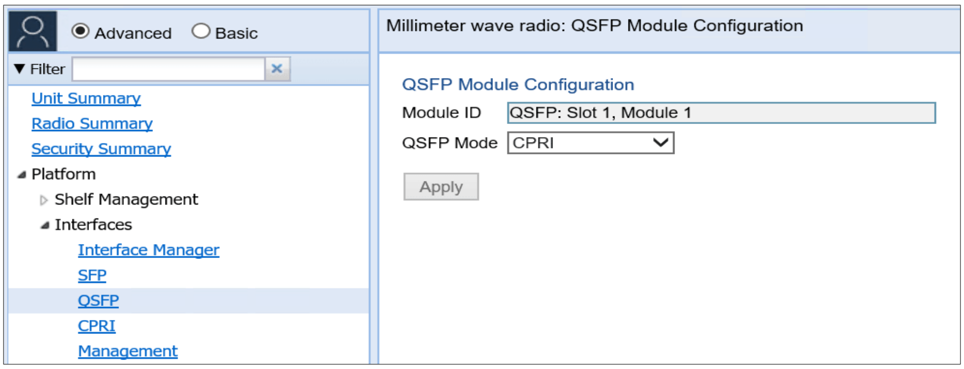
Once these conditions are met, the following configurations must be made for P4:

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

Setting the QSFP Mode to CPRI

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

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



Millimeter wave radio: QSFP Module Configuration

QSFP Module Configuration

Module ID: QSFP: Slot 1, Module 1

QSFP Mode: CPRI

Figure 51: QSFP Module Configuration Page – CPRI

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

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

- CPRI Slot 1 Port 1

Creating an Ethernet Service for CPRI Traffic

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

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

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

Configuring Synchronization for CPRI Traffic

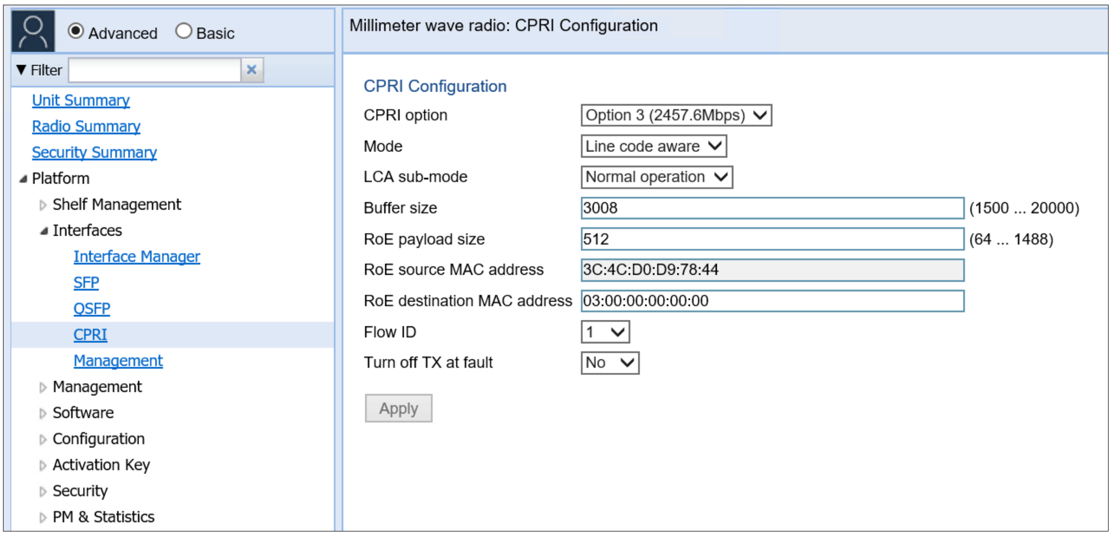
Synchronization for the CPRI module should be configured as follows:

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

Configuring the CPRI Parameters

To configure the CPRI parameters:

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



Millimeter wave radio: CPRI Configuration

CPRI Configuration

CPRI option	Option 3 (2457.6Mbps)	
Mode	Line code aware	
LCA sub-mode	Normal operation	
Buffer size	3008	(1500 ... 20000)
RoE payload size	512	(64 ... 1488)
RoE source MAC address	3C:4C:D0:D9:78:44	
RoE destination MAC address	03:00:00:00:00:00	
Flow ID	1	
Turn off TX at fault	No	

Figure 52: CPRI Configuration Page

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

The following options are available:

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

Note: **Option 4** and **Option 6** also appear in the drop-down list, but these options are not supported. Make sure to select one of the options listed above.

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

The following options are available:

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

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

The following options are available:

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

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

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

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

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

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

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

Note: The **RoE source MAC address** field is read only, and displays the MAC address of the CPRI module in the unit you are configuring.

- In the **RoE destination MAC address** field, enter the following:

- If the CPRI module is connected to a BBU, enter the MAC address of the CPRI module connected to the RRH.
- If the CPRI module is connected to a RRH, enter the MAC address of the CPRI module connected to the BBU.

- In the **Flow ID** field, select an ID to be used in the RoE conversion. Options are 0-10. The default is 1. This parameter must be set to the same value on both sides of the CPRI link.

- In the **Turn off TX at fault** field, select **No** (default) or **Yes**.
  If this parameter is set to **Yes**, the TX is turned off if a fault is discovered.
- Click **Apply**.

Enabling the CPRI Port

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

Chapter 3: Configuration Guide

System Configurations

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

Table 15 System Configurations

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

Chapter 4: Configuring an PTP 850 Unit Using Basic Mode

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

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

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

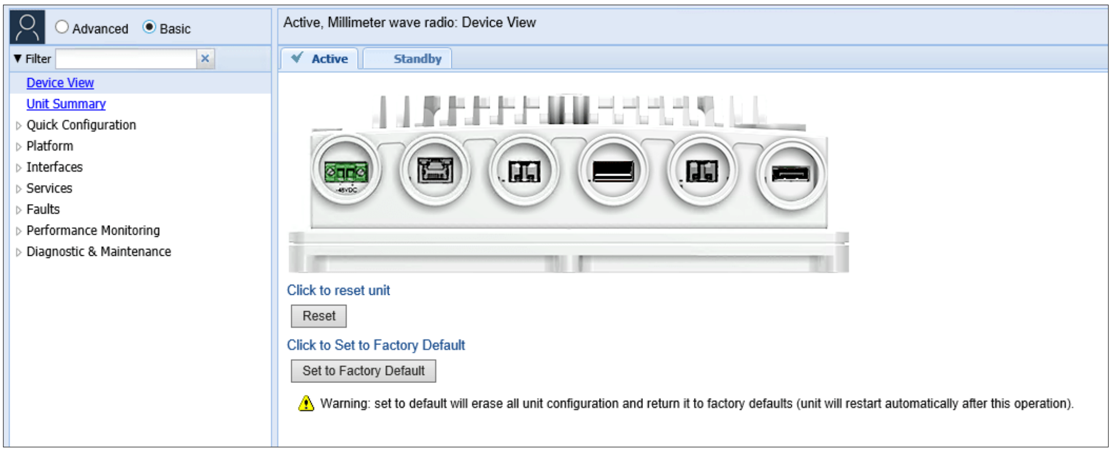
default configuration settings.

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

Device View

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

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



Active, Millimeter wave radio: Device View

Click to reset unit

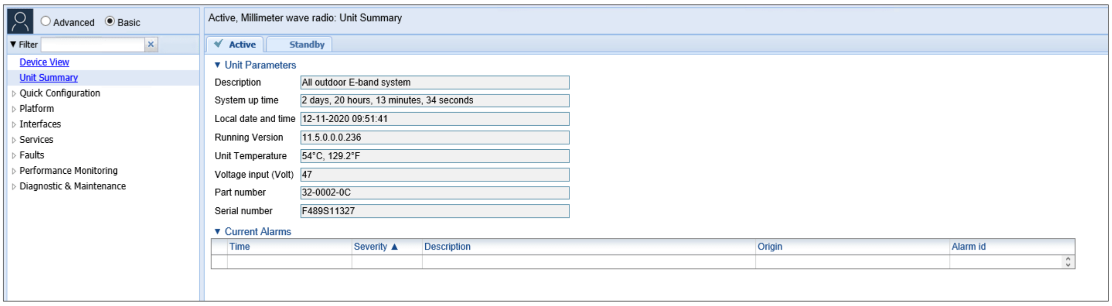
Click to Set to Factory Default

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

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

Unit Summary

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



Active, Millimeter wave radio: Unit Summary

▼ Unit Parameters

Description	All outdoor E-band system
System up time	2 days, 20 hours, 13 minutes, 34 seconds
Local date and time	12-11-2020 09:51:41
Running Version	11.5.0.0.0.236
Unit Temperature	54°C, 129.2°F
Voltage input (Volt)	47
Part number	32-0002-0C
Serial number	F489S11327

▼ Current Alarms

Time	Severity ▲	Description	Origin	Alarm id

Figure 54: Basic Mode – Unit Summary Page

Quick Configuration

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

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

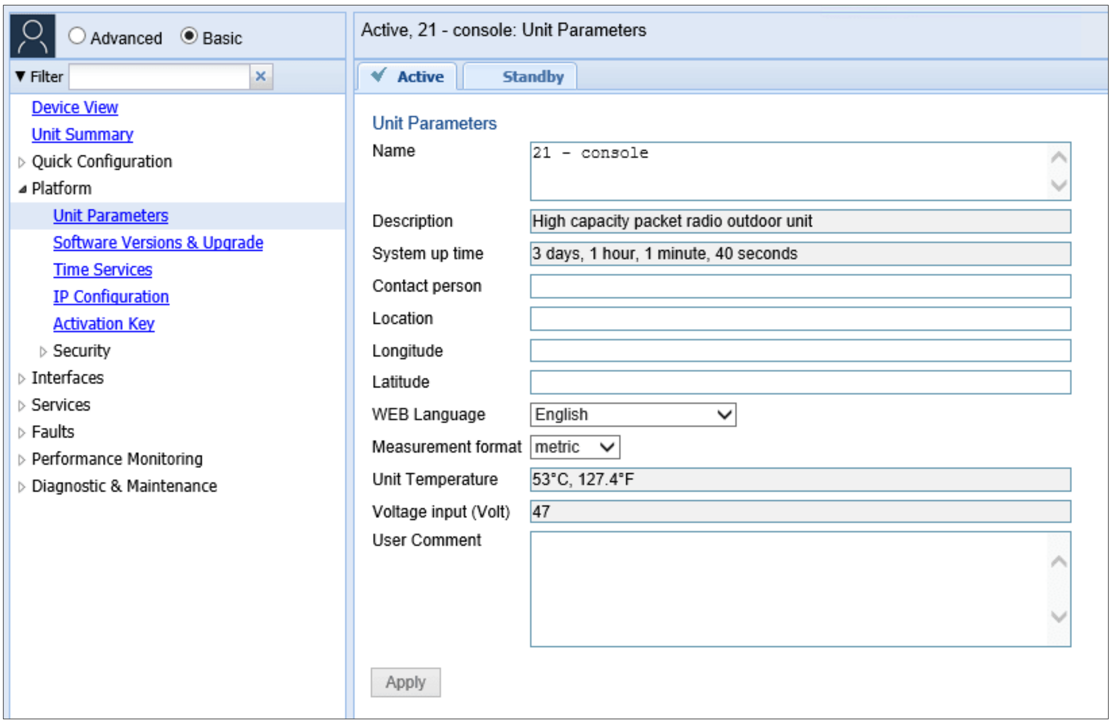
Platform

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

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

Unit Parameters Page

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



Active, 21 - console: Unit Parameters

Unit Parameters

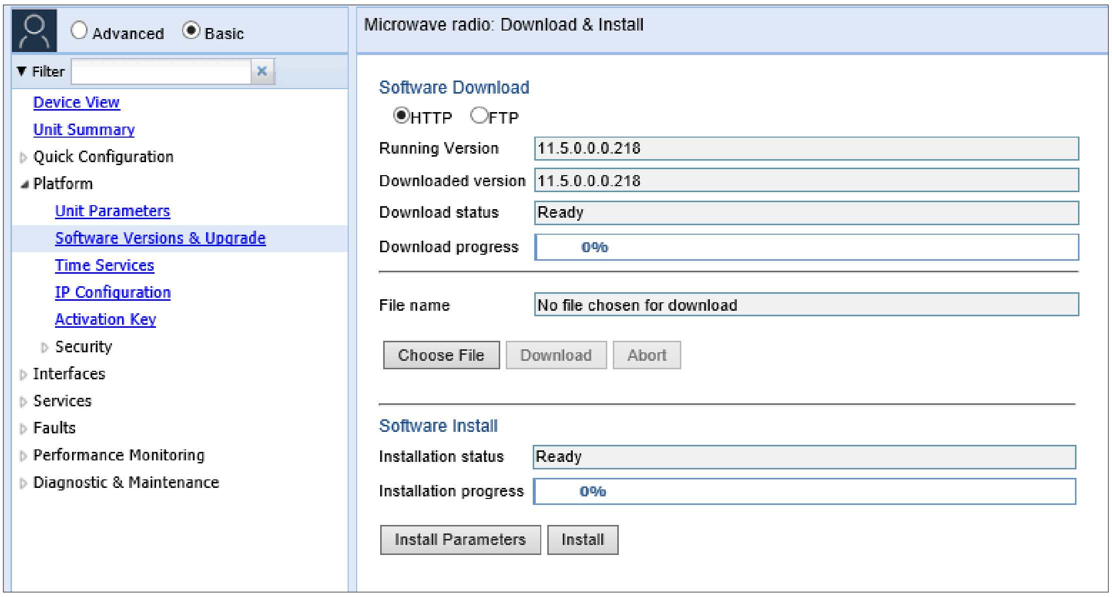
Name	21 – console
Description	High capacity packet radio outdoor unit
System up time	3 days, 1 hour, 1 minute, 40 seconds
Contact person	
Location	
Longitude	
Latitude	
WEB Language	English
Measurement format	metric
Unit Temperature	53°C, 127.4°F
Voltage input (Volt)	47
User Comment	

Figure 55: Basic Mode – Unit Parameters Page

Software Versions & Upgrade Page

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

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



Microwave radio: Download & Install

Software Download

●HTTP ○FTP

Running Version	11.5.0.0.0.218
Downloaded version	11.5.0.0.0.218
Download status	Ready
Download progress	0%
File name	No file chosen for download

Software Install

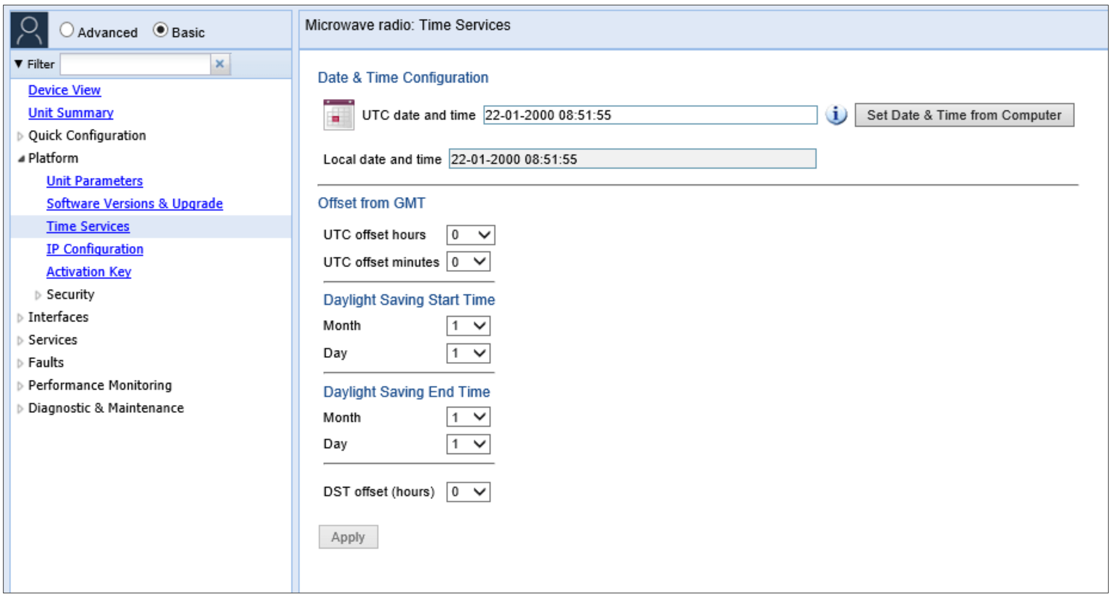
Installation status	Ready
Installation progress	0%

Figure 56: Basic Mode – Software Versions & Upgrade Page

Time Services Page

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

Setting the Time and Date (Optional).



Microwave radio: Time Services

Date & Time Configuration

UTC date and time: 22-01-2000 08:51:55

Local date and time: 22-01-2000 08:51:55

Offset from GMT

UTC offset hours: 0

UTC offset minutes: 0

Daylight Saving Start Time

Month: 1

Day: 1

Daylight Saving End Time

Month: 1

Day: 1

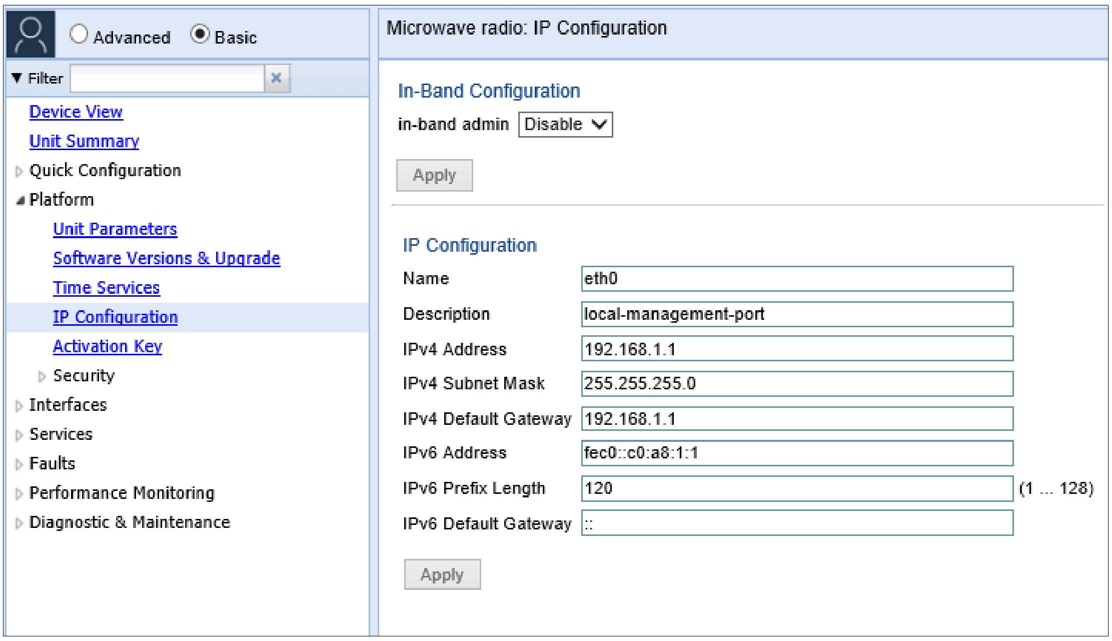
DST offset (hours): 0

Figure 57: Basic Mode – Software Versions & Upgrade Page

IP Configuration Page

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

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



Microwave radio: IP Configuration

In-Band Configuration

in-band admin: Disable

IP Configuration

Name: eth0

Description: local-management-port

IPv4 Address: 192.168.1.1

IPv4 Subnet Mask: 255.255.255.0

IPv4 Default Gateway: 192.168.1.1

IPv6 Address: fec0::c0:a8:1:1

IPv6 Prefix Length: 120 (1 ... 128)

IPv6 Default Gateway: ::

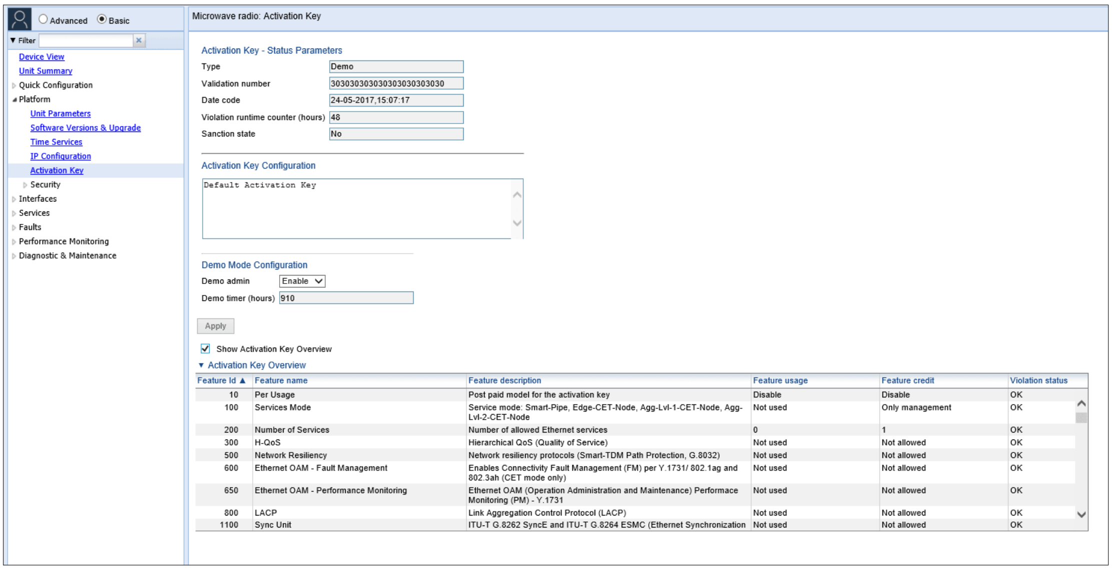
Figure 58: Basic Mode – IP Configuration Page

Activation Key Page

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

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

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



Microwave radio: Activation Key

Activation Key - Status Parameters

Type	Demo
Validation number	30303030303030303030303030
Date code	24-05-2017,15:07:17
Violation runtime counter (hours)	48
Sanction state	No

Activation Key Configuration

```
Default Activation Key
```

Demo Mode Configuration

Demo admin: Enable

Demo timer (hours): 910

☑ Show Activation Key Overview

▼ Activation Key Overview

Feature Id ▲	Feature name	Feature description	Feature usage	Feature credit	Violation status
10	Per Usage	Post paid model for the activation key	Disable	Disable	OK
100	Services Mode	Service mode: Smart-Pipe, Edge-CET-Node, Agg-Lvl-1-CET-Node, Agg-Lvl-2-CET-Node	Not used	Only management	OK
200	Number of Services	Number of allowed Ethernet services	0	1	OK
300	H-QoS	Hierarchical QoS (Quality of Service)	Not used	Not allowed	OK
500	Network Resiliency	Network resiliency protocols (Smart-TDM Path Protection, G.8032)	Not used	Not allowed	OK
600	Ethernet OAM - Fault Management	Enables Connectivity Fault Management (FM) per Y.1731/ 802.1ag and 802.3ah (CET mode only)	Not used	Not allowed	OK
650	Ethernet OAM - Performance Monitoring	Ethernet OAM (Operation Administration and Maintenance) Performace Monitoring (PM) - Y.1731	Not used	Not allowed	OK
800	LACP	Link Aggregation Control Protocol (LACP)	Not used	Not allowed	OK
1100	Sync Unit	ITU-T G.8262 SyncE and ITU-T G.8264 ESMC (Ethernet Synchronization	Not used	Not allowed	OK

Figure 59: Basic Mode – Activation Key Page

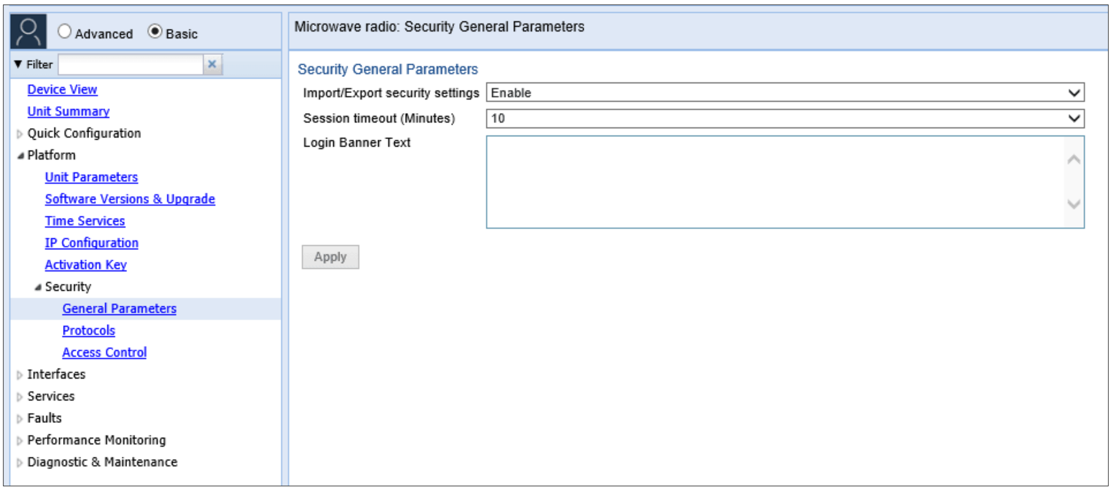
Security Pages

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

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

General Parameters Page

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



Microwave radio: Security General Parameters

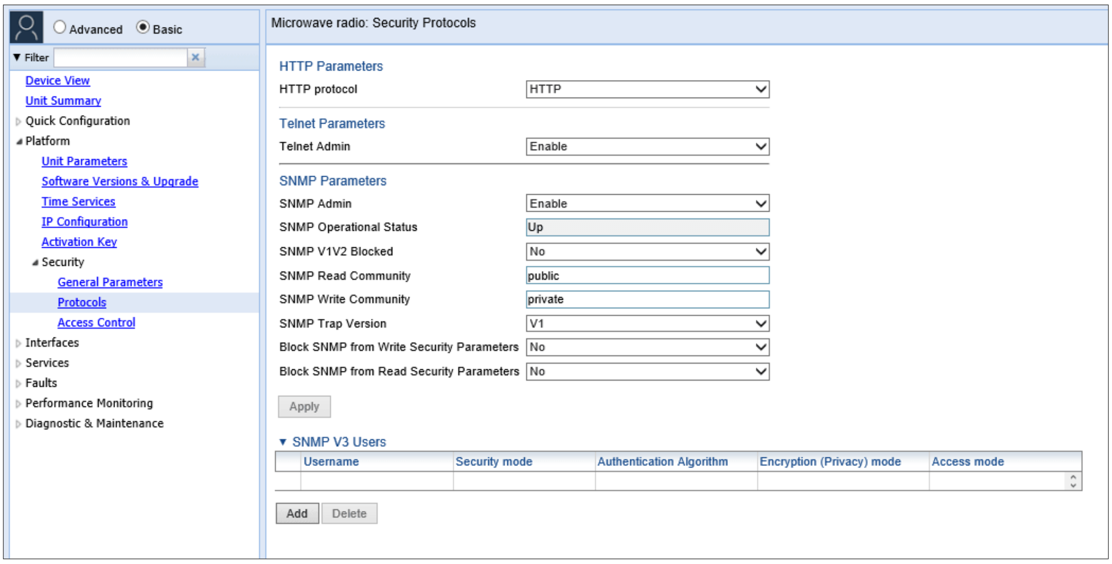
Security General Parameters

Import/Export security settings	Enable
Session timeout (Minutes)	10
Login Banner Text	

Figure 60: Basic Mode – Security – General Parameters Page

Protocols Page

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



Microwave radio: Security Protocols

HTTP Parameters

HTTP protocol	HTTP

Telnet Parameters

Telnet Admin	Enable

SNMP Parameters

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

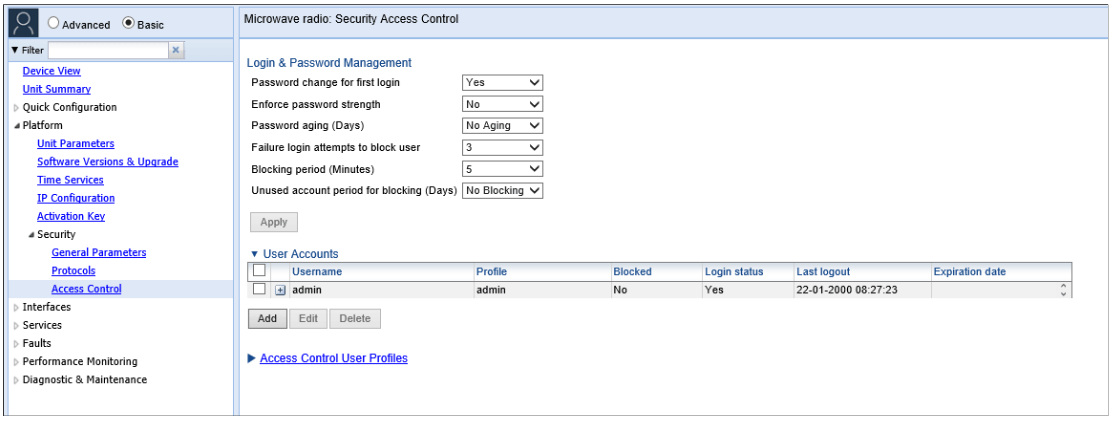
▼ SNMP V3 Users

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

Figure 61: Basic Mode – Security – Protocols Page

Access Control Page

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



Microwave radio: Security Access Control

Login & Password Management

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

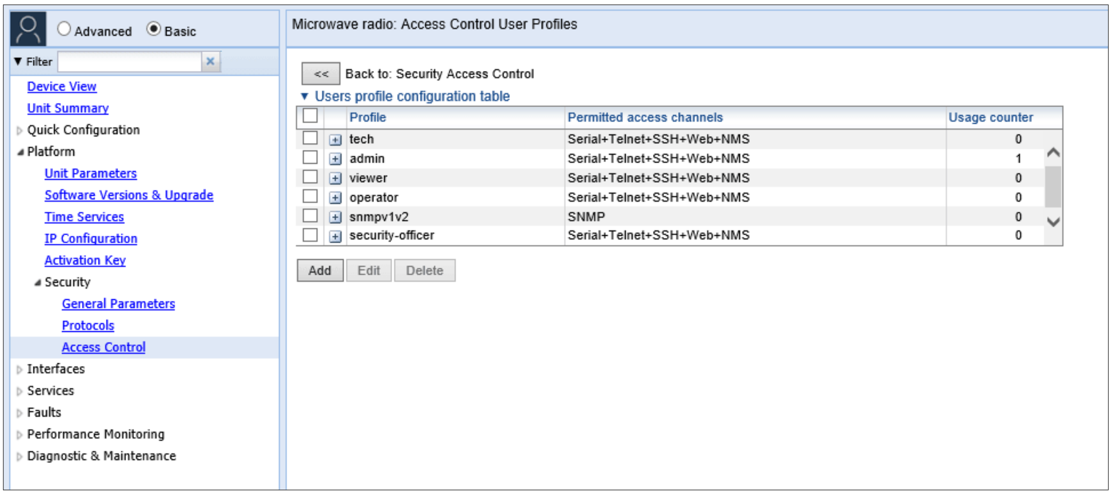
▼ User Accounts

□		Username	Profile	Blocked	Login status	Last logout	Expiration date
□	⊞	admin	admin	No	Yes	22-01-2000 08:27:23	

▶ Access Control User Profiles

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

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



Microwave radio: Access Control User Profiles

Back to: Security Access Control

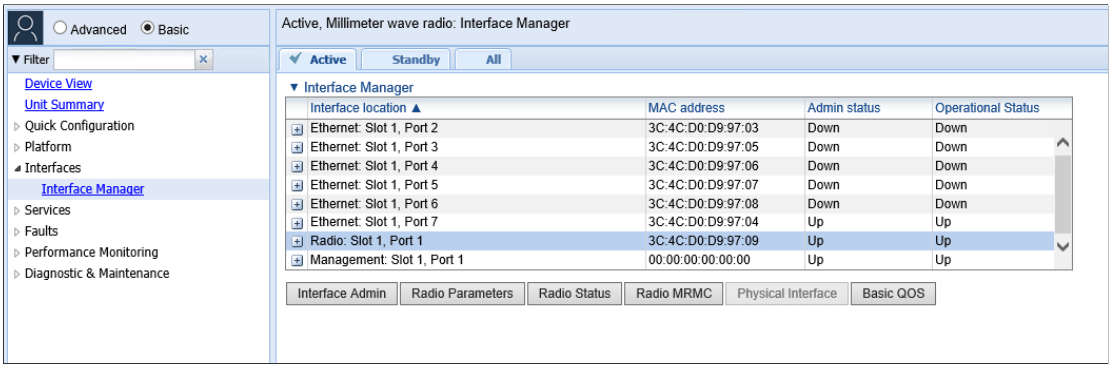
▼ Users profile configuration table

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

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

Interfaces

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



Active, Millimeter wave radio: Interface Manager

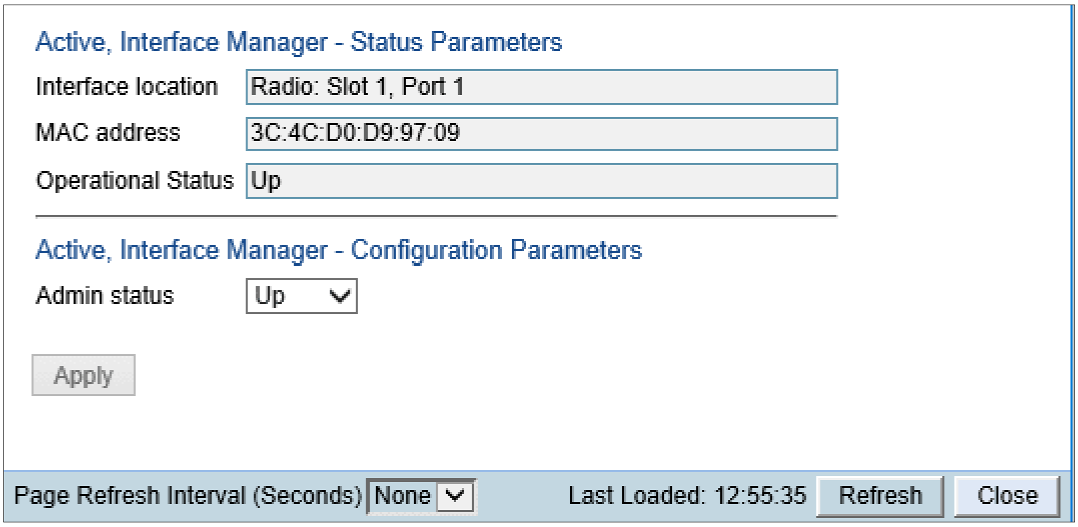
▼ Interface Manager

	Interface location ▲	MAC address	Admin status	Operational Status
⊞	Ethernet: Slot 1, Port 2	3C:4C:D0:D9:97:03	Down	Down
⊞	Ethernet: Slot 1, Port 3	3C:4C:D0:D9:97:05	Down	Down
⊞	Ethernet: Slot 1, Port 4	3C:4C:D0:D9:97:06	Down	Down
⊞	Ethernet: Slot 1, Port 5	3C:4C:D0:D9:97:07	Down	Down
⊞	Ethernet: Slot 1, Port 6	3C:4C:D0:D9:97:08	Down	Down
⊞	Ethernet: Slot 1, Port 7	3C:4C:D0:D9:97:04	Up	Up
⊞	Radio: Slot 1, Port 1	3C:4C:D0:D9:97:09	Up	Up
⊞	Management: Slot 1, Port 1	00:00:00:00:00:00	Up	Up

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

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

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



Active, Interface Manager - Status Parameters

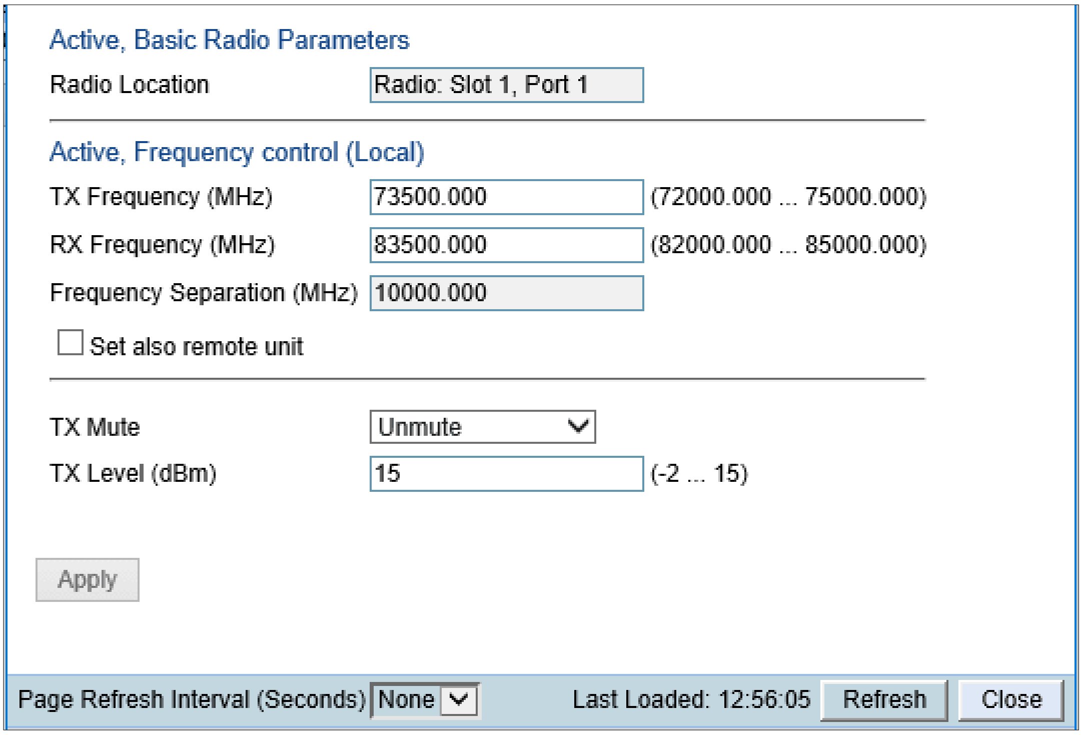
Interface location	Radio: Slot 1, Port 1
MAC address	3C:4C:D0:D9:97:09
Operational Status	Up

Active, Interface Manager - Configuration Parameters

Admin status	Up

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

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



Active, Basic Radio Parameters

Radio Location	Radio: Slot 1, Port 1

Active, Frequency control (Local)

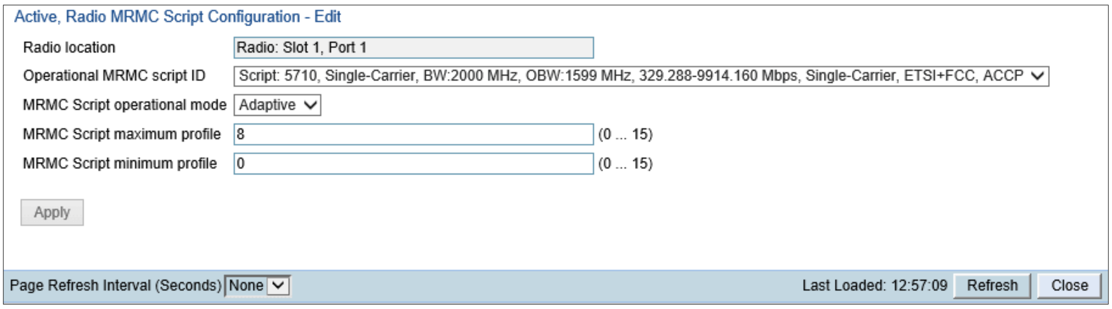
TX Frequency (MHz)	73500.000	(72000.000 ... 75000.000)
RX Frequency (MHz)	83500.000	(82000.000 ... 85000.000)
Frequency Separation (MHz)	10000.000	

☐ Set also remote unit

TX Mute	Unmute	
TX Level (dBm)	15	(-2 ... 15)

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

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

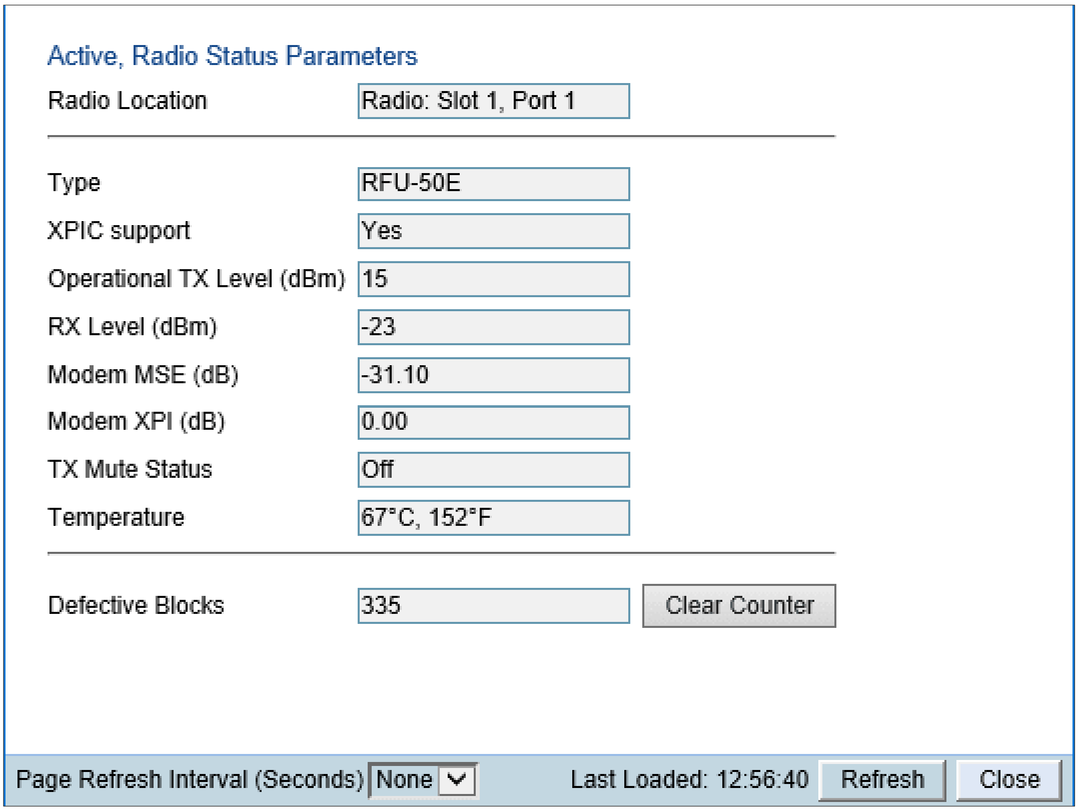


Active, Radio MRMC Script Configuration - Edit

Radio location	Radio: Slot 1, Port 1
Operational MRMC script ID	Script: 5710, Single-Carrier, BW:2000 MHz, OBW:1599 MHz, 329.288-9914.160 Mbps, Single-Carrier, ETSI+FCC, ACCP
MRMC Script operational mode	Adaptive
MRMC Script maximum profile	8 (0 ... 15)
MRMC Script minimum profile	0 (0 ... 15)

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

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

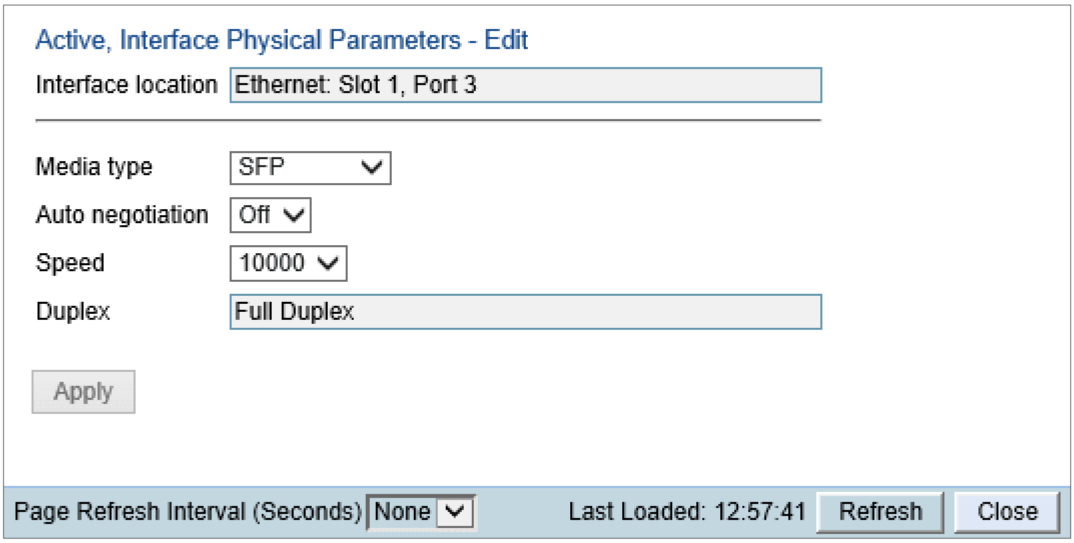


Active, Radio Status Parameters

Radio Location	Radio: Slot 1, Port 1
Type	RFU-50E
XPIC support	Yes
Operational TX Level (dBm)	15
RX Level (dBm)	-23
Modem MSE (dB)	-31.10
Modem XPI (dB)	0.00
TX Mute Status	Off
Temperature	67°C, 152°F
Defective Blocks	335

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

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



Active, Interface Physical Parameters - Edit

Interface location: Ethernet: Slot 1, Port 3

Media type: SFP

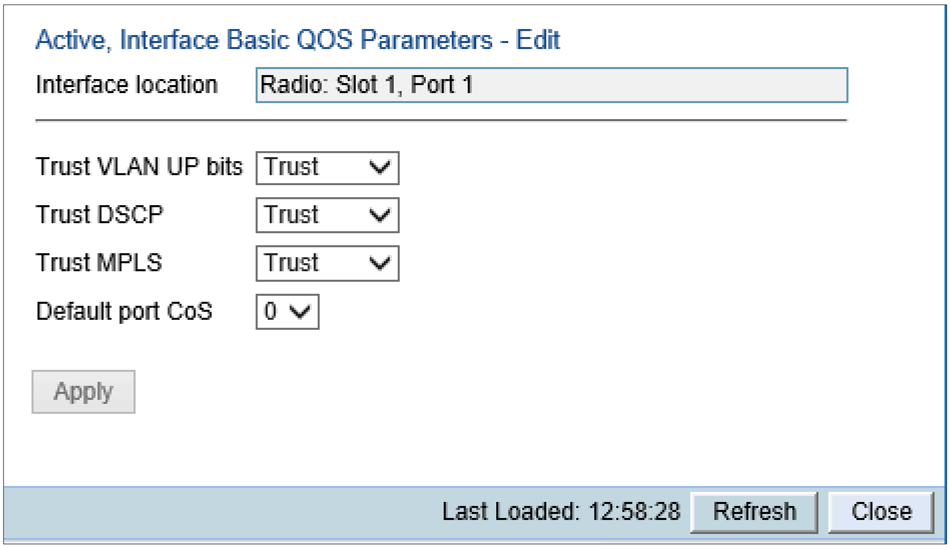
Auto negotiation: Off

Speed: 10000

Duplex: Full Duplex

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

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



Active, Interface Basic QOS Parameters - Edit

Interface location: Radio: Slot 1, Port 1

Trust VLAN UP bits: Trust

Trust DSCP: Trust

Trust MPLS: Trust

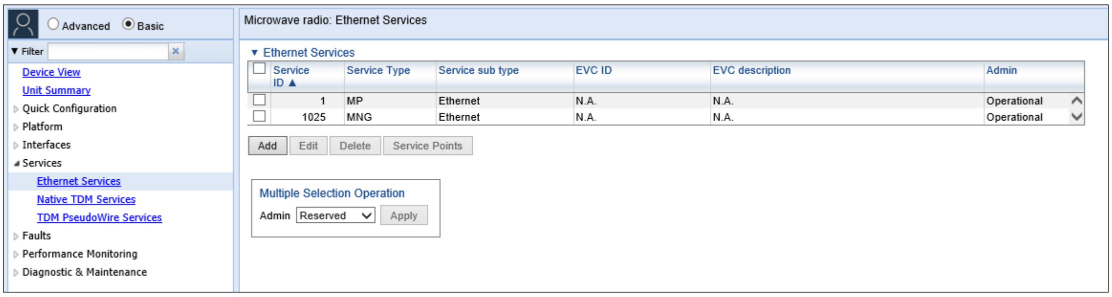
Default port CoS: 0

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

Services

The Services menu enables you to create Ethernet services.

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



Microwave radio: Ethernet Services

▼ Ethernet Services

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

Multiple Selection Operation

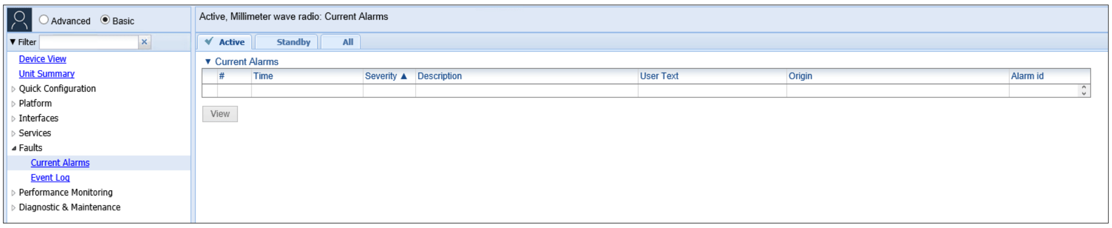
Admin: Reserved

Figure 71: Basic Mode – Ethernet Services

Faults

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

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



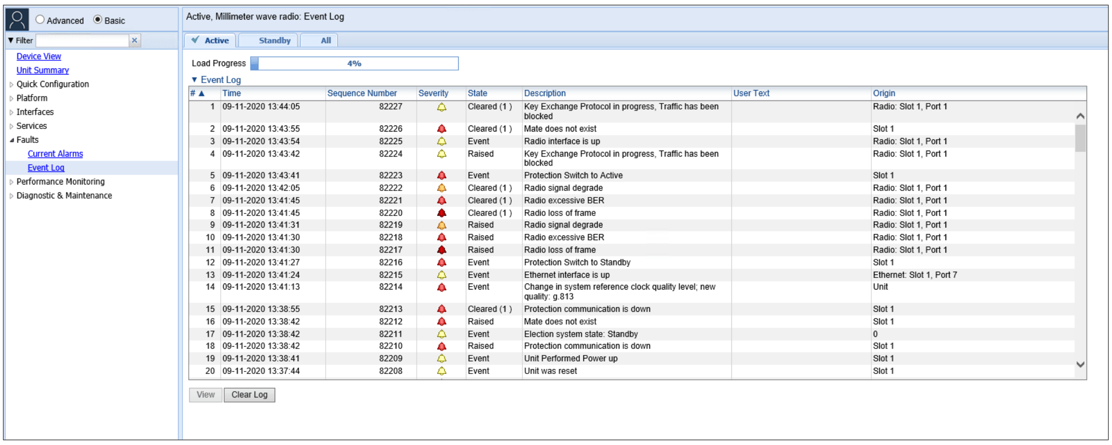
Active, Millimeter wave radio: Current Alarms

▼ Current Alarms

#	Time	Severity ▲	Description	User Text	Origin	Alarm id

Figure 72: Basic Mode – Current Alarms

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



Active, Millimeter wave radio: Event Log

Load Progress 4%

▼ Event Log

# ▲	Time	Sequence Number	Severity	State	Description	User Text	Origin
1	09-11-2020 13:44:05	82227	🔔	Cleared (1)	Key Exchange Protocol in progress, Traffic has been blocked		Radio: Slot 1, Port 1
2	09-11-2020 13:43:55	82226	🔔	Cleared (1)	Mate does not exist		Slot 1
3	09-11-2020 13:43:54	82225	🔔	Event	Radio interface is up		Radio: Slot 1, Port 1
4	09-11-2020 13:43:42	82224	🔔	Raised	Key Exchange Protocol in progress, Traffic has been blocked		Radio: Slot 1, Port 1
5	09-11-2020 13:43:41	82223	🔔	Event	Protection Switch to Active		Slot 1
6	09-11-2020 13:42:05	82222	🔔	Cleared (1)	Radio signal degrade		Radio: Slot 1, Port 1
7	09-11-2020 13:41:45	82221	🔔	Cleared (1)	Radio excessive BER		Radio: Slot 1, Port 1
8	09-11-2020 13:41:45	82220	🔔	Cleared (1)	Radio loss of frame		Radio: Slot 1, Port 1
9	09-11-2020 13:41:31	82219	🔔	Raised	Radio signal degrade		Radio: Slot 1, Port 1
10	09-11-2020 13:41:30	82218	🔔	Raised	Radio excessive BER		Radio: Slot 1, Port 1
11	09-11-2020 13:41:30	82217	🔔	Raised	Radio loss of frame		Radio: Slot 1, Port 1
12	09-11-2020 13:41:27	82216	🔔	Event	Protection Switch to Standby		Slot 1
13	09-11-2020 13:41:24	82215	🔔	Event	Ethernet interface is up		Ethernet: Slot 1, Port 7
14	09-11-2020 13:41:13	82214	🔔	Event	Change in system reference clock quality level; new quality: g.813		Unit
15	09-11-2020 13:38:55	82213	🔔	Cleared (1)	Protection communication is down		Slot 1
16	09-11-2020 13:38:42	82212	🔔	Raised	Mate does not exist		Slot 1
17	09-11-2020 13:38:42	82211	🔔	Event	Election system state: Standby		0
18	09-11-2020 13:38:42	82210	🔔	Raised	Protection communication is down		Slot 1
19	09-11-2020 13:38:41	82209	🔔	Event	Unit Performed Power up		Slot 1
20	09-11-2020 13:37:44	82208	🔔	Event	Unit was reset		Slot 1

Figure 73: Basic Mode – Event Log

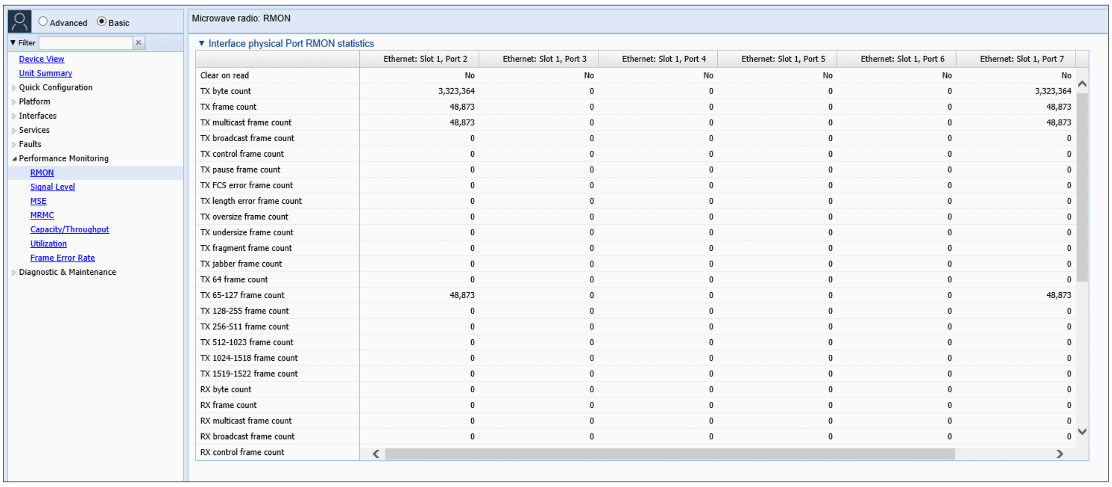
Performance Monitoring

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

- RMON
- Signal Level
- MSE
- MRMC
- Capacity/Throughput
- Utilization
- Frame Error Rate

RMON

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



Microwave radio: RMON

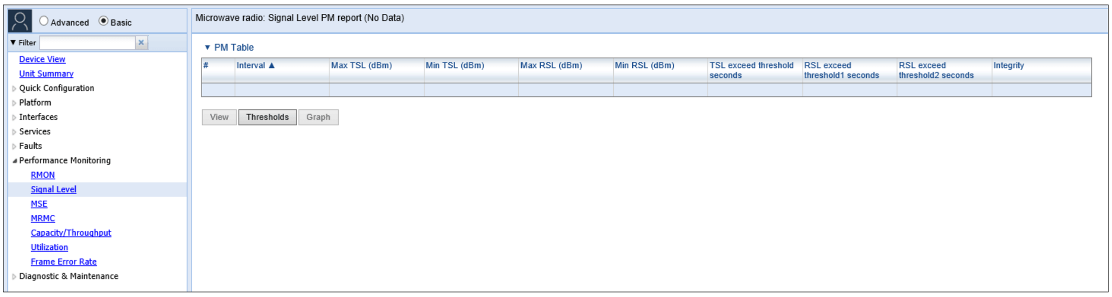
▼ Interface physical Port RMON statistics

	Ethernet: Slot 1, Port 2	Ethernet: Slot 1, Port 3	Ethernet: Slot 1, Port 4	Ethernet: Slot 1, Port 5	Ethernet: Slot 1, Port 6	Ethernet: Slot 1, Port 7
Clear on read	No	No	No	No	No	No
TX byte count	3,323,364	0	0	0	0	3,323,364
TX frame count	48,873	0	0	0	0	48,873
TX multicast frame count	48,873	0	0	0	0	48,873
TX broadcast frame count	0	0	0	0	0	0
TX control frame count	0	0	0	0	0	0
TX pause frame count	0	0	0	0	0	0
TX FCS error frame count	0	0	0	0	0	0
TX length error frame count	0	0	0	0	0	0
TX oversize frame count	0	0	0	0	0	0
TX undersize frame count	0	0	0	0	0	0
TX fragment frame count	0	0	0	0	0	0
TX jabber frame count	0	0	0	0	0	0
TX 64 frame count	0	0	0	0	0	0
TX 65-127 frame count	48,873	0	0	0	0	48,873
TX 128-255 frame count	0	0	0	0	0	0
TX 256-511 frame count	0	0	0	0	0	0
TX 512-1023 frame count	0	0	0	0	0	0
TX 1024-1518 frame count	0	0	0	0	0	0
TX 1519-1522 frame count	0	0	0	0	0	0
RX byte count	0	0	0	0	0	0
RX frame count	0	0	0	0	0	0
RX multicast frame count	0	0	0	0	0	0
RX broadcast frame count	0	0	0	0	0	0
RX control frame count						

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

Signal Level

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



Microwave radio: Signal Level PM report (No Data)

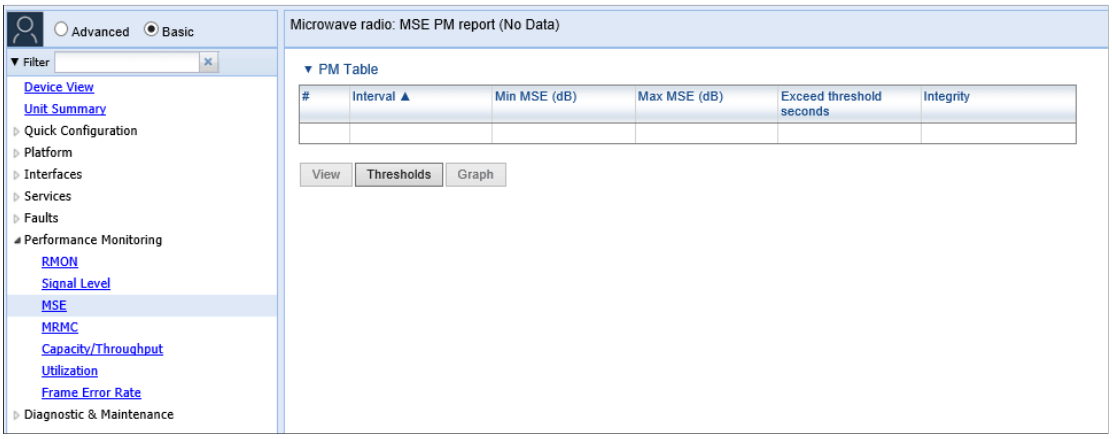
▼ PM Table

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

Figure 75: Basic Mode – Signal Level Page

MSE

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



Microwave radio: MSE PM report (No Data)

▼ PM Table

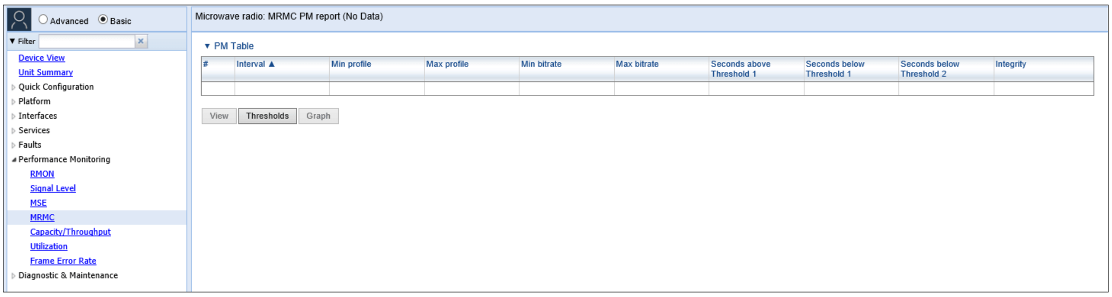
#	Interval ▲	Min MSE (dB)	Max MSE (dB)	Exceed threshold seconds	Integrity

Figure 76: Basic Mode – MSE Page

MRMC

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

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



Microwave radio: MRMC PM report (No Data)

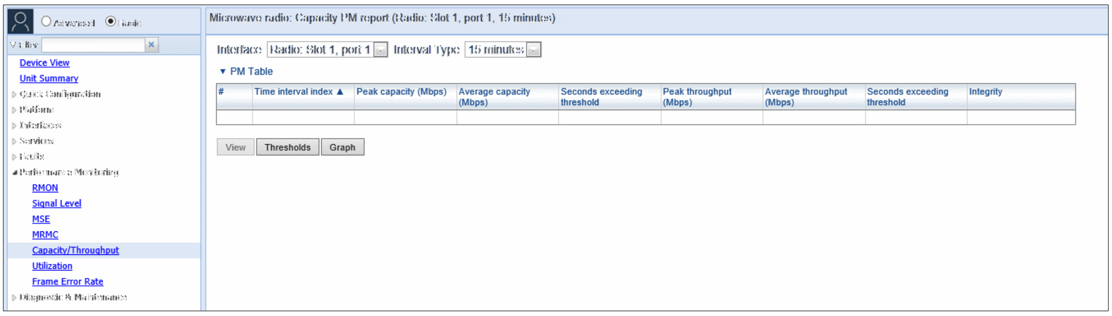
▼ PM Table

#	Interval ▲	Min profile	Max profile	Min bitrate	Max bitrate	Seconds above Threshold 1	Seconds below Threshold 1	Seconds below Threshold 2	Integrity

Figure 77: Basic Mode – MRMC Page

Capacity/Throughput

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



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

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

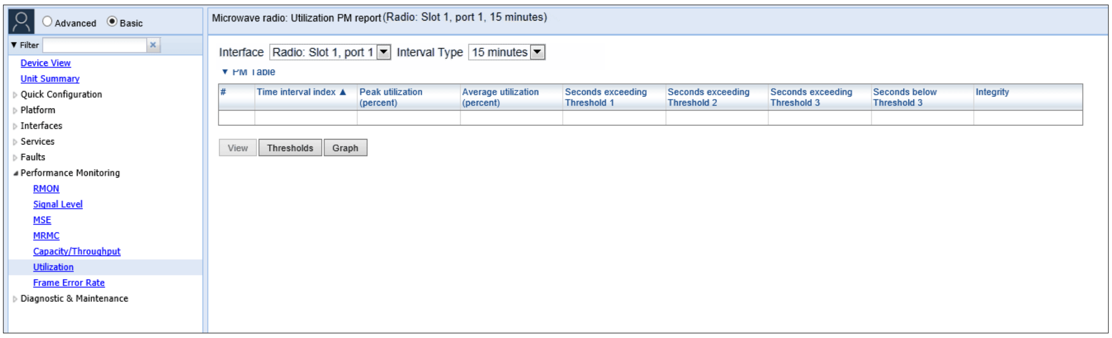
▼ PM Table

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

Figure 78: Basic Mode – Capacity/Throughput Page

Utilization

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



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

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

▼ PM Table

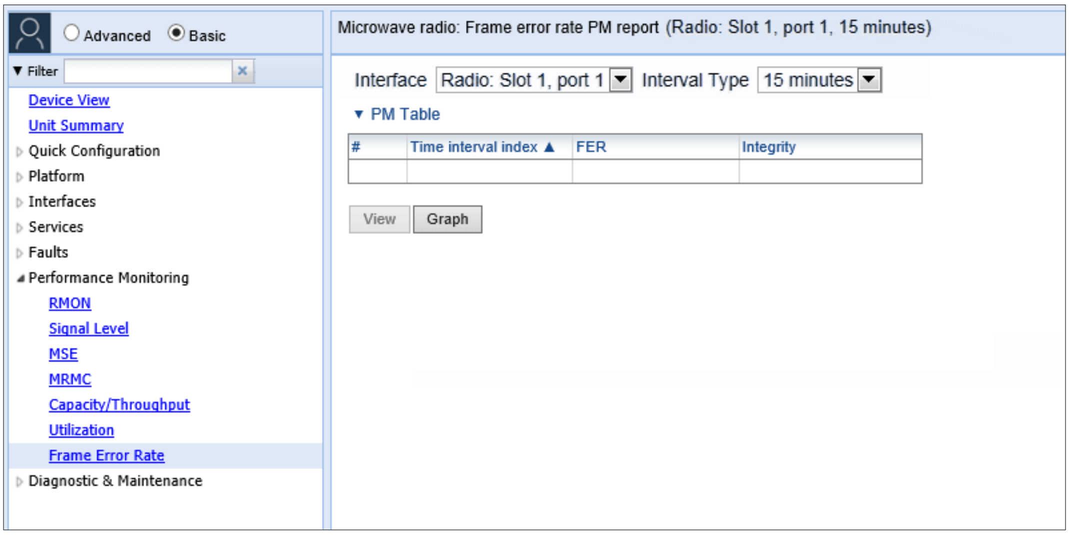
#	Time interval index ▲	Peak utilization (percent)	Average utilization (percent)	Seconds exceeding Threshold 1	Seconds exceeding Threshold 2	Seconds exceeding Threshold 3	Seconds below Threshold 3	Integrity

Figure 79: Basic Mode – Utilization Page

Frame Error Rate

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

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



Microwave radio: Frame error rate PM report (Radio: Slot 1, port 1, 15 minutes)

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

▼ PM Table

#	Time interval index ▲	FER	Integrity

Figure 80: Basic Mode – Frame Error Rate Page

Diagnostic & Maintenance

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

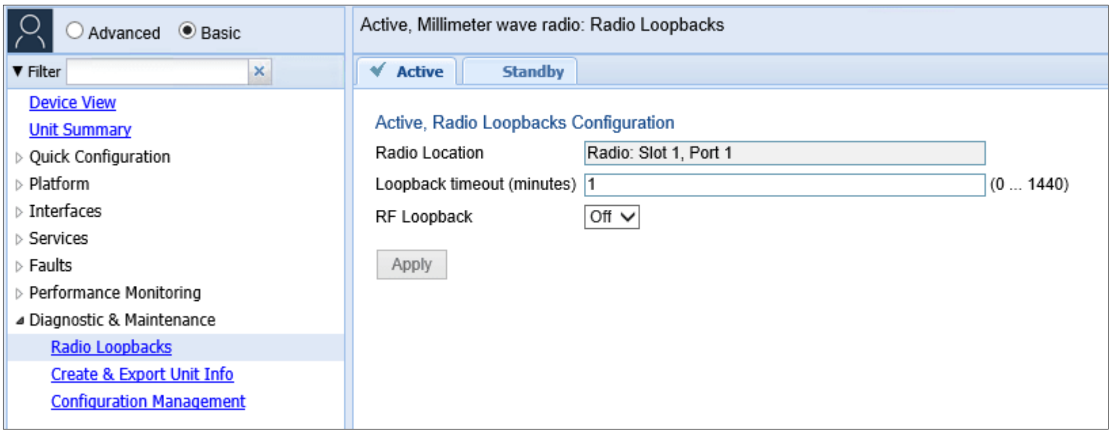
- *Radio Loopback* – Perform radio loopback
- *Unit Info* – Generate and export a user info file, used primarily for troubleshooting.
- *Configuration Management* – Import and export unit configuration files, used to backup and restore system configurations.

Radio Loopback

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

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

Performing Radio Loopback.



Active, Millimeter wave radio: Radio Loopbacks

Active, Radio Loopbacks Configuration

Radio Location: Radio: Slot 1, Port 1

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

RF Loopback: Off

Figure 81: Basic Mode – Radio Loopbacks Page

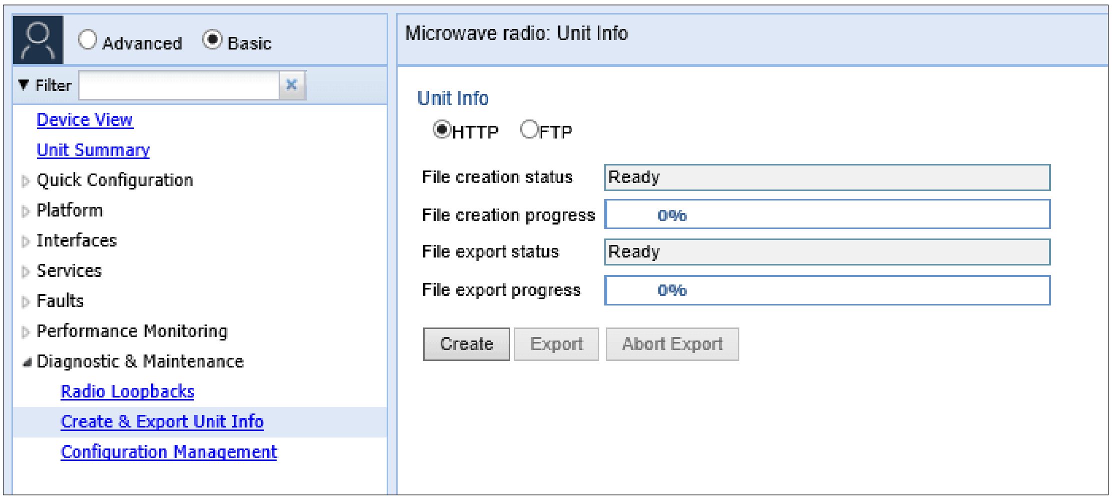
Unit Info

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

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

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

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



Microwave radio: Unit Info

Unit Info

● HTTP ○ FTP

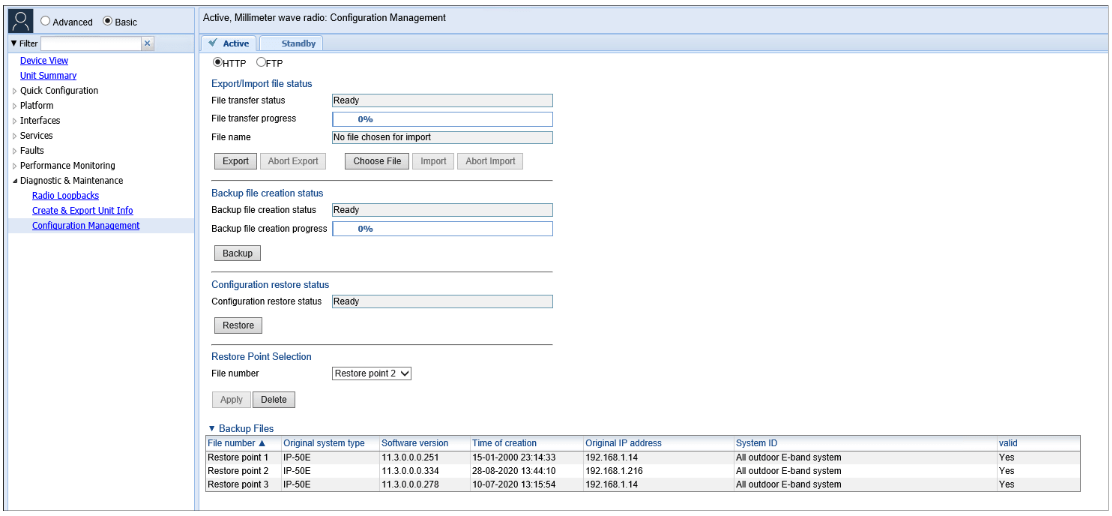
File creation status	Ready
File creation progress	0%
File export status	Ready
File export progress	0%

Figure 82: Basic Mode – Unit Info Page

Configuration Management

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

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



Active, Millimeter wave radio: Configuration Management

● HTTP ○ FTP

Export/Import file status

File transfer status: Ready

File transfer progress: 0%

File name: No file chosen for import

Backup file creation status

Backup file creation status: Ready

Backup file creation progress: 0%

Configuration restore status

Configuration restore status: Ready

Restore Point Selection

File number: Restore point 2

▼ Backup Files

File number ▲	Original system type	Software version	Time of creation	Original IP address	System ID	valid
Restore point 1	IP-50E	11.3.0.0.0.251	15-01-2000 23:14:33	192.168.1.14	All outdoor E-band system	Yes
Restore point 2	IP-50E	11.3.0.0.0.334	28-08-2020 13:44:10	192.168.1.216	All outdoor E-band system	Yes
Restore point 3	IP-50E	11.3.0.0.0.278	10-07-2020 13:15:54	192.168.1.14	All outdoor E-band system	Yes

Figure 83: Basic Mode – Configuration Management Page

Chapter 5: Configuring a Link Using the Quick Configuration Wizard

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

1+0 – Configures a 1+0 radio link consisting of a user-selected Ethernet and radio interface connected. This link passes traffic between the radio and Ethernet interfaces via a point-to-point pipe service. See Configuring a 1+0 Link Using the Quick Configuration Wizard.

This wizard can also be used to configure XPIC on the unit. XPIC must be configured individually on each PTP 850E unit in the XPIC pair. See XPIC Overview.

Enhanced Multi-Carrier ABC – Configures a 2 + 0 Multi-Carrier ABC group consisting of an Ethernet interface or LAG and the two radio interfaces. See *Configuring a 2+0 Multi-Carrier ABC Link Using the Quick Configuration Wizard*

Multiband – Configures a link that bundles E-Band and microwave radios in a single group that is shared with an Ethernet interface. A Multiband link uses an PTP 850E and an PTP 820C, PTP 820C-HP, PTP 820S, or third-party microwave unit. The Multiband group is only configured on the PTP 850E unit. See Configuring a Multiband (Enhanced Multi-Carrier ABC) Link Using the Quick Configuration Wizard.

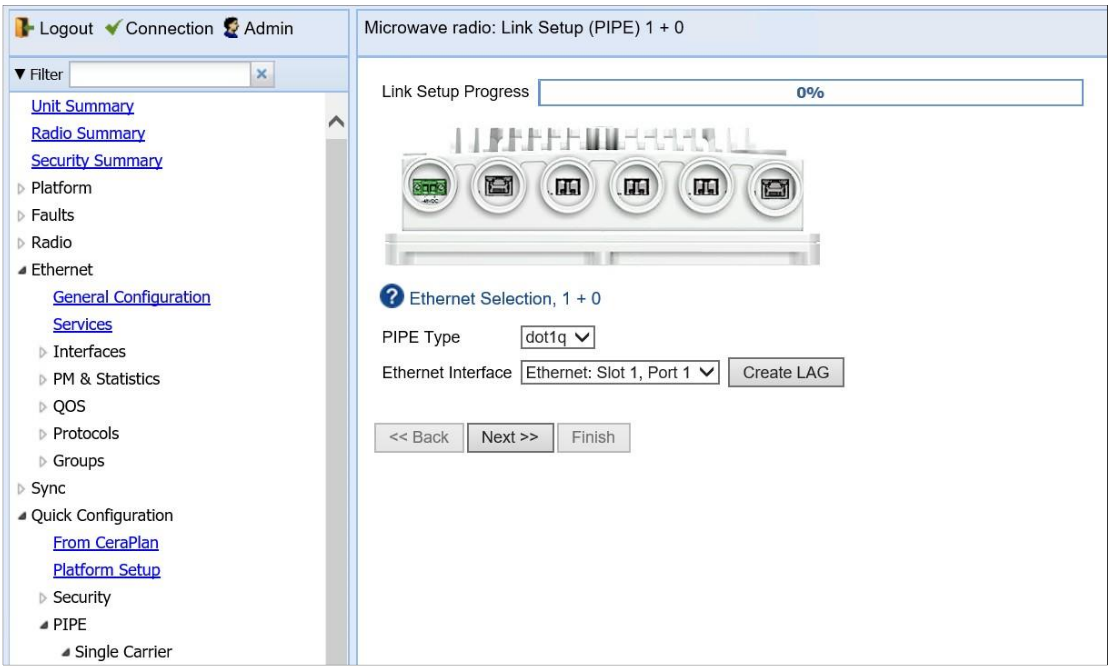
Because the Quick Configuration wizard creates Pipe links, you cannot add an interface to a link using the Quick Configuration wizard if any service points are attached to the interface prior to configuring the link. See Deleting a Service Point.

Configuring a 1+0 Link Using the Quick Configuration Wizard

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

1. Select **Quick Configuration > PIPE > Single Carrier > 1+0**. Page 1 of the 1+0 Quick Configuration wizard opens.

Figure 47 1+0 Quick Configuration Wizard – Ethernet Selection (PTP 850C)



Logout ✓ Connection Admin

Microwave radio: Link Setup (PIPE) 1 + 0

▼ Filter

- Unit Summary
- Radio Summary
- Security Summary
- Platform
- Faults
- Radio
- Ethernet
  - General Configuration
  - Services
  - Interfaces
  - PM & Statistics
  - QOS
  - Protocols
  - Groups
- Sync
- Quick Configuration
  - From CeraPlan
  - Platform Setup
  - Security
  - PIPE
    - Single Carrier

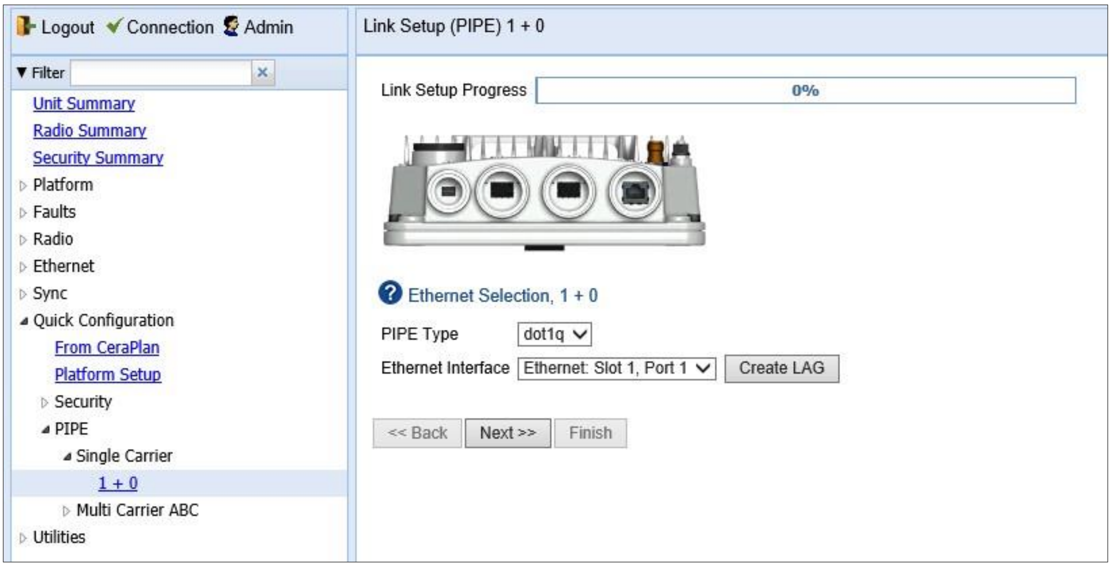
Link Setup Progress 0%

Ethernet Selection, 1 + 0

PIPE Type: dot1q

Ethernet Interface: Ethernet: Slot 1, Port 1

Figure 48 1+0 Quick Configuration Wizard – Ethernet Selection (PTP 850C)



Logout ✓ Connection Admin

Link Setup (PIPE) 1 + 0

▼ Filter

- Unit Summary
- Radio Summary
- Security Summary
- Platform
- Faults
- Radio
- Ethernet
- Sync
- Quick Configuration
  - From CeraPlan
  - Platform Setup
  - Security
  - PIPE
    - Single Carrier
      - 1 + 0
    - Multi Carrier ABC
- Utilities

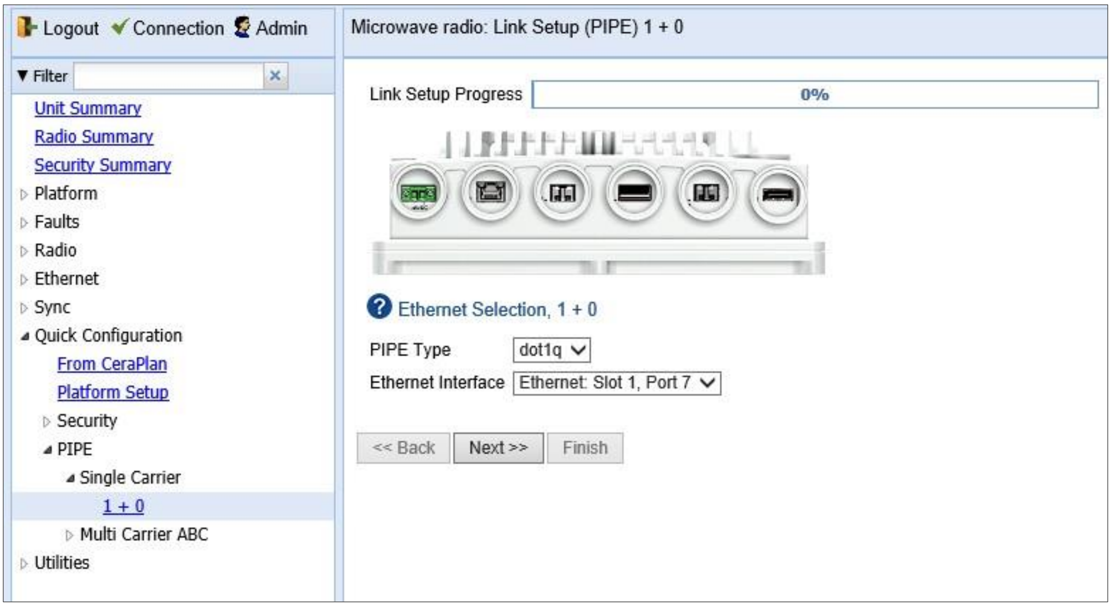
Link Setup Progress 0%

Ethernet Selection, 1 + 0

PIPE Type: dot1q

Ethernet Interface: Ethernet: Slot 1, Port 1

Figure 49 1+0 Quick Configuration Wizard – Ethernet Selection (PTP 850E)



Microwave radio: Link Setup (PIPE) 1 + 0

Link Setup Progress 0%

Ethernet Selection, 1 + 0

PIPE Type: dot1q

Ethernet Interface: Ethernet: Slot 1, Port 7

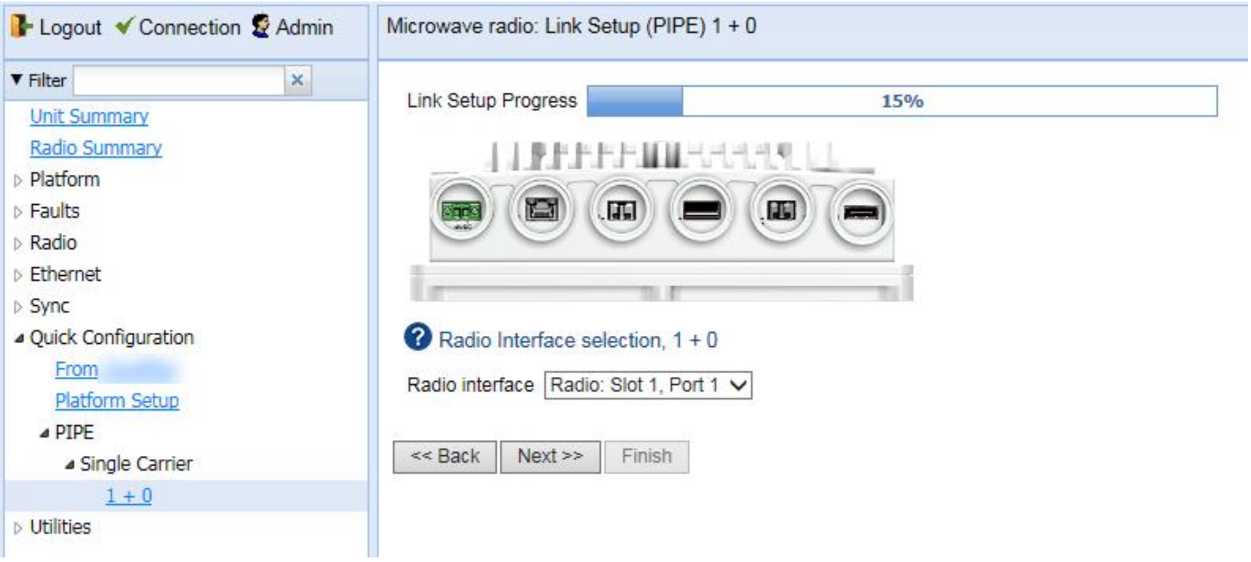
2. In the **PIPE Type** field, select the Attached Interface type for the service that will connect the radio and Ethernet interfaces. Options are:
   - **dot1q** – All C-VLANs and untagged frames are classified into the service.
   - **s-tag** – All S-VLANs and untagged frames are classified into the service.

Note

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

3. In the **Ethernet Interface** field, select an Ethernet interface for the link.
4. lick **Next**. Page 2 of the 1+0 Quick Configuration wizard opens

Figure 50 1+0 Quick Configuration Wizard – Page 2



Microwave radio: Link Setup (PIPE) 1 + 0

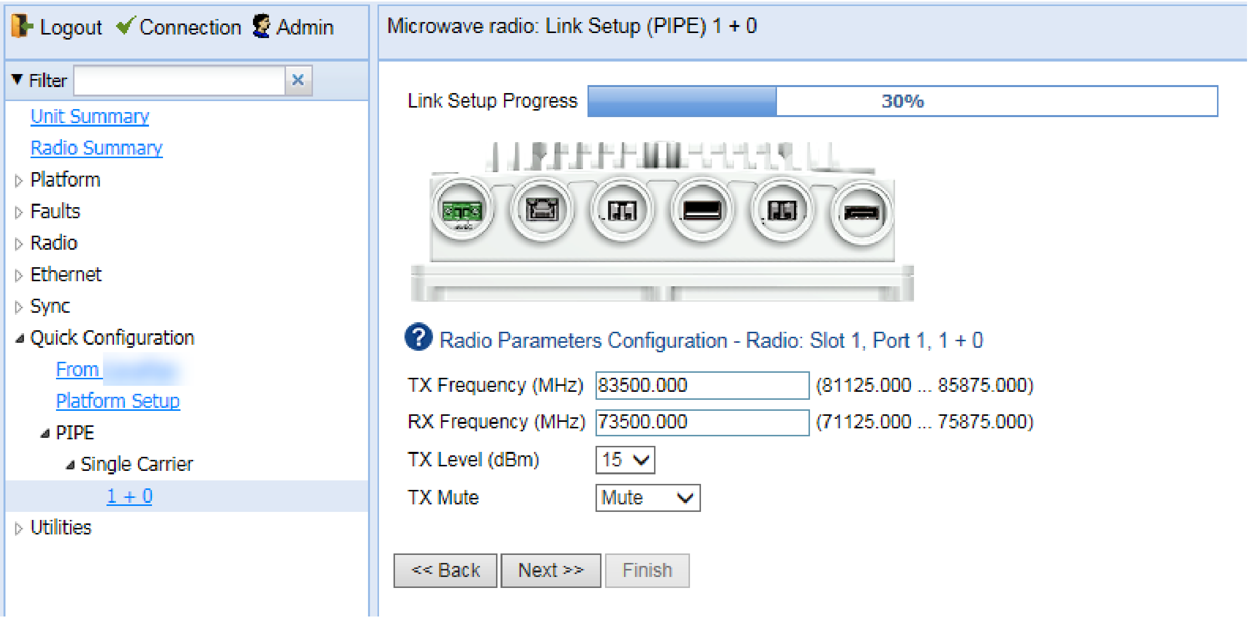
Link Setup Progress 15%

Radio Interface selection, 1 + 0

Radio interface: Radio: Slot 1, Port 1

5. In the **Radio Interface** field, select **Radio: Slot 1, Port 1**.
6. Click **Next**. Page 3 of the 1+0 Quick Configuration wizard opens.

Figure 51 1+0 Quick Configuration Wizard – Page 3



Microwave radio: Link Setup (PIPE) 1 + 0

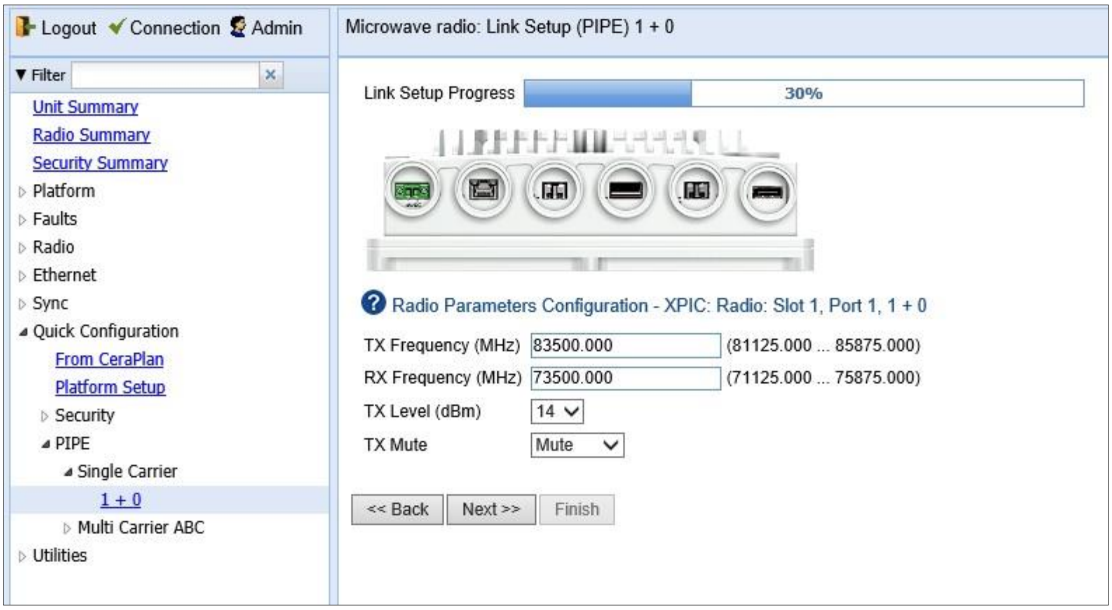
Link Setup Progress 30%

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

TX Frequency (MHz) 83500.000 (81125.000 ... 85875.000)
RX Frequency (MHz) 73500.000 (71125.000 ... 75875.000)
TX Level (dBm) 15
TX Mute Mute

7. If the unit is part of an XPIC link, select XPIC.
8. If you select XPIC, the Member Role field is displayed. In the Member Role field, select Horizontal or Vertical. Make sure the Member Role you select matches the actual polarization of the PTP 850E unit, and that the Member Role you configure in the paired unit is not the same as the role you configure here. For full instructions on configuring an XPIC link, including alignment instructions, see Configuring XPIC.
9. Click Next. Page 4 of the 1+0 Quick Configuration wizard opens.`

Figure 52 1+0 Quick Configuration Wizard – Page 4



Microwave radio: Link Setup (PIPE) 1 + 0

Link Setup Progress 30%

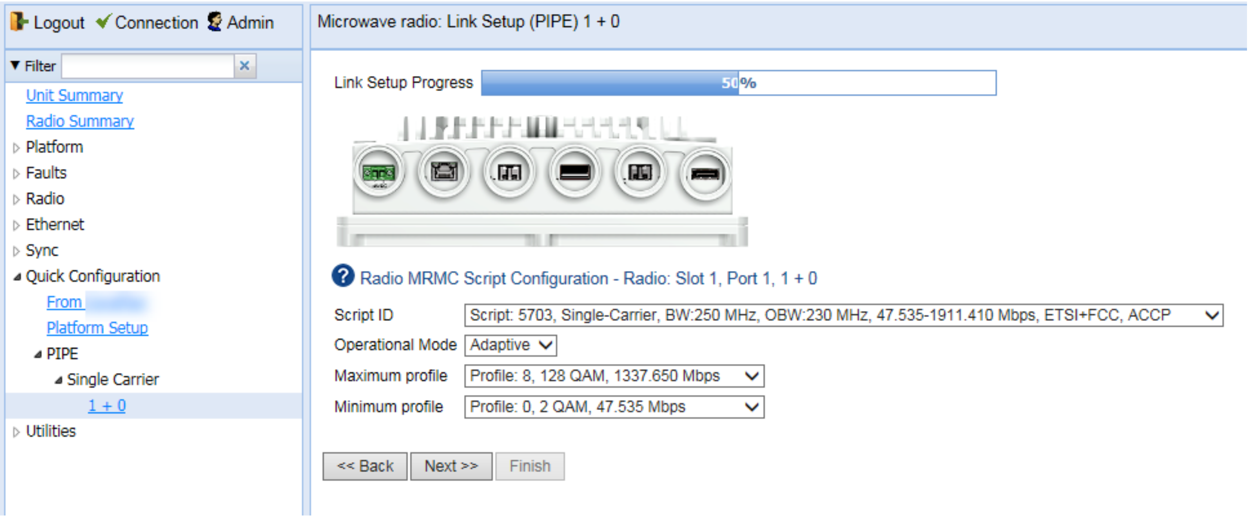
Radio Parameters Configuration - XPIC: Radio: Slot 1, Port 1, 1 + 0

TX Frequency (MHz) 83500.000 (81125.000 ... 85875.000)
RX Frequency (MHz) 73500.000 (71125.000 ... 75875.000)
TX Level (dBm) 14
TX Mute Mute

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

11. In the **RX Frequency (MHz)** field, set the received radio frequency in MHz.
12. In the **TX Level (dBm)** field, enter the desired TX signal level (TSL). The range of values depends on the frequency and RFU type.
13. To mute the TX output of the radio, select **Mute** in the **TX mute** field. To unmute the TX output of the radio, select **Unmute**.
14. Click **Next**. Page 5 of the 1+0 Quick Configuration wizard opens.

Figure 53 1+0 Quick Configuration Wizard – Page 5



Microwave radio: Link Setup (PIPE) 1 + 0

Link Setup Progress 50%

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

Script ID: Script: 5703, Single-Carrier, BW:250 MHz, OBW:230 MHz, 47.535-1911.410 Mbps, ETSI+FCC, ACCP

Operational Mode: Adaptive

Maximum profile: Profile: 8, 128 QAM, 1337.650 Mbps

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

15. In the **Script ID** field, select the MRMC script you want to assign to the radio. For a full explanation of choosing an MRMC script, see ***Error! Reference source not found.***.

1 In the **Operational Mode** field, select the ACM mode: **Adaptive** or **Fixed**.

- In Adaptive ACM mode, TX and RX rates are dynamic. An ACM-enabled radio system automatically chooses which profile to use according to the channel fading conditions.
- Fixed ACM mode applies constant TX and RX rates. However, unlike regular scripts, with a Fixed ACM script you can specify a maximum profile to inhibit inefficient transmission levels.

2 Do one of the following:

- If you selected **Adaptive** in the **Operational Mode** field, the following two fields are displayed:
- **Maximum profile** – Enter the maximum profile for the script. See ***Error! Reference source not found.***.
- **Minimum profile** – Enter the minimum profile for the script. See ***Error! Reference source not found.***.

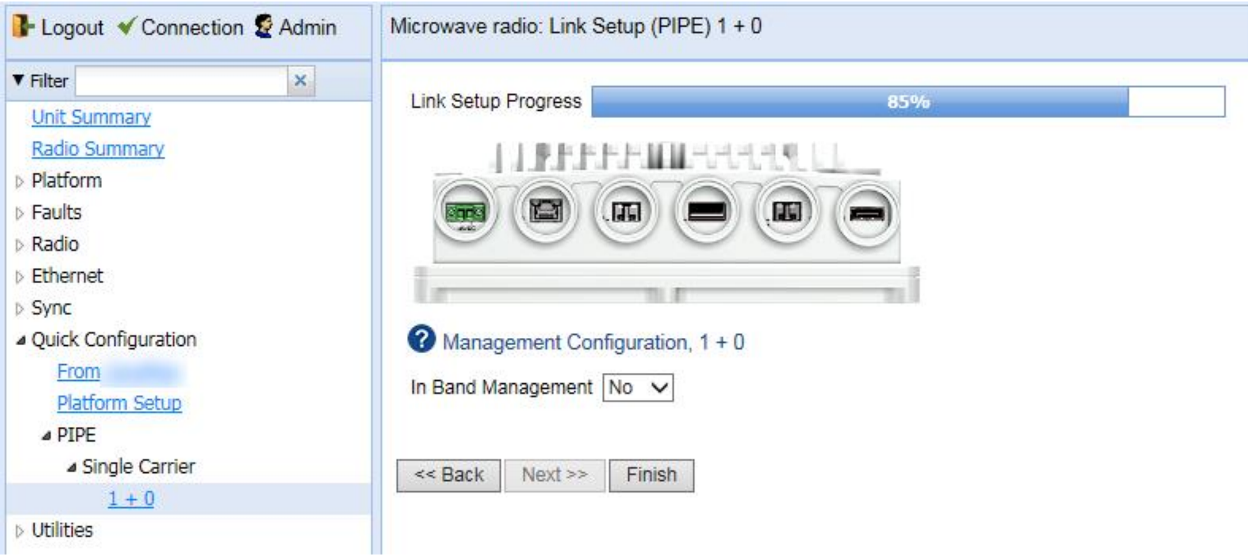
Note

The default minimum profile is 2.

- If you selected **Fixed** in the **Operational Mode** field, the next field is **Profile**. Select the ACM profile for the radio in the **Profile** field.

3 Click **Next**. Page 5 of the 1+0 Quick Configuration wizard opens.

Figure 54 **1+0 Quick Configuration Wizard – Page 6**



Microwave radio: Link Setup (PIPE) 1 + 0

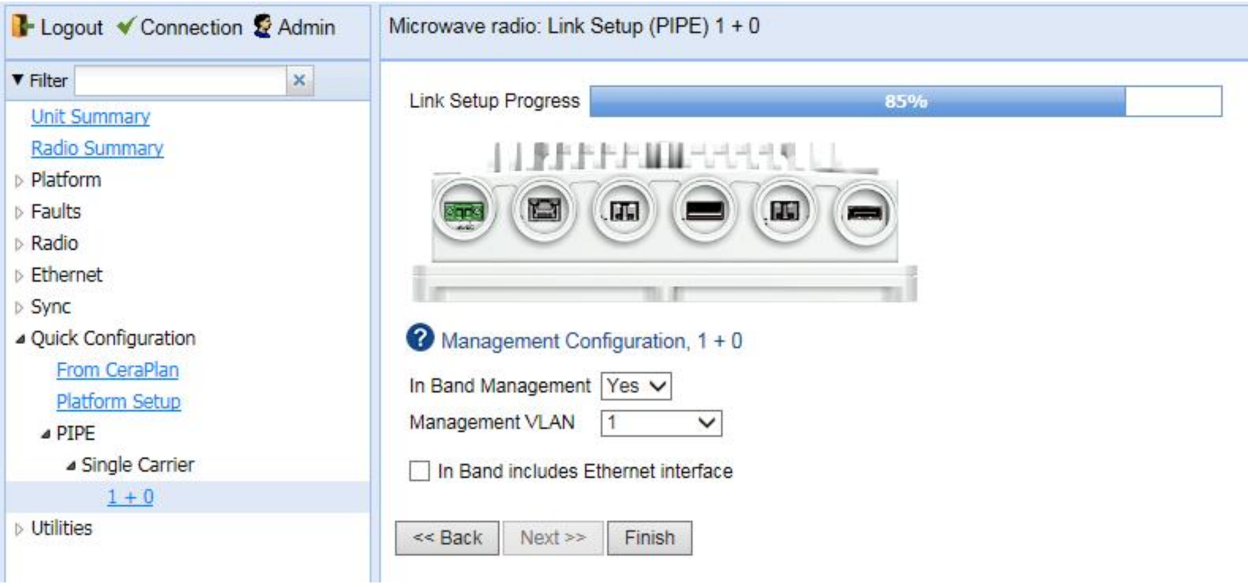
Link Setup Progress 85%

Management Configuration, 1 + 0

In Band Management: No

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

Figure 55 1+0 Quick Configuration Wizard – Page 5 (In Band Management = Yes)



Microwave radio: Link Setup (PIPE) 1 + 0

Link Setup Progress 85%

Management Configuration, 1 + 0

In Band Management: Yes

Management VLAN: 1

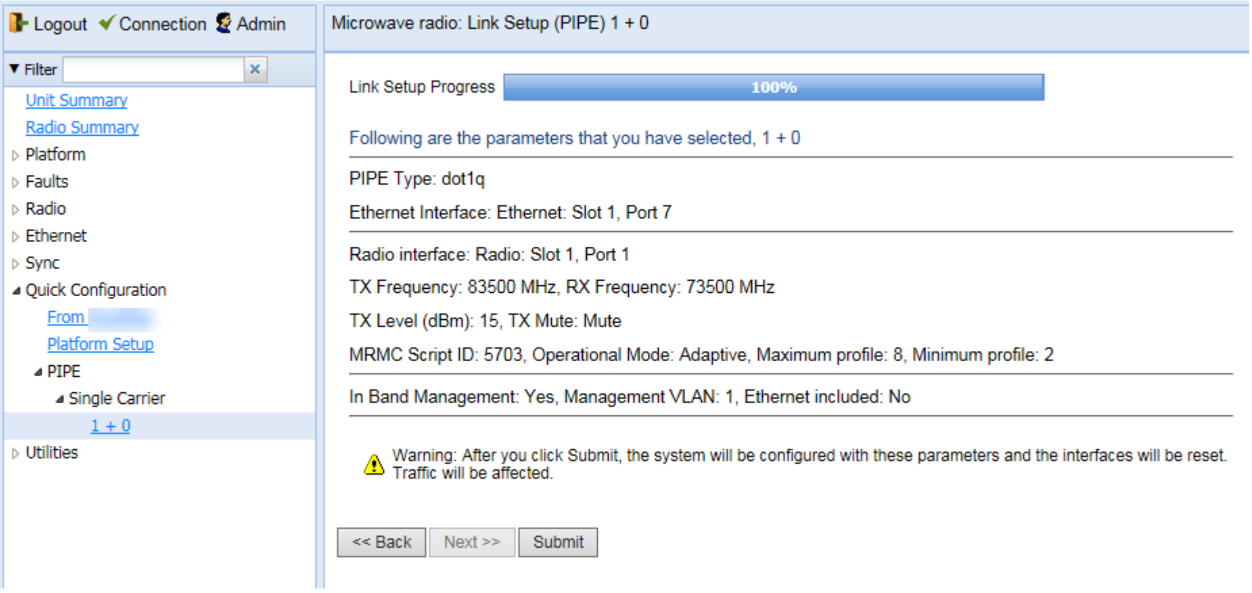
□ In Band includes Ethernet interface

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

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

7 Click **Finish**. Page 6 of the 1+0 Quick Configuration wizard opens. This page displays the parameters you have selected for the link.

Figure 56 1+0 Quick Configuration Wizard – Page 7 (Summary Page)



Microwave radio: Link Setup (PIPE) 1 + 0

Link Setup Progress 100%

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

PIPE Type: dot1q

Ethernet Interface: Ethernet: Slot 1, Port 7

Radio interface: Radio: Slot 1, Port 1

TX Frequency: 83500 MHz, RX Frequency: 73500 MHz

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

MRMC Script ID: 5703, Operational Mode: Adaptive, Maximum profile: 8, Minimum profile: 2

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

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

8 To complete configuration of the link, click **Submit**. If you want to go back and change any of the parameters, click **Back**. After you click **Submit**, the unit is reset.

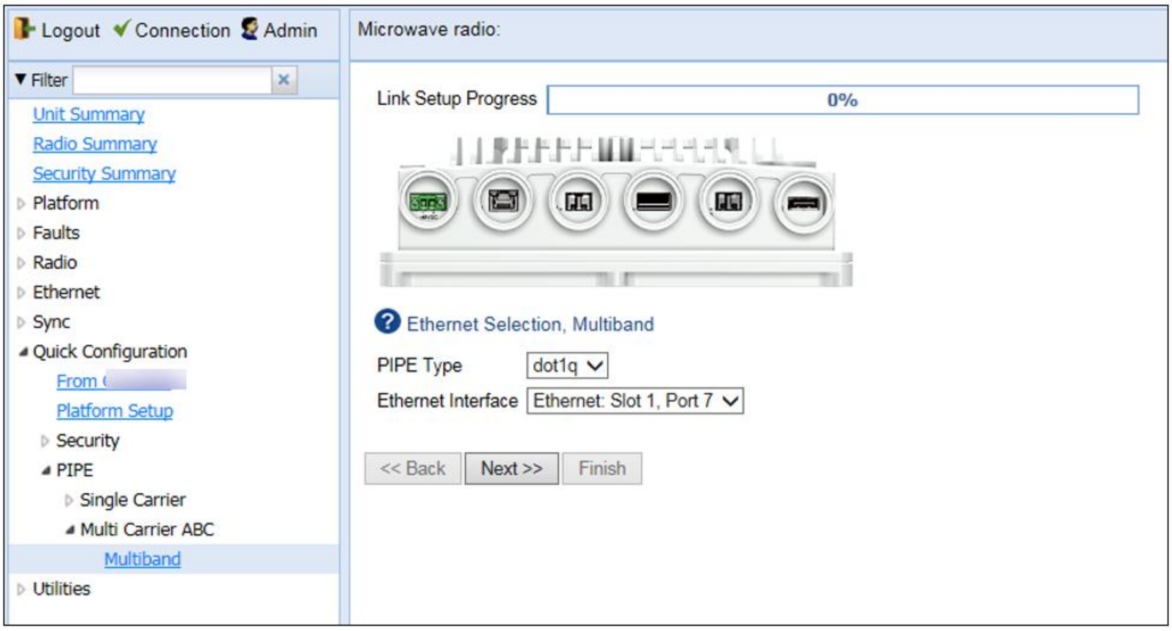
Configuring a Multiband (Enhanced Multi-Carrier ABC) Link Using the Quick Configuration Wizard

For important general information about Multiband links, see *Multiband Overview*.

To configure a Multiband node using the Quick Configuration wizard:

1. Connect the external switch to any operational traffic port on the PTP 850E.
2. Connect Port 3 (Eth2) on the PTP 850E to the unit paired with the PTP 850E. When the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, use Eth2 on the PTP 820C, PTP 820C-HP, or PTP 820S.
3. Verify that the **Admin** status of Eth2 on the PTP 850E is **Down**. See Enabling the Interfaces (Interface Manager).
4. Verify that no service points are configured on the Eth2 port of the PTP 850E. If there are service points on Eth2, remove them. See Deleting a Service Point.
5. On the PTP 850E, select **Quick Configuration > PIPE > Multi Carrier ABC > Multiband**. Page 1 of the Multiband Quick Configuration wizard opens.

Figure 57 Multiband Quick Configuration Wizard – Page 1



Microwave radio:

Link Setup Progress 0%

Ethernet Selection, Multiband

PIPE Type: dot1q

Ethernet Interface: Ethernet: Slot 1, Port 7

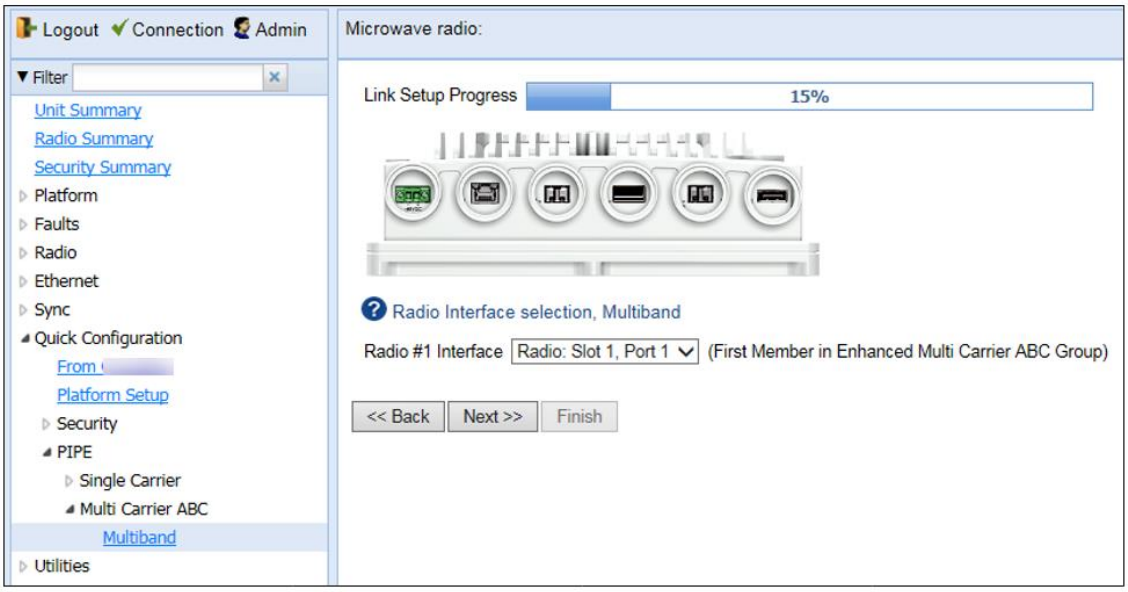
6. In the **Pipe Type** field, select the Attached Interface type for the service that will connect the radio and Ethernet interfaces. Options are:
   - **s-tag** – All S-VLANs and untagged frames are classified into the service.
   - **dot1q** – All C-VLANs and untagged frames are classified into the service.

Note

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

7. In the **Ethernet Interface** field, select the port connected to the external switch.
8. Click **Next**. Page 2 of the Multiband Quick Configuration wizard opens.

Figure 58 Multiband Quick Configuration Wizard – Page 2



Microwave radio:

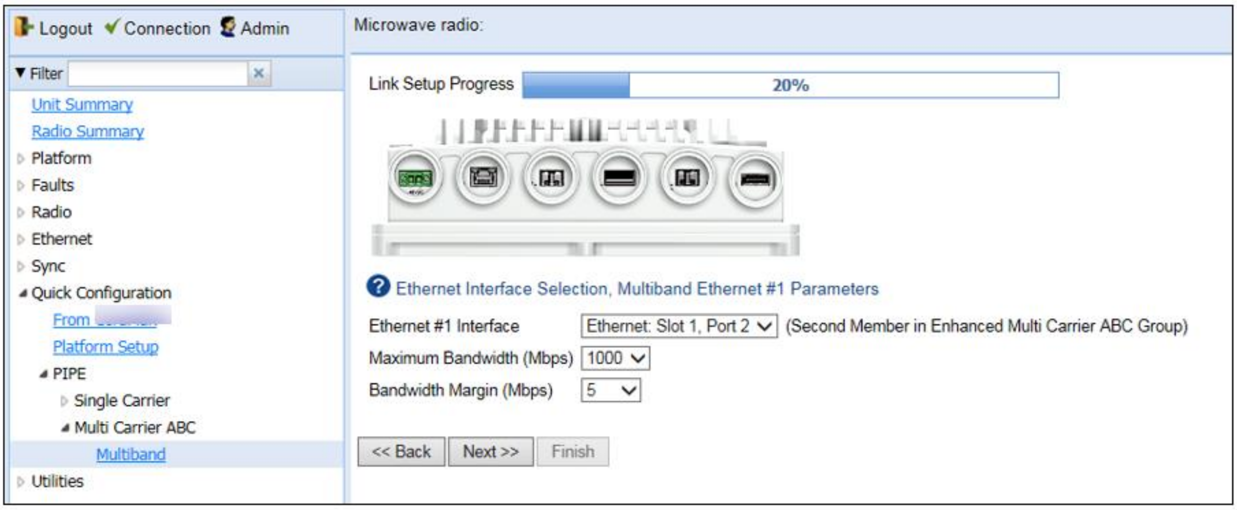
Link Setup Progress 15%

Radio Interface selection, Multiband

Radio #1 Interface: Radio: Slot 1, Port 1 (First Member in Enhanced Multi Carrier ABC Group)

9. In the Radio #1 Interface field, select Radio: Slot 1, Port 1.
10. Click Next. Page 3 of the Multiband Quick Configuration wizard opens.

Figure 59 Multiband Quick Configuration Wizard – Page 3



Microwave radio:

Link Setup Progress 20%

Ethernet Interface Selection, Multiband Ethernet #1 Parameters

Ethernet #1 Interface: Ethernet: Slot 1, Port 2 (Second Member in Enhanced Multi Carrier ABC Group)

Maximum Bandwidth (Mbps): 1000

Bandwidth Margin (Mbps): 5

11. In the **Ethernet #1 Interface** field, select Ethernet: Slot 1, Port 2.
12. In the **Maximum Bandwidth (Mbps)** field, select the maximum traffic that the PTP 850E will pass to the paired unit.
    - When using Fixed ACM mode, set this parameter to the actual rate you want the paired unit to broadcast.
    - When using Adaptive ACM mode, set this parameter to the maximum of the paired unit’s capacity.

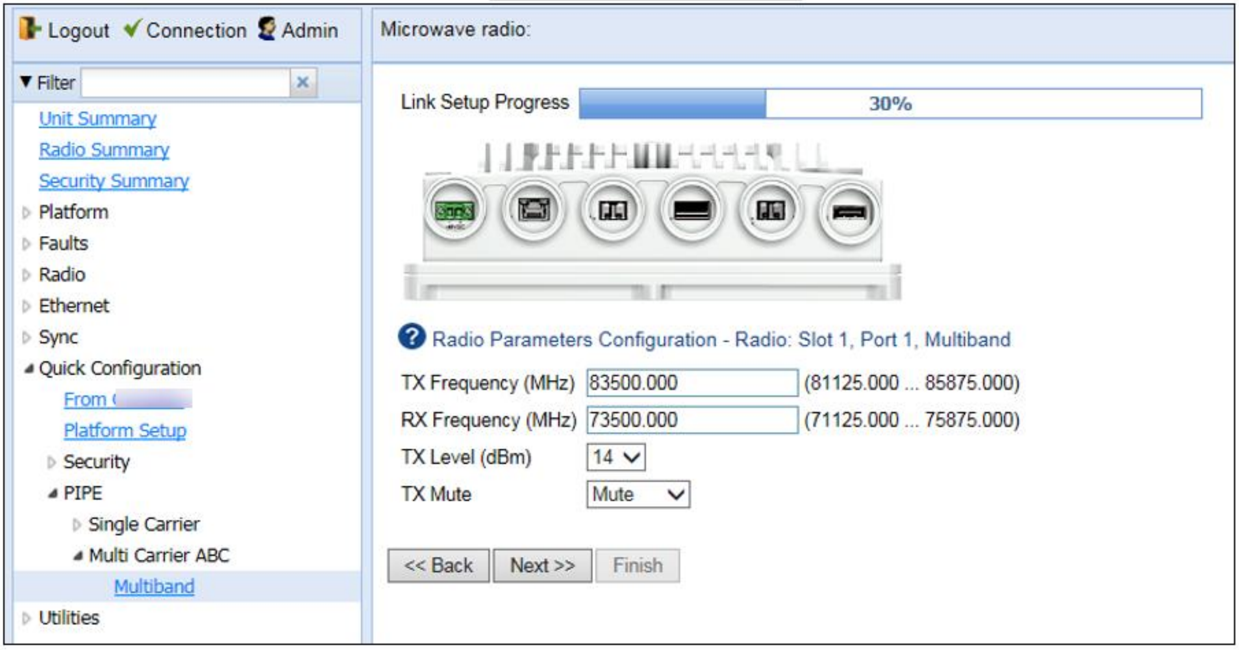
    The default value is 1000 Mbps.

> Note
>
> The Maximum Bandwidth represents the L1 capacity of the radio link connected to the Ethernet member. The actual bandwidth that will be available for traffic is less due to overhead.
>
> When using a third-party radio as the paired unit, it is particularly important to set this parameter properly in order to ensure optimal performance. Failure to properly set this parameter may lead to frequent pauses as the queue fills up during low capacity periods, such as when weather conditions cause the ACM profile to drop.

13. In the **Bandwidth Margin (Mbps)** field, select the bandwidth margin, in Mbps. This parameter deducts the specified throughput from the throughput the PTP 850E would otherwise pass to the paired unit. The purpose of this parameter is to provide a margin of safety that will avoid loss of traffic in the event that the ACM profile is reduced on the paired unit. It is recommended to configure this parameter as follows:
    - If the paired unit is an PTP 820 microwave radio or a third-party device with a bandwidth notification mechanism that will inform the PTP 850E of an impending reduction of the ACM profile before the reduction takes place, it is recommended to leave this parameter at its default value of 5 Mbps.
    - If the paired unit is a third-party device without a bandwidth notification mechanism that will inform the PTP 850E of an impending reduction of the ACM profile before the reduction takes place, it is recommended to set this parameter to an amount equal to or greater than the largest throughput differential between any two adjacent profiles for the script configured on the paired unit.

    The range of values is 5 to 100 Mbps.
14. Click Next. Page 4 of the Multiband Quick Configuration wizard opens.

Figure 60 Multiband Quick Configuration Wizard – Page 4



Link Setup Progress 30%

Radio Parameters Configuration - Radio: Slot 1, Port 1, Multiband

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

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

TX Level (dBm) 14

TX Mute Mute

15. Configure the following radio parameters.

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

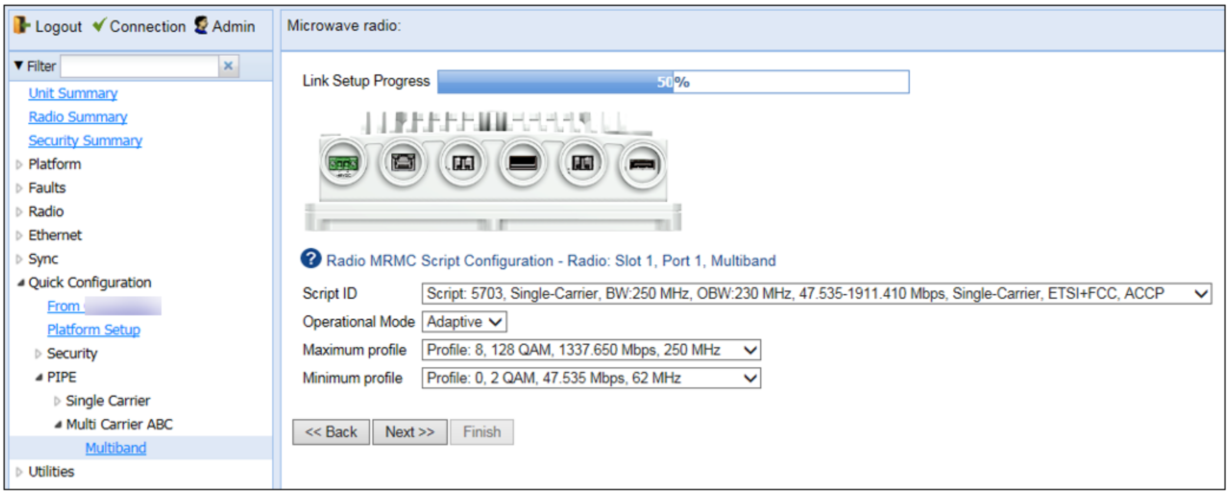
b. In the RX **Frequency (MHz)** field, set the received radio frequency in MHz.

c. In the **TX Level (dBm)** field, enter the desired TX signal level (TSL). The range of values depends on the frequency and RFU type.

d. To mute the TX output of the radio, select **Mute** in the **TX mute** field. To unmute the TX output of the radio, select **Unmute**.

16. Click **Next**. Page 5 of the Multiband Quick Configuration wizard opens.

Figure 61 Multiband Quick Configuration Wizard – Page 5



Radio MRMC Script Configuration - Radio: Slot 1, Port 1, Multiband

Script ID: Script: 5703, Single-Carrier, BW:250 MHz, OBW:230 MHz, 47.535-1911.410 Mbps, Single-Carrier, ETSI+FCC, ACCP

Operational Mode: Adaptive

Maximum profile: Profile: 8, 128 QAM, 1337.650 Mbps, 250 MHz

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

17. In the **Script ID** field, select the MRMC script you want to assign to the radio. For a full explanation of choosing an MRMC script, see ***Error! Reference source not found.***.

18. In the **Operational Mode** field, select **Adaptive**. The following two fields are displayed:

- **Maximum profile** – Enter the maximum profile for the script. See **Error! Reference source not f ound.**.
- **Minimum profile** – Enter the minimum profile for the script. See Error! Reference source n ot found..

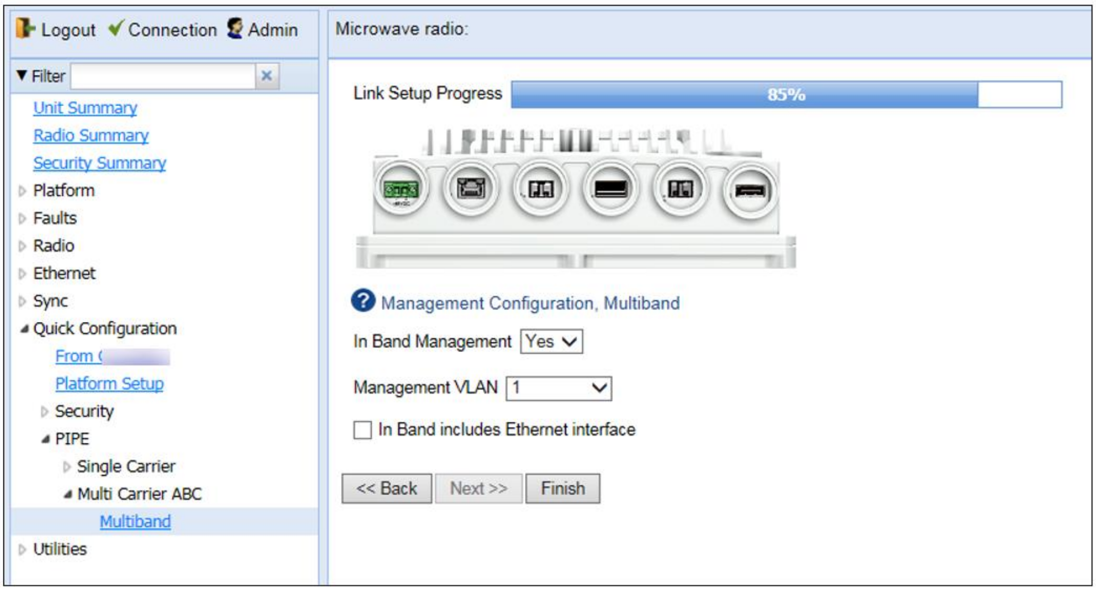
Note

Fixed mode is not supported for Multiband.

For Multiband links, ake sure the Maximum profile and **Mi**nimum profile are set to different values for Multiband links.

19. Click **Next**. Page 6 of the Multiband Quick Configuration wizard opens.

Figure 62 Multiband Quick Configuration Wizard – Page 6



Link Setup Progress 85%

Management Configuration, Multiband

In Band Management: Yes

Management VLAN: 1

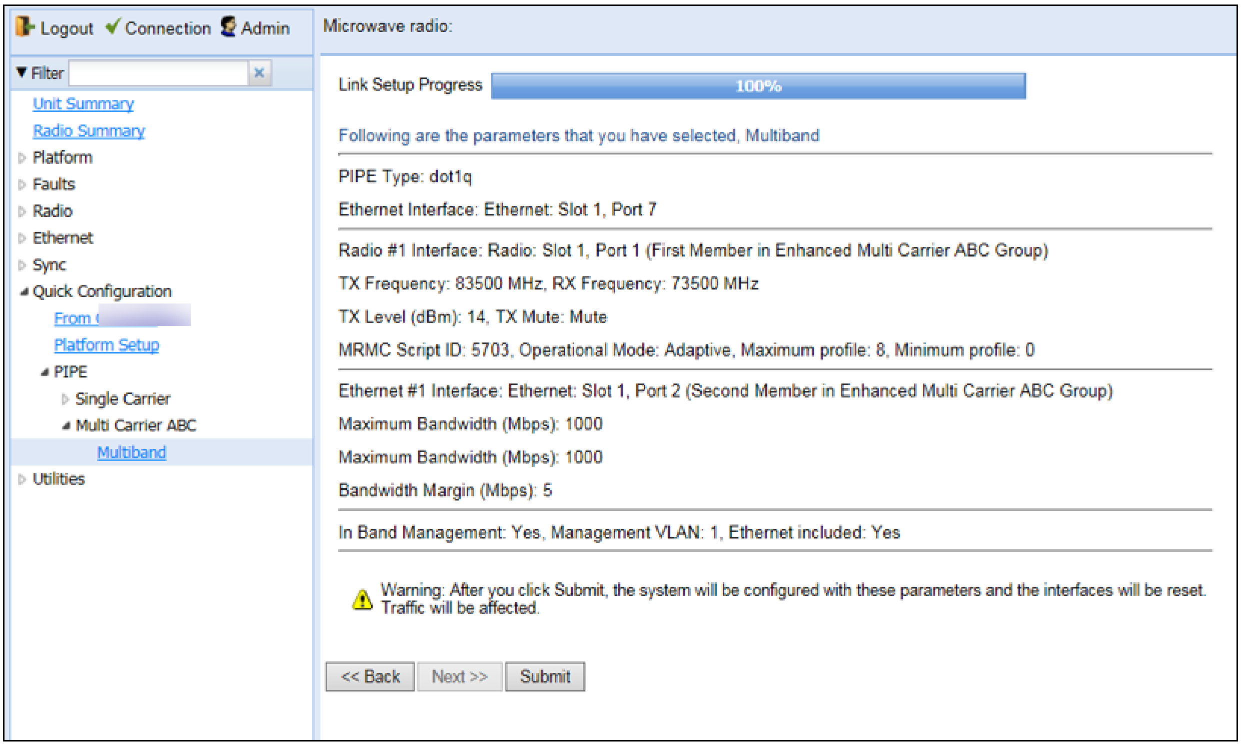
□ In Band includes Ethernet interface

20. In the **In Band Management** field, select **Yes** to configure in-band management, or **No** if you do not need in-band management. If you select **Yes**, the **Management VLAN** field appears.
21. If you selected **Yes** in the **In Band Management** field, select the management VLAN in the **Management VLAN** field.
22. If you want to use the Ethernet interface as well as the radio interface for in-band management, select **In Band includes Ethernet interface.**

> Note
>
> If you want to manage the paired unit via the PTP 850E, refer to the instructions in Inband Management via the PTP 850E.

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

Figure 63 Multiband Quick Configuration Wizard – Summary Page



Following are the parameters that you have selected, Multiband

PIPE Type: dot1q

Ethernet Interface: Ethernet: Slot 1, Port 7

Radio #1 Interface: Radio: Slot 1, Port 1 (First Member in Enhanced Multi Carrier ABC Group)

TX Frequency: 83500 MHz, RX Frequency: 73500 MHz

TX Level (dBm): 14, TX Mute: Mute

MRMC Script ID: 5703, Operational Mode: Adaptive, Maximum profile: 8, Minimum profile: 0

Ethernet #1 Interface: Ethernet: Slot 1, Port 2 (Second Member in Enhanced Multi Carrier ABC Group)

Maximum Bandwidth (Mbps): 1000

Maximum Bandwidth (Mbps): 1000

Bandwidth Margin (Mbps): 5

In Band Management: Yes, Management VLAN: 1, Ethernet included: Yes

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

24. To complete configuration of the Multiband group on the PTP 850E, click **Submit**. If you want to go back and change any of the parameters, click **Back**.
25. Enable the Eth2 interface. See *Enabling the Interfaces (Interface Manager)*.

When the PTP 850E is paired with an PTP 820 microwave radio, the following must be configured on the PTP 820 microwave radio:

- A **service** must be configured between the Ethernet port connected to the PTP 850E and the radio or Multi-Carrier ABC group being used for the Multiband link.

Note

If the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, the service must be a Pipe service. However, this service must be given higher priority than any other service attached to the interfaces used for Multiband.

- Automatic State Propagation must be configured, with **ASP trigger by remote fault** enabled.
- Radio Bandwidth Notification must be enabled.

For instructions, refer to the User Guide for the PTP 820 product you are using.

When the PTP 850E is paired with a third-party unit, the following must be configured on the third-party unit:

- The unit's switching mechanism must be set to Pipe mode and a Pipe service must be configured between the Ethernet port connected to the PTP 850E and the paired unit's radio or radio group.
- Automatic State Propagation must be configured, with **ASP trigger by remote fault** enabled.
- 802.3X Flow Control must be enabled.
- Ethernet Bandwidth Notification must be enabled

Chapter 6: Configuring Multi-Carrier ABC

This section includes:

- Configuring Multi-Carrier ABC
- Configuring Multiband
- Configuring XPIC
- Configuring 1+1 HSB Unit Protection
- Configuring Link Aggregation (LAG) and LACP

Configuring Multi-Carrier ABC

Multi-Carrier ABC Overview

Multi-Carrier Adaptive Bandwidth Control (ABC) enables multiple separate radio carriers to be shared by a single Ethernet port. This provides an Ethernet link over the radio with the total sum of the capacity of all the radios in the group, while still behaving as a single Ethernet interface. In Multi-Carrier ABC mode, traffic is dynamically divided among the carriers, at the Layer 1 level, without requiring Ethernet Link Aggregation.

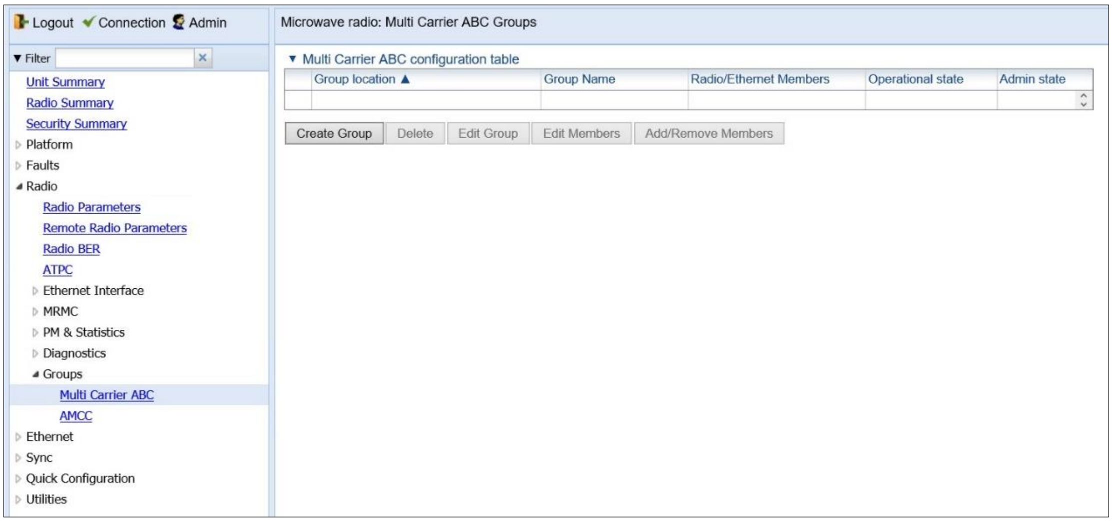
Load balancing is performed regardless of the number of MAC addresses or the number of traffic flows. During fading events which cause ACM modulation changes, each carrier fluctuates independently with hitless switchovers between modulations, increasing capacity over a given bandwidth and maximizing spectrum utilization. The result is close to 100% utilization of radio resources in which traffic load is balanced based on instantaneous radio capacity per carrier.

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

Configuring a Multi-Carrier ABC Group

To configure a Multi-Carrier ABC group:

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



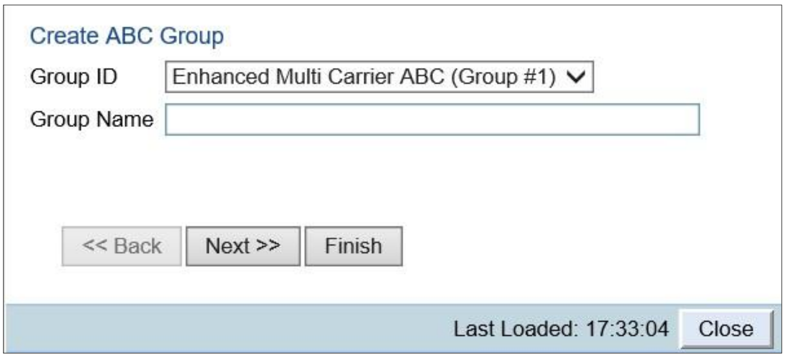
Microwave radio: Multi Carrier ABC Groups

Multi Carrier ABC configuration table

Group location ▲	Group Name	Radio/Ethernet Members	Operational state	Admin state

Figure 89: Multi-Carrier ABC Group Page (Empty)

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



Create ABC Group

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

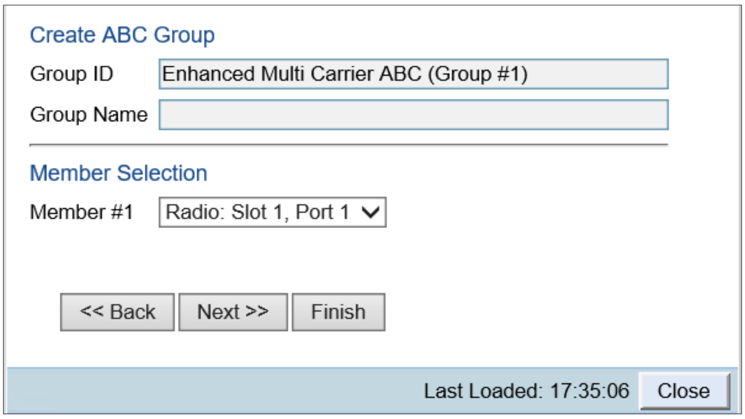
Group Name:

Last Loaded: 17:33:04

Figure 90: Create ABC Group Wizard – Group Name

3 Optionally, enter a descriptive name for the group in the **Group Name** field.

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



Create ABC Group

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

Group Name:

Member Selection

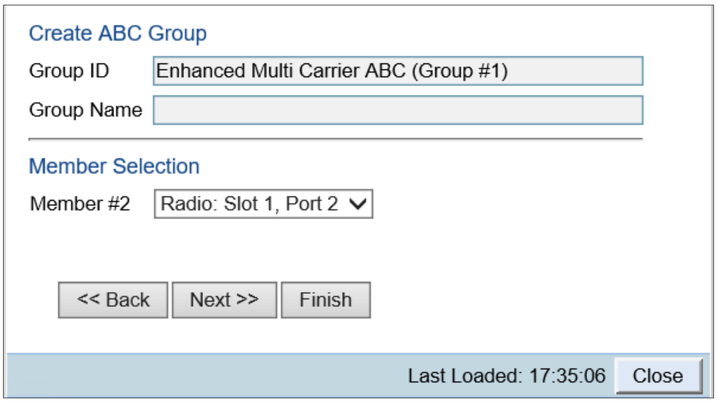
Member #1: Radio: Slot 1, Port 1

Last Loaded: 17:35:06

Figure 91: Create ABC Group Wizard – Member Selection 1

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

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



Create ABC Group

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

Group Name:

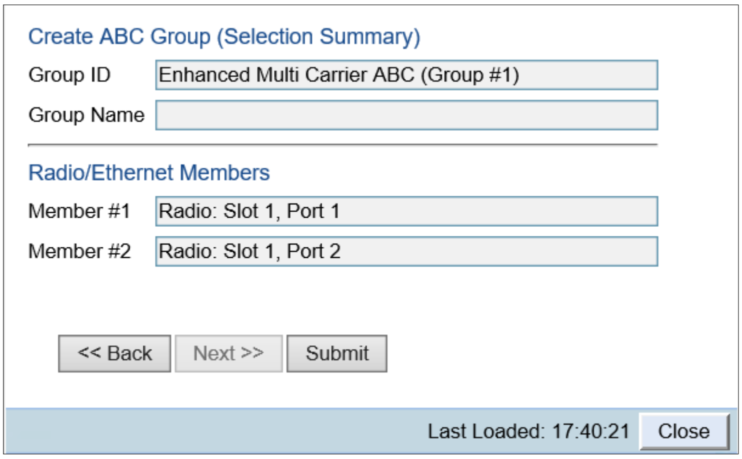
Member Selection

Member #2: Radio: Slot 1, Port 2

Figure 92: Create ABC Group Wizard – Member Selection 2

7 In the **Member 2** field, select a radio interface.

8 Click **Next**. A summary page opens.



Create ABC Group (Selection Summary)

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

Group Name:

Radio/Ethernet Members

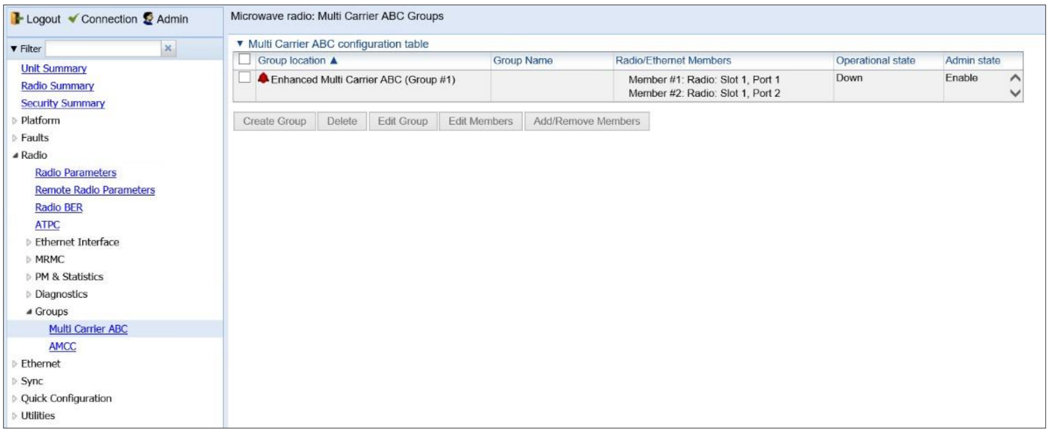
Member #1: Radio: Slot 1, Port 1

Member #2: Radio: Slot 1, Port 2

Figure 93: Create ABC Group Wizard – Summary Page

9 Click **Submit**. A message appears indicating whether or not the operation was successful.

10 Click **Close** to close the Create Group wizard. You must click **Submit** before clicking **Close**, or the selections you made will be discarded and the process cancelled.



Microwave radio: Multi Carrier ABC Groups

▼ Multi Carrier ABC configuration table

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

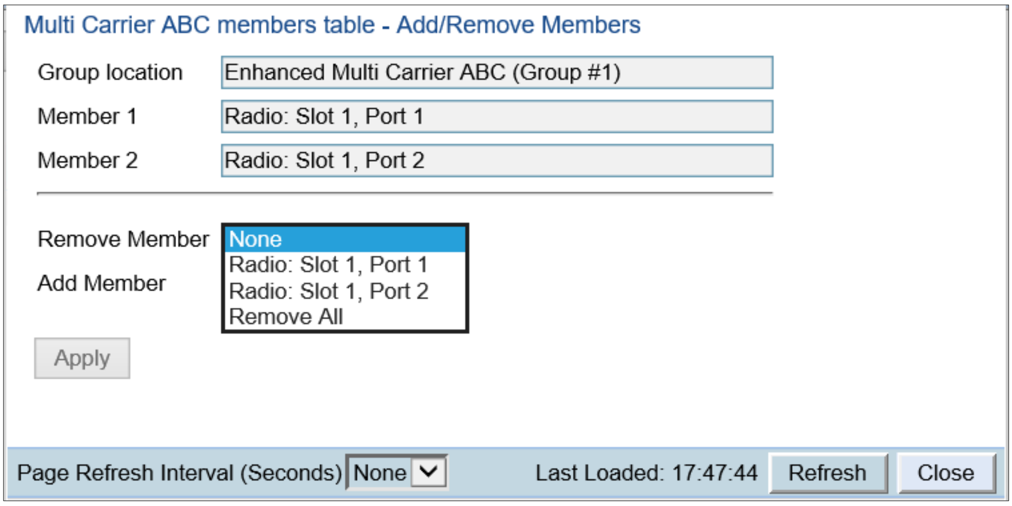
Figure 94: Multi-Carrier ABC Group Page (Populated)

Adding and Removing Group Members

You can add and remove interfaces from the group after creating the group. This is relevant if you want to delete a Multi-Carrier ABC group, since you must remove the members individually before deleting the group.

To remove interfaces:

1 Select the group in the Multi-Carrier ABC table and click **Add/Remove Members**. The Add/Remove Members page opens.



Multi Carrier ABC members table - Add/Remove Members

Group location	Enhanced Multi Carrier ABC (Group #1)
Member 1	Radio: Slot 1, Port 1
Member 2	Radio: Slot 1, Port 2
Remove Member	None
Add Member	

Page Refresh Interval (Seconds) None Last Loaded: 17:47:44

Figure 95: Multi Carrier ABC Group - Add/Remove Members Page

2 Select a member in the **Remove Member** field or select **Remove All**.

3 Click **Apply**.

4 Repeat these steps to remove additional members from the group.

Deleting a Multi-Carrier ABC Group

To delete a Multi-Carrier ABC group:

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

2 Select the group in the Multi-Carrier ABC table and click **Add/Remove Members**. The Add/Remove Members page opens.

3 Remove each member of the group. See *Adding and Removing Group Members*.

4 Click **Close** to close the Multi Carrier ABC – Add/Remove Members page.

5 Select the group and click **Delete.**

Configuring Multiband

This feature requires:

When used with PTP 820C, PTP 820C-HP, or PTP 820S, an ESS hardware version (two SFP ports) is required in order to configure synchronization and/or in-band management for the PTP 820C, PTP 820C-HP, or PTP 820S. For PTP 820C, a 2E2SX hardware version can also be used.

Multiband Overview

Multiband bundles E-Band and microwave radios in a single group that is shared with an Ethernet interface. This provides an Ethernet link over the radio with capacity of up to 10 Gbps. A Multiband link is highly resilient because the microwave link acts, in effect, as a backup for the E-Band link.

In the event of radio failure in one device, the other device continues to operate to the extent of its available capacity. Thus, operators benefit from both the high capacity of E-Band and the high reliability of microwave.

Multiband Operation

A Multiband node consists of an PTP 850E unit and an PTP 820C, PTP 820C-HP, or PTP 820S unit or a third-party microwave radio.

In a Multiband configuration, all traffic enters the node via the SFP/SFP+ traffic port (P5, Eth7) or the QSFP port (P4, Eth3 – Eth6). Traffic is passed to a Multiband group that includes the Multiband port (P3, Eth2) and the radio carrier.

The unit paired with the PTP 850E acts as a pipe. When traffic is passed from the PTP 850E to the paired unit, it is transmitted to either a single radio carrier or 2+0 Multi-Carrier ABC group.

In most circumstances, traffic is passed to the paired unit only when the PTP 850E radio has reached full capacity, or if the ACM profile drops to a point where the PTP 850E's capacity is temporarily less than the traffic load. If the PTP 850E reaches its minimum configured profile, all traffic is passed to the paired unit until the profile rises to a level above the minimum.

To ensure a smooth traffic flow, certain configurations must be performed on the paired unit.

When the PTP 850E is paired with an PTP 820C, PTP 820C-HP, or PTP 820S, the following must be configured on the PTP 820C, PTP 820C-HP, or PTP 820S:

- A Pipe service must be configured between Eth2 and the radio or Multi-Carrier ABC group.
- Automatic State Propagation must be configured, with ASP trigger by remote fault enabled.
- Radio Bandwidth Notification must be enabled.

When the PTP 850E is paired with a third-party unit, the following must be configured on the third-party unit:

- The unit's switching mechanism must be set to Pipe mode.
- Automatic State Propagation must be configured, with ASP trigger by remote fault enabled.
- 802.3X Flow Control must be enabled.
- Ethernet Bandwidth Notification must be enabled

Note

Fixed ACM mode is not supported for Multiband groups.

A Pipe service must be configured between the Ethernet port connected to the PTP 850E and the paired unit's radio or radio group.

Note

If the paired unit is an PTP 820C, PTP 820C-HP, PTP 820S, or third-party microwave radio, the service must be a Pipe service. However, this service must be given higher priority than any other service attached to the interfaces used for Multiband.

The latency differential between the PTP 850E and the paired unit cannot be more than 1.6 ms. That means that under all foreseeable conditions, such as a high ACM profile on one unit and a low ACM profile on the other unit, there should be no more than a 1.6 ms difference between the latency of the two radio carriers in the Multiband link.

Figure 64 illustrates Multiband operation with an PTP 850E and PTP 820C. *Figure 64* illustrates a configuration that includes synchronization and management of the PTP 820C via the PTP 850E. Both of these items are optional, and require an optical cable between Eth3 on the PTP 820C (or PTP 820C-HP or PTP 820S) and any free 1G Ethernet port on the PTP 850E, as described in the following sections.

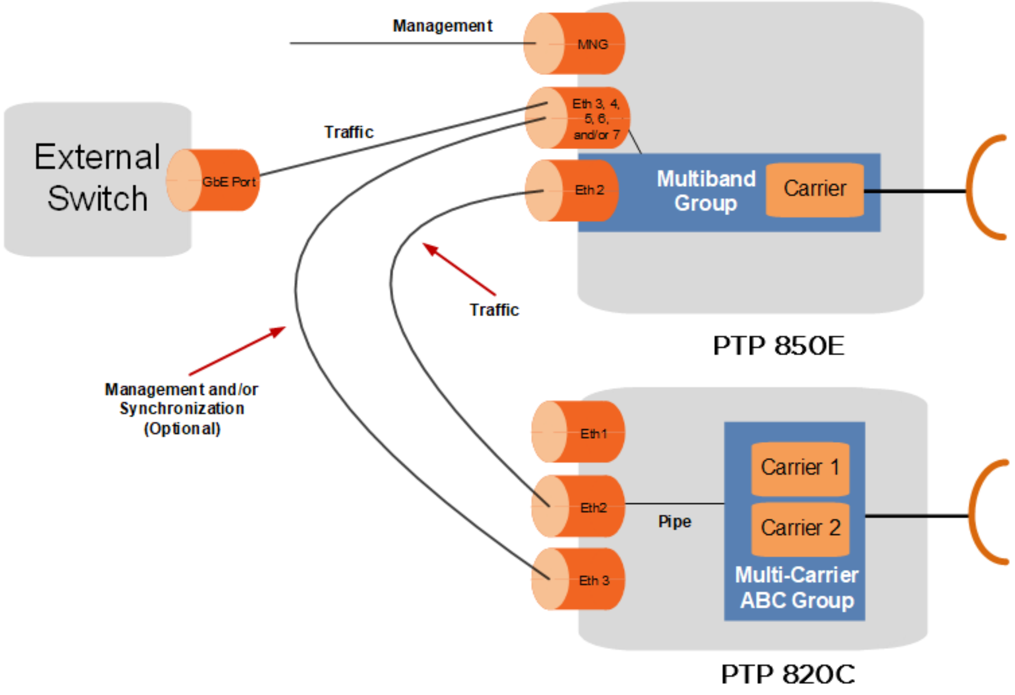


Figure 64: Multiband Operation – PTP 850E and PTP 820C

Figure 65 illustrates Multiband operation with an PTP 850E and a third-party unit. *Figure 65* illustrates a configuration that includes synchronization and management of the third-party unit via the PTP 850E. Synchronization via the PTP 850E requires an optical cable between an Ethernet port on the third-party unit and any free 1G Ethernet port on the PTP 850E, as described in the following sections.

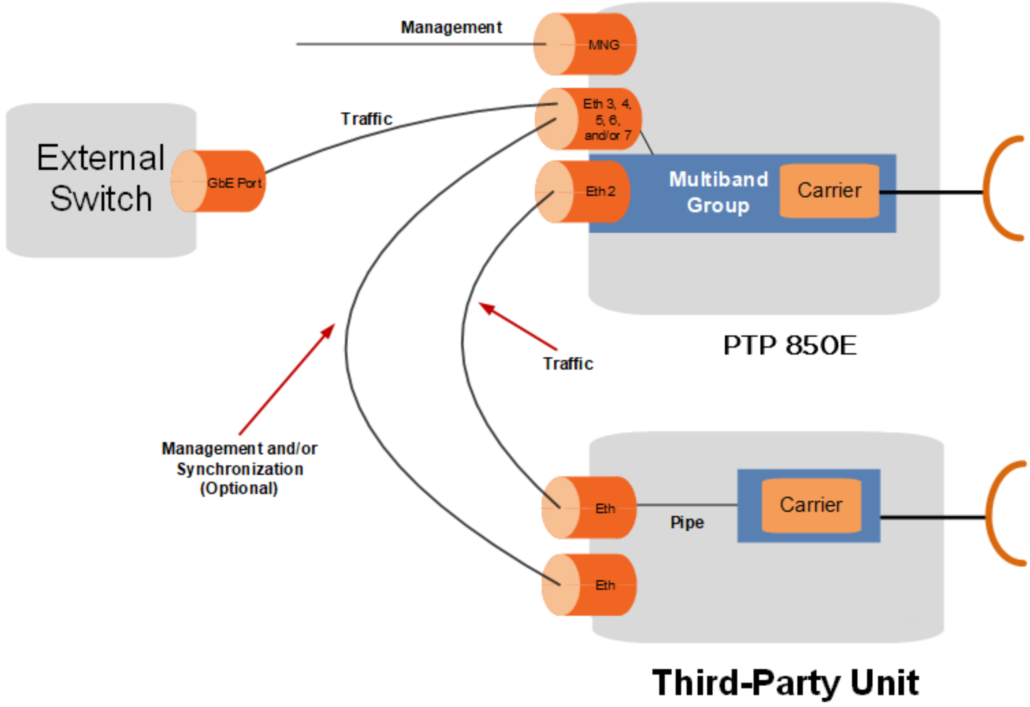


Figure 65: Multiband Operation – PTP 850E and Third-Party Unit

Multiband Configuration

To configure a Multiband node:

1 Connect the external switch to any operational traffic port on the PTP 850E.

2 Connect the Multiband port on the PTP 850E (Port 3, Eth2) to the paired unit. When the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, use the Eth2 port on the PTP 820C, PTP 820C-HP, or PTP 820S.

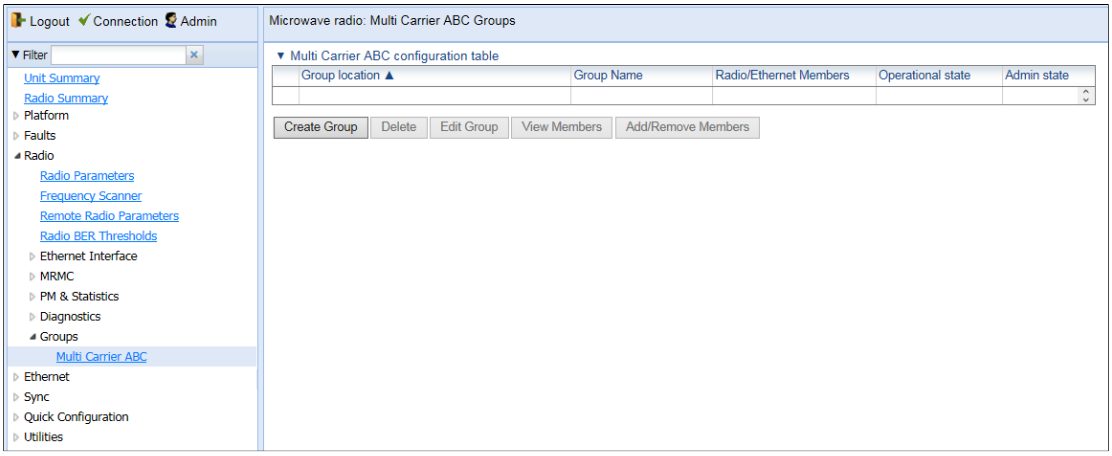
3 Verify that the **Admin** status of Eth2 on the PTP 850E is **Down**. See *Enabling the Interfaces (Interface Manager)*.

4 Verify that no service points are configured on Eth2 of the PTP 850E. If there are service points on Eth2, remove them. See *Deleting a Service Point*.

5 Configure the script and radio settings for the PTP 850E and the paired unit. Note that Fixed ACM mode is not supported for an PTP 850E in a Multiband node.

6 On the PTP 850E, configure a Multiband group that includes Eth2 and the radio:

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



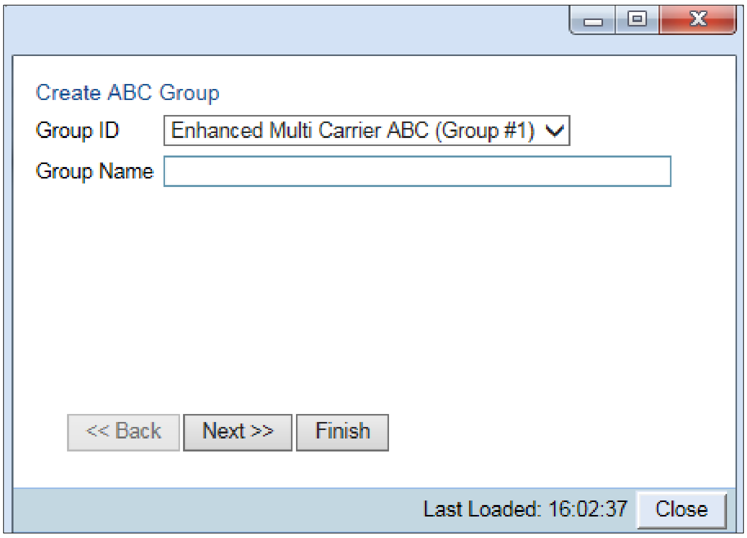
Microwave radio: Multi Carrier ABC Groups

Multi Carrier ABC configuration table

Group location ▲	Group Name	Radio/Ethernet Members	Operational state	Admin state

Figure 66: Multi Carrier ABC Groups Page (Empty)

ii Click **Create Group**. Page 1 of the Create ABC Group wizard opens.



Create ABC Group

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

Group Name:

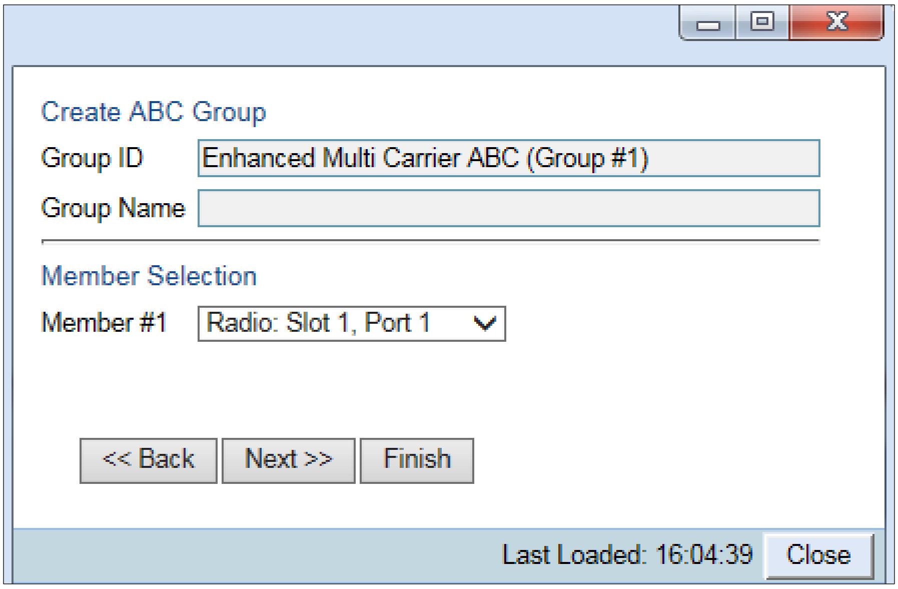
Last Loaded: 16:02:37

Figure 67: Create ABC Group Wizard – Page 1

iii In the **Group ID** field, select **Enhanced Multi Carrier ABC (Group #1)**.

iv Optionally, in the **Group Name** field, enter a descriptive name for the group.

v Click **Next**. Page 2 of the Create ABC Group wizard opens.



Create ABC Group

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

Group Name:

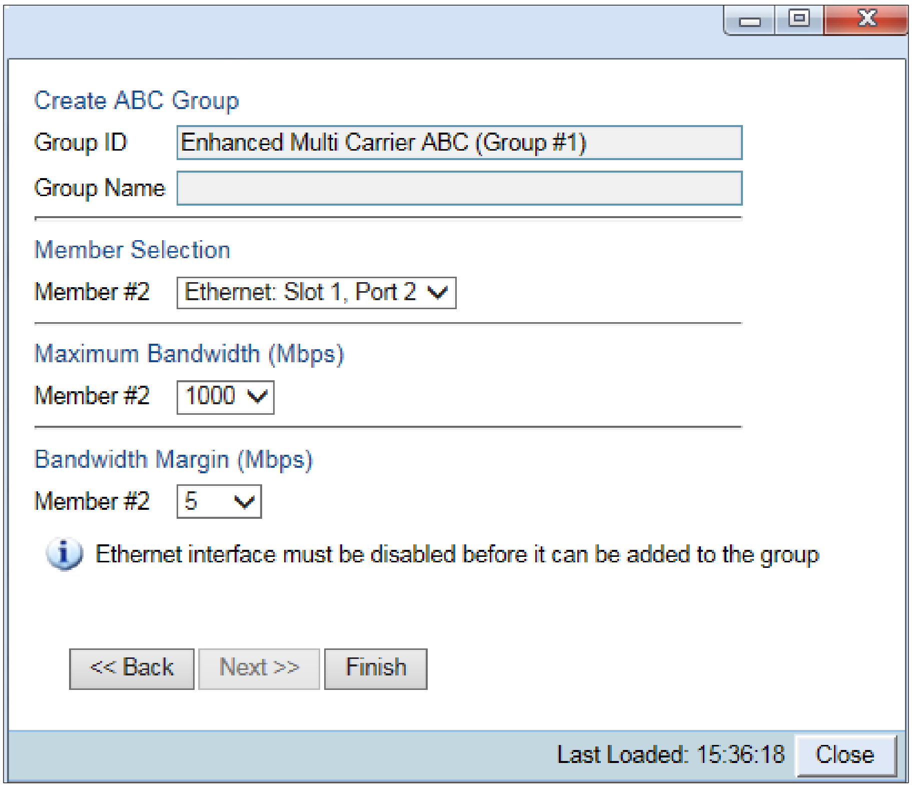
Member Selection

Member #1: Radio: Slot 1, Port 1

Figure 68: Create ABC Group Wizard – Page 2

vi In the **Member #1** field, select **Radio: Slot 1, Port 1**.

vii Click **Next**. Page 3 of the Create ABC Group wizard opens.



Create ABC Group

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

Group Name:

Member Selection

Member #2: Ethernet: Slot 1, Port 2

Maximum Bandwidth (Mbps)

Member #2: 1000

Bandwidth Margin (Mbps)

Member #2: 5

Ethernet interface must be disabled before it can be added to the group

Figure 69: Create ABC Group Wizard – Page 3

viiiIn the **Member #2** field under **Member Selection**, select **Ethernet: Slot 1, Port 2**.

ix In the **Member #2** field under **Maximum Bandwidth (Mbps)**, select the maximum traffic that the PTP 850E will pass to the paired unit. This parameters should be set to the maximum of the paired unit's capacity.

The default value is 1000 Mbps.

> Note
>
> The Maximum Bandwidth represents the L1 capacity of the radio link connected to the Ethernet member. The actual bandwidth that will be available for traffic is less due to overhead.
>
> When using a third-party radio as the paired unit, it is particularly
>
> important to set this parameter properly in order to ensure optimal performance. Failure to properly set this parameter may lead to frequent pauses as the queue fills up during low capacity periods, such as when weather conditions cause the ACM profile to drop.

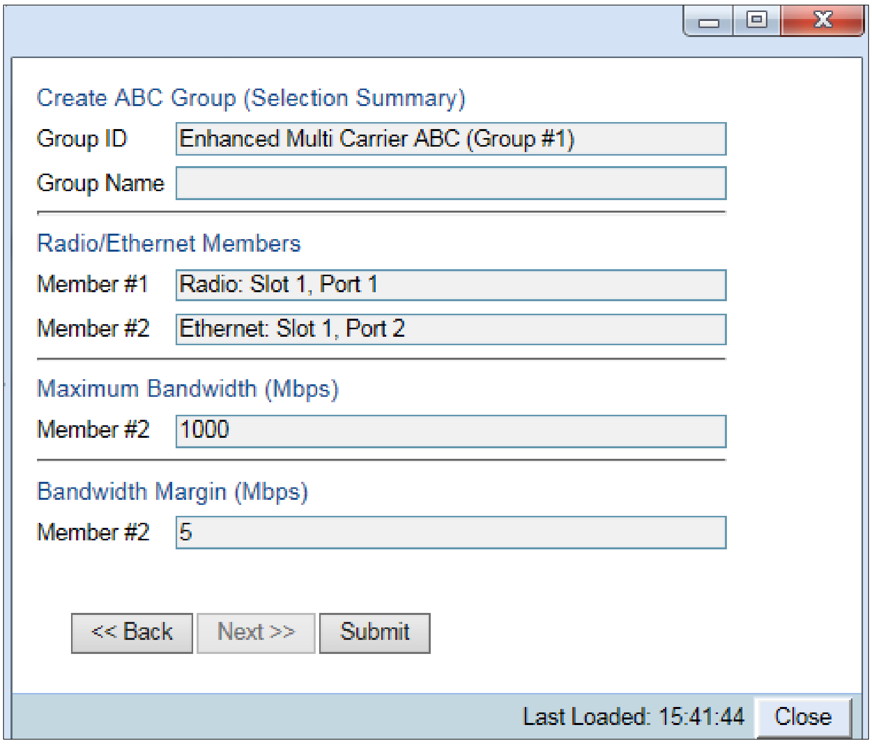
When using a third-party radio as the paired unit, it is particularly important to set this parameter properly in order to ensure optimal performance. Failure to properly set this parameter may lead to frequent pauses as the queue fills up during low capacity periods, such as when weather conditions cause the ACM profile to drop.

x In the **Member #2** field under **Bandwidth Margin (Mbps)**, select the bandwidth margin, in Mbps. This parameter deducts the specified throughput from the throughput the PTP 850E would otherwise pass to the paired unit. The purpose of this parameter is to provide a margin of safety that will avoid loss of traffic in the event that the ACM profile is reduced on the paired unit. It is recommended to configure this parameter as follows:

- If the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, or a third-party device with a bandwidth notification mechanism that will inform the PTP 850E of an impending reduction of the ACM profile before the reduction takes place, it is recommended to leave this parameter at its default value of 5 Mbps.
- If the paired unit is a third-party device without a bandwidth notification mechanism that will inform the PTP 850E of an impending reduction of the ACM profile before the reduction takes place, it is recommended to set this parameter to an amount equal to or greater than the largest throughput differential between any two adjacent profiles for the script configured on the paired unit.

The range of values is 5 to 100 Mbps.

xi Click Finish. The Selection Summary page of the Create ABC Group wizard opens.



Create ABC Group (Selection Summary)

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

Group Name:

Radio/Ethernet Members

Member #1: Radio: Slot 1, Port 1

Member #2: Ethernet: Slot 1, Port 2

Maximum Bandwidth (Mbps)

Member #2: 1000

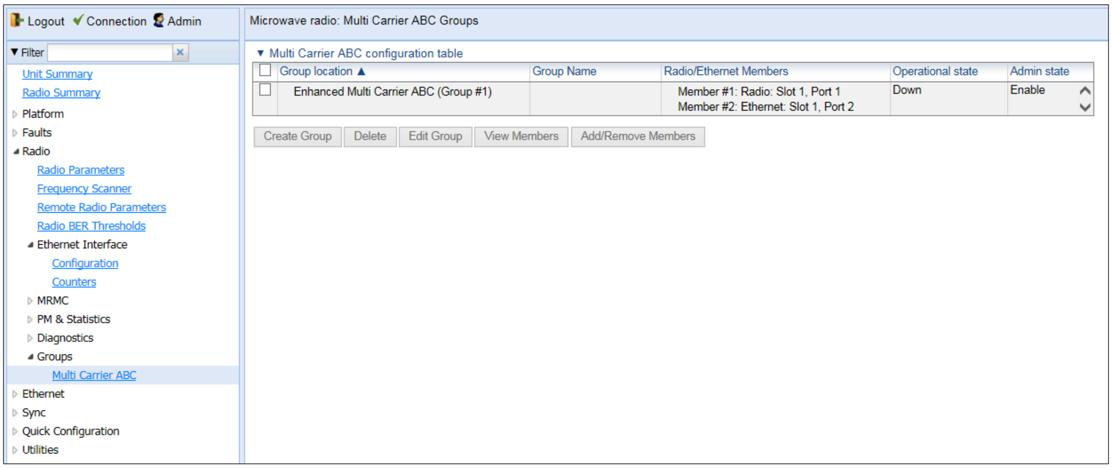
Bandwidth Margin (Mbps)

Member #2: 5

Last Loaded: 15:41:44

Figure 70: Create ABC Group Wizard – Selection Summary

xii Click **Submit**. The group is added to the Multi Carrier ABC page.



Microwave radio: Multi Carrier ABC Groups

▼ Multi Carrier ABC configuration table

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

Figure 71: Multi Carrier ABC Groups Page (Populated with Multiband Group)

7 Enable the Eth2 interface. See *Enabling the Interfaces (Interface Manager)*.

8 If the paired unit is an PTP 820C or PTP 820C-HP, verify that XPIC is disabled on the PTP 820C or PTP 820C-HP.

9 On the paired unit, configure a Pipe service between the port receiving traffic from the PTP 850E and the radio or Multi-Carrier ABC group.

10 On the paired unit, configure Automatic State Propagation with **ASP trigger by remote fault** enabled.

11 If the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, configure Radio BNM. For instructions, refer to the *User Guide for PTP 820 All-Outdoor Products*. Make sure to define a Name for the Radio BNM group.

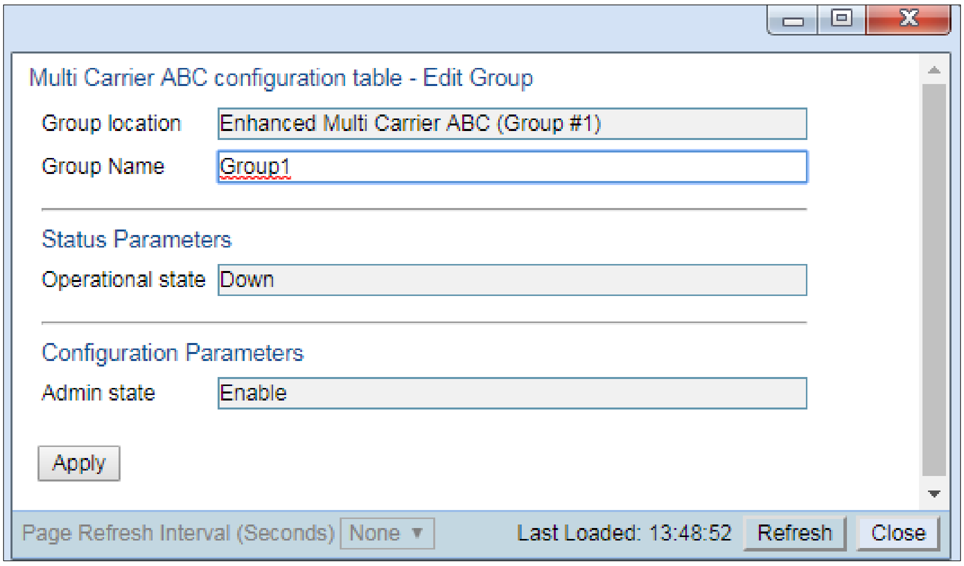
Note

If the paired unit is a third-party radio, enable 802.3X Flow Control.

Editing a Multiband Group or its Members

To change the Group Name of the Multiband group:

1 In the Multi Carrier ABC Groups page, select the group and click **Edit Group**. The Edit Group page opens.



Multi Carrier ABC configuration table - Edit Group

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

Group Name: Group1

Status Parameters

Operational state: Down

Configuration Parameters

Admin state: Enable

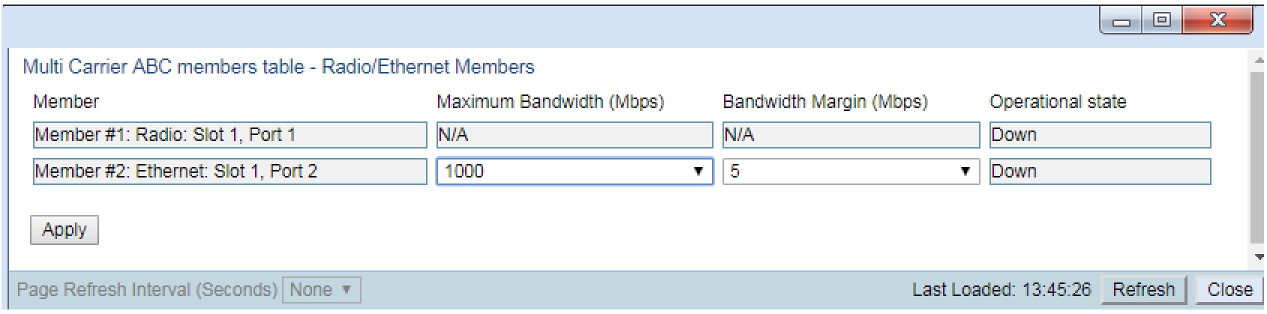
Figure 72: Multi Carrier ABC Groups – Edit Group Page

2 In the **Group Name** field, enter the new name.

3 Click **Apply**.

To change the **Maximum Bandwidth** and the **Bandwidth Margin** parameters:

1 In the Multi Carrier ABC Groups page, select the group and click **Edit Members**. The Edit Members page opens.



Multi Carrier ABC members table - Radio/Ethernet Members

Member	Maximum Bandwidth (Mbps)	Bandwidth Margin (Mbps)	Operational state
Member #1: Radio: Slot 1, Port 1	N/A	N/A	Down
Member #2: Ethernet: Slot 1, Port 2	1000	5	Down

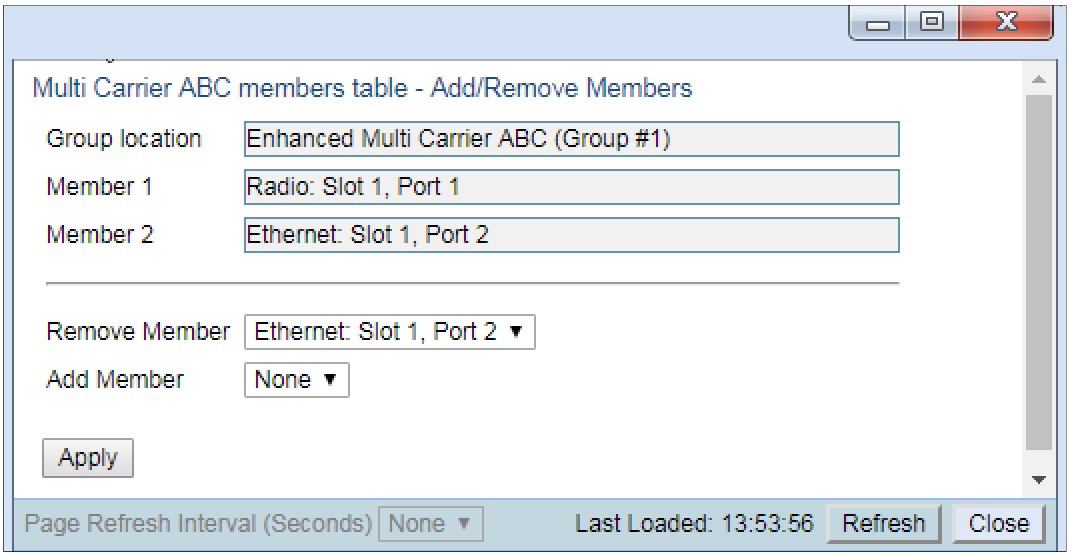
Figure 73: Multi Carrier ABC Groups – Edit Members Page

2 Edit the **Maximum Bandwidth** and/or **Bandwidth Margin** fields in the row of the Ethernet interface.

3 Click **Apply**.

To add or remove members to or from the group:

1 In the Multi Carrier ABC Groups page, select the group and click **Add/Remove Members**. The Add/Remove Members page opens.



Multi Carrier ABC members table - Add/Remove Members

Group location	Enhanced Multi Carrier ABC (Group #1)
Member 1	Radio: Slot 1, Port 1
Member 2	Ethernet: Slot 1, Port 2
Remove Member	Ethernet: Slot 1, Port 2
Add Member	None

Figure 74: Multi Carrier ABC Groups – Add/Remove Members Page

2 In the **Remove Member** field, select a member or select **Remove All**.

3 In the Add **Member field**, select a member.

4 Click **Apply**.

Multiband Management

The PTP 850E unit in a Multiband configuration can be managed normally, as in any other configuration. For in-band management of the PTP 850E, configure the management service on the PTP 850E Multiband group. See **Error! Reference source not found.**.

The following options are available for managing the paired unit in a Multiband configuration:

- Inband management via the PTP 850E
- Inband management directly from the external switch
- Out-of-Band management

Inband Management via the PTP 850E

The paired unit can managed via the PTP 850E. In-band management via the PTP 850E requires that the paired unit must have at least two free SFP ports. When the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, this requires an ESS hardware version for the PTP 820C, PTP 820C-HP, or PTP 820S or, for PTP 820C, a 2E2SX hardware version. To manage the paired unit via the PTP 850E, an optical cable must be connected between any free 1G Ethernet port on the PTP 850E and Eth3 on the PTP 820C, PTP 820C-HP, or PTP 820S or the Ethernet port receiving management data on the third-party unit.

A management service must be defined between the management port of the PTP 850E and the port on the PTP 850E that is connected to the paired unit for management. This transmits management to the paired unit. See **Error! Reference source not found.**.

The paired unit's management service should only have a service point for the Ethernet port connected to the PTP 850E for management. No service point should be defined on the radio or Multi-Carrier ABC group.

Note

To avoid loops, do not configure management between the paired unit and third-party equipment.

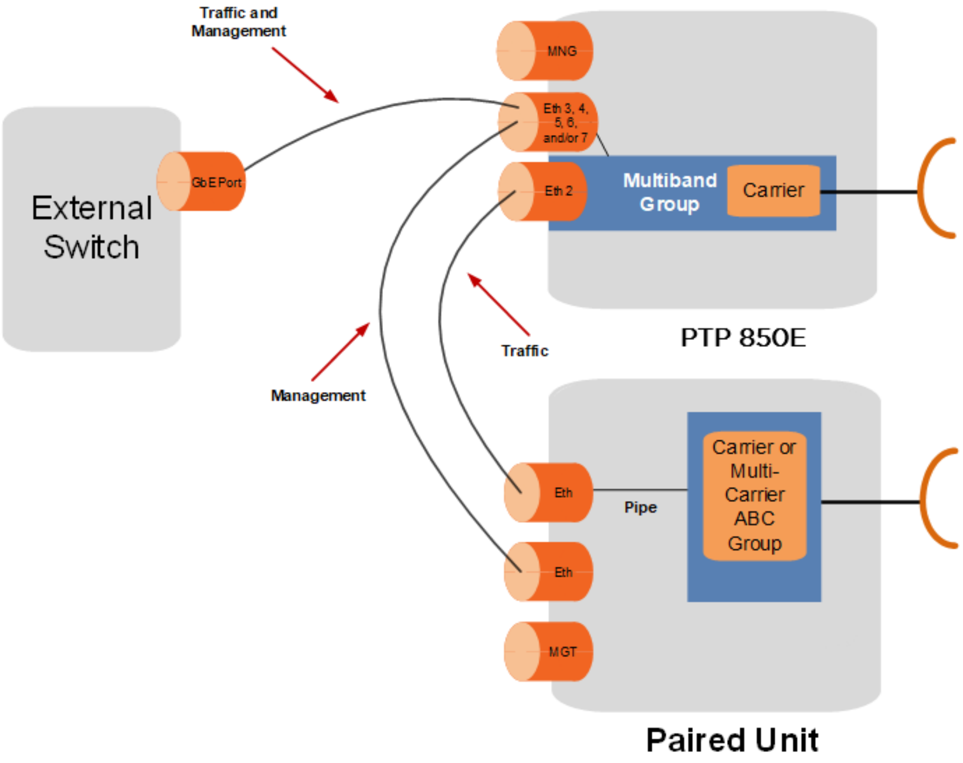


Figure 75: Multiband Configuration with Direct Inband Management to the Paired Unit

Inband Management Directly via the External Switch

The unit paired with the PTP 850E can be managed by means of a TP cable connected to the MGT port on the paired unit and to the LAN port on a PC or laptop. If the paired unit is a third-party radio, it can also be managed via out-of-band management.

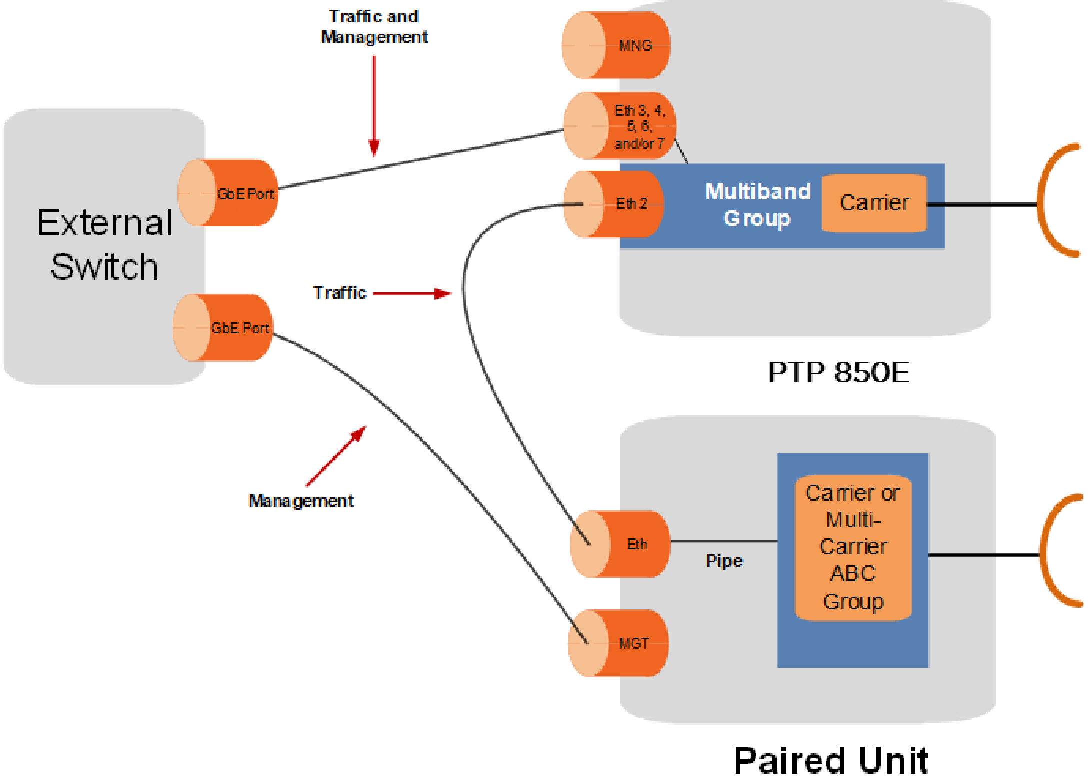


Figure 76: Multiband Configuration with Direct Inband Management to the Paired Unit

Out-of-Band Management

The paired unit can be managed by means of a TP cable connected to the MGT port on the paired unit and to the LAN port on a PC or laptop.

In this scenario, the PTP 850E is managed by connecting the PC or laptop used for management to the PoE Injector, which provides transfers power and management to the MGT/PoE port of the PTP 850E.

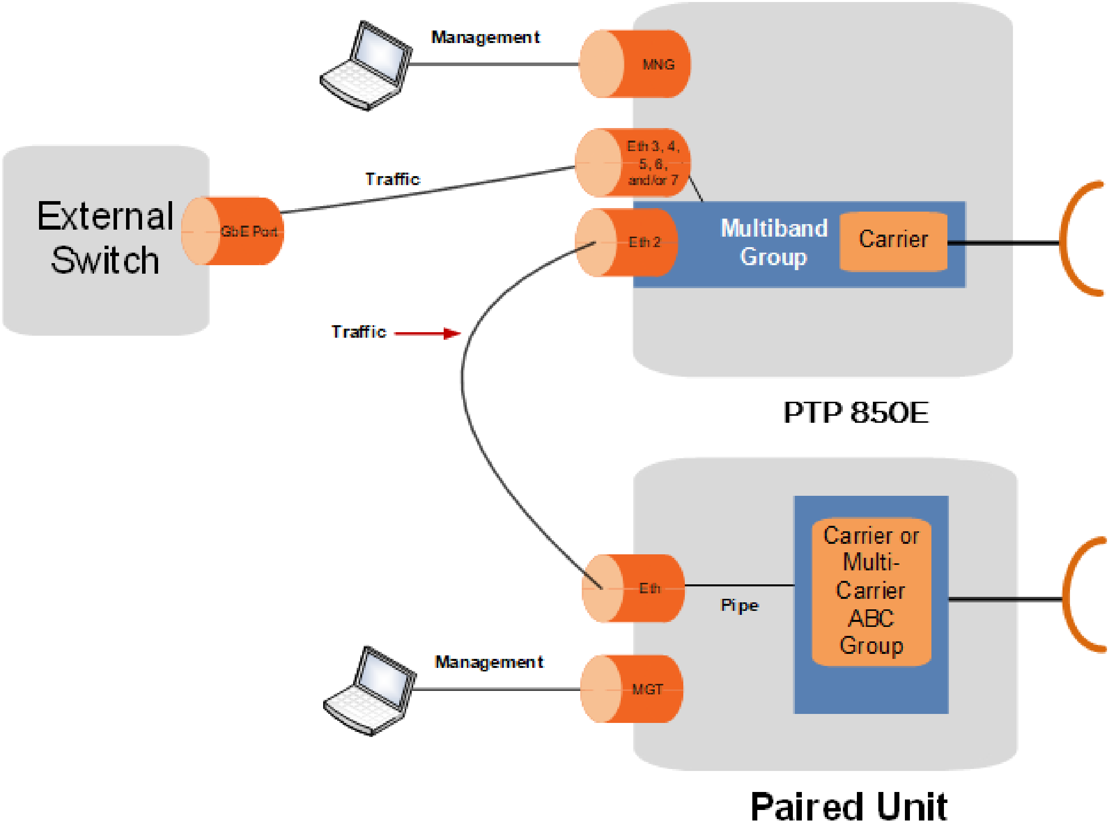


Figure 77: Multiband Configuration with Out-of-Band Management to Both Units

Configuring Synchronization in a Multiband Node

SyncE and 1588 PTP can be used in Multiband nodes. SyncE and 1588 PTP can be configured for both the PTP 850E and the Microwave unit paired with the PTP 850E. For SyncE via the PTP 850E, the paired unit must have at least two free SFP ports. When the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, this requires an ESS hardware version for the PTP 820C, PTP 820C-HP, or PTP 820S or, for PTP 820C, a 2E2SX hardware version. SyncE for the paired unit requires an optical cable between any free 1G Ethernet port on the PTP 850E and Eth3 on the PTP 820C, PTP 820C-HP, or PTP 820S or the Ethernet port receiving management data on the third-party unit. The same cable can be used for both SyncE and in-band management.

Note

When a third-party unit is paired with the PTP 850E, it is a prerequisite that the third-party radio unit support SyncE in order to provide synchronization for the Multiband node.

When a third-party unit is paired with the PTP 850E, it is a prerequisite that the third-party radio unit support SyncE and, if required, 1588 PTP in order to provide synchronization for the Multiband node.

To configure SyncE on a Multiband node:

1 On the PTP 850E, configure the following synchronization sources:
   - The Ethernet port attached to the external switch must be configured as the outgoing clock to the downstream interface
   - The PTP 850E radio interface must be configured with SSM enabled and first priority
   - The Ethernet port on the PTP 850E transmitting synchronization to the paired unit must be configured with SSM enabled and second priority

   Do not configure Eth2 as a synchronization source.

2 On the paired unit, configure two synchronization sources: the Ethernet port receiving synchronization from the PTP 850E, and the radio. When using Multi-Carrier ABC, configure both radios as synchronization sources.

In ring configurations, configure priority order in the direction of traffic on the ring.

For instructions on configuring SyncE, see *Configuring the Sync Source*.

Configuring SyncE in a Multiband Node

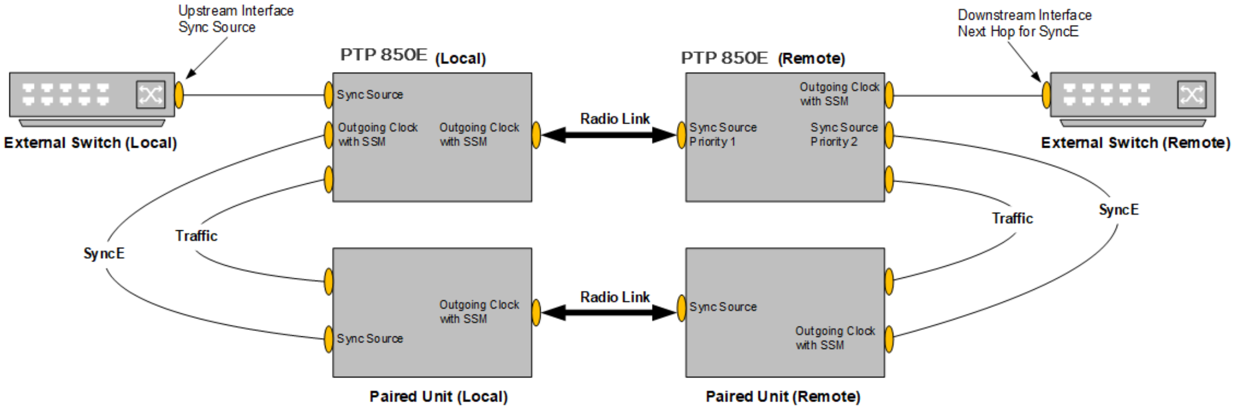
SyncE for a Multiband node requires an optical cable between the PTP 850E and the paired unit, in addition to the cable carrying traffic between the two units. Therefore, the paired unit must have at least two free SFP ports. The same connection can be used for both SyncE and in-band management.

- On the PTP 850E, use any free SFP port for the SyncE connection with the paired unit.
- When the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, an ESS or 2E2SX (PTP 820C) hardware version is required. Use Eth3 for the SyncE connection.

To configure SyncE on a Multiband node:

- On the PTP 850E connected to the upstream sync source, configure the following:
  - Configure the port connected to the external switch as a sync source.
  - Configure the radio interface as outgoing clock, with SSM enabled.
  - Configure the port transmitting SyncE to the paired unit as outgoing clock, with SSM enabled.
- On the local paired unit, configure the following:
  - Configure the port receiving SyncE from the PTP 850E as a sync source.
  - Configure the radio interface or Multi-Carrier ABC group as outgoing clock, with SSM enabled.
- On the PTP 850E connected to the downstream interface, configure the following:
  - Configure the port connected to the external switch as outgoing clock, with SSM enabled.
  - Configure the radio interface as a sync source with priority 1.
  - Configure the port receiving SyncE from the paired unit as a sync source with priority 2.
- On the remote paired unit, configure the following:
  - Configure the port transmitting SyncE to the PTP 850E as outgoing clock, with SSM enabled.
  - Configure the radio interface or Multi-Carrier ABC group as a sync source.

Figure 78 Multiband Configuration with SyncE



In ring configurations, configure priority order in the direction of traffic on the ring.

For instructions on configuring SyncE, see *Configuring the Sync Source*.

Configuring 1588 PTP in a Multiband Node

To use 1588 PTP on an PTP 850E Multiband node, you must configure Boundary Clock on the PTP 850E units and Transparent Clock on all of the units, as described below.

Note

If the Microwave link goes down, 1588 packets will not be transmitted to the other side of the Multiband link.

To configure 1588 PTP for the PTP 850E Multiband node:

1. Configure SyncE following the instructions in *Configuring SyncE in a Multiband Node*.
2. Enable 1588 PTP on each unit, including the PTP 850E and the paired unit on both sides of the link:
   a. Select **Sync > 1588 > General Configuration**. The 1588 – General Configuration page.
   b. In the **1588 PTP** field, select **Enable**.
   c. Click **Apply**.
3. On each PTP 850E unit, enable Boundary clock on:
   - The port connected to the external switch.
   - The port used for synchronization with the paired unit.

See ***Error! Reference source not found.***.

4. Configure a point-to-point service between the following ports on the paired unit:
   - The port used for synchronization with the PTP 850E.
   - The radio interface or group.

Configuring XPIC

This section includes:

- XPIC Overview
- Configuring the Radio Carriers
- Deleting an AMCC (XPIC) Group
- **Error! Reference source not found.**
- **Error! Reference source not found.**

XPIC Overview

Cross Polarization Interference Canceller (XPIC) is a feature that enables two radio carriers to use the same frequency with a polarity separation between them. Since they will never be completely orthogonal, some signal cancelation is required.

With PTP 850C, XPIC is configured with the two carriers of a single PTP 850C unit on each side of the link.

With PTP 850C, XPIC uses two PTP 850E units on each side of the link.

XPIC enables PTP 850E links of up to 20 Gbps, consisting of 10 Gbps per each PTP 850E unit.

XPIC with PTP 850C - Overview

XPIC enables PTP 850C links of up to 2 Gbps, consisting of 1 Gbps per carrier.[12] XPIC can be installed in either of the following configurations:

- Direct Mount – The PTP 850C unit is connected to the antenna via an OMT.
- Remote Mount – The PTP 850C unit is connected to the antenna via two flexible waveguides. Some configurations also require an OMT.

To configure and enable XPIC:

- Install the PTP 850C unit in a dual polarization configuration, according to the instructions in the PTP 850C Installation Guide.
- Configure the carriers – See *Configuring the Radio Carriers*
- Perform antenna alignment – See *Performing Antenna Alignment for XPIC*

In order for XPIC to be operational, all the following conditions must be met:

- The frequency of both carriers should be equal.
- The same script must be loaded in both carriers.

XPIC with PTP 850E - Overview

XPIC enables PTP 850E links of up to 20 Gbps, consisting of 10 Gbps per each PTP 850E unit.

An PTP 850E 2+0 XPIC configuration requires two PTP 850E units on each side of the link. Two options are available:

An PTP 850E 2+0 XPIC configuration requires two PTP 850E units on each side of the link. Two options are available:

- Direct Mount – The PTP 850E units are connected to the antenna via an OMT. One unit must be installed with horizontal polarization and the other must be installed with vertical polarization.
- Integrated Antenna – One PTP 850E unit and integrated antenna is assembled with a vertical polarization and the other PTP 850E unit and integrated antenna is assembled with a horizontal polarization.

For both options, the following cables must be used to connect the two units:

- An XPIC cable must be connected between the Protection/XPIC ports (P6) of each unit. This cable carries the data necessary for each unit to perform interference cancellation.
- A Clock Sharing cable must be connected between the TNC ports of each unit. This cable transmits clock frequency information between the two units, enabling synchronization.

On each side of the link, the unit with the higher MAC address is automatically assigned the role of clock master unit.

Each PTP 850E unit receives traffic from the external switch independently of the other unit. The traffic flows are completely independent, with no traffic sharing or load balancing between the units.

Management data is not shared between the two PTP 850E units. Therefore, management must be configured independently for each PTP 850E unit. Inband management can be used as long as LAG is not configured on the external switch. However, if LAG *is* configured on the external switch, inband management cannot be used, since there is no mechanism for sharing management traffic between the PTP 850E units.

Figure 79 2+0 XPIC Configuration – Direct Mount

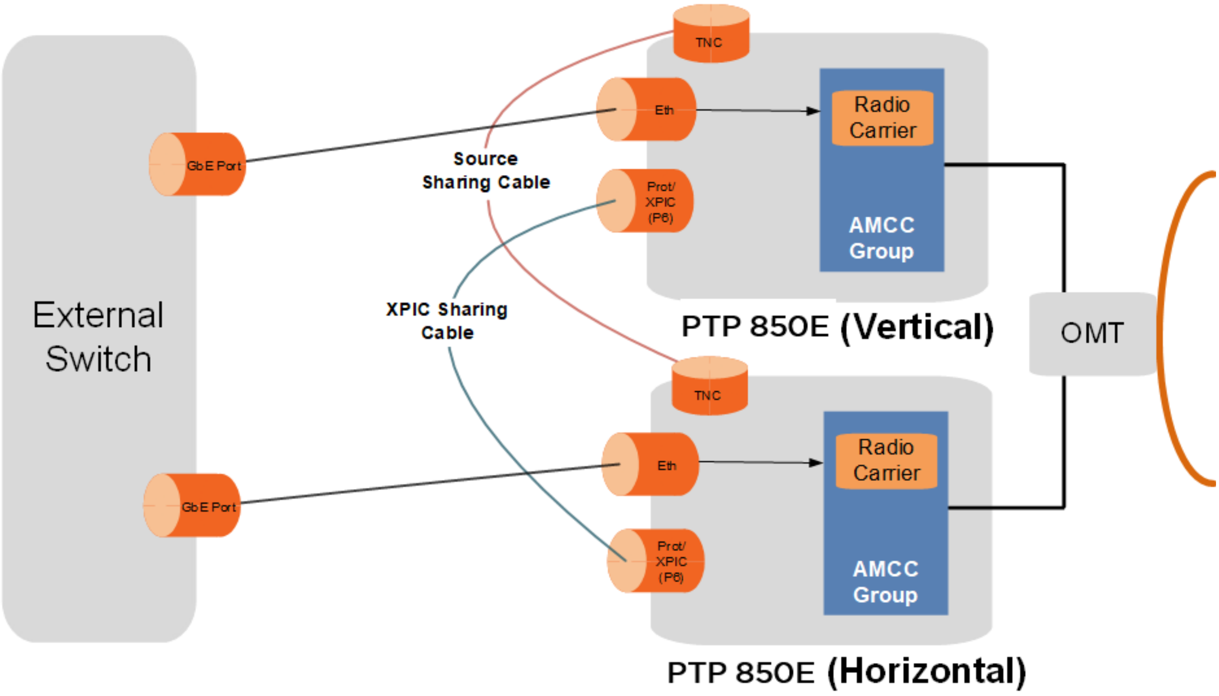
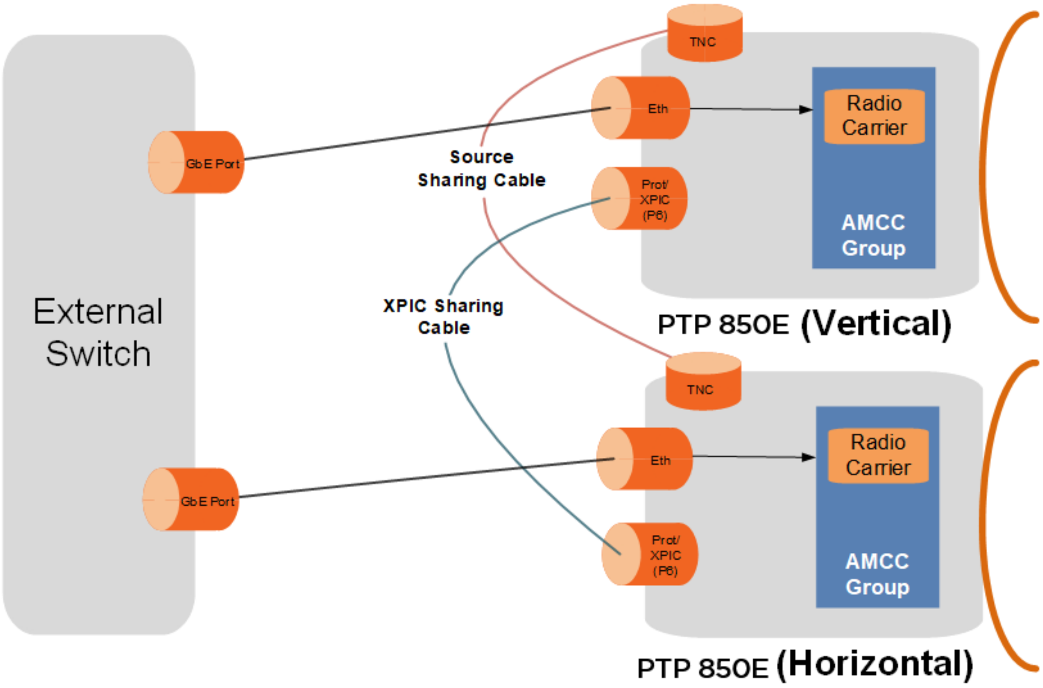


Figure 80 2+0 XPIC Configuration – Integrated Antenna



In order for XPIC to be operational, all the following conditions must be met:

- The frequency of both carriers should be equal.
- The same script must be loaded in both carriers.

Note

Power redundancy and PoE cannot be used with XPIC.

To configure and enable XPIC:

- Install the PTP 850E units and cables – See the PTP 850E Installation Guide, Section 5.5, 2+0 (XPIC) with 43 dBi Flat Antenna and Alignment Device or Section 6.3, 2+0 Direct Mount Dual Polarization (XPIC).
- Configure the carriers – See Configuring the Radio Carriers
- Perform antenna alignment – See **Error! Reference source not found.**

Configuring the Radio Carriers

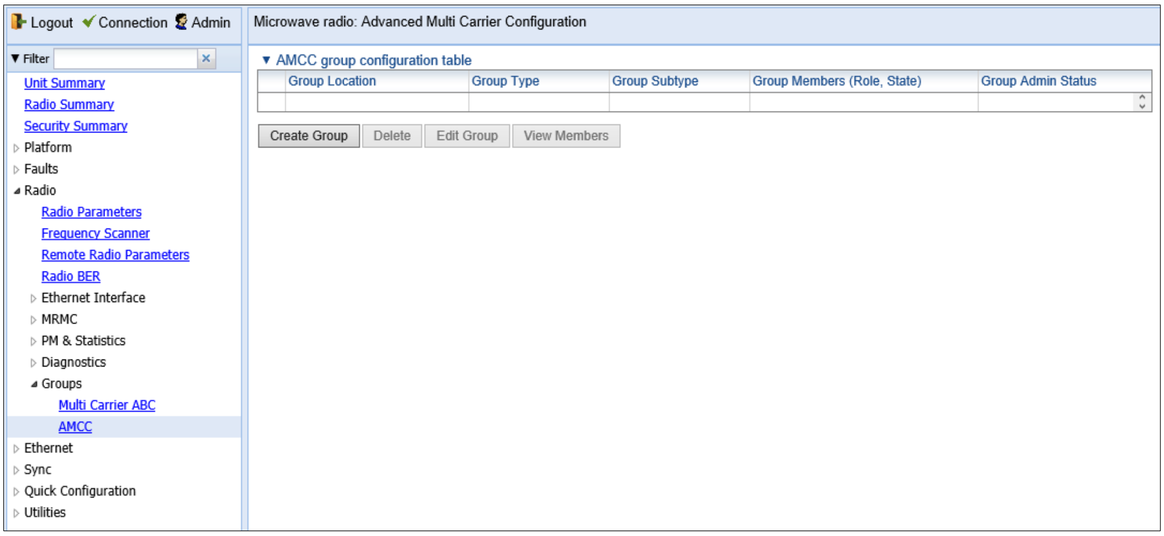
Note

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

Configuring XPIC on the Radio Carriers – PTP 850C

1. Configure each radio carrier unit on both sides of the link to the desired frequency channel. Both carriers must be configured to the same frequency channel.
2. Create an AMCC group .To create an AMCC group:
   a. Select **Radio > Groups > AMCC**. The Advanced Multi Carrier Configuration page opens.

Figure 81 Advanced Multi Carrier Configuration Page



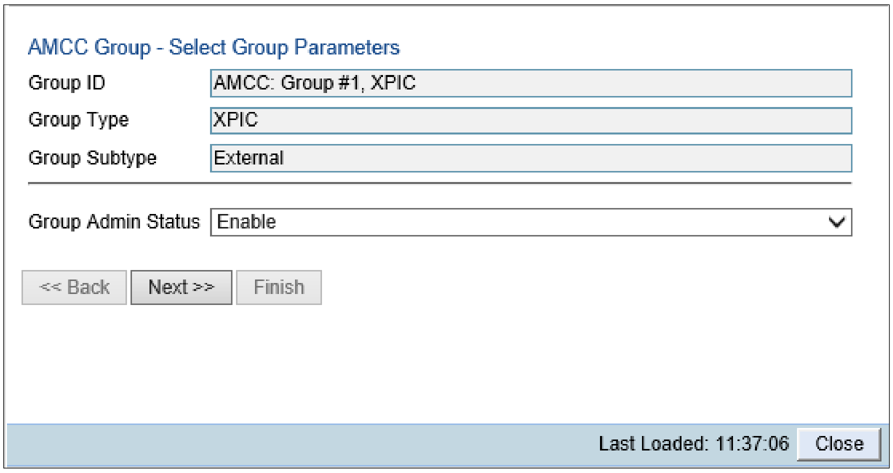
Microwave radio: Advanced Multi Carrier Configuration

▼ AMCC group configuration table

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

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

Figure 82 AMCC Group – Select Group Parameters Page



AMCC Group - Select Group Parameters

Group ID: AMCC: Group #1, XPIC

Group Type: XPIC

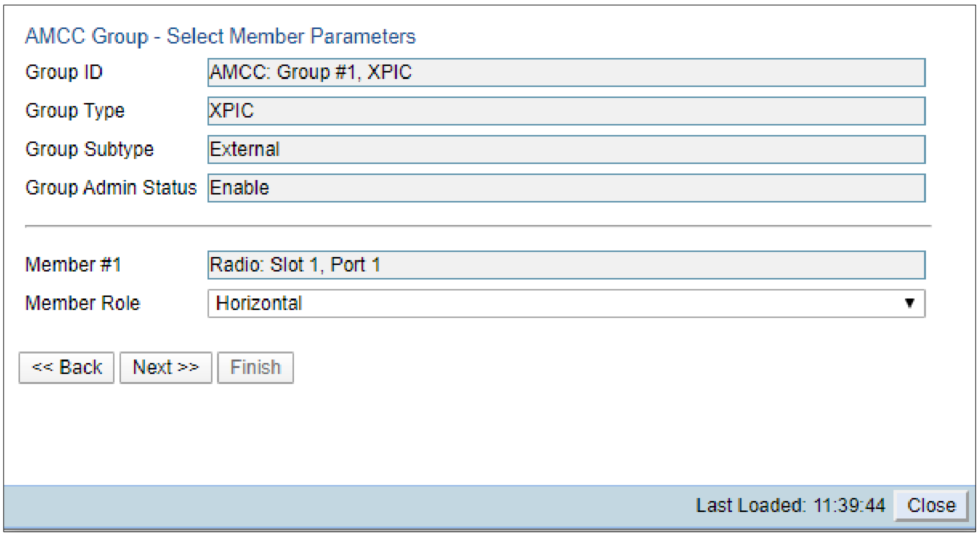
Group Subtype: External

Group Admin Status: Enable

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

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

Figure 83 AMCC Group – Select Member Parameters Page



AMCC Group - Select Member Parameters

Group ID: AMCC: Group #1, XPIC

Group Type: XPIC

Group Subtype: External

Group Admin Status: Enable

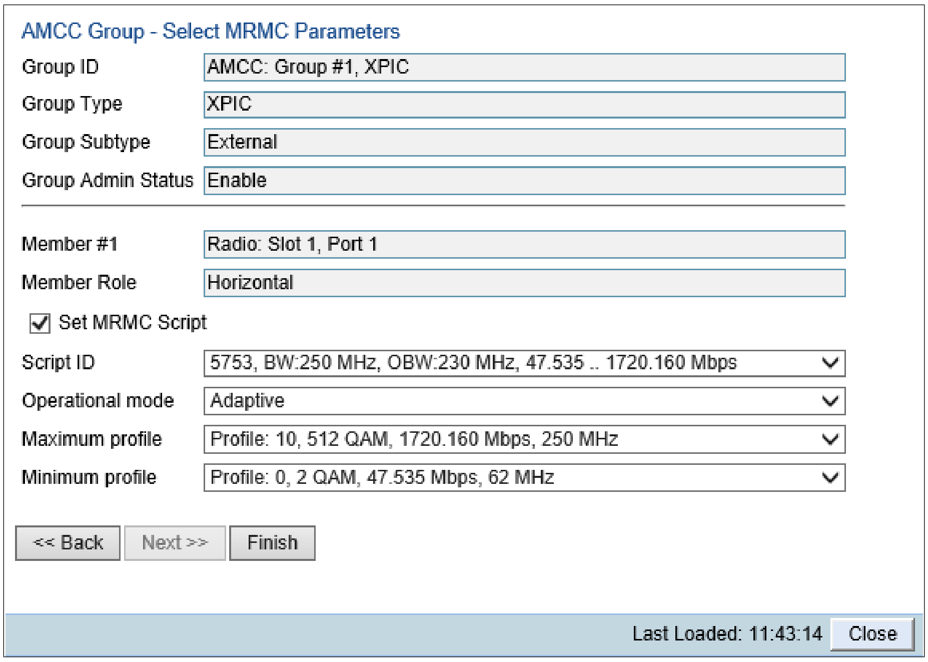
Member #1: Radio: Slot 1, Port 1

Member Role: Horizontal

e. In the **Member Role** field, select **Horizontal** or **Vertical**. Make sure the Member Role you select matches the actual polarization of the PTP 850E unit, and that the Member Role you configure in the paired unit is not the same as the role you configure here.

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

Figure 84 AMCC Group – Select MRMC Parameters Page



AMCC Group - Select MRMC Parameters

Group ID: AMCC: Group #1, XPIC

Group Type: XPIC

Group Subtype: External

Group Admin Status: Enable

Member #1: Radio: Slot 1, Port 1

Member Role: Horizontal

☑ Set MRMC Script

Script ID: 5753, BW:250 MHz, OBW:230 MHz, 47.535 .. 1720.160 Mbps

Operational mode: Adaptive

Maximum profile: Profile: 10, 512 QAM, 1720.160 Mbps, 250 MHz

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

Last Loaded: 11:43:14

g. Make sure **Set MRMC Script** is selected.

h. In the **Script ID** field, select the MRMC script you want to assign to the radio. Only XPIC scripts will appear in this field. For a full explanation of choosing an MRMC script, see ***Error! Reference source not found.***.

i. In the Operational **Mode** field, select the ACM mode: **Adaptive** or **Fixed**.

- In Adaptive ACM mode, TX and RX rates are dynamic. An ACM-enabled radio system automatically chooses which profile to use according to the channel fading conditions.
- Fixed ACM mode applies constant TX and RX rates. However, unlike regular scripts, with a Fixed ACM script you can specify a maximum profile to inhibit inefficient transmission levels.

j. Do one of the following:

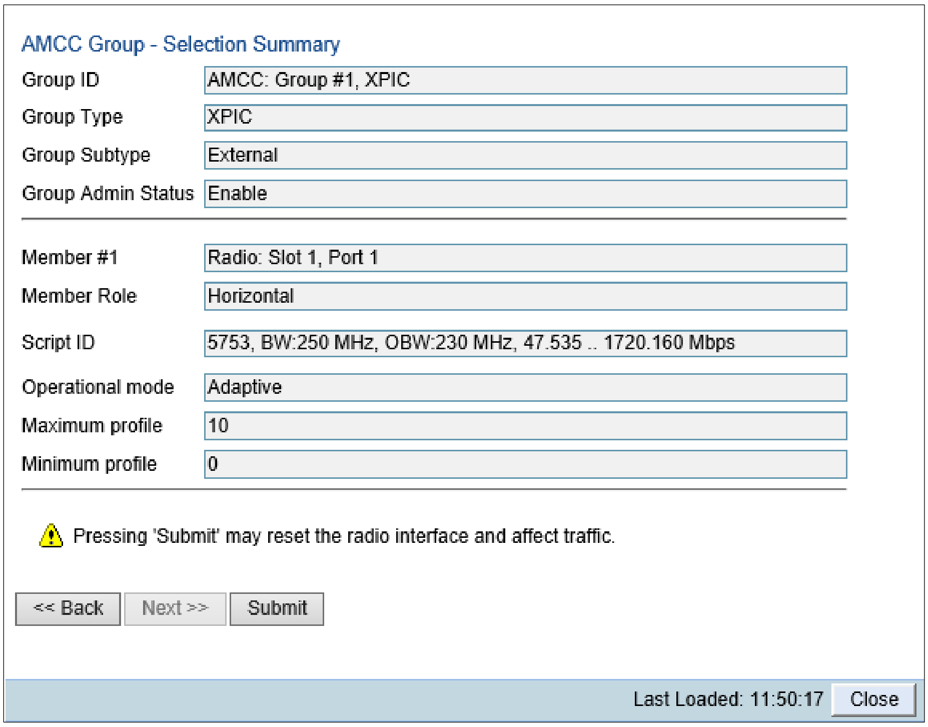
- If you selected Adaptive in the Operational Mode field, the following two fields are displayed:
  - Maximum profile – Enter the maximum profile for the script. See **Error! R eference source not found.**.
  - Minimum profile – Enter the minimum profile for the script. See **Error! R eference source not found.**.

> Note
>
> The default minimum profile is 2.

- If you selected **Fixed** in the **Operational Mode** field, the next field is **Profile**. Select the ACM profile for the radio in the **Profile** field.

k. Click **Finish**. The AMCC Group – Selection Summary page opens.

Figure 85 AMCC Group – Selection Summary Page



AMCC Group - Selection Summary

Group ID	AMCC: Group #1, XPIC
Group Type	XPIC
Group Subtype	External
Group Admin Status	Enable
Member #1	Radio: Slot 1, Port 1
Member Role	Horizontal
Script ID	5753, BW:250 MHz, OBW:230 MHz, 47.535 .. 1720.160 Mbps
Operational mode	Adaptive
Maximum profile	10
Minimum profile	0

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

Last Loaded: 11:50:17

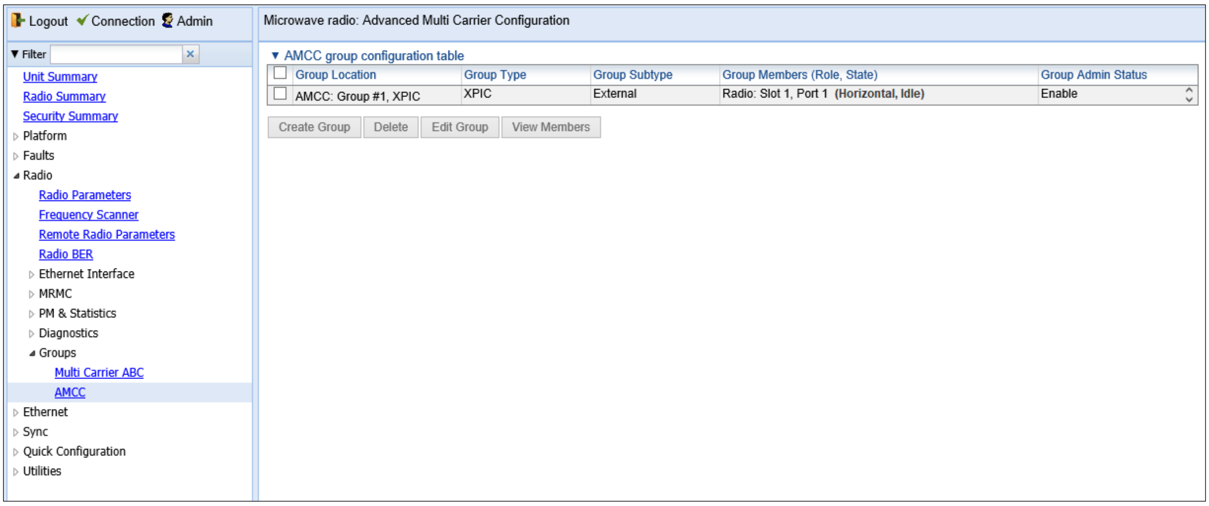
I. Review the parameters you have selected. If they are correct, click **Submit**. If you want to change any of the configurable parameters, click **Back**.

Deleting an AMCC (XPIC) Group

To delete an AMCC (XPIC) group:

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

Figure 86 Advanced Multi Carrier Configuration Page (Populated)



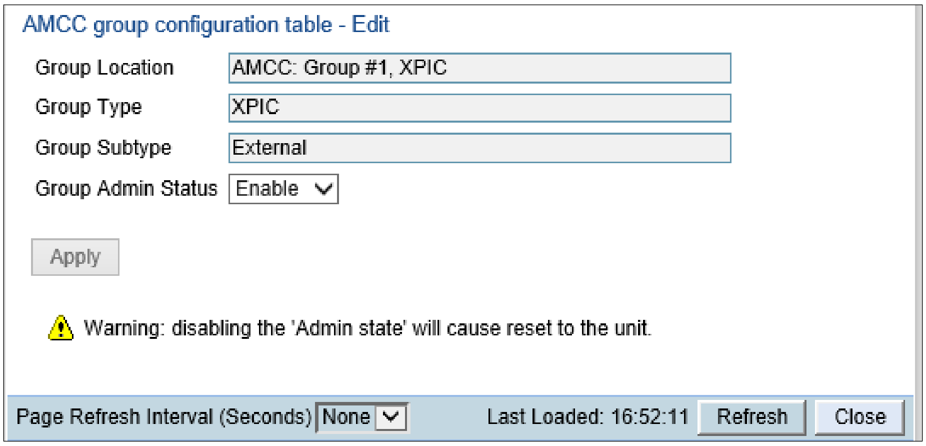
Microwave radio: Advanced Multi Carrier Configuration

▼ AMCC group configuration table

□ Group Location	Group Type	Group Subtype	Group Members (Role, State)	Group Admin Status
□ AMCC: Group #1, XPIC	XPIC	External	Radio: Slot 1, Port 1 (Horizontal, Idle)	Enable

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

Figure 87 AMCC Group – Edit Page



AMCC group configuration table - Edit

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

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

Page Refresh Interval (Seconds) None Last Loaded: 16:52:11

3. In the Group Admin Status field, select Disable.
4. Click Apply, then Close.
5. In the Advanced Multi Carrier Configuration page, select the group and click

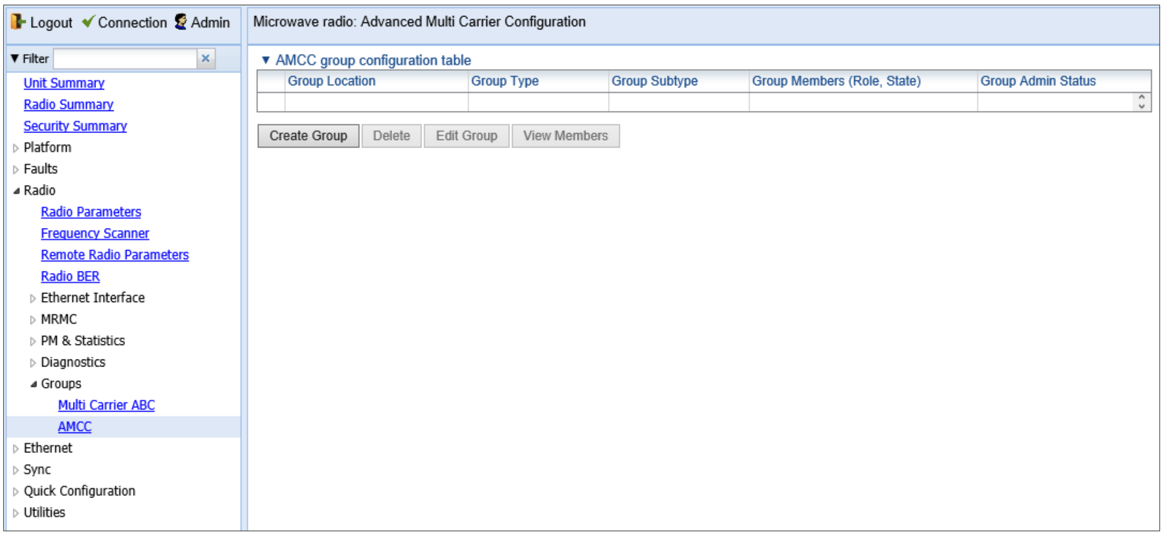
Configuring XPIC on the Radio Carriers – PTP 850E

To configure the radio carriers:

1 Configure each PTP 850E unit on both sides of the link to the desired frequency channel. Both carriers must be configured to the same frequency channel. See *Configuring the Radio Parameters*.

2 Create an AMCC group for the radio carrier. You must create a group on each PTP 850E unit, even though each group consists of only one radio carrier. To create an AMCC group:

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



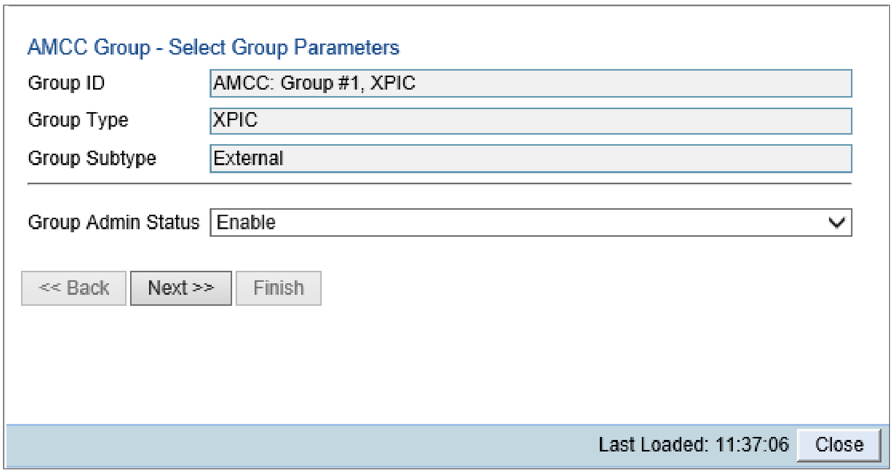
Microwave radio: Advanced Multi Carrier Configuration

AMCC group configuration table

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

Figure 122: Advanced Multi Carrier Configuration Page

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



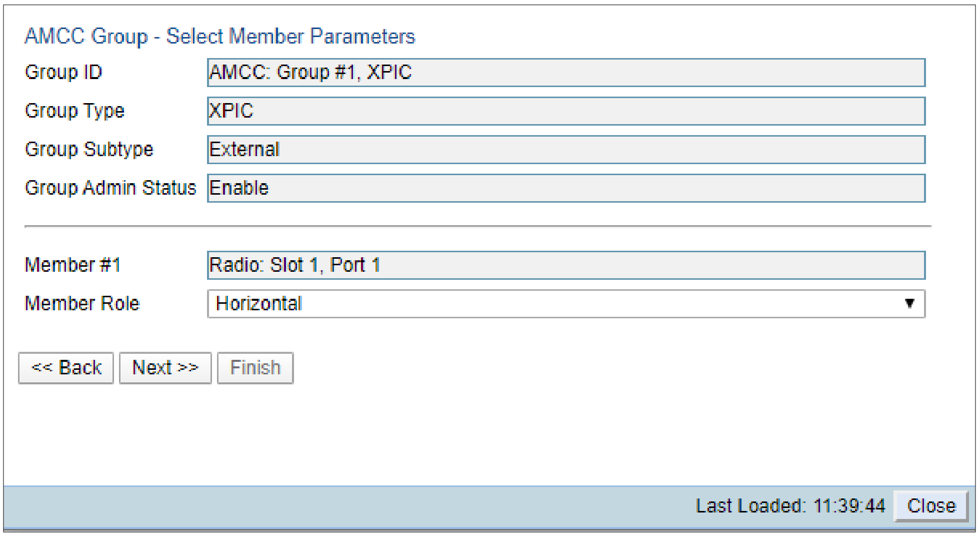
AMCC Group - Select Group Parameters

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

Figure 123: AMCC Group – Select Group Parameters Page

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

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



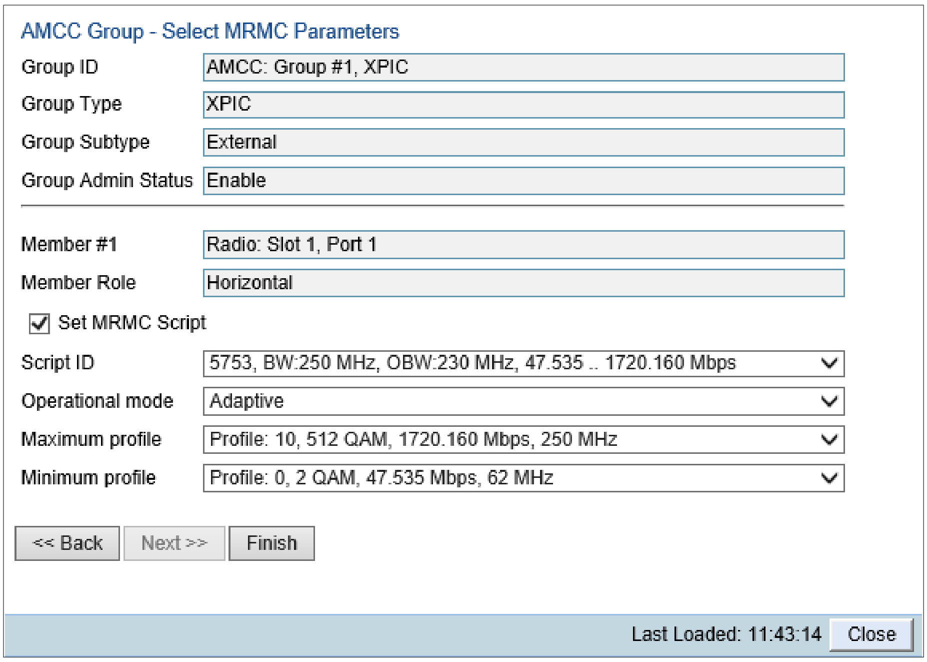
AMCC Group - Select Member Parameters

Group ID	AMCC: Group #1, XPIC
Group Type	XPIC
Group Subtype	External
Group Admin Status	Enable
Member #1	Radio: Slot 1, Port 1
Member Role	Horizontal

Figure 124: AMCC Group – Select Member Parameters Page

v In the Member Role field, select Horizontal or Vertical. Make sure the Member Role you select matches the actual polarization of the PTP 850E unit, and that the Member Role you configure in the paired unit is not the same as the role you configure here.

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



AMCC Group - Select MRMC Parameters

Group ID	AMCC: Group #1, XPIC
Group Type	XPIC
Group Subtype	External
Group Admin Status	Enable
Member #1	Radio: Slot 1, Port 1
Member Role	Horizontal

☑ Set MRMC Script

Script ID	5753, BW:250 MHz, OBW:230 MHz, 47.535 .. 1720.160 Mbps
Operational mode	Adaptive
Maximum profile	Profile: 10, 512 QAM, 1720.160 Mbps, 250 MHz
Minimum profile	Profile: 0, 2 QAM, 47.535 Mbps, 62 MHz

Figure 125: AMCC Group – Select MRMC Parameters Page

vii Make sure Set MRMC Script is selected.

viii In the Script ID field, select the MRMC script you want to assign to the radio. Only XPIC scripts will appear in this field. For a full explanation of choosing an MRMC script, see *Configuring the Radio (MRMC) Script(s)*.

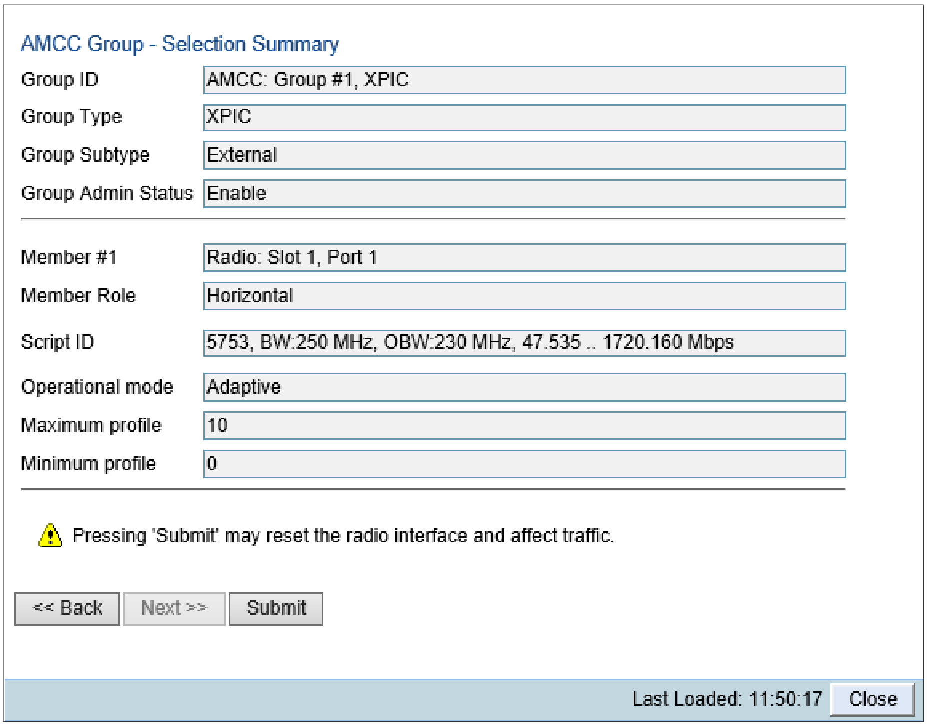
ix In the **Operational** Mode field, select the ACM mode: Adaptive or Fixed.

- In Adaptive ACM mode, TX and RX rates are dynamic. An ACM-enabled radio system automatically chooses which profile to use according to the channel fading conditions.
- Fixed ACM mode applies constant TX and RX rates. However, unlike regular scripts, with a Fixed ACM script you can specify a maximum profile to inhibit inefficient transmission levels.

x Do one of the following:

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

xi Click Finish. The AMCC Group – Selection Summary page opens.



AMCC Group - Selection Summary

Group ID	AMCC: Group #1, XPIC
Group Type	XPIC
Group Subtype	External
Group Admin Status	Enable
Member #1	Radio: Slot 1, Port 1
Member Role	Horizontal
Script ID	5753, BW:250 MHz, OBW:230 MHz, 47.535 .. 1720.160 Mbps
Operational mode	Adaptive
Maximum profile	10
Minimum profile	0

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

Last Loaded: 11:50:17

Figure 126: AMCC Group – Selection Summary Page

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

Performing Antenna Alignment for XPIC

The antenna alignment procedure for XPIC depends on whether you are using a direct mount configuration with a single antenna and OMT or an integrated antenna configuration with two PTP 850E-integrated antenna assemblies.

XPIC Alignment for PTP 850C

1 Align the antennas for the first carrier. While you are aligning these antennas, mute the second carrier. See *Configuring the Radio Parameters*.

2 Adjust the antenna alignment until you achieve the maximum RSL for the first-carrier link (the “RSL$_{wanted}$”). This RSL should be no more than +/-2 dB from the expected level. Record the RSL of the first carrier as the “RSL$_{wanted}$”).

3 Measure the RSL of the second carrier and record it as the “RSL$_{unwanted}$”).

4 Determine the XPD by subtracting RSL$_{unwanted}$ from the RSL$_{wanted}$.

5 The XPD should be between 25dB and 30dB. If it is not, you should adjust the OMT assembly on the back of the antenna at one side of the link until you achieve the highest XPD, which should be no less than 25dB. Adjust the OMT very slowly in a right-left direction. OMT adjustment requires very fine movements and it may take several minutes to achieve the best possible XPD.

6 Unmute all the carriers and check the RSL levels of all the carriers on both sides of the link. The RSL of the horizontal carrier of the local unit should match the RSL of the vertical carrier of the remote unit, within ±2dB. The RSL of the vertical carrier of the local unit should match the RSL of the horizontal carrier of the remote unit, within ±2dB.

7 Check the XPI levels of all the carriers on both sides of the link. All the carriers should have approximately the same XPI value. Do not adjust the XPI at the remote side of the link, as this may cause the XPI at the local side of the link to deteriorate.

> **Note:** In some cases, the XPI might not exceed the required 25dB minimum due to adverse atmospheric conditions. If you believe this to be the case, you can leave the configuration at the lower values, but be sure to monitor the XPI to make sure it subsequently exceeds 25dB. A normal XPI level in clear sky conditions is between 25 and 30dB.

XPIC Alignment for PTP 850E Direct Mount Configurations

1. Make sure the antennas have been properly leveled on both sides of the link. Proper leveling is crucial in order to optimize XPIC performance.
2. Mute the horizontal unit.
3. Adjust the antenna alignment until you achieve the maximum RSL for the vertical unit (the “RSL_{wanted}”). This RSL should be no more than +/-2 dB from the expected level. Record the RSL of the first carrier as the “RSL_{wanted}”).
4. Measure the RSL of the horizontal unit and record it as the “$RSL_{unwanted}$”).
5. Determine the XPD by subtracting the $RSL_{unwanted}$ from the RSL_{wanted}.
6. The XPD should be between 25dB and 30dB balanced on the vertical and horizontal units. If it is not, you should adjust the OMT assembly on the back of the antenna at one side of the link until you achieve the balance and highest XPD, which should be no less than 25dB. Adjust the OMT very slowly in a right-left direction. OMT adjustment requires very fine movements and it may take several minutes to achieve the best possible XPD.
7. Unmute all the carriers and check the RSL levels of all the carriers on both sides of the link. The RSL of the horizontal unit at the local site should match the RSL of the vertical unit at the local site, within ±2dB. The RSL of the vertical unit at the remote site should match the RSL of the horizontal unit at the remote site, within ±2dB.

XPIC Alignment for PTP 850E Integrated Antenna Configurations

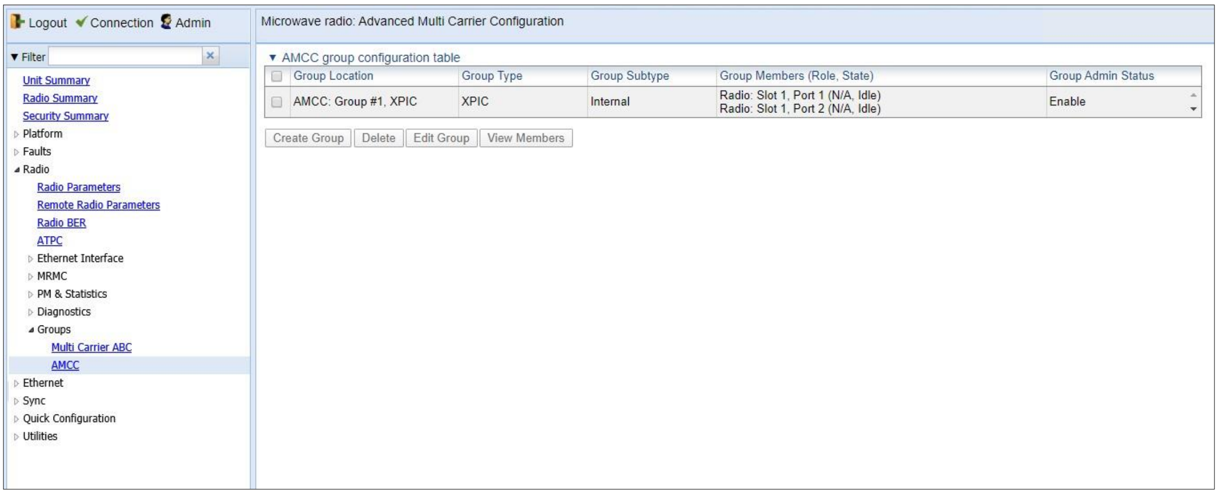
1. Make sure the horizontal antenna is roughly aligned to the horizontal antenna at the other side of the link and that the vertical antenna is roughly aligned to the vertical antenna at the other side of the link.
2. Mute the horizontal unit.
3. Adjust the antenna alignment of the vertical unit until you achieve the maximum RSL for the vertical unit (the “RSL_{wanted}”). This RSL should be no more than +/-2 dB from the expected level. Record the RSL of the vertical unit as the “RSL_{wanted}”). For instructions on adjusting the antenna alignment, see the PTP 850E Installation Guide, Section 5.4, *Performing Antenna Alignment Using the Enhanced Alignment Kit*.
4. Measure the RSL of the horizontal unit and record it as the “$RSL_{unwanted}$”).
5. Determine the XPD by subtracting the $RSL_{unwanted}$ from the RSL_{wanted}.
6. The XPD should be between 25dB and 30dB. If it is not, you should adjust the alignment of the horizontal unit until you achieve the highest XPD, which should be no less than 25dB.
7. Unmute all the PTP 850E units and check the RSL levels of all the units on both sides of the link. The RSL of the local horizontal unit should match the RSL of the remote vertical unit, within ±2dB. The RSL of the local vertical

unit should match the RSL of the remote horizontal unit, within ±2dB.

XPIC Status and Troubleshooting

The XPIC status for the radio carrier is displayed in the Group Members (Role, State) column of the Advanced Multi Carrier Configuration page.

Figure 88 Advanced Multi Carrier Configuration Page (Populated) – PTP 850C

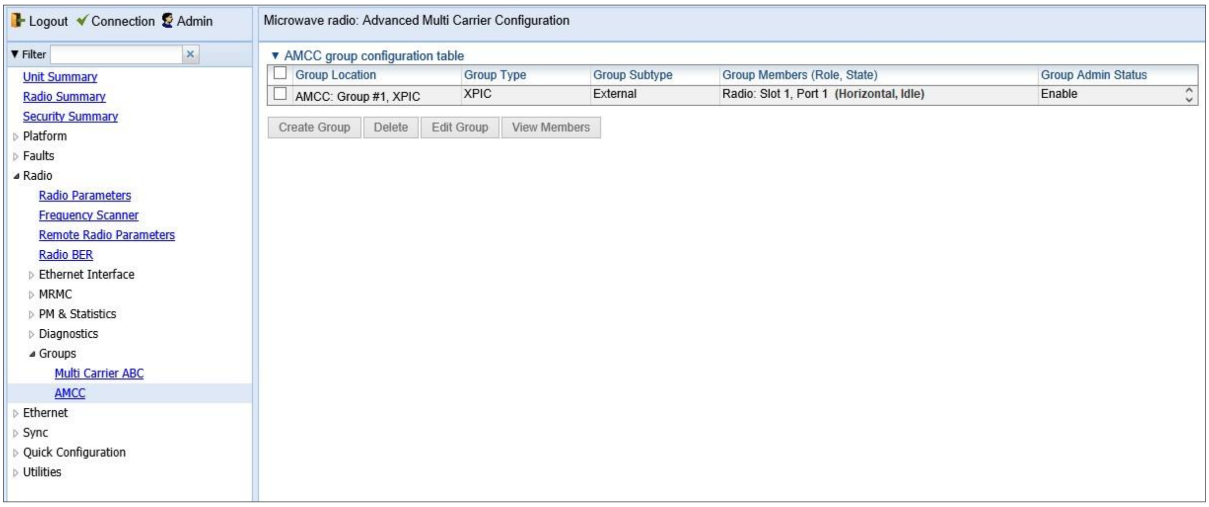


Microwave radio: Advanced Multi Carrier Configuration

▼ AMCC group configuration table

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

Figure 89 Advanced Multi Carrier Configuration Page (Populated) – PTP 850E



Microwave radio: Advanced Multi Carrier Configuration

▼ AMCC group configuration table

□	Group Location	Group Type	Group Subtype	Group Members (Role, State)	Group Admin Status
□	AMCC: Group #1, XPIC	XPIC	External	Radio: Slot 1, Port 1 (Horizontal, Idle)	Enable

Possible statuses are:

Idle – XPIC is working properly.

INIT – Indicates that the Admin state of the radio interface is Down. Go to the Interface Manager and set the Admin status of the radio interface to Up. See Enabling the Interfaces (Interface Manager).

Configuration not supported – Indicates that the MRMC script configured for the radio carrier does not support XPIC. See Configuring the Radio Carriers.

Single Channel – Indicates one of the following:

The Clock Sharing cable is not connected to one of the units, or is defective.

The XPIC cable is not connected to one of the units, or is defective.

One of the PTP 850E units in the XPIC pair is down.

If this status appears, make sure that both units are up and check that all the cables are properly connected.

Configuring 1+1 HSB Unit Protection

Note: This section is only relevant for PTP 850E.

This section includes:

- 1+1 HSB Unit Protection Overview
- Configuring Ethernet Interface Protection
- Configuring HSB Unit Protection
- Configuring Revertive Protection
- Viewing the Configuration of the Standby unit
- Editing Standby Unit Settings
- Viewing Link and Protection Status and Activity
- Manually Switching to the Standby Unit
- Disabling Automatic Switchover to the Standby Unit
- Disabling Unit Protection

1+1 HSB Unit Protection Overview

1+1 HSB protection utilizes two PTP 850E units connected to a single antenna via a coupler (PTP 820E-CPLR-Kit). to provide hardware redundancy for the radio link and Ethernet traffic.

One PTP 850E operates in active mode and the other operates in standby mode. Each PTP 850E monitors its own radio. If a protection switchover occurs, the roles are switched. The active unit goes into standby mode and the standby unit goes into active mode.

The standby unit is managed by the active unit. The standby unit's transmitter is muted, but the standby unit's receiver is kept on in order to monitor the link.

However, the received signal is terminated at the switch level.

1+1 HSB Unit Protection Management

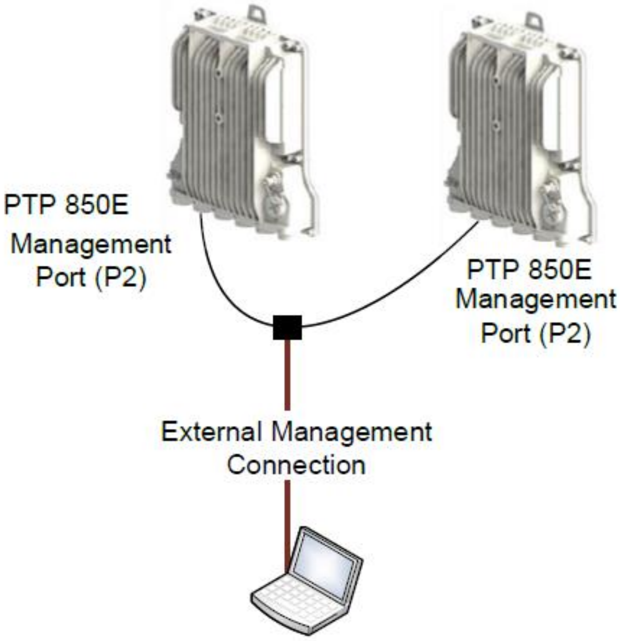
PTP 850E units in a redundancy configuration must have their CPUs interconnected in order to synchronize their protection status. The same IP address is used for both PTP 850E units, to ensure that management is not lost in the event of switchover.

Note: If the units are not initially assigned the same IP address, a mismatch alarm is raised when protection is configured. When copy-to-mate is performed, the IP address of the active unit is copied also to the standby unit, and the alarm is cleared.

A protection cable is required to enable this connectivity. This cable connects the two PTP 850E units via their Protection ports (P6).

For local management, a splitter cable is required to connect the management ports (P2) of the two PTP 850E units and an external management station.

Figure 90 Management Splitter Connection



Note that when external protection is enabled, the management port is automatically set to:

- Auto Negotiation = Off
- Speed = 100 Mbps.

The active and standby units must have the same configuration. The configuration of the active unit can be manually copied to the standby unit. Upon copying, the standby unit is reset and a temporary loss of management connection should be expected. Therefore, it is important to ensure that the units are fully and properly configured when the system is initially brought into service.

1+1 HSB Unit Protection Revertive Mode

PTP 850E supports revertive HSB protection. In revertive HSB protection mode, the user defines the primary radio on each side of the link. The primary radio should be the radio on the coupler's main path and the secondary radio should be the radio on the coupling path.

The system monitors the availability of the primary path at all times. Whenever the primary path is operational and available, without any alarms, but the secondary path is active, a timer is activated. The timer is user-configurable from ten seconds to ten minutes. The default values is 60 seconds.

If the primary path remains operational and available for the period of the timer, the system initiates a revertive protection switch. Every revertive protection switch is recorded as an event in the event log.

1+1 HSB Unit Protection Switchover

In the event of switchover, the standby unit becomes the active unit and the active unit becomes the standby unit. Switchover takes less than 50 msec.

The following events trigger switchover for HSB protection according to their priority, with the highest priority triggers listed first:

1. Force switch
2. Radio Failures (LOF, Excessive BER)
3. Line Failures
4. Manual switch

In the event that the local active unit is not powered off or its radio transmitter is malfunctioning, the remote unit sends a Change Remote message to the local standby unit, which then becomes the active unit. This is possible because the active remote unit monitors radio failures such as LOF and Excessive BER, for both itself and its mate unit. The Change Remote message is sent when both remote units encounter LOF or Excessive BER at the same time.

1+1 HSB Unit Protection Configuration Overview

To configure unit protection, you must perform the following steps:

1. Configure Ethernet interface protection. See *Configuring Ethernet Interface Protection*.
2. Configure HSB unit protection. See *Configuring HSB Unit Protection*.
3. Optionally, you can configure revertive protection to ensure that the primary path is used whenever possible. See *Configuring Revertive Protection*.

Configuring Ethernet Interface Protection

The Ethernet interfaces can be protected in either of two ways:

- **Split Protection Mode** – For Port 5 (SFP+, Eth 7), an optical splitter is used to route traffic to Port 5 on each PTP 850E unit. For Port 4 (QSFP, Eth3-6), an optical splitter is used with MPO-MPO cables to route traffic to the QSFP splitter for each PTP 850E unit.
- **Line Protection Mode** – Traffic is routed from two Ethernet ports on the external switch to a port on the active PTP 850E unit and a port on the standby PTP 850E unit. LACP protocol is used to determine which PTP 850E port is active and which port is standby, and traffic is only forwarded to the active port. Line Protection mode can be used with all PTP 850E Ethernet ports supported for traffic.

Configuring Split Ethernet Interface Protection Mode (CLI)

To configure split Ethernet interface protection mode:

1. For each Ethernet link, use an optical splitter to route traffic between the Ethernet port on the external switch and an Ethernet port on each PTP 850E unit or each QSFP splitter.
2. Proceed to *Configuring HSB Unit Protection*.

Configuring Line Protection Mode

To configure line protection mode:

1. Configure the Ethernet ports on the external switch in LACP mode.
   The external switch must support LACP.

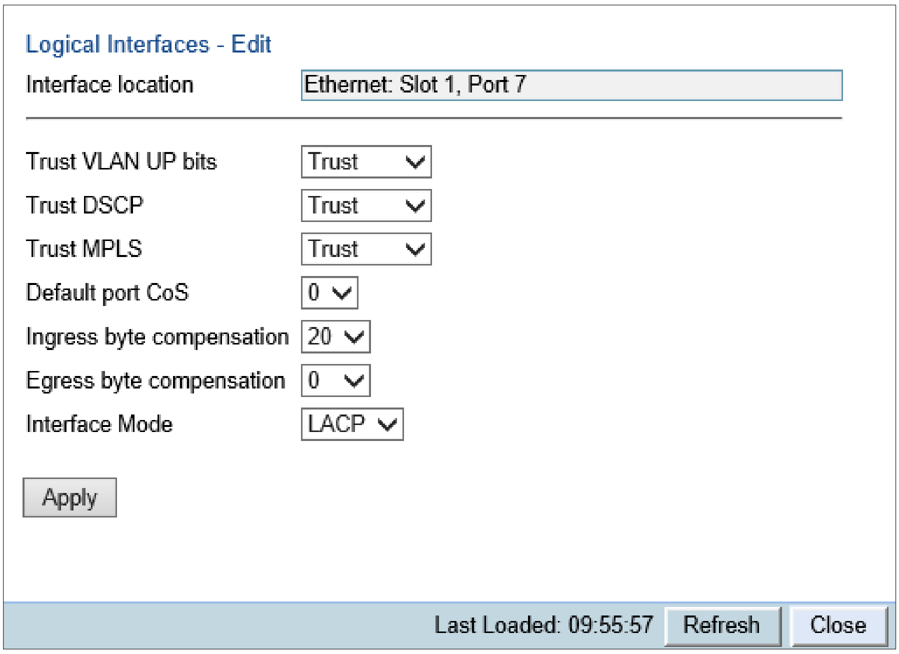
Note: PTP 850 supports a special LACP implementation for purposes of line protection only. This LACP implementation is configured on the logical interface level, as described below. Regular LACP is configured as part of the LAG configuration, and is not supported with unit redundancy. See Configuring Link Aggregation (LAG) and LACP.

2 For each Ethernet link, connect one port on the external switch to an Ethernet port on the active PTP 850E (or QSFP splitter), and the other port on the external switch to an Ethernet port on the standby PTP 850E (or QSFP splitter).

3 Enable LACP on the Ethernet interface connected to the external switch on the active PTP 850E:

i Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (*Figure 253*).

ii Select the interface and click **Edit**. The Logical Interfaces – Edit page opens.



Logical Interfaces - Edit

Interface location	Ethernet: Slot 1, Port 7
Trust VLAN UP bits	Trust
Trust DSCP	Trust
Trust MPLS	Trust
Default port CoS	0
Ingress byte compensation	20
Egress byte compensation	0
Interface Mode	LACP

Last Loaded: 09:55:57

Figure 133: Logical Interfaces – Edit Page

iii In the **Interface Mode** field, select **LACP**. iv

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

Configuring HSB Unit Protection

To configure HSB unit protection:

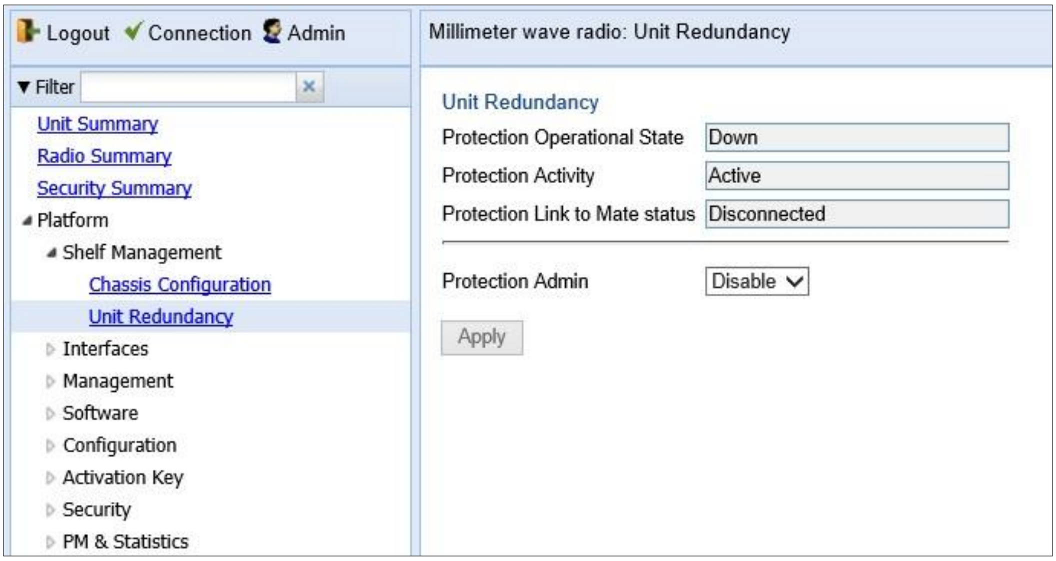
1 Before enabling protection, you must:

i Verify that both units have the same hardware part number (see *Displaying Unit Inventory*) and the same software version (see *Viewing Current Software Versions*). If the units do not have the same software version, upgrade each unit to the most recent software release (see *Upgrading the Software*).

ii Assign an IP address to each unit. For instructions, see *Changing the Management IP Address*.

iii Establish a management connection to one of the units. You can select either unit; once you enable Protection Administration, the system will determine which unit becomes the Active unit.

2 Select **Platform > Shelf Management > Unit Redundancy**. The Unit Redundancy page opens.



Millimeter wave radio: Unit Redundancy

Unit Redundancy

Protection Operational State: Down

Protection Activity: Active

Protection Link to Mate status: Disconnected

Protection Admin: Disable

Figure 134: Unit Redundancy Page

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

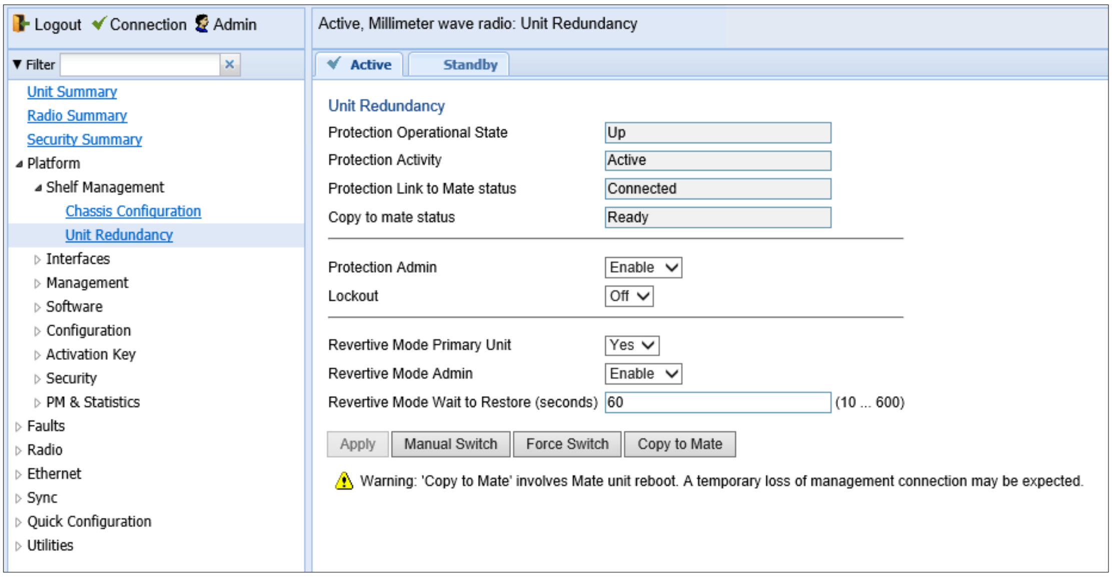
4 Click Apply.

The system configures itself for HSB protection:

- The system determines which unit is the Active unit based on a number of pre-defined criteria.
- When the system returns online, all management must be performed via the Active unit using the IP address you defined for that unit.
- The IP address you defined for the unit which is now the Standby unit is no longer valid, and the management port of the Standby unit becomes non- operational.
- Management of the Standby unit is performed via the Active unit, via the cable between the two Protection ports connecting the two units.
- HSB protection is enabled on both units.

- The Unit Redundancy page refreshes to include additional fields.

Figure 91 Unit Redundancy Page when Redundancy Enabled



Active, Millimeter wave radio: Unit Redundancy

Unit Redundancy

Protection Operational State	Up
Protection Activity	Active
Protection Link to Mate status	Connected
Copy to mate status	Ready
Protection Admin	Enable
Lockout	Off
Revertive Mode Primary Unit	Yes
Revertive Mode Admin	Enable
Revertive Mode Wait to Restore (seconds)	60 (10 ... 600)

Warning: 'Copy to Mate' involves Mate unit reboot. A temporary loss of management connection may be expected.

In additional, almost every Web EMS page will now include two tabs on top of the main section of the page:

- **Active** – Enables you to configure the Active unit.
- **Standby** – In most cases, this tab is read-only and enables you to display Standby unit parameters. Even when a switchover occurs, the unit displayed in the Web EMS is always the currently Active unit.

5 Once you have enabled Protection:

i Perform all necessary radio configurations on the Active unit, such as setting the frequency, assigning MRMC scripts, and unmuting the radio.

ii Perform all necessary Ethernet configurations on the Active unit, such as defining Ethernet services.

iii In the Unit Redundancy page, click **Copy to Mate** to copy the configuration of the Active unit to the Standby unit. Confirm the action in the confirmation window that appears.

To keep the Standby unit up-to-date, after any change to the configuration of the Active unit click **Copy to Mate** to copy the configuration to the Standby unit.

If you change the configuration of the Active unit but do not perform **Copy to Mate**, a Configuration Mismatch alarm appears in the **Faults** > **Current Alarms** page.

Configuring Revertive Protection

To configure revertive mode:

1 Select **Platform > Shelf Management > Unit Redundancy**. The Unit Redundancy page opens (*Figure 135*).

2 In the **Revertive Mode Primary Unit** field:

- To set the Active unit as the primary unit, click **Yes** in the screen for the Active unit and click **Apply**, then click **No** in the screen for the Standby unit and click **Apply**.
- To set the Standby unit as the primary unit, click **No** in the screen for the Active unit and click **Apply**, then click **Yes** in the screen for the Standby unit and click **Apply**.

3 In the **Revertive Mode Admin** field, select **Enable** to enable revertive protection or **Disable** to disable revertive protection.

4 In the **Revertive Mode Wait to Restore** field, configure the timer (in seconds). The range of values is 10 to 600 seconds. The default values is 60 seconds.

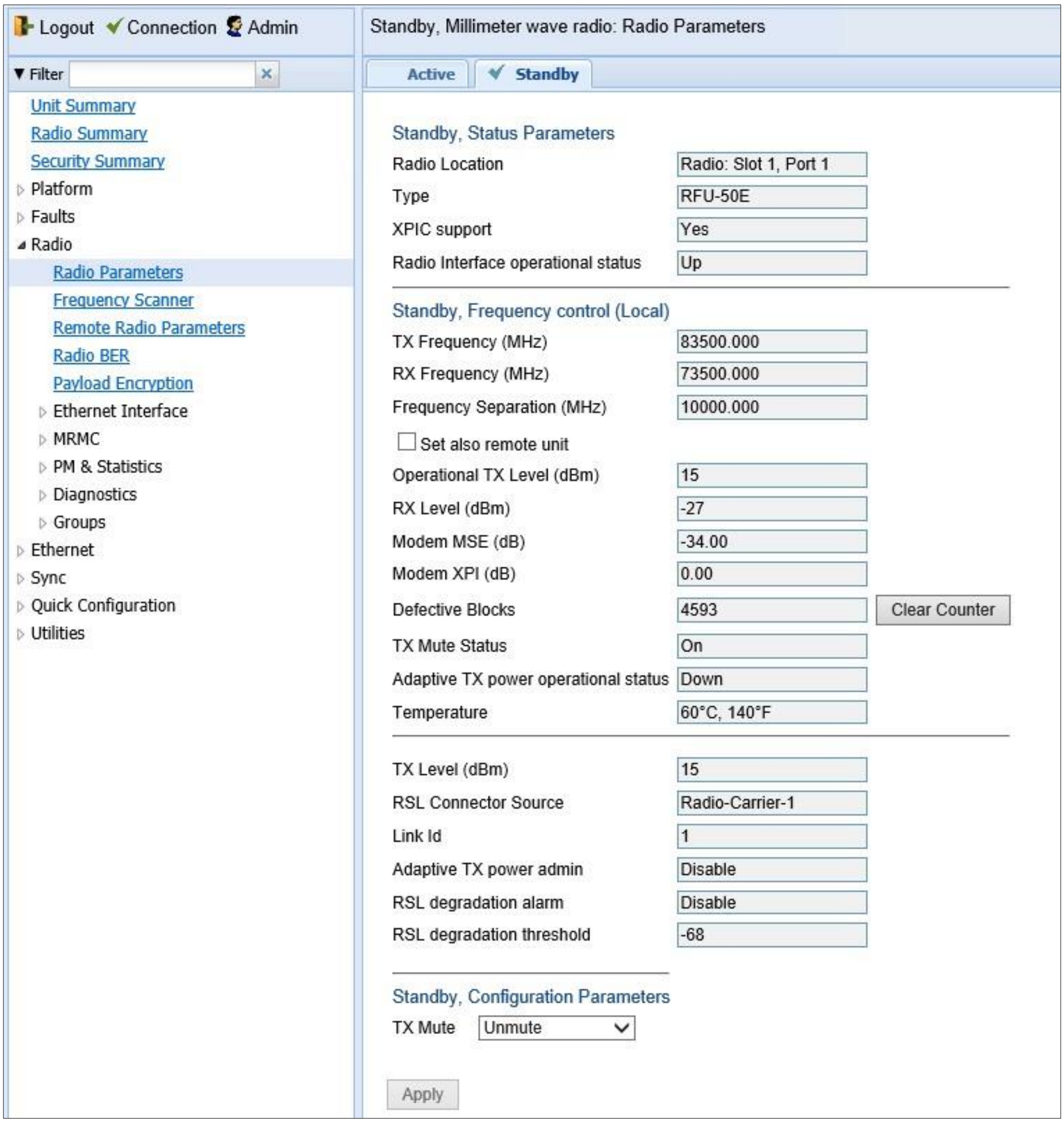
5 Click **Apply**.

Viewing the Configuration of the Standby unit

You can view the settings of the standby unit any time.

To view the settings of the standby unit, click the **Standby** tab of the desired page. The following is an example of the **Standby** tab of the Radio Parameters page after **Protection Admin** has been enabled.

Figure 92 Standby Tab of Radio Parameters Page



Standby, Millimeter wave radio: Radio Parameters

Standby, Status Parameters

Radio Location	Radio: Slot 1, Port 1
Type	RFU-50E
XPIC support	Yes
Radio Interface operational status	Up

Standby, Frequency control (Local)

TX Frequency (MHz)	83500.000
RX Frequency (MHz)	73500.000
Frequency Separation (MHz)	10000.000

□ Set also remote unit

Operational TX Level (dBm)	15
RX Level (dBm)	-27
Modem MSE (dB)	-34.00
Modem XPI (dB)	0.00
Defective Blocks	4593
TX Mute Status	On
Adaptive TX power operational status	Down
Temperature	60°C, 140°F
TX Level (dBm)	15
RSL Connector Source	Radio-Carrier-1
Link Id	1
Adaptive TX power admin	Disable
RSL degradation alarm	Disable
RSL degradation threshold	-68

Standby, Configuration Parameters

TX Mute: Unmute

Editing Standby Unit Settings

Almost all settings of the standby unit are view-only. However, several settings are editable on the Standby unit. They must be configured separately for the Standby unit, and are not copied via copy-to-mate, nor do they trigger a configuration mismatch in the CLI.

In the Web EMS, failure to synchronize these configuration settings causes a configuration mismatch alarm.

The following settings must be configured separately on the standby unit:

- Revertive Mode – If Revertive Mode is enabled, you must set the **Revertive Mode Primary Unit** field in the standby unit to the opposite setting as the active unit. See *Configuring Revertive Protection*.
- Setting the Unit Name – in the **Name** field of the Unit Parameters page (see *Configuring Unit Parameters*).

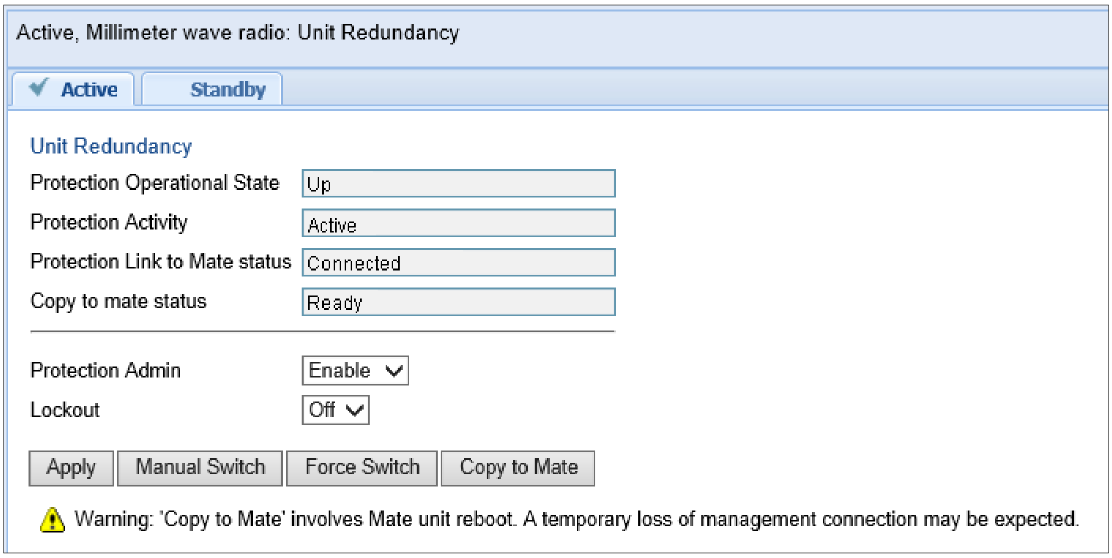
- Disabling/enabling Radio TX-mute – in the **TX mute** field of the Edit Radio Parameters page. Refer to *Configuring the Radio Parameters*.
- Clearing the Radio and RMON counters – in the **Clear Counter** field of the Counters page. Refer to *Displaying and Clearing Defective Block Counters*.
- Setting the activation key configuration – in the **Activation Key** and **Demo admin** fields of the *Activation Key Configuration Page* (see *Configuring the Activation Key*).
- Defining user accounts – Refer to the *Access Control User Accounts Page* (see *Configuring Users*).
- Setting synchronization settings – See *Synchronization*.

Viewing Link and Protection Status and Activity

You can view link and protection status and activity any time. To view link and protection status and activity:

1 Select **Platform > Shelf Management > Unit Redundancy**. The Unit Redundancy page opens.

Figure 93 Unit Redundancy Page



Active, Millimeter wave radio: Unit Redundancy

Unit Redundancy

Protection Operational State: Up

Protection Activity: Active

Protection Link to Mate status: Connected

Copy to mate status: Ready

Protection Admin: Enable

Lockout: Off

⚠ Warning: 'Copy to Mate' involves Mate unit reboot. A temporary loss of management connection may be expected.

The following information is displayed:

- **Protection Operational State** – Indicates whether HSB protection is functional (available in practice). Unit protection is not functional if any of the following occurred:
  - The management connection to the mate is down.
- **Protection Activity** – The activity state of the device: Active or Standby.
- **Protection Link to Mate Status** – Indicates whether the two units (the Active and the Standby) are physically connected.
- **Copy to mate status** – Indicates the status of the last copy-to-mate operation
- **Protection Admin –** Indicates whether HSB protection is enabled or disabled.
- **Lockout –** Indicates whether lockout is enabled (**On**) or disabled (**Off**).

Manually Switching to the Standby Unit

At any point, you can manually switch to the Standby unit, provided that the highest protection fault level in the Standby unit is no higher than the highest protection fault level on the Active unit.

To manually switchover to the Standby unit:

1. Select **Platform > Management > Unit Redundancy**. The Unit Redundancy page opens (*Figure 134*).
2. Click **Manual Switch**.
3. Confirm the action in the confirmation window that appears.

Disabling Automatic Switchover to the Standby Unit

At any point, you can perform lockout, which disables automatic switchover to the standby unit.

To disable automatic switchover to the Standby unit:

1. Select **Platform > Shelf Management > Unit Redundancy**. The Unit Redundancy page opens (*Figure 134*).
2. Select **On** in the **Lockout** field.
3. Click **Apply**.

To re-enable automatic switchover, select **Off** in the **Lockout** field and then click **Apply**.

Disabling Unit Protection

You can disable unit protection at any time. If you disable unit protection, keep in mind that while the unit that was formerly the active unit maintains its IP address, the unit that was formerly the standby unit is assigned the default IP address (192.168.1.1)

To disable protection:

1. Select **Platform > Shelf Management > Unit Redundancy**. The Unit Redundancy page opens (*Figure 134*).
2. Select **Disable** in the **Protection Admin** field.
3. Click **Apply**.

Configuring Link Aggregation (LAG) and LACP

Note: This section is only relevant for PTP 850S.

Link aggregation (LAG) enables you to group several physical Ethernet or radio interfaces into a single logical interface bound to a single MAC address. This logical interface is known as a LAG group. Traffic sent to the interfaces in a LAG group is distributed by means of a load balancing mechanism. PTP 850S uses a distribution function of up to Layer 4 in order to generate the most efficient distribution among the LAG physical ports.

This section explains how to configure LAG and includes the following topics:

- LAG Overview
- Configuring a LAG Group
- Enabling and Disabling LAG Group Shutdown in Case of Degradation Event
- Configuring Enhanced LAG Distribution
- Deleting a LAG Group
- Displaying LACP Parameters and Statistics

LAG Overview

LAG can be used to provide redundancy for Ethernet interfaces, both on the same PTP 850S unit (line protection) and on separate units (line protection and equipment protection). LAGs can also be used to provide redundancy for radio links.

LAG can also be used to aggregate several interfaces in order to create a wider (aggregate) link. For example, LAG can be used to create a 4 Gbps channel.

You can create up to four LAG groups. The following restrictions exist with respect to LAG groups:

- Only physical interfaces (including radio interfaces), not logical interfaces, can belong to a LAG group.
- Interfaces can only be added to the LAG group if no services or service points are attached to the interface.
- Any classification rules defined for the interface are overridden by the classification rules defined for the LAG group.
- When removing an interface from a LAG group, the removed interface is assigned the default interface values.

There are no restrictions on the number of interfaces that can be included in a LAG. It is recommended, but not required, that each interface in the LAG have the same parameters (e.g., speed, duplex mode).

The LAG page lists all LAG groups configured on the unit.

Note

To add or remove an Ethernet interface to a LAG group, the interface must be in an administrative state of “down”. This restriction does not apply to radio interfaces. For instructions on setting the administrative state of an interface, see Enabling the Interfaces (Interface Manager).

PTP 850S supports LACP, which expands the capabilities of static LAG and provides interoperability with third-party equipment that uses LACP. LACP improves the communication between LAG members. This improves error detection capabilities in situations such as improper LAG configuration or improper cabling. It also enables the LAG to detect uni-directional failure and remove the link from the LAG, preventing packet loss.

LACP is enabled as part of the LAG configuration process. It should only be used if the LAG is in a link with another LACP-enabled LAG.

Note

LACP can only be used with Ethernet interfaces.

LACP cannot be used with Enhanced LAG Distribution or with the LAG

Group Shutdown in Case of Degradation Event feature.

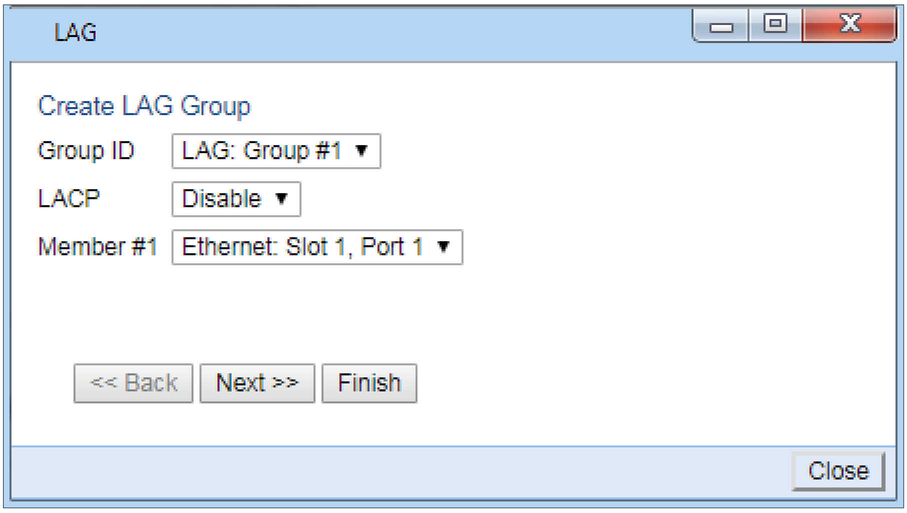
Configuring a LAG Group

Adding and Removing Group Members

To create a LAG group:

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

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



LAG

Create LAG Group

Group ID: LAG: Group #1

LACP: Disable

Member #1: Ethernet: Slot 1, Port 1

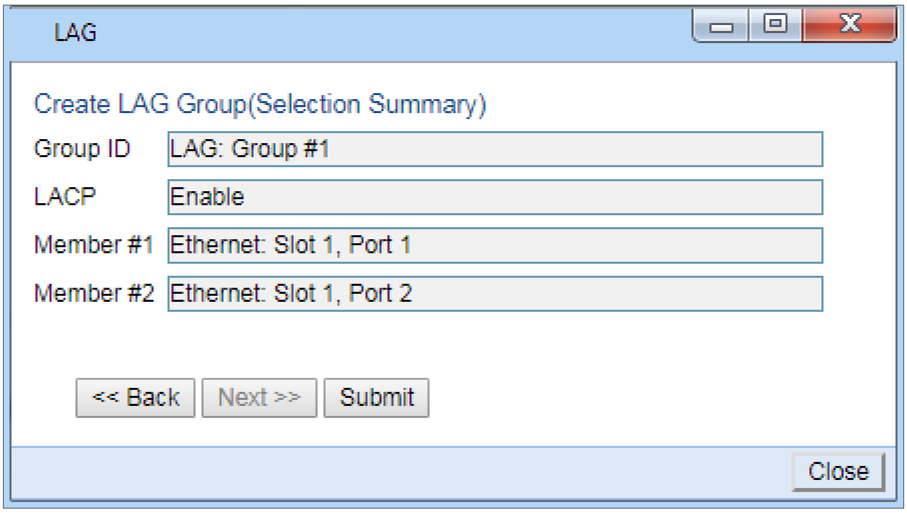
Figure 94 Create LAG Group – Page 1

In the **Group ID** field, select a LAG Group ID. Only LAG IDs that are not already assigned to a LAG group appear in the dropdown list.

In the **LACP** field, select **Enable** to enable LACP on the LAG or **Disable** to disable LACP on the LAG. The default value is **Disable**.

In the **Member 1** field, select an interface to assign to the LAG group. Only interfaces not already assigned to a LAG group appear in the dropdown list.

Click **Next**. A new Create LAG Group page opens.



Create LAG Group(Selection Summary)

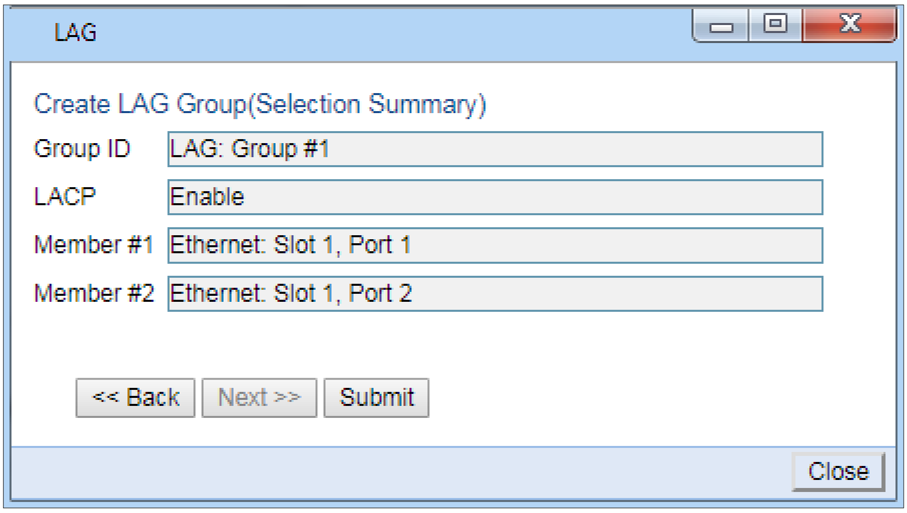
Group ID	LAG: Group #1
LACP	Enable
Member #1	Ethernet: Slot 1, Port 1
Member #2	Ethernet: Slot 1, Port 2

Figure 95 Create LAG Group – Page 2

In the **Member 2** field, select an additional interface to assign to the LAG Group.

To add additional interfaces to the LAG group, repeat steps 5 and 6.

When you have finished adding interfaces to the LAG group, click **Finish**. A new Create LAG Group page opens displaying all the interfaces you have selected to include in the LAG group.



Create LAG Group(Selection Summary)

Group ID	LAG: Group #1
LACP	Enable
Member #1	Ethernet: Slot 1, Port 1
Member #2	Ethernet: Slot 1, Port 2

Figure 96 Create LAG Group – Final Page

Click **Submit**. If all the interfaces meet the criteria listed above, a message appears that the LAG group has been successfully created. If not, a message appears indicating that the LAG group was not created and giving the reason.

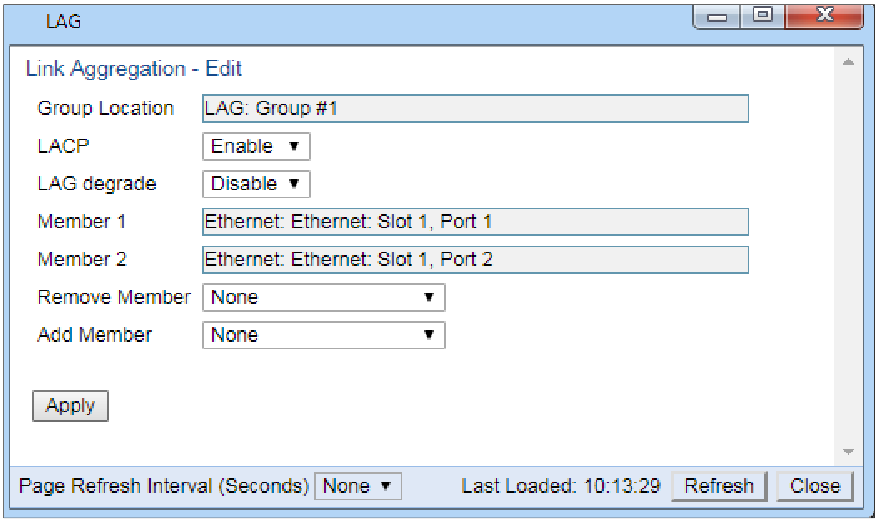
Editing a LAG Group

To edit an existing LAG group:

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

Select the LAG group you want to edit in the Link Aggregation table.

Click **Edit** underneath the Link Aggregation table. The Link Aggregation - Edit page opens.



Link Aggregation - Edit

Group Location: LAG: Group #1

LACP: Enable

LAG degrade: Disable

Member 1: Ethernet: Ethernet: Slot 1, Port 1

Member 2: Ethernet: Ethernet: Slot 1, Port 2

Remove Member: None

Add Member: None

Figure 97 Link Aggregation - Edit Page

Do any of the following:

To enable or disable LACP, select Enable or Disable in the LACP field. See

LAG Overview for restrictions.

To enable or disable LAG Group Shutdown in case of Degradation Event, select Enable or Disable in the LAG degrade field. See Enabling and Disabling LAG Group Shutdown in Case of Degradation Event for restrictions.

To remove an interface from the LAG Group, select the interface in the Remove Member field.

To add an interface to the LAG Group, select the interface in the Add Member field.

Click Apply.

To remove or add additional interfaces, repeat steps 4 and 5.

When you are finished, click Close to close the Link Aggregation – Edit page.

Note

When removing an interface from a LAG group, the removed interface

is assigned the default interface values.

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

Enabling and Disabling LAG Group Shutdown in Case of Degradation Event

> Note
>
> LAG Group Shutdown in Case of Degradation Event cannot be used
>
> with LACP.

A LAG group can be configured to be automatically closed in the event of LAG degradation. This option is used if you want traffic from the switch to be re-routed during such time as the link is providing less than a certain capacity.

By default, the LAG group shutdown in case of degradation event option is disabled. When enabled, the LAG is automatically closed in the event that any one or more ports in the LAG fail. When all ports in the LAG are again operational, the LAG is automatically re-opened.

> Note
>
> Failure of a port in the LAG also triggers a lag-degraded alarm, Alarm
>
> ID 100.

To enable or disable the LAG group shutdown in case of degradation event option:

Select **Ethernet > Groups > LAG** to open the LAG page.

Select the LAG group in the Link Aggregation table.

Click **Edit** underneath the Link Aggregation table. The Link Aggregation - Edit page opens (*Figure 91*).

In the **LAG degrade** field, select **Enable** to enable the LAG group shutdown in case of degradation event option or **Disable** to disable the LAG group shutdown in case of degradation event option.

Click **Apply**.

Configuring Enhanced LAG Distribution

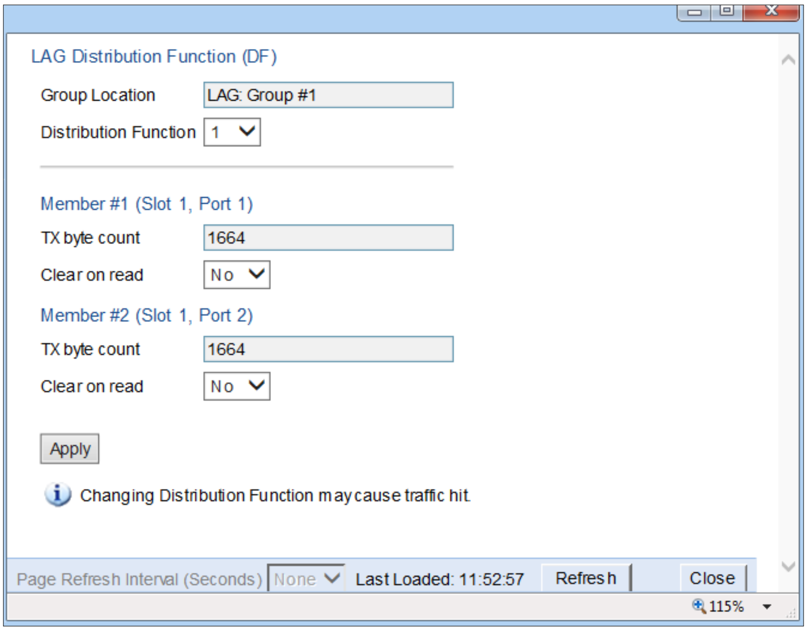
You can change the distribution function by selecting from ten pre-defined LAG distribution schemes. The feature includes a display of the TX throughput for each interface in the LAG, to help you identify the best LAG distribution scheme for the specific link.

> Note
>
> Enhanced LAG distribution is only available for LAG groups that consist of exactly two interfaces. It cannot be used with LACP.

To configure enhanced LAG distribution:

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

Click **LAG DF** underneath the Link Aggregation table. The LAG Distribution Function (DF) page opens.



LAG Distribution Function (DF)

Group Location: LAG: Group #1

Distribution Function: 1

Member #1 (Slot 1, Port 1)

TX byte count: 1664

Clear on read: No

Member #2 (Slot 1, Port 2)

TX byte count: 1664

Clear on read: No

Changing Distribution Function may cause traffic hit

Page Refresh Interval (Seconds): None

Last Loaded: 11:52:57

Figure 98 LAG Distribution Function (DF) Page

In the **Distribution Function** field, select a pre-set distribution scheme, from 1 to 10. It is recommended to experiment with the various schemes, monitoring the **TX byte count** fields for each interface to determine the efficiency of each distribution scheme for the link. The default distribution scheme is 1. The default LAG distribution pattern is 1.

To clear the TX byte counts, select **Clear on read** for one or both interfaces. The byte counts will be cleared when you close the LAG Distribution Function (DF) page or click **Refresh**.

Note

This counter will also be cleared for the members of the LAG in the Port RMON Statistics page.

Click **Apply** to apply the selected distribution scheme.

Deleting a LAG Group

In order to delete a LAG group, you must first make sure that no service points are attached to the LAG group.

To delete a LAG group:

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

Select the LAG group you want to delete in the Link Aggregation table.

Click **Delete** underneath the Link Aggregation table. The LAG group is deleted. To delete multiple LAG groups:

Select the LAG groups in the Link Aggregation table or select all the LAG groups by selecting the check box in the top row.

Click **Delete** underneath the Link Aggregation table.

Displaying LACP Parameters and Statistics

You can display the following LACP parameters and statistics:

LACP Aggregation (per LAG)
LACP Port Status
LACP Port Statistics
LACP Port Debug Statistics

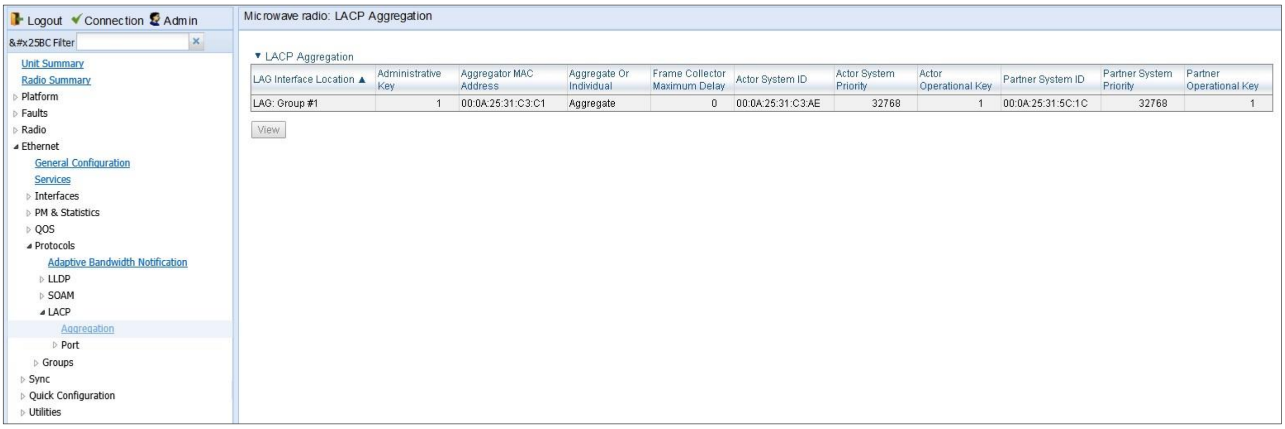
Note

PTP 850S does not support any LACP write parameters.

Displaying LACP Aggregation Status Parameters

To display LACP aggregation status parameters:

Select **Ethernet > Protocols > LACP > Aggregation** to open the LACP Aggregation page.



Microwave radio: LACP Aggregation

▼ LACP Aggregation

LAG Interface Location ▲	Administrative Key	Aggregator MAC Address	Aggregate Or Individual	Frame Collector Maximum Delay	Actor System ID	Actor System Priority	Actor Operational Key	Partner System ID	Partner System Priority	Partner Operational Key
LAG: Group #1	1	00:0A:25:31:C3:C1	Aggregate	0	00:0A:25:31:C3:AE	32768	1	00:0A:25:31:5C:1C	32768	1

Figure 99 LACP Aggregation Page

Table 16 LACP Aggregation Status Parameters

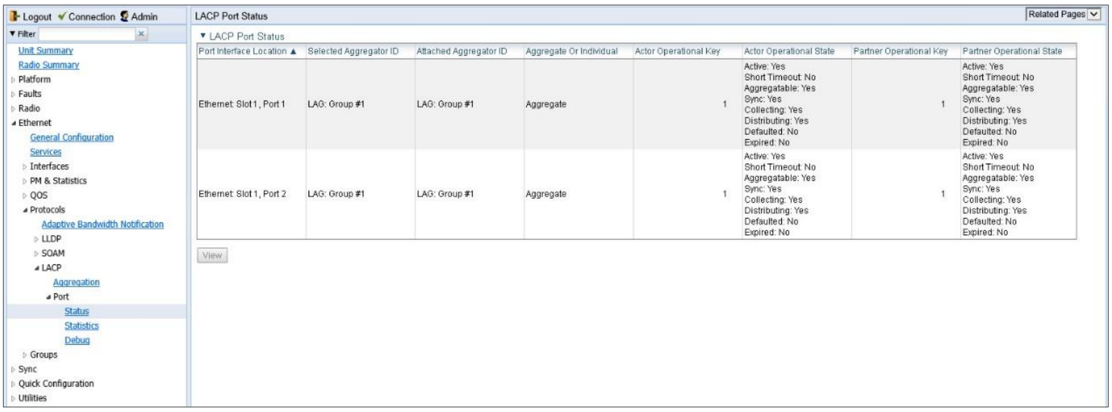
Parameter	Definition
LAG Interface Location	Identifies the LAG group.
Administrative Key	The current administrative value of the key for the Aggregator.
Aggregator MAC Address	The individual MAC address assigned to the Aggregator.
Aggregate or Individual	Indicates whether the Aggregator represents an aggregate or an individual link.
Frame Collector Maximum Delay	The maximum delay, in tens of microseconds.
Actor System ID	The MAC address value used as a unique identifier for the system that contains this Aggregator.
Actor System Priority	The priority value associated with the Actor’s System ID.
Actor Operational Key	The current operational value of the Key for the Aggregator.
Partner System ID	The MAC address value consisting of the unique identifier for the current protocol Partner of this Aggregator.
Partner System Priority	The priority value associated with the Partner’s System ID.

Partner Operational Key	The current operational value of the Key for the Aggregator's current Protocol partner.

Displaying LACP Port Status Parameters

To display LACP port status parameters:

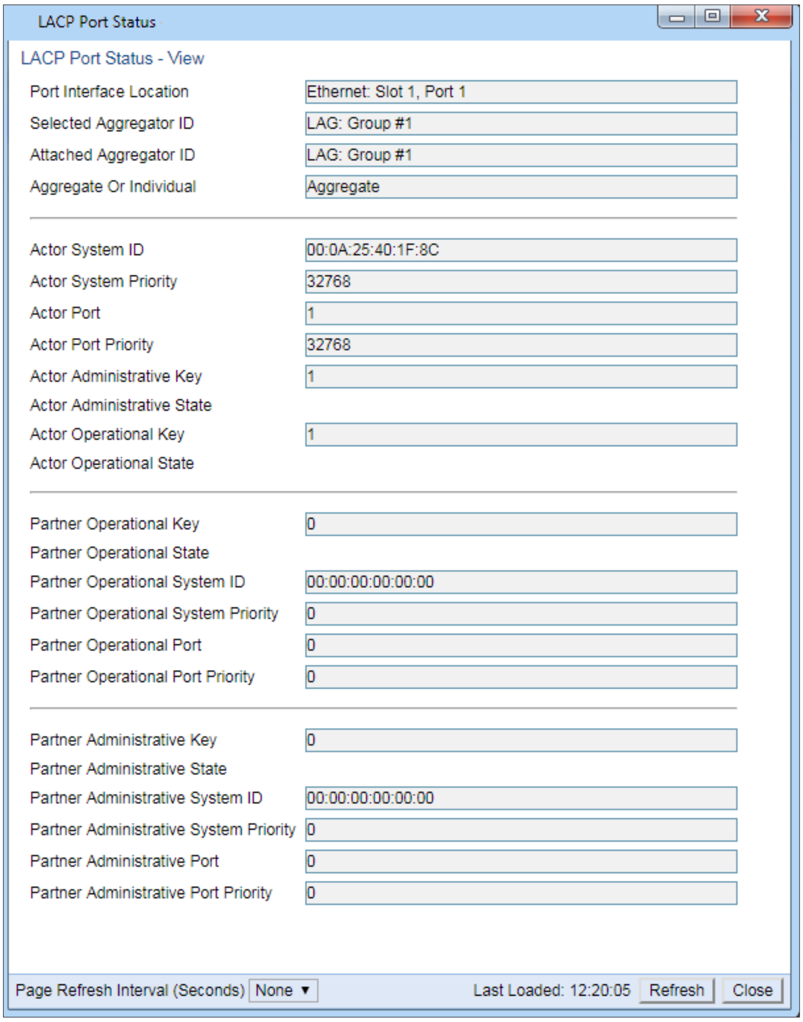
Select **Ethernet > Protocols > LACP > Port > Status** to open the LACP Port Status page.



Port Interface Location ▲	Selected Aggregator ID	Attached Aggregator ID	Aggregate Or Individual	Actor Operational Key	Actor Operational State	Partner Operational Key	Partner Operational State
Ethernet: Slot 1, Port 1	LAG: Group #1	LAG: Group #1	Aggregate	1	Active: Yes Short Timeout: No Aggregatable: Yes Sync: Yes Collecting: Yes Distributing: Yes Defaulted: No Expired: No	1	Active: Yes Short Timeout: No Aggregatable: Yes Sync: Yes Collecting: Yes Distributing: Yes Defaulted: No Expired: No
Ethernet: Slot 1, Port 2	LAG: Group #1	LAG: Group #1	Aggregate	1	Active: Yes Short Timeout: No Aggregatable: Yes Sync: Yes Collecting: Yes Distributing: Yes Defaulted: No Expired: No	1	Active: Yes Short Timeout: No Aggregatable: Yes Sync: Yes Collecting: Yes Distributing: Yes Defaulted: No Expired: No

Figure 100 LACP Port Status Page

The LACP Port Status page displays the major port status parameters, per port. display all the available LACP port status parameters, select a port and click View. The LACP Port Status – View page is displayed.



Port Interface Location: Ethernet: Slot 1, Port 1
Selected Aggregator ID: LAG: Group #1
Attached Aggregator ID: LAG: Group #1
Aggregate Or Individual: Aggregate

Actor System ID: 00:0A:25:40:1F:8C
Actor System Priority: 32768
Actor Port: 1
Actor Port Priority: 32768
Actor Administrative Key: 1
Actor Administrative State
Actor Operational Key: 1
Actor Operational State

Partner Operational Key: 0
Partner Operational State
Partner Operational System ID: 00:00:00:00:00:00
Partner Operational System Priority: 0
Partner Operational Port: 0
Partner Operational Port Priority: 0

Partner Administrative Key: 0
Partner Administrative State
Partner Administrative System ID: 00:00:00:00:00:00
Partner Administrative System Priority: 0
Partner Administrative Port: 0
Partner Administrative Port Priority: 0

Page Refresh Interval (Seconds): None
Last Loaded: 12:20:05

Figure 101 *LACP Port Status – View Page*

Table 17 LACP Port Status Parameters

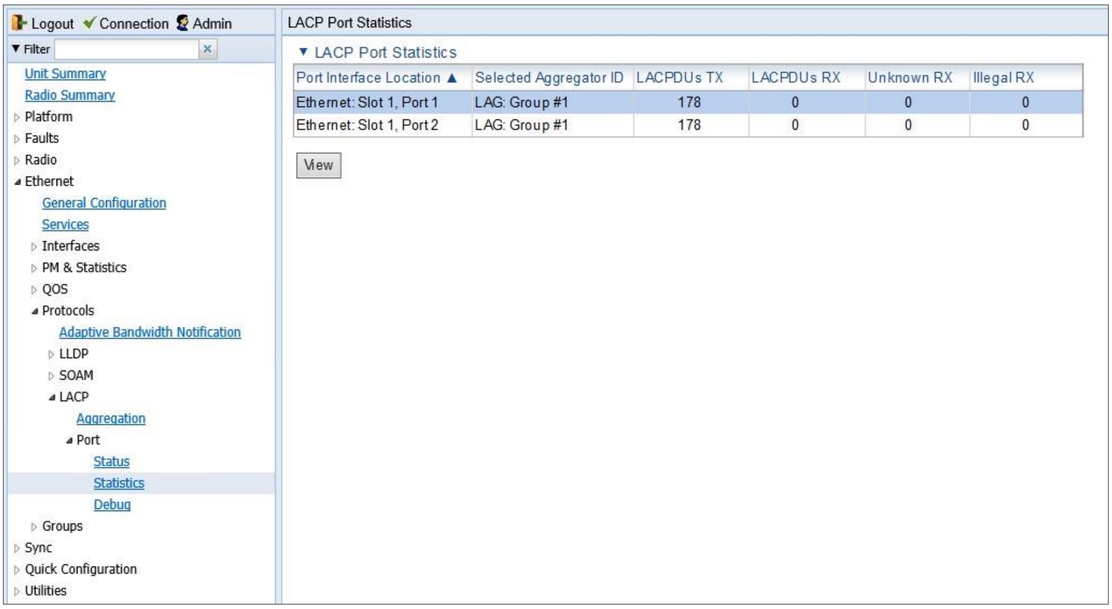
Parameter	Definition
Port Interface Location	The location of the port.
Selected Aggregator ID	The identifier value of the Aggregator that this Aggregation port has currently selected.
Attached Aggregator ID	The identifier value of the Aggregator that this Aggregation port is currently attached to.
Aggregate or Individual	Indicates whether the Aggregation Port is able to aggregate or is only able to operate as an individual link.
Actor System ID	The MAC Address value that defines the value of the System ID for the system that contains this Aggregation Port.
Actor System Priority	The priority value associated with the Actor's System ID.
Actor Port	The port number locally assigned to the Aggregation Port.

Actor Port Priority	The priority value assigned to this Aggregation Port.
Actor Administrative Key	The current administrative value of the Key for the Aggregation Port.
Actor Administrative State	The administrative values of the Actor's state as transmitted by the Actor
Actor Operational Key	The current operational value of the Key for the Aggregation Port.
Actor Operational State	The current operational values of the Actor's state as transmitted by the Actor via LACPDUs.
Partner Operational Key	The current operational value of the Key for the protocol Partner.
Partner Operational State	The current values of Actor State in the most recently received LACPDU transmitted by the protocol Partner.
Partner Operational System ID	The MAC Address value representing the current value of the Aggregation Port's protocol Partner's System ID.
Partner Operational System Priority	The operational value of priority associated with the Partner's System ID.
Partner Operational Port	The operational port number assigned to this Aggregation port by the Aggregation port's port Partner.
Partner Operational Port Priority	The Priority value assigned to this Aggregation port by the Partner.
Partner Administrative Key	The current administrative value of the Key for the protocol Partner.
Partner Administrative State	The current administrative value of Actor state for the protocol Partner.
Partner Administrative System ID	The MAC Address value representing the administrative value of the Aggregation Port's Protocol partner's System ID.
Partner Administrative System Priority	The administrative priority value associated with the Partner's System ID.
Partner Administrative Port	The current administrative value of the port number for the protocol partner.
Partner Administrative Port Priority	The current administrative value of the port priority for the protocol partner.

Displaying LACP Port Statistics

To display LACP port statistics:

1 Select **Ethernet > Protocols > LACP > Port > Statistics** to open the LACP Port Statistics page.



LACP Port Statistics

Port Interface Location ▲	Selected Aggregator ID	LACPDUs TX	LACPDUs RX	Unknown RX	Illegal RX
Ethernet: Slot 1, Port 1	LAG: Group #1	178	0	0	0
Ethernet: Slot 1, Port 2	LAG: Group #1	178	0	0	0

Figure 102 LACP Port Statistics Page

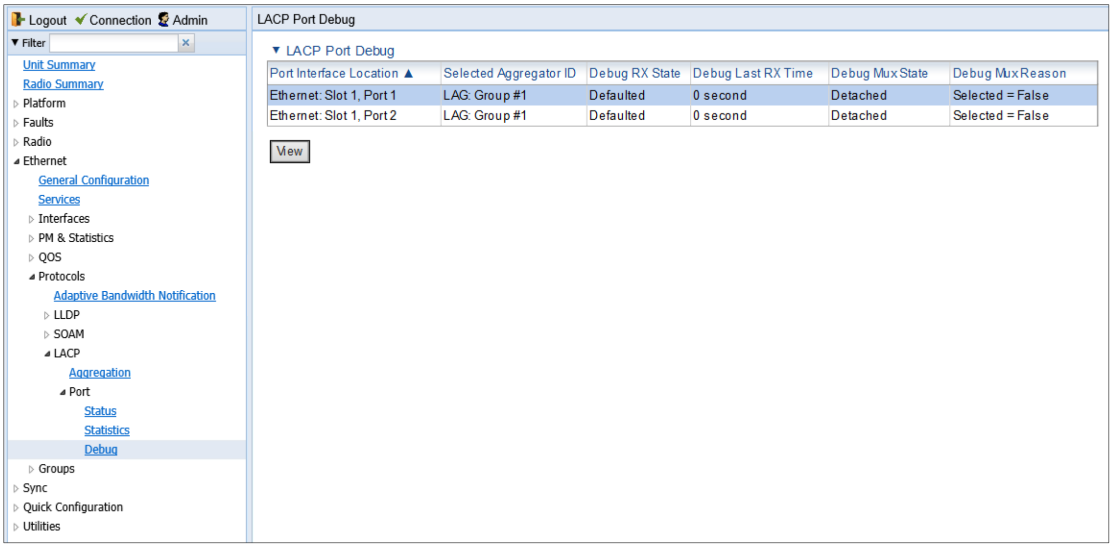
Table 18 LACP Port Statistics

Parameter	Definition
Port Interface Location	The location of the port.
Selected Aggregator ID	The identifier value of the Aggregator that this Aggregation port has currently selected.
LACPDUs TX	The number of LACPDUs that this port has transmitted.
LACPDUs RX	The number of LACPDUs that this port has received.
Unknown RX	The number of unknown protocol frames that this port has received.
Illegal RX	The number of illegal protocol frames that this port has received.

Displaying LACP Port Debug Statistics

To display LACP port debug statistics:

1 Select **Ethernet > Protocols > LACP > Port > Debug** to open the LACP Port Debug page.



LACP Port Debug

▼ LACP Port Debug

Port Interface Location ▲	Selected Aggregator ID	Debug RX State	Debug Last RX Time	Debug Mux State	Debug Mux Reason
Ethernet: Slot 1, Port 1	LAG: Group #1	Defaulted	0 second	Detached	Selected = False
Ethernet: Slot 1, Port 2	LAG: Group #1	Defaulted	0 second	Detached	Selected = False

Figure 103 LACP Port Debug Page

Table 19 LACP Port Debug Statistics

Parameter	Definition
Port Interface Location	The location of the port.
Selected Aggregator ID	The identifier value of the Aggregator that this Aggregation port has currently selected.
Debug RX State	The state of the receive state machine for the Aggregation port. Possible values are: **Current** – An LACPDU was received before expiration of the most recent timeout period. **Expired** – No LACPDU was received before expiration of the most recent timeout period. **Defaulted** – No LACPDU was received during the two most recent timeout periods.
Debug Last RX Time	The value of a TimeSinceSystemReset (F.2.1) when the last LACPDU was received by this Aggregation port.
Debug Mux State	The state of the Mux state machine for the Aggregation port. Possible values are Collecting, Distributing, Attached, and Detached.
Debug Mux Reason	A text string indicating the reason for the most reason change in the state of the Mux machine.

Chapter 7: Unit Management

This section includes:

- Defining the IP Protocol Version for Initiating Communications
- Configuring the Remote Unit's IP Address
- Configuring SNMP
- Configuring Trap Managers
- Installing and Configuring an FTP or SFTP Server
- Configuring the Internal Ports for FTP or SFTP
- Upgrading the Software
- Backing Up and Restoring Configurations
- Setting the Unit to the Factory Default Configuration
- Performing a Hard (Cold) Reset
- Configuring Unit Parameters
- Configuring NTP
- Displaying Unit Inventory
- Displaying SFP DDM and Inventory Information
- Defining a Login Banner

Related topics:

- Setting the Time and Date (Optional)
- Enabling the Interfaces (Interface Manager)
- Uploading Unit Info
- Changing the Management IP Address

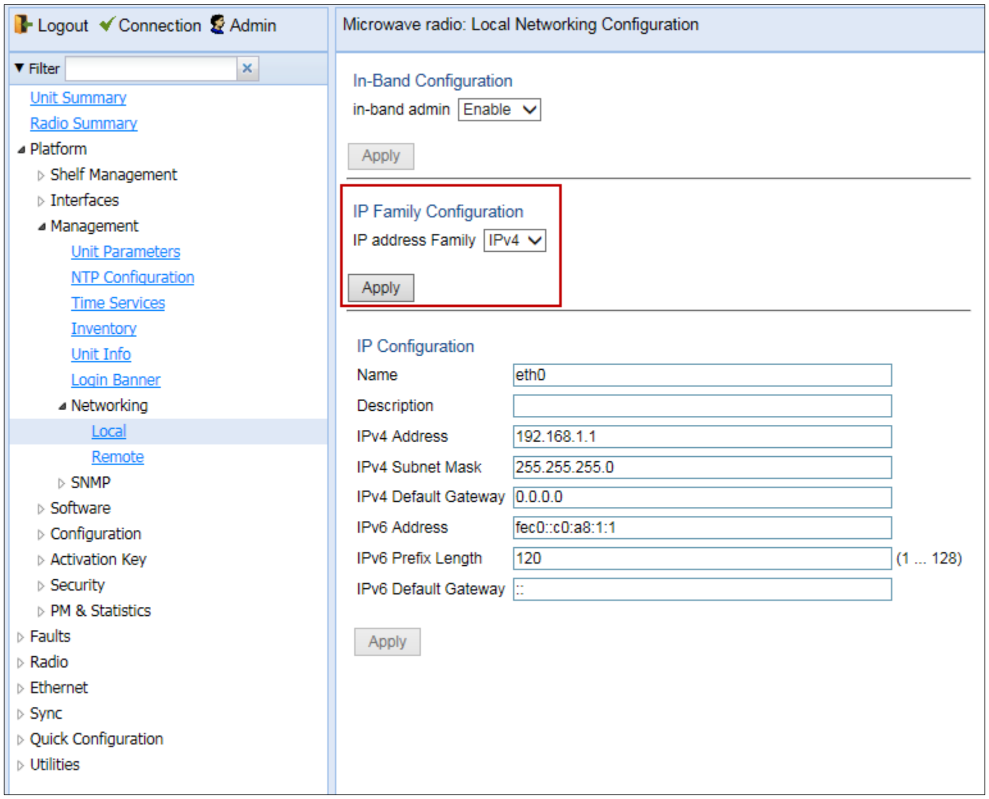
Defining the IP Protocol Version for Initiating Communications

You can specify which IP protocol the unit will use when initiating communications, such as downloading software, sending traps, pinging, or exporting configurations. The options are IPv4 or IPv6.

To set the IP protocol version of the local unit:

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

Figure 104 Local Networking Configuration Page



Microwave radio: Local Networking Configuration

In-Band Configuration

in-band admin: Enable

IP Family Configuration

IP address Family: IPv4

IP Configuration

Name	eth0
Description	
IPv4 Address	192.168.1.1
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	0.0.0.0
IPv6 Address	fec0::c0:a8:1:1
IPv6 Prefix Length	120 (1 ... 128)
IPv6 Default Gateway	::

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

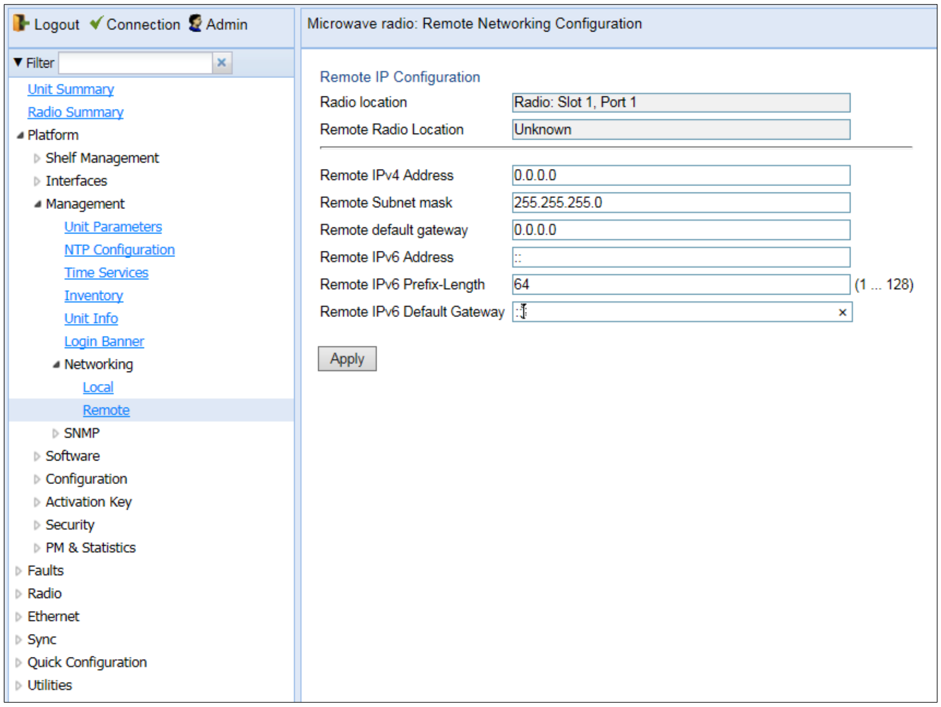
Configuring the Remote Unit's IP Address

You can configure the IP address of a remote unit.

To configure the IP address of a remote unit:

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

Figure 105 Remote Networking Configuration Page



Microwave radio: Remote Networking Configuration

Remote IP Configuration

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

2. In the **Remote IPv4 address** field, enter an IPv4 address for the remote unit. You can enter the address in IPv4 format in this field, and/or in IPv6 format in the **IPv6 Address** field. The remote unit will receive communications whether they are sent to its IPv4 address or its IPv6 address.
3. In the **Remote Subnet mask** field, enter the subnet mask of the remote radio.
4. Optionally, in the **Remote default gateway** field, enter the default gateway address for the remote radio.
5. Optionally, in the **Remote IPv6 Address** field, enter an IPv6 address for the remote unit. You can enter the address in IPv6 format in this field, and/or in IPv4 format in the **Remote IPv4 Address** field. The unit will receive communications whether they are sent to its IPv4 address or its IPv6 address.
6. If you entered an IPv6 address, enter the IPv6 prefix length in the **Remote IPv6 Prefix-Length** field.
7. Optionally, if you entered an IPv6 address, enter the default gateway in IPv6 format in the **Remote IPv6 Default Gateway** field.
8. Click **Apply**.

Changing the Subnet of the Remote IP Address

If you wish to change the **Remote IPv4 Address** to a different subnet:

1. Change the address of the **Remote Default Gateway** to 0.0.0.0.
2. Click **Apply**.
3. Set the **Remote IPv4 Address** as desired, and the **Remote Default Gateway** as desired.

Similarly, if you wish to change the **Remote IPv6 Address** to a different subnet:

1. Change the address of the **Remote IPv6 Default Gateway** to 0:0:0:0:0:0:0:0.
2. Click **Apply**.
3. Set the **Remote IPv6 Address** as desired, and the **Remote IPv6 Default Gateway** as desired.

Configuring SNMP

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

PTP 850E support the following MIBs:

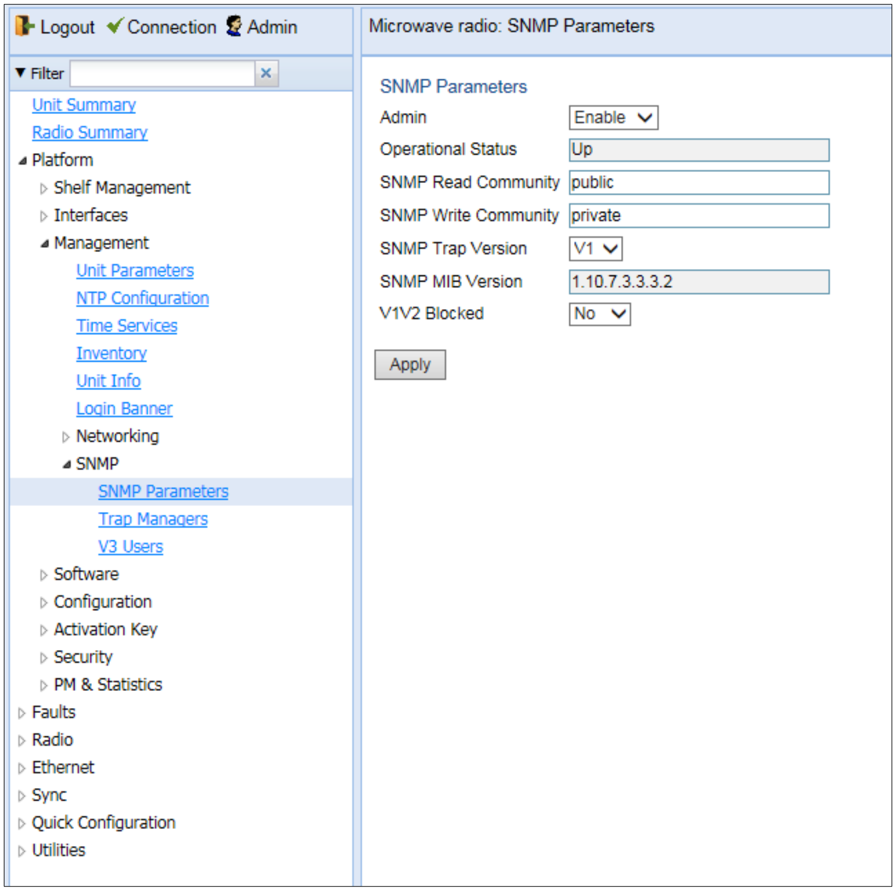
- RFC-1213 (MIB II).
- RMON MIB.
- Proprietary MIB.

Access to the unit is provided by making use of the community and context fields in SNMPv1 and SNMPv2c/SNMPv3, respectively.

To configure SNMP:

1. Select **Platform > Management > SNMP > SNMP Parameters**. The SNMP Parameters page opens.

Figure 106 SNMP Parameters Page



Microwave radio: SNMP Parameters

SNMP Parameters

Admin	Enable
Operational Status	Up
SNMP Read Community	public
SNMP Write Community	private
SNMP Trap Version	V1
SNMP MIB Version	1.10.7.3.3.3.2
V1V2 Blocked	No

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

Note

The **Operational Status** field indicates whether SNMP monitoring is currently active (**Up**) or inactive (**Down**).

3. In the **SNMP Read Community** field, enter the community string for the SNMP read community.
4. In the **SNMP Write Community** field, enter the community string for the SNMP write community
5. In the **SNMP Trap Version** field, select **V1**, **V2**, or **V3** to specify the SNMP version.

Note

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

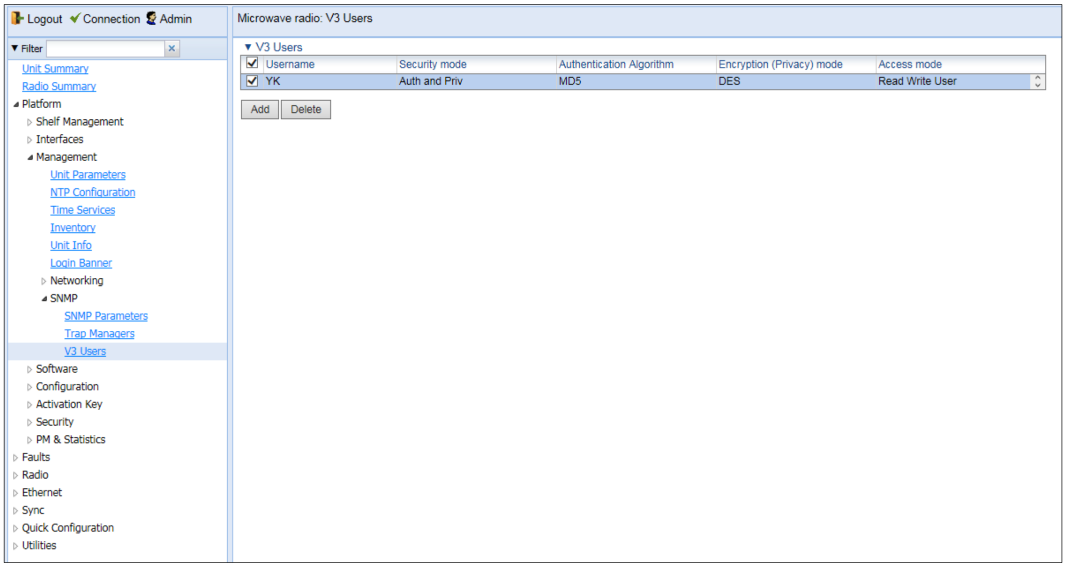
6. **In** the **V1V2 Blocked** field, select **Yes** if you want to block SNMPv1 and SNMPv2 access so that only SNMPv3 access will be enabled.
7. Click **Apply**.

If you are using SNMPv3, you must also configure SNMPv3 users. SNMPv3 security parameters are configured per SNMPv3 user.

To add an SNMP user:

1. Select **Platform > Management SNMP > V3 Users**. The V3 Users page opens.

Figure 107 V3 Users Page



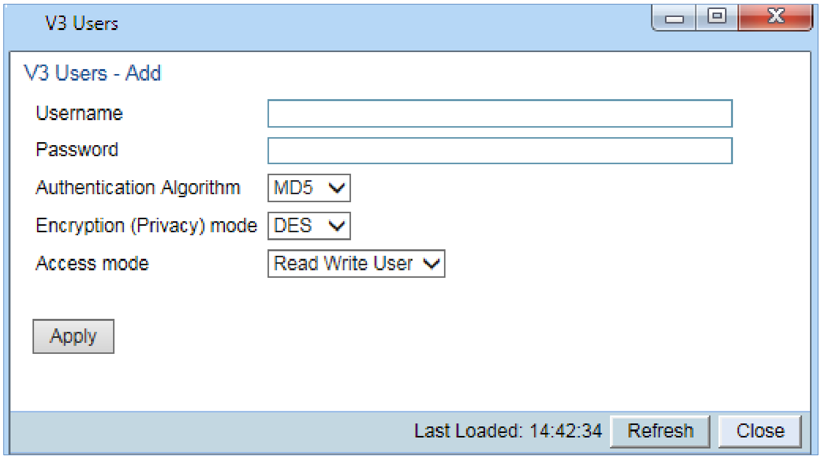
Microwave radio: V3 Users

▼ V3 Users

☑	Username	Security mode	Authentication Algorithm	Encryption (Privacy) mode	Access mode
☑	YK	Auth and Priv	MD5	DES	Read Write User

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

Figure 108 V3 Users - Add Page



Username

Password

Authentication Algorithm: MD5

Encryption (Privacy) mode: DES

Access mode: Read Write User

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

Table 20 SNMP V3 Authentication Parameters

Parameter	Definition
User Name	Enter the SNMPv3 user name.
Password	Enter a password for SNMPv3 authentication. The password must be at least eight characters.
Authentication Algorithm	Select an authentication algorithm for the user. Options are: **None** **SHA** **MD5**
Encryption (Privacy) Mode	Select an encryption (privacy) protocol for the user. Options are: **None** **DES** **AES**
Access Mode	Select an access permission level for the user. Options are: **Read Write User** **Read Only User**

.

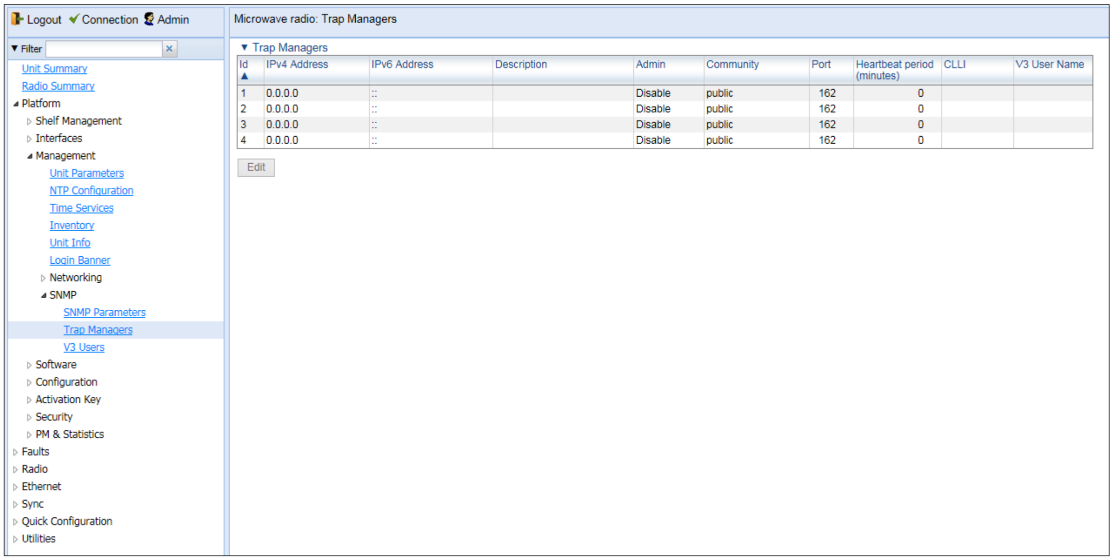
Configuring Trap Managers

You can configure trap forwarding parameters by editing the Trap Managers table. Each line in the Trap Managers table displays the setup for a manager defined in the system.

To configure trap managers:

1. Select **Platform > Management SNMP > Trap Managers**. The Trap Managers page opens.

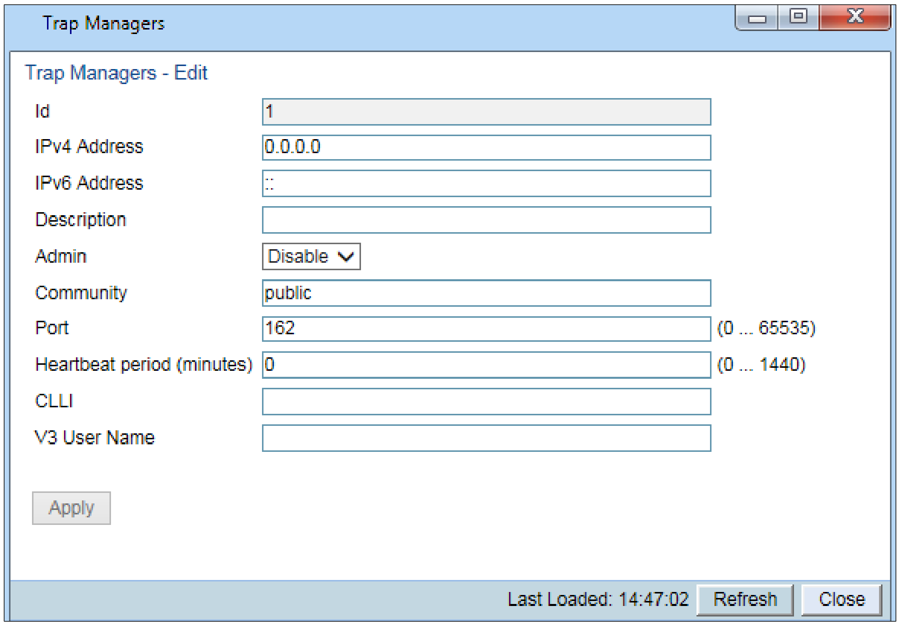
Figure 109 Trap Managers Page



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

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

Figure 110 Trap Managers - Edit Page



Trap Managers - Edit

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

3. Configure the trap manager parameters, as described in Table 21 Trap Manager Parameters.
4. Click **Apply**, then **Close**.

Table 21 Trap Manager Parameters

Parameter	Definition
IPv4 Address	If the IP address family is configured to be IPv4, enter the destination IPv4 address. Traps will be sent to this IP address. See Defining the IP Protocol Version for Initiating Communications.
IPv6 Address	If the IP address family is configured to be IPv6, enter the destination IPv6 address. Traps will be sent to this IP address. See Defining the IP Protocol Version for Initiating Communications.
Description	Enter a description of the trap manager (optional).
Admin	Select **Enable** or **Disable** to enable or disable the selected trap manager.
Community	Enter the community string for the SNMP read community.
Port	Enter the number of the port through which traps will be sent.
Heartbeat Period	Enter the interval, in minutes, between each heartbeat trap.
CLLI	Enter a Common Language Location Identifier (CLLI). The CLLI is free text that will be sent with the trap. You can enter up to 100 characters.

Parameter	Definition
V3 User Name	If the SNMP Trap version selected in Figure 106 SNMP Parameters Page page is **V3**, enter the name of a V3 user defined in the system. To view or define a V3 user, use the Figure 107 V3 Users Page page. **Note**: Make sure that an identical V3 user is also defined on the manager's side.

Installing and Configuring an FTP or SFTP Server

Several tasks, such as software upgrade (except when performed using HTTP or HTTPS) and configuration backup, export, and import, require the use of FTP or SFTP. The PTP 850 can function as an FTP or SFTP client. If you wish to use FTP/SFTP, you must install FTP/SFTP server software on the PC or laptop you are using.

Note

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

If you are using IPv6 to perform the operation, make sure to use FileZilla version 0.9.38 or higher to ensure IPv6 support. If you are using another type of FTP or SFTP server, make sure the application version supports IPv6.

To install and configure FTP or SFTP server software on the PC or laptop:

1. Create a user and (optional) password on the FTP/SFTP server. For example, in FileZilla Server, perform the following:

From the Edit menu, select Users.

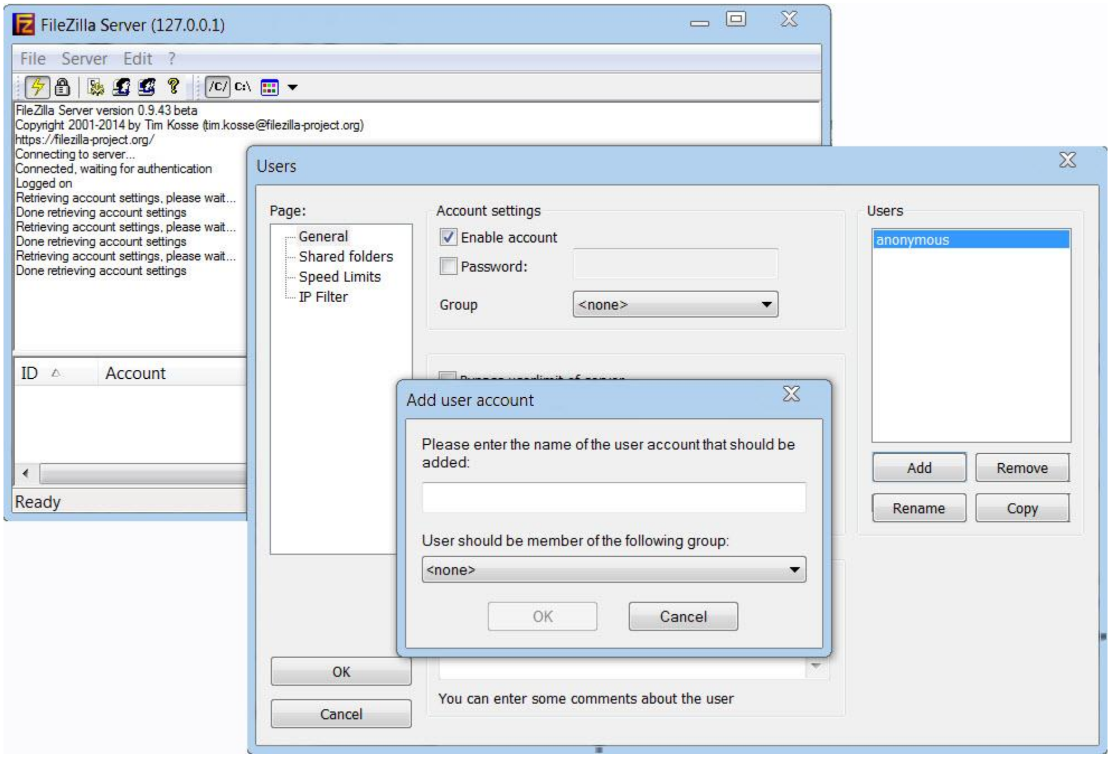
I. In the Users window, click Add.

II. In the Add user account window, enter a user name and click OK.

III. In the Users window, select Enable account and, optionally, select Password and enter a password.

IV. In the Users window, click OK.

Figure 111 FileZilla Server User Configuration



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

☑ Enable account

□ Password:

Group <none>

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

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

You can enter some comments about the user

2. Create a shared FTP/SFTP folder on the PC or laptop you are using to perform the software upgrade (for example, *C:\FTPServer*).
3. In the FTP/SFTP server, set up the permissions for the shared FTP/SFTP folder. For example, in FileZilla Server:

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

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

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

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

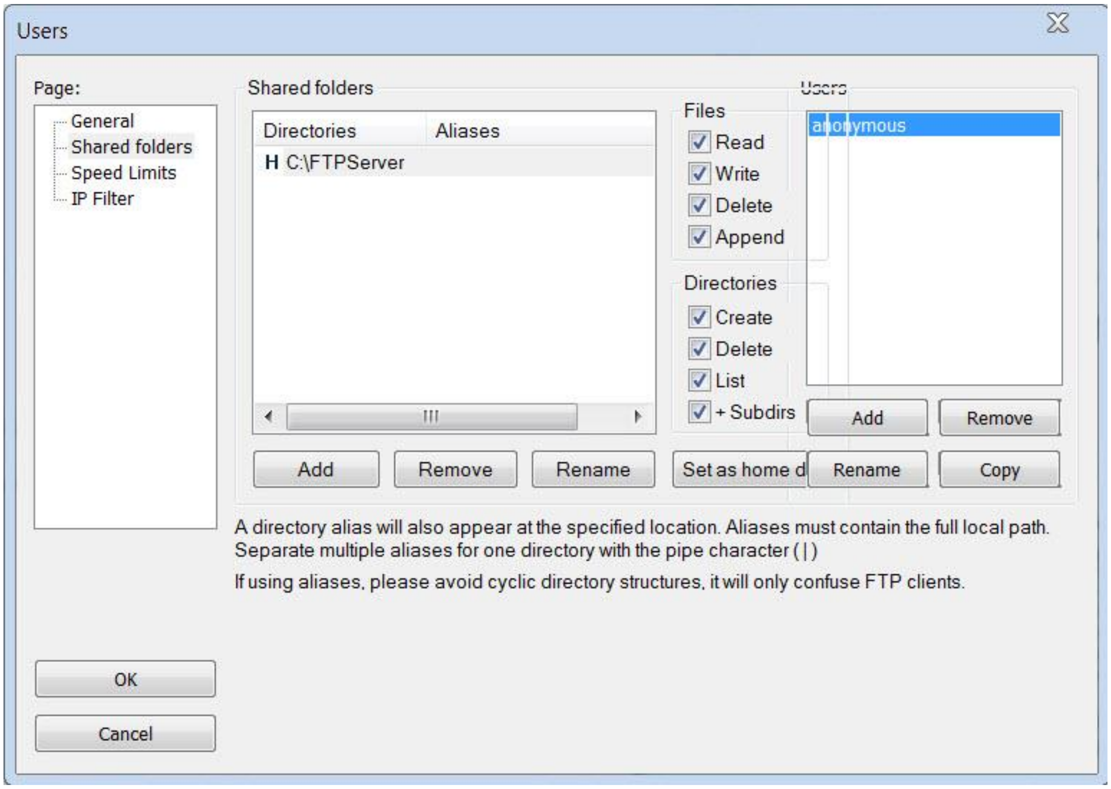
   V. In the Shared folders section, select your shared FTP folder.

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

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

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

Figure 112 FileZilla Server Shared Folder Setup



Directories	Aliases
H C:\FTPServer	

Files

☑ Read
☑ Write
☑ Delete
☑ Append

Directories

☑ Create
☑ Delete
☑ List
☑ + Subdirs

Users: anonymous

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

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

Configuring the Internal Ports for FTP or SFTP

By default, the following PTP 850 ports are used for FTP and SFTP when the PTP 850 unit is acting as an FTP or SFTP client (e.g., software downloads, configuration file backup and restore operations):

FTP – 21

SFTP – 22

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

Platform > Management > Unit Info

Platform > Management > Unit Info

Platform > Software > Download & Install

Platform > Configuration > Configuration Management

Platform > Security > General > Security Log Upload

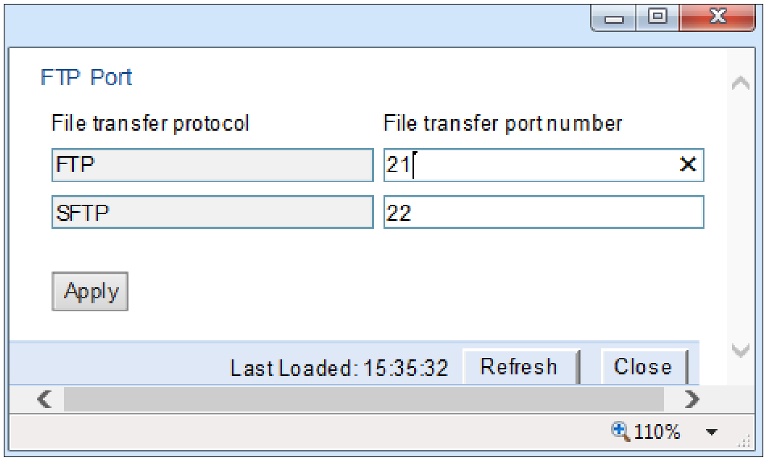
Platform > Security > General > Configuration Log Upload

Platform > Security > X.509 Certificate > CSR

Platform > Security > X.509 Certificate > Download & Install

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

Figure 113 FTP Port Page



FTP Port

File transfer protocol	File transfer port number
FTP	21
SFTP	22

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

Upgrading the Software

PTP 850 software and firmware releases are provided in a single bundle that includes software and firmware for all components in the system. Software is first downloaded to the system, then installed. After installation, a reset is automatically performed on all components whose software was upgraded.

This section includes:

Viewing Current Software Versions

Software Upgrade Overview

Downloading and Installing Software

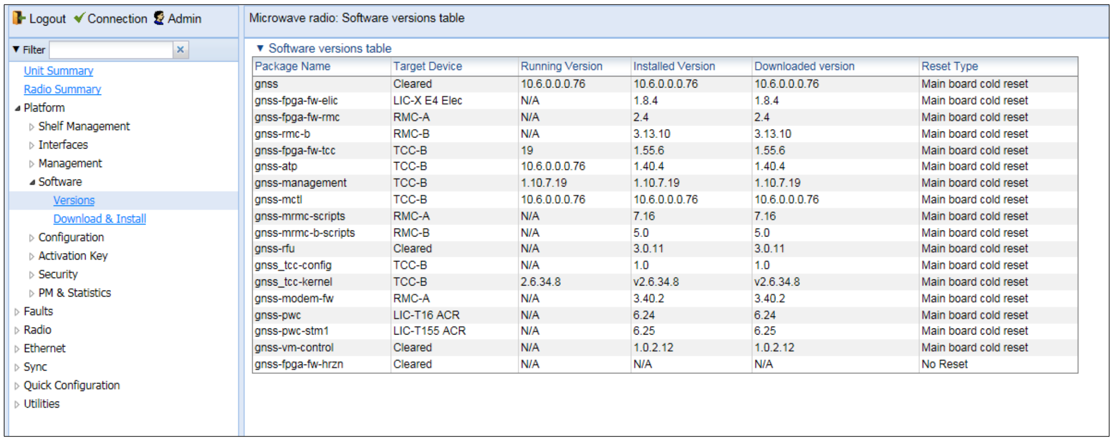
Configuring a Timed Installation

Viewing Current Software Versions

To display a list of software packages currently installed and running on the system modules:

1. Select **Platform > Software > Versions**. The Versions page opens. For a description of the information provided in the Versions page, see Table 22 Software Versions Page Columns.

Figure 114 Versions Page



Microwave radio: Software versions table

Software versions table

Package Name	Target Device	Running Version	Installed Version	Downloaded version	Reset Type
gnss	Cleared	10.6.0.0.0.76	10.6.0.0.0.76	10.6.0.0.0.76	Main board cold reset
gnss-fpga-fw-elic	LIC-X E4 Elec	N/A	1.8.4	1.8.4	Main board cold reset
gnss-fpga-fw-rmc	RMC-A	N/A	2.4	2.4	Main board cold reset
gnss-rmc-b	RMC-B	N/A	3.13.10	3.13.10	Main board cold reset
gnss-fpga-fw-tcc	TCC-B	19	1.55.6	1.55.6	Main board cold reset
gnss-atp	TCC-B	10.6.0.0.0.76	1.40.4	1.40.4	Main board cold reset
gnss-management	TCC-B	1.10.7.19	1.10.7.19	1.10.7.19	Main board cold reset
gnss-mctl	TCC-B	10.6.0.0.0.76	10.6.0.0.0.76	10.6.0.0.0.76	Main board cold reset
gnss-mrmc-scripts	RMC-A	N/A	7.16	7.16	Main board cold reset
gnss-mrmc-b-scripts	RMC-B	N/A	5.0	5.0	Main board cold reset
gnss-rfu	Cleared	N/A	3.0.11	3.0.11	Main board cold reset
gnss_tcc-config	TCC-B	N/A	1.0	1.0	Main board cold reset
gnss_tcc-kernel	TCC-B	2.6.34.8	v2.6.34.8	v2.6.34.8	Main board cold reset
gnss-modem-fw	RMC-A	N/A	3.40.2	3.40.2	Main board cold reset
gnss-pwc	LIC-T16 ACR	N/A	6.24	6.24	Main board cold reset
gnss-pwc-stm1	LIC-T155 ACR	N/A	6.25	6.25	Main board cold reset
gnss-vm-control	Cleared	N/A	1.0.2.12	1.0.2.12	Main board cold reset
gnss-fpga-fw-hrzn	Cleared	N/A	N/A	N/A	No Reset

Table 22 Software Versions Page Columns

Parameter	Definition
Package Name	The name of the software package.
Target Device	The specific component on which the software runs.
Running Version	The software version currently running on the component.

Parameter	Definition
Installed Version	The software version currently installed for the component. If the installed version is not already the running version, it will become the running version after the next reset takes place.
Downloaded Version	The version, if any, that has been downloaded from the server but not yet installed. Upon installation, this version will become the Installed Version.
Reset Type	The level of reset required by the component in order for the Installed Version to become the Active Version. A cold (hard) reset powers down and powers back up the component. A warm (soft) reset simply reboots the software or firmware in the component.

Software Upgrade Overview

The PTP 850 software installation process includes the following steps:

1. **Download** – The files required for the installation or upgrade are downloaded from a remote server.
2. **Installation** – The downloaded software and firmware files are installed in all modules and components of the PTP 850 that are currently running an older version.
3. **Reset** – The PTP 850 is restarted in order to boot the new software and firmware versions.

Software and firmware releases are provided in a single bundle that includes software and firmware for all components in the system. When you download a software bundle, the system verifies the validity of the bundle. The system also compares the files in the bundle to the files currently installed in the PTP 850 and its components, so that only files that need to be updated are actually downloaded. A message is displayed for each file that is actually downloaded.

Note

When downloading an older version, all files in the bundle may be downloaded, including files that are already installed.

Software bundles can be downloaded via HTTP, HTTPS, FTP or SFTP. After the software download is complete, you can initiate the installation.

Downloading and Installing Software

You can download software using HTTP, HTTPS, FTP or SFTP.

When downloading software via HTTPS or HTTPS, the PTP 850E functions as the server, and you can download the software directly to the PTP 850E unit.

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

Downloading Software Via HTTP or HTTPS

To download and install a new software version using HTTP or HTTPS:

1. Before performing a software upgrade, it is important to verify that the system date and time are correct. See
2. Table 10 Activation Key-Enabled-Features Description

3. Activation Key Name	Description
Services Mode	Enables a number of Ethernet services, depending on the type of activation key: • Smart-Pipe –Smart Pipe (L1) services only (unlimited) and a single management service. • Edge-CET Node – Up to 8 services (all supported service types). • Agg-Lvl-1-CET-Node – Up to 64 services (all supported service types). • Agg-Lvl-2-CET-Node – Up to 1024 services (all supported service types). Any CET activation key also enables the following: • A GbE traffic port in addition to the port provided by the default activation key, for a total of 2 GbE traffic ports. • Full QoS for all services including basic queue buffer management (fixed queues buffer size limit, tail-drop only) and eight queues per port, no H-QoS.
Number of Services	Indicates how many services are allowed according to the Services Mode activation key, and how many are actually configured on the device.
H-QoS	Not relevant in the current release.
Network Resiliency	Not relevant for PTP 850.
Ethernet OAM – Fault Management	Enables Connectivity Fault Management (FM) per Y.1731 (CET mode only).
Ethernet OAM – Performance Monitoring	Not relevant in the current release.
LACP	Not relevant in the current release.
Sync Unit	Enables the G.8262 synchronization unit. This activation key is required in order to provide end-to-end synchronization distribution on the physical layer. This activation key is also required to use SyncE.
IEEE 1588 Transparent Clock	Enables IEEE-1588 Transparent Clock.

3. Activation Key Name	Description
IEEE 1588 Ordinary Clock (quantity)	Not relevant in the current release.
IEEE 1588 Boundary Clock	Enables IEEE-1588 Boundary Clock.
Main Card Redundancy	Not relevant for PTP 850.
TDM Pseudowire	Not relevant for PTP 850.
Frame cut-through	Not relevant in the current release.
Secured Management	Enables secure management protocols (SSH, HTTPS, SFTP, SNMPv3, and RADIUS).
FE traffic ports (quantity)	Displays the number of FE traffic ports allowed under the current activation key.
GbE traffic ports (quantity)	Displays the number of GbE traffic ports allowed under the current activation key.
10GbE traffic ports (quantity)	Displays the number of 10G traffic ports allowed under the current activation key.
ACM (quantity)	Displays the number of radio carriers that are allowed to use ACM under the current activation key.
Narrow CHBW 1.75MHz script (quantity)	Not relevant for PTP 850.
Header De-Duplication (quantity)	Displays the number of radio carriers that are allowed to use Header De-Duplication. Only relevant for PTP 850S.
XPIC (quantity)	Displays the number of radio carriers that are allowed to use XPIC. Each carrier in the XPIC pair requires an XPIC activation key.
Multi-Carrier ABC (quantity)	Not relevant for PTP 850.
MIMO	Not relevant for PTP 850.
SD	Not relevant for PTP 850.
ASD	Not relevant for PTP 850.
AFR 1+0 (quantity)	Not relevant for PTP 850.
ACMB Adaptive BW	Displays the number of radio carriers for which there is permission to use ACMB, which enables the use of radio profiles 1 and 2.

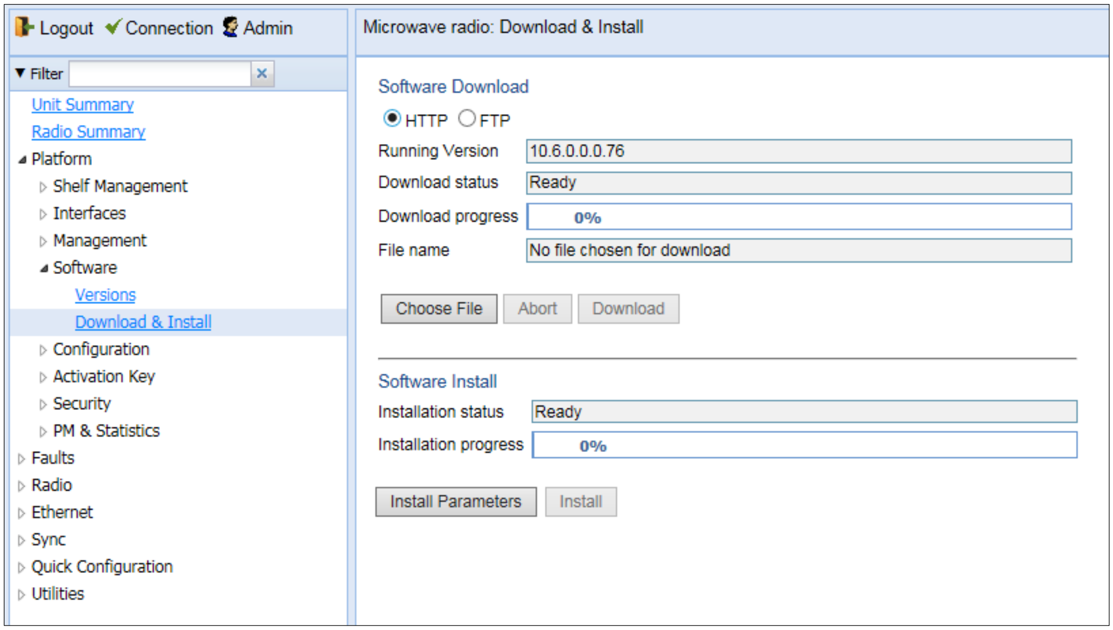
3. Activation Key Name	Description
Payload Encryption AES-256 (quantity)	Displays the number of radio carriers that can use of AES-256 encryption Note that: • If no AES activation key is configured for the unit and the user attempts to enable AES on a radio carrier, in addition to an Activation Key Violation alarm the feature will remain inactive and no encryption will be performed. • After entering an AES activation key, the user must reset the unit before AES can be activated. Unit reset is only necessary for the first AES activation key. If AES activation keys are acquired later for additional radio carriers, unit reset is not necessary. Only relevant for PTP 850E.
Second core activation	Not relevant for PTP 850.
Second core activation for RFU-D	Not relevant for PTP 850.
Second core activation for HP	Not relevant for PTP 850.
Second modem activation	Not relevant for PTP 850.
RFU port activation key	Not relevant for PTP 850.
Radio capacity level 1	Displays the number of radio carriers for which there is permission to use up to 10 Mbps. This is the default level, so every radio carrier on the device has this capacity level.
Radio capacity level 2	Displays the number of radio carriers for which there is permission to use up to 50 Mbps.
Radio capacity level 3	Displays the number of radio carriers for which there is permission to use up to 100 Mbps.
Radio capacity level 4	Displays the number of radio carriers for which there is permission to use up to 150 Mbps.
Radio capacity level 5	Displays the number of radio carriers for which there is permission to use up to 200 Mbps.
Radio capacity level 6	Displays the number of radio carriers for which there is permission to use up to 225 Mbps.
Radio capacity level 7	Displays the number of radio carriers for which there is permission to use up to 250 Mbps.
Radio capacity level 8	Displays the number of radio carriers for which there is permission to use up to 300 Mbps.
Radio capacity level 9	Displays the number of radio carriers for which there is permission to use up to 350 Mbps.

3. Activation Key Name	Description
Radio capacity level 10	Displays the number of radio carriers for which there is permission to use up to 400 Mbps.
Radio capacity level 11	Displays the number of radio carriers for which there is permission to use up to 450 Mbps.
Radio capacity level 12	Displays the number of radio carriers for which there is permission to use up to 500 Mbps.
Radio capacity level 13	Displays the number of radio carriers for which there is permission to use up to 650 Mbps.
Radio capacity level 14	Displays the number of radio carriers for which there is permission to use up to 1000 Mbps.
Radio capacity level 15	Displays the number of radio carriers for which there is permission to use up to 1600 Mbps.
Radio capacity level 16	Displays the number of radio carriers for which there is permission to use up to 2000 Mbps.
Radio capacity level 17	Displays the number of radio carriers for which there is permission to use up to 2500 Mbps.
Radio capacity level 18	Displays the number of radio carriers for which there is permission to use up to 3000 Mbps.
Radio capacity level 19	Displays the number of radio carriers for which there is permission to use up to 4000 Mbps.
Radio capacity level 20	Displays the number of radio carriers for which there is permission to use up to 5000 Mbps.
Radio capacity level 21	Displays the number of radio carriers for which there is permission to use up to 6000 Mbps.
Radio capacity level 22	Displays the number of radio carriers for which there is permission to use up to 7000 Mbps.
Radio capacity level 23	Displays the number of radio carriers for which there is permission to use up to 8000 Mbps.
Radio capacity level 24	Displays the number of radio carriers for which there is permission to use up to 9000 Mbps.
Radio capacity level 25	Displays the number of radio carriers for which there is permission to use up to 10000 Mbps.
Auto State Propagation and LLF	Enables the use of Link Loss Forwarding (LLF) with Automatic State Propagation (ASP). Without the activation key, only one LLF ID can be configured. This means that only one ASP pair can be configured per radio interface or radio group.

3. Activation Key Name	Description
Enhanced Multi-Carrier ABC (quantity)	Enables the configuration and use of a Multiband (Enhanced Multi-Carrier ABC) link. Two activation keys are required per Multiband node, on the IP 50E. One of these activation keys is for the radio port, the other is for the Ethernet port carrying traffic to the unit paired with the PTP 850E. No activation key is required for the unit paired with the PTP 850E.

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

Figure 115 Download & Install Page – HTTP/ HTTPS Download – No File Selected



Microwave radio: Download & Install

Software Download

● HTTP ○ FTP

Running Version: 10.6.0.0.76

Download status: Ready

Download progress: 0%

File name: No file chosen for download

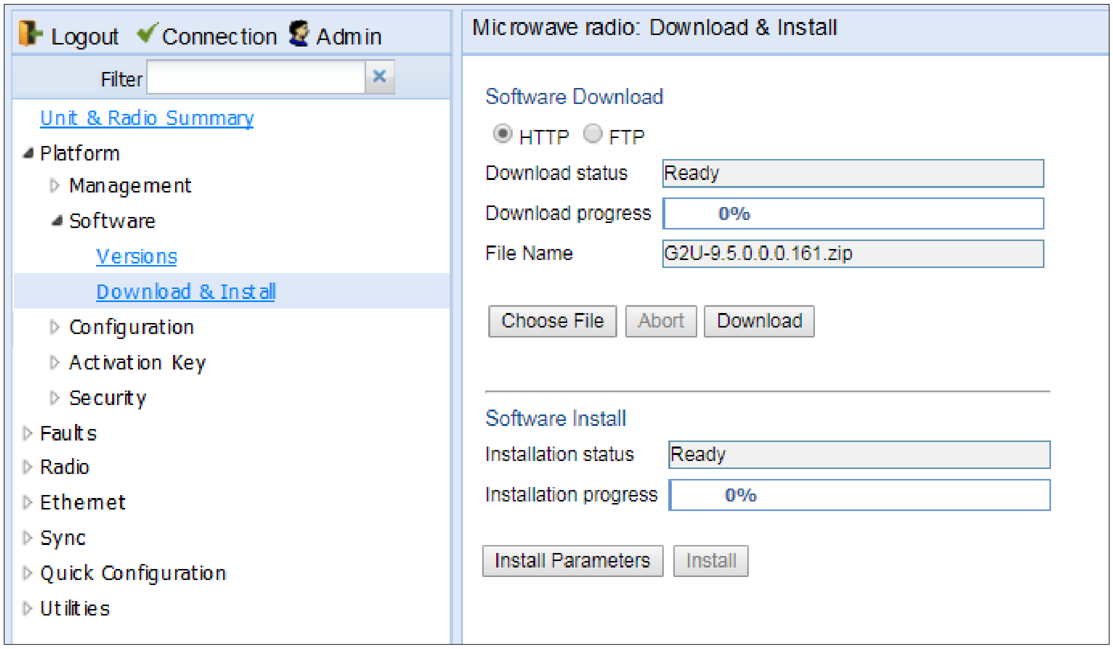
Software Install

Installation status: Ready

Installation progress: 0%

6. Select **HTTP**
7. Click **Choose File.** A browser window opens.
8. Navigate to the directory in which the software file is located and selected the file. The selected file must be a ZIP file.
9. Click **Open**. The file name of the selected file appears in the **File Name** field.

Figure 116 Download & Install page – HTTP/ HTTPS Download – File Selected



Microwave radio: Download & Install

Software Download

● HTTP ○ FTP

Download status: Ready

Download progress: 0%

File Name: G2U-9.5.0.0.0.161.zip

Software Install

Installation status: Ready

Installation progress: 0%

10. Click **Download**. The download begins. You can view the status of the download in the **Download Status** field.

Note

To Discontinue the download process, Click **Abort.**

11. Once the download has been completed, verify that the version you want to install has been downloaded. You can check the downloaded version for each component by viewing the *Downloaded Version* column in the Versions page. See Viewing Current Software versions.

Downloading Software Via FTP or SFTP

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

1. Before performing a software upgrade, it is important to verify that the system date and time are correct. See
2. Table 10 Activation Key-Enabled-Features Description

3. Activation Key Name	Description
Services Mode	Enables a number of Ethernet services, depending on the type of activation key: • Smart-Pipe –Smart Pipe (L1) services only (unlimited) and a single management service. • Edge-CET Node – Up to 8 services (all supported service types). • Agg-Lvl-1-CET-Node – Up to 64 services (all supported service types). • Agg-Lvl-2-CET-Node – Up to 1024 services (all supported service types). Any CET activation key also enables the following: • A GbE traffic port in addition to the port provided by the default activation key, for a total of 2 GbE traffic ports. • Full QoS for all services including basic queue buffer management (fixed queues buffer size limit, tail-drop only) and eight queues per port, no H-QoS.
Number of Services	Indicates how many services are allowed according to the Services Mode activation key, and how many are actually configured on the device.
H-QoS	Not relevant in the current release.
Network Resiliency	Not relevant for PTP 850.
Ethernet OAM – Fault Management	Enables Connectivity Fault Management (FM) per Y.1731 (CET mode only).
Ethernet OAM – Performance Monitoring	Not relevant in the current release.
LACP	Not relevant in the current release.
Sync Unit	Enables the G.8262 synchronization unit. This activation key is required in order to provide end-to-end synchronization distribution on the physical layer. This activation key is also required to use SyncE.
IEEE 1588 Transparent Clock	Enables IEEE-1588 Transparent Clock.
IEEE 1588 Ordinary Clock (quantity)	Not relevant in the current release.
IEEE 1588 Boundary Clock	Enables IEEE-1588 Boundary Clock.
Main Card Redundancy	Not relevant for PTP 850.
TDM Pseudowire	Not relevant for PTP 850.
Frame cut-through	Not relevant in the current release.
Secured Management	Enables secure management protocols (SSH, HTTPS, SFTP, SNMPv3, and RADIUS).

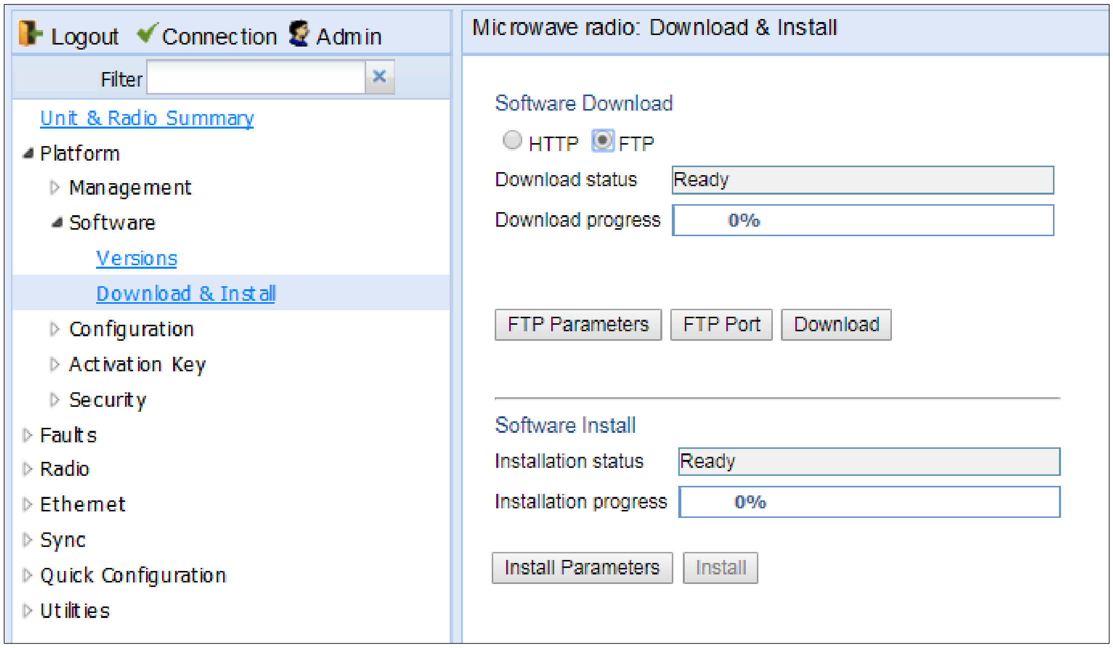
3. Activation Key Name	Description
FE traffic ports (quantity)	Displays the number of FE traffic ports allowed under the current activation key.
GbE traffic ports (quantity)	Displays the number of GbE traffic ports allowed under the current activation key.
10GbE traffic ports (quantity)	Displays the number of 10G traffic ports allowed under the current activation key.
ACM (quantity)	Displays the number of radio carriers that are allowed to use ACM under the current activation key.
Narrow CHBW 1.75MHz script (quantity)	Not relevant for PTP 850.
Header De-Duplication (quantity)	Displays the number of radio carriers that are allowed to use Header De-Duplication. Only relevant for PTP 850S.
XPIC (quantity)	Displays the number of radio carriers that are allowed to use XPIC. Each carrier in the XPIC pair requires an XPIC activation key.
Multi-Carrier ABC (quantity)	Not relevant for PTP 850.
MIMO	Not relevant for PTP 850.
SD	Not relevant for PTP 850.
ASD	Not relevant for PTP 850.
AFR 1+0 (quantity)	Not relevant for PTP 850.
ACMB Adaptive BW	Displays the number of radio carriers for which there is permission to use ACMB, which enables the use of radio profiles 1 and 2.
Payload Encryption AES-256 (quantity)	Displays the number of radio carriers that can use of AES-256 encryption Note that: • If no AES activation key is configured for the unit and the user attempts to enable AES on a radio carrier, in addition to an Activation Key Violation alarm the feature will remain inactive and no encryption will be performed. • After entering an AES activation key, the user must reset the unit before AES can be activated. Unit reset is only necessary for the first AES activation key. If AES activation keys are acquired later for additional radio carriers, unit reset is not necessary. Only relevant for PTP 850E.
Second core activation	Not relevant for PTP 850.
Second core activation for RFU-D	Not relevant for PTP 850.

3. Activation Key Name	Description
Second core activation for HP	Not relevant for PTP 850.
Second modem activation	Not relevant for PTP 850.
RFU port activation key	Not relevant for PTP 850.
Radio capacity level 1	Displays the number of radio carriers for which there is permission to use up to 10 Mbps. This is the default level, so every radio carrier on the device has this capacity level.
Radio capacity level 2	Displays the number of radio carriers for which there is permission to use up to 50 Mbps.
Radio capacity level 3	Displays the number of radio carriers for which there is permission to use up to 100 Mbps.
Radio capacity level 4	Displays the number of radio carriers for which there is permission to use up to 150 Mbps.
Radio capacity level 5	Displays the number of radio carriers for which there is permission to use up to 200 Mbps.
Radio capacity level 6	Displays the number of radio carriers for which there is permission to use up to 225 Mbps.
Radio capacity level 7	Displays the number of radio carriers for which there is permission to use up to 250 Mbps.
Radio capacity level 8	Displays the number of radio carriers for which there is permission to use up to 300 Mbps.
Radio capacity level 9	Displays the number of radio carriers for which there is permission to use up to 350 Mbps.
Radio capacity level 10	Displays the number of radio carriers for which there is permission to use up to 400 Mbps.
Radio capacity level 11	Displays the number of radio carriers for which there is permission to use up to 450 Mbps.
Radio capacity level 12	Displays the number of radio carriers for which there is permission to use up to 500 Mbps.
Radio capacity level 13	Displays the number of radio carriers for which there is permission to use up to 650 Mbps.
Radio capacity level 14	Displays the number of radio carriers for which there is permission to use up to 1000 Mbps.
Radio capacity level 15	Displays the number of radio carriers for which there is permission to use up to 1600 Mbps.

3. Activation Key Name	Description
Radio capacity level 16	Displays the number of radio carriers for which there is permission to use up to 2000 Mbps.
Radio capacity level 17	Displays the number of radio carriers for which there is permission to use up to 2500 Mbps.
Radio capacity level 18	Displays the number of radio carriers for which there is permission to use up to 3000 Mbps.
Radio capacity level 19	Displays the number of radio carriers for which there is permission to use up to 4000 Mbps.
Radio capacity level 20	Displays the number of radio carriers for which there is permission to use up to 5000 Mbps.
Radio capacity level 21	Displays the number of radio carriers for which there is permission to use up to 6000 Mbps.
Radio capacity level 22	Displays the number of radio carriers for which there is permission to use up to 7000 Mbps.
Radio capacity level 23	Displays the number of radio carriers for which there is permission to use up to 8000 Mbps.
Radio capacity level 24	Displays the number of radio carriers for which there is permission to use up to 9000 Mbps.
Radio capacity level 25	Displays the number of radio carriers for which there is permission to use up to 10000 Mbps.
Auto State Propagation and LLF	Enables the use of Link Loss Forwarding (LLF) with Automatic State Propagation (ASP). Without the activation key, only one LLF ID can be configured. This means that only one ASP pair can be configured per radio interface or radio group.
Enhanced Multi-Carrier ABC (quantity)	Enables the configuration and use of a Multiband (Enhanced Multi-Carrier ABC) link. Two activation keys are required per Multiband node, on the IP 50E. One of these activation keys is for the radio port, the other is for the Ethernet port carrying traffic to the unit paired with the PTP 850E. No activation key is required for the unit paired with the PTP 850E.

4. Setting the Time and Date (Optional).
5. Install and configure FTP or SFTP server software on the PC or laptop you are using to perform the software upgrade, as described in Installing and Configuring an FTP or SFTP Server.
6. Unzip the new software package for PTP 850 into your shared FTP or SFTP folder.
7. In the PTP 850's Web EMS, select **Platform > Software > Download & Install**. The Download & Install page opens.
8. Select **FTP**.

Figure 117 Download & Install Page - FTP



Microwave radio: Download & Install

Software Download

○ HTTP ● FTP

Download status: Ready

Download progress: 0%

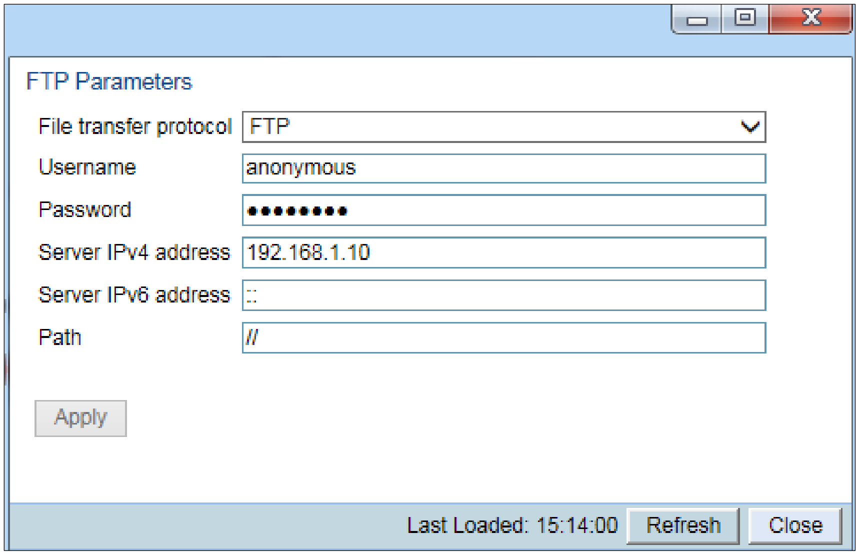
Software Install

Installation status: Ready

Installation progress: 0%

9. Click **FTP Parameters** to view the FTP Parameters page.

Figure 118 FTP Parameters Page



FTP Parameters

File transfer protocol: FTP

Username: anonymous

Password: ●●●●●●●●●

Server IPv4 address: 192.168.1.10

Server IPv6 address: ::

Path: //

10. In the **File Transfer Protocol** field, select the file transfer protocol you want to use (**FTP** or **SFTP**).
11. In the **Username** field, enter the user name you configured in the FTP server.
12. In the **password** field, enter the password you configured in the FTP server. If you did not configure a password for your FTP/SFTP user, simply leave this field blank.
13. If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the FTP/SFTP server in the **Server IPv4 address** field. See Defining the IP Protocol Version for Initiating Communications.
14. If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the FTP/SFTP server in the **Server IPv6 Address** field. See Defining the IP Protocol Version for Initiating Communications.
15. In the **Path** field, enter the directory path from which you are downloading the files. Enter the path relative to the FTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
16. Click **Apply** to save your settings, and **Close** to close the FTP Parameters page.
17. Click **Download**. The download begins. You can view the status of the download in the **Download Status** field of the Download & Install page. See Table 23 Download & Install Status Parameters.
18. Once the download has been completed, verify that the version you want to install has been downloaded. You can check the downloaded version for each component by viewing the *Downloaded Version* column in the Versions page. See Viewing Current Software Versions.

Installing Software

Note

For Instructions on how to configure a timed installation, see Configuring a Timed Installation.

To Install software:

1. Download the software version you want to install. See Downloading and installing Software.
2. Select **Platform > Software > Download & Install**. The Download & Install page opens. (Figure 117).
3. Click **Install**. The installation begins. You can view the status of the installation in the Download & Install - Status Parameters section of the Download & Install Download & Install page. See Table 23 Download & Install Status Parameters.

Upon completion of the installation, the system performs an automatic reset.

Note

DO NOT reboot the unit during the software installation process. As soon as the process is successfully completed, the unit will reboot itself.

Sometimes the installation process can take up to 30 minutes.

Only in the event that software installation was not successfully finished and more than 30 minutes have passed can the unit be rebooted..

Table 23 Download & Install Status Parameters

Parameter	Definition
Download status	The status of any pending software download. Possible values are: • **Ready** – The default value, which appears when no download is in progress. • **Verifying download files** – The system is verifying the files to be downloaded. • **Download in progress** – The download files have been verified, and the download is in progress. If an error occurs during the download, an appropriate error message is displayed in this field. When the download is complete, one of the following status indications appears: • **Download Success** • **Download Failure** • **All components already found in the system** When the system is reset, the **Download Status** returns to **Ready**.
Download progress	Displays the progress of the current software download.
Install status	The status of any pending software installation. Possible values are: • **Ready** – The default value, which appears when no installation is in progress. • **Verifying installation files** – The system is verifying the files to be installed. • **Installation in progress** – The installation files have been verified, and the installation is in progress. If an error occurs during the installation, an appropriate error message is displayed in this field. When the installation is complete, one of the following status indications appears: • **Installation Success** • **Installation Partial Success** • **Installation Failure** • **incomplete-sw-version** When the system is reset, the **Installation Status** returns to **Ready**.
Install progress	Displays the progress of the current software installation.

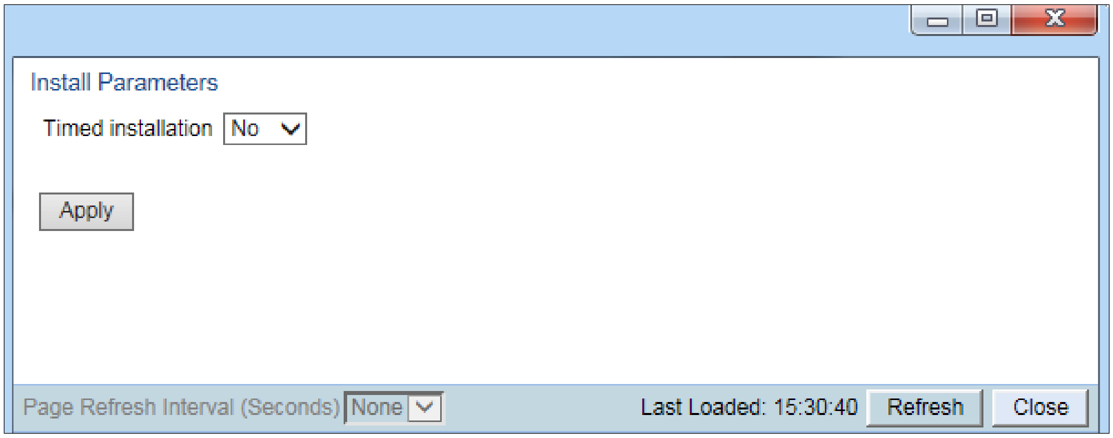
Configuring a Timed Installation

You can schedule a timed (deferred) software installation to take place at any time within 24 hours after you configure the installation.

To schedule a timed software installation:

1. Download the software version you want to install. See Downloading and Installing Software.
2. Select **Platform > Software > Download & Install. The Download & Install page opens.**
3. Click **Install Parameters**. The Install Parameters page opens.

Figure 119 Install parameters Page.



Install Parameters

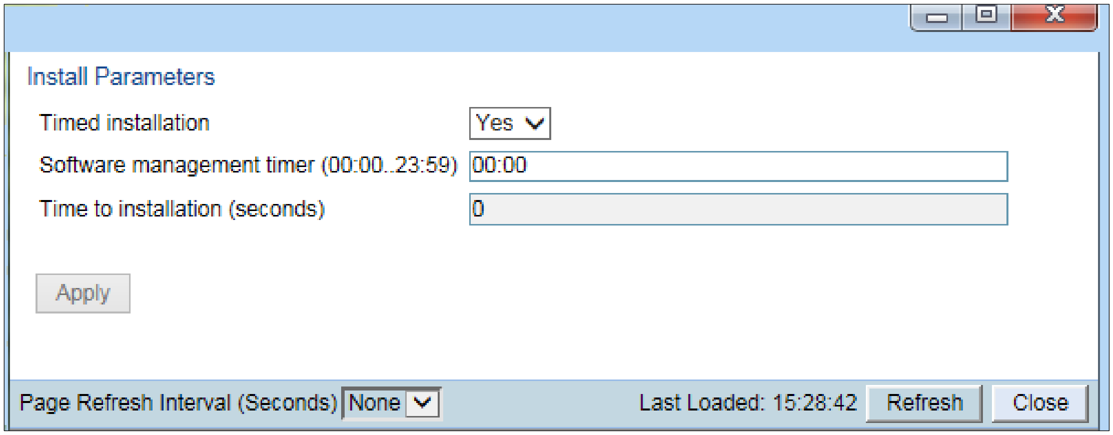
Timed installation: No

Page Refresh Interval (Seconds): None

Last Loaded: 15:30:40

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

Figure 120 Install parameters page- Software Management Timer.



Install Parameters

Timed installation: Yes

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

Time to installation (seconds): 0

Page Refresh Interval (Seconds): None

Last Loaded: 15:28:42

6. In the **Software management timer** field, enter the amount of time, in hours and minutes, you want to defer the installation. For example, inFigure 116, the timer is set for two hours after the timer was configured (02:00).
7. Click **Apply**, then **Close** to close the Install Parameters page.

Backing Up and Restoring Configurations

You can import and export PTP 850 configuration files. This enables you to copy the system configuration to multiple PTP 850 units. You can also backup and save configuration files.

Configuration files can only be copied between units of the same type, i.e., PTP 850E to PTP 850E to PTP 850E.

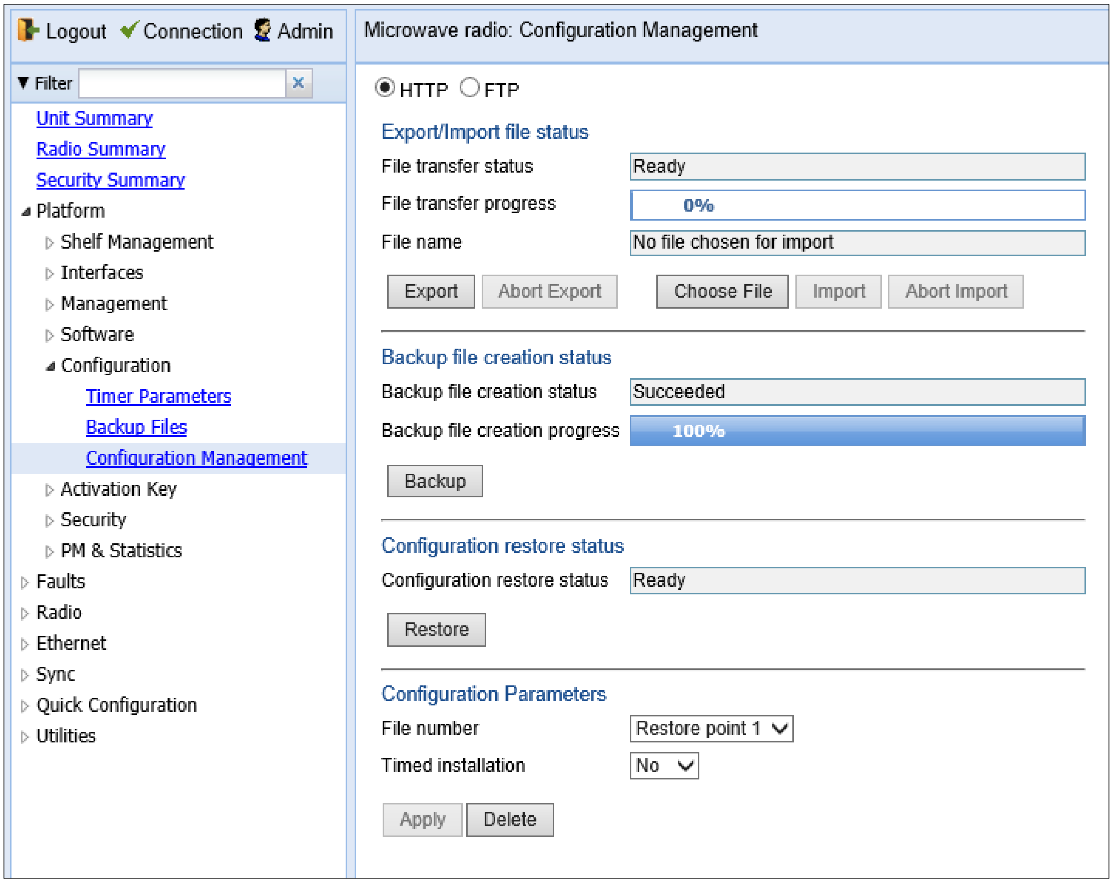
This section includes:

Configuration Management Overview

Viewing Current Backup Files

Setting the Configuration Management Parameters

Exporting a Configuration File



Microwave radio: Configuration Management

● HTTP ○ FTP

Export/Import file status

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

Backup file creation status

Backup file creation status	Succeeded
Backup file creation progress	100%

Configuration restore status

Configuration restore status	Ready

Configuration Parameters

File number	Restore point 1
Timed installation	No

Figure 124 Configuration Management Page – HTTP/HTTPS

1 In the **File number** field, select the restore point from which to export the file.

Note: The Timed installation field is reserved for future use.

2 Click **Export**. The export begins. You can view the status of the export in the **File Transfer status** field in the Export/Import file status section. Possible values are:

- **Ready** - The default value, which appears when no import or export is in progress.
- **File-in-Transfer** – The file export is in progress.
- If an error occurs during the import or export, an appropriate error message is displayed in this field.

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

- Succeeded
- Failure

The next time the system is reset, the File Transfer status field returns to

Ready.

3 To abort the export, click Abort Export.

Exporting a Configuration File Via FTP or SFTP

To export a configuration file via FTP or SFTP:

1 Verify that you have followed all the steps in *Setting the FTP/SFTP Configuration Management Parameters*.

2 Select Platform > Configuration > Configuration Management. The Configuration Management page opens (*Figure 116*).

3 Select **FTP**.

4 In the File Number field, select the restore point from which you want to export the file.

Note: The Timed installation field is reserved for future use.

5 Click Apply to save your settings.

6 Click Export. The export begins. You can view the status of the export in the File Transfer status field in the Export/Import file status section. Possible values are:

- Ready – The default value, which appears when no import or export is in progress.
- File-in-Transfer – The file export is in progress.
- If an error occurs during the import or export, an appropriate error message is displayed in this field.

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

- Succeeded
- Failure

The next time the system is reset, the File Transfer status field returns to Ready.

Configuration Management Overview

System configuration files consist of a zip file that contains three components:

A binary configuration file used by the system to restore the configuration.

A text file which enables users to examine the system configuration in a readable format. The file includes the value of all system parameters at the time of creation of the backup file.

An additional text file which enables you to write CLI scripts in order to make desired changes in the backed-up configuration. This file is executed by the system after restoring the configuration.

The system provides three restore points to manage different configuration files. Each restore point contains a single configuration file. Files can be added to the restore points by creating backups of the current system state or by importing them from an external server. For example, you may want to use one restore point to keep a last good configuration, another to import changes from an external server, and the third to store the current configuration.

You can apply a configuration file to the system from any of the restore points.

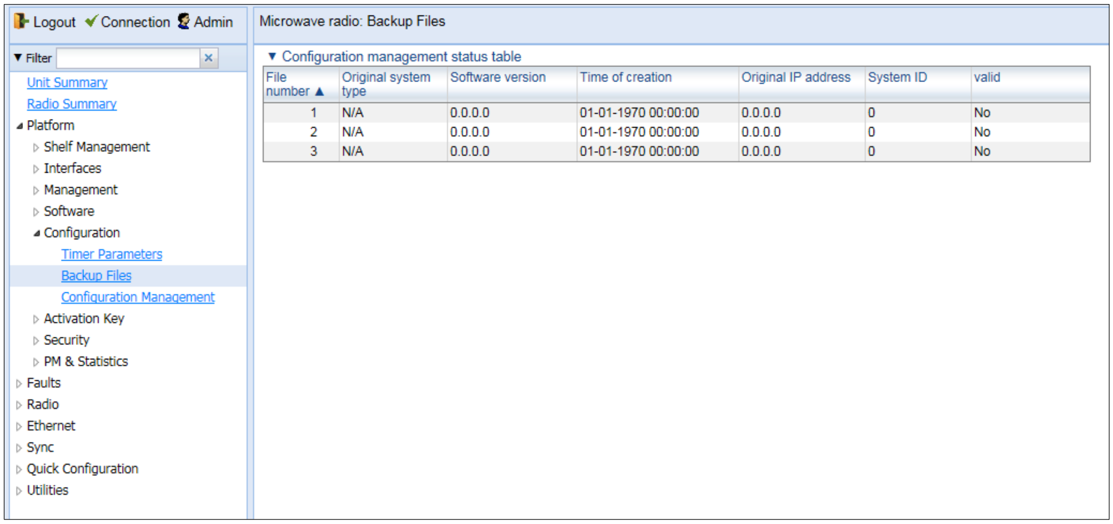
Viewing Current Backup Files

The system provides three restore points to manage different configuration files. Each restore point contains a single configuration file. Files can be added to the restore points by creating backups of the current system state or by importing them from an external server. For example, you may want to use one restore point to keep a last good configuration, another to import changes from an external server, and the third to store the current configuration.

To display the configuration files currently saved at the system restore points:

1. Select **Platform > Configuration > Backup Files**. The Backup Files page opens. For a description of the information provided in the Backup Files page, see Table 24 Backup Files Page Columns.

Figure 121 Backup Files Page



Microwave radio: Backup Files

Configuration management status table

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

Table 24 Backup Files Page Columns

Parameter	Definition
File number	A number from 1 to 3 that identifies the restore point.
Original system type	The type of unit from which the backup configuration file was created.
Software version	The software version of the unit from which the backup configuration file was created.
Time of creation	The time and date on which the configuration file was created.
Original IP address	The IP address of the unit from which the configuration file was created.
System ID	The System ID, if any, of the unit from which the configuration file was created. This is taken from the **Name** field in the Unit Parameters page. See Configuring Unit Parameters.
Valid	Reserved for future use.

Setting the Configuration Management Parameters

When importing and exporting configuration files, the PTP 850 functions as an FTP or SFTP client. You must install FTP or SFTP server software on the PC or laptop you are using to perform the import or export. For details, see Installing and Configuring an FTP or SFTP Server.

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

1. Verify that the system date and time are correct. See
2. Table 10 Activation Key-Enabled-Features Description

3. Activation Key Name	Description
Services Mode	Enables a number of Ethernet services, depending on the type of activation key: • Smart-Pipe –Smart Pipe (L1) services only (unlimited) and a single management service. • Edge-CET Node – Up to 8 services (all supported service types). • Agg-Lvl-1-CET-Node – Up to 64 services (all supported service types). • Agg-Lvl-2-CET-Node – Up to 1024 services (all supported service types). Any CET activation key also enables the following: • A GbE traffic port in addition to the port provided by the default activation key, for a total of 2 GbE traffic ports. • Full QoS for all services including basic queue buffer management (fixed queues buffer size limit, tail-drop only) and eight queues per port, no H-QoS.
Number of Services	Indicates how many services are allowed according to the Services Mode activation key, and how many are actually configured on the device.
H-QoS	Not relevant in the current release.
Network Resiliency	Not relevant for PTP 850.
Ethernet OAM – Fault Management	Enables Connectivity Fault Management (FM) per Y.1731 (CET mode only).
Ethernet OAM – Performance Monitoring	Not relevant in the current release.
LACP	Not relevant in the current release.
Sync Unit	Enables the G.8262 synchronization unit. This activation key is required in order to provide end-to-end synchronization distribution on the physical layer. This activation key is also required to use SyncE.
IEEE 1588 Transparent Clock	Enables IEEE-1588 Transparent Clock.
IEEE 1588 Ordinary Clock (quantity)	Not relevant in the current release.
IEEE 1588 Boundary Clock	Enables IEEE-1588 Boundary Clock.
Main Card Redundancy	Not relevant for PTP 850.
TDM Pseudowire	Not relevant for PTP 850.
Frame cut-through	Not relevant in the current release.

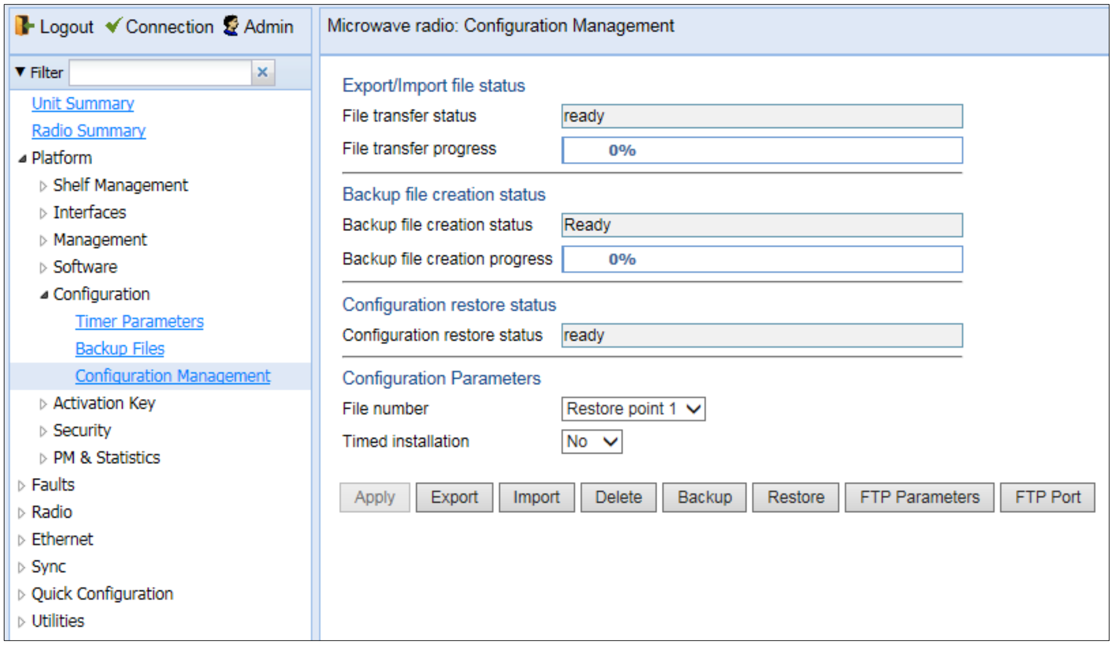
3. Activation Key Name	Description
Secured Management	Enables secure management protocols (SSH, HTTPS, SFTP, SNMPv3, and RADIUS).
FE traffic ports (quantity)	Displays the number of FE traffic ports allowed under the current activation key.
GbE traffic ports (quantity)	Displays the number of GbE traffic ports allowed under the current activation key.
10GbE traffic ports (quantity)	Displays the number of 10G traffic ports allowed under the current activation key.
ACM (quantity)	Displays the number of radio carriers that are allowed to use ACM under the current activation key.
Narrow CHBW 1.75MHz script (quantity)	Not relevant for PTP 850.
Header De-Duplication (quantity)	Displays the number of radio carriers that are allowed to use Header De-Duplication. Only relevant for PTP 850S.
XPIC (quantity)	Displays the number of radio carriers that are allowed to use XPIC. Each carrier in the XPIC pair requires an XPIC activation key.
Multi-Carrier ABC (quantity)	Not relevant for PTP 850.
MIMO	Not relevant for PTP 850.
SD	Not relevant for PTP 850.
ASD	Not relevant for PTP 850.
AFR 1+0 (quantity)	Not relevant for PTP 850.
ACMB Adaptive BW	Displays the number of radio carriers for which there is permission to use ACMB, which enables the use of radio profiles 1 and 2.
Payload Encryption AES-256 (quantity)	Displays the number of radio carriers that can use of AES-256 encryption Note that: • If no AES activation key is configured for the unit and the user attempts to enable AES on a radio carrier, in addition to an Activation Key Violation alarm the feature will remain inactive and no encryption will be performed. • After entering an AES activation key, the user must reset the unit before AES can be activated. Unit reset is only necessary for the first AES activation key. If AES activation keys are acquired later for additional radio carriers, unit reset is not necessary. Only relevant for PTP 850E.
Second core activation	Not relevant for PTP 850.

3. Activation Key Name	Description
Second core activation for RFU-D	Not relevant for PTP 850.
Second core activation for HP	Not relevant for PTP 850.
Second modem activation	Not relevant for PTP 850.
RFU port activation key	Not relevant for PTP 850.
Radio capacity level 1	Displays the number of radio carriers for which there is permission to use up to 10 Mbps. This is the default level, so every radio carrier on the device has this capacity level.
Radio capacity level 2	Displays the number of radio carriers for which there is permission to use up to 50 Mbps.
Radio capacity level 3	Displays the number of radio carriers for which there is permission to use up to 100 Mbps.
Radio capacity level 4	Displays the number of radio carriers for which there is permission to use up to 150 Mbps.
Radio capacity level 5	Displays the number of radio carriers for which there is permission to use up to 200 Mbps.
Radio capacity level 6	Displays the number of radio carriers for which there is permission to use up to 225 Mbps.
Radio capacity level 7	Displays the number of radio carriers for which there is permission to use up to 250 Mbps.
Radio capacity level 8	Displays the number of radio carriers for which there is permission to use up to 300 Mbps.
Radio capacity level 9	Displays the number of radio carriers for which there is permission to use up to 350 Mbps.
Radio capacity level 10	Displays the number of radio carriers for which there is permission to use up to 400 Mbps.
Radio capacity level 11	Displays the number of radio carriers for which there is permission to use up to 450 Mbps.
Radio capacity level 12	Displays the number of radio carriers for which there is permission to use up to 500 Mbps.
Radio capacity level 13	Displays the number of radio carriers for which there is permission to use up to 650 Mbps.
Radio capacity level 14	Displays the number of radio carriers for which there is permission to use up to 1000 Mbps.

3. Activation Key Name	Description
Radio capacity level 15	Displays the number of radio carriers for which there is permission to use up to 1600 Mbps.
Radio capacity level 16	Displays the number of radio carriers for which there is permission to use up to 2000 Mbps.
Radio capacity level 17	Displays the number of radio carriers for which there is permission to use up to 2500 Mbps.
Radio capacity level 18	Displays the number of radio carriers for which there is permission to use up to 3000 Mbps.
Radio capacity level 19	Displays the number of radio carriers for which there is permission to use up to 4000 Mbps.
Radio capacity level 20	Displays the number of radio carriers for which there is permission to use up to 5000 Mbps.
Radio capacity level 21	Displays the number of radio carriers for which there is permission to use up to 6000 Mbps.
Radio capacity level 22	Displays the number of radio carriers for which there is permission to use up to 7000 Mbps.
Radio capacity level 23	Displays the number of radio carriers for which there is permission to use up to 8000 Mbps.
Radio capacity level 24	Displays the number of radio carriers for which there is permission to use up to 9000 Mbps.
Radio capacity level 25	Displays the number of radio carriers for which there is permission to use up to 10000 Mbps.
Auto State Propagation and LLF	Enables the use of Link Loss Forwarding (LLF) with Automatic State Propagation (ASP). Without the activation key, only one LLF ID can be configured. This means that only one ASP pair can be configured per radio interface or radio group.
Enhanced Multi-Carrier ABC (quantity)	Enables the configuration and use of a Multiband (Enhanced Multi-Carrier ABC) link. Two activation keys are required per Multiband node, on the IP 50E. One of these activation keys is for the radio port, the other is for the Ethernet port carrying traffic to the unit paired with the PTP 850E. No activation key is required for the unit paired with the PTP 850E.

4. Setting the Time and Date (Optional).
5. Install and configure an FTP server on the PC or laptop you are using to perform the import or export. See Installing and Configuring an FTP or SFTP Server.
6. In the PTP 850E Web EMS, select **Platform > Configuration > Configuration Management**. The Configuration Management page opens.

Figure 122 Configuration Management Page



Microwave radio: Configuration Management

Export/Import file status

File transfer status: ready

File transfer progress: 0%

Backup file creation status

Backup file creation status: Ready

Backup file creation progress: 0%

Configuration restore status

Configuration restore status: ready

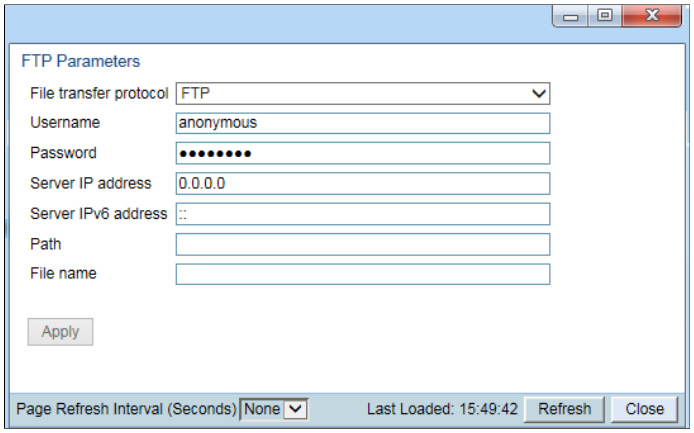
Configuration Parameters

File number: Restore point 1

Timed installation: No

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

Figure 123 FTP Parameters Page



FTP Parameters

File transfer protocol: FTP

Username: anonymous

Password: ••••••••

Server IP address: 0.0.0.0

Server IPv6 address: ::

Path:

File name:

Page Refresh Interval (Seconds): None

Last Loaded: 15:49:42

5. In the **File transfer protocol** field, select the file transfer protocol you want to use (**FTP** or **SFTP**).
6. In the **Username** field, enter the user name you configured in the FTP server.
7. In the **Password** field, enter the password you configured in the FTP server. If you did not configure a password for your FTP user, simply leave this field blank.
8. If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the FTP server in the **Server IP address** field. See *Defining the IP Protocol Version for Initiating Communications*.
9. If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the FTP server in the **Server IPv6 Address** field. See *Defining the IP Protocol Version for Initiating Communications*.
10. In the **Path** field, enter the location of the file you are downloading or uploading. If the location is the root shared folder, it should be left empty. If the location is a sub-folder under the root shared folder, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".

11. In the **File name** field, enter the name of the file you are importing, or the name you want to give the file you are exporting.

> **Note**
>
> You must add the suffix **.zip** to the file name. Otherwise, the file import may fail. You can export the file using any name, then add the suffix **.zip** manually.

12. Click **Apply**, then **Close**, to save the FTP parameters and return to the Configuration Management page
13. In the **File number** field, select from three system restore points:
    - When you import a configuration file, the file is saved to the selected restore point, and overwrites whichever file was previously held in that restore point.
    - When you export a configuration file, the file is exported from the selected restore point.
    - When you back up the current configuration, the backup configuration file is saved to the selected restore point, and overwrites whichever file was previously held in that restore point.
    - When you restore a configuration, the configuration file in the selected restore point is the file that is restored.

> **Note**
>
> The **Timed installation** field is reserved for future use.

14. Click **Apply** to save your settings.

Exporting a Configuration File

You can export a saved configuration file from one of the system's three restore points to a PC or laptop.

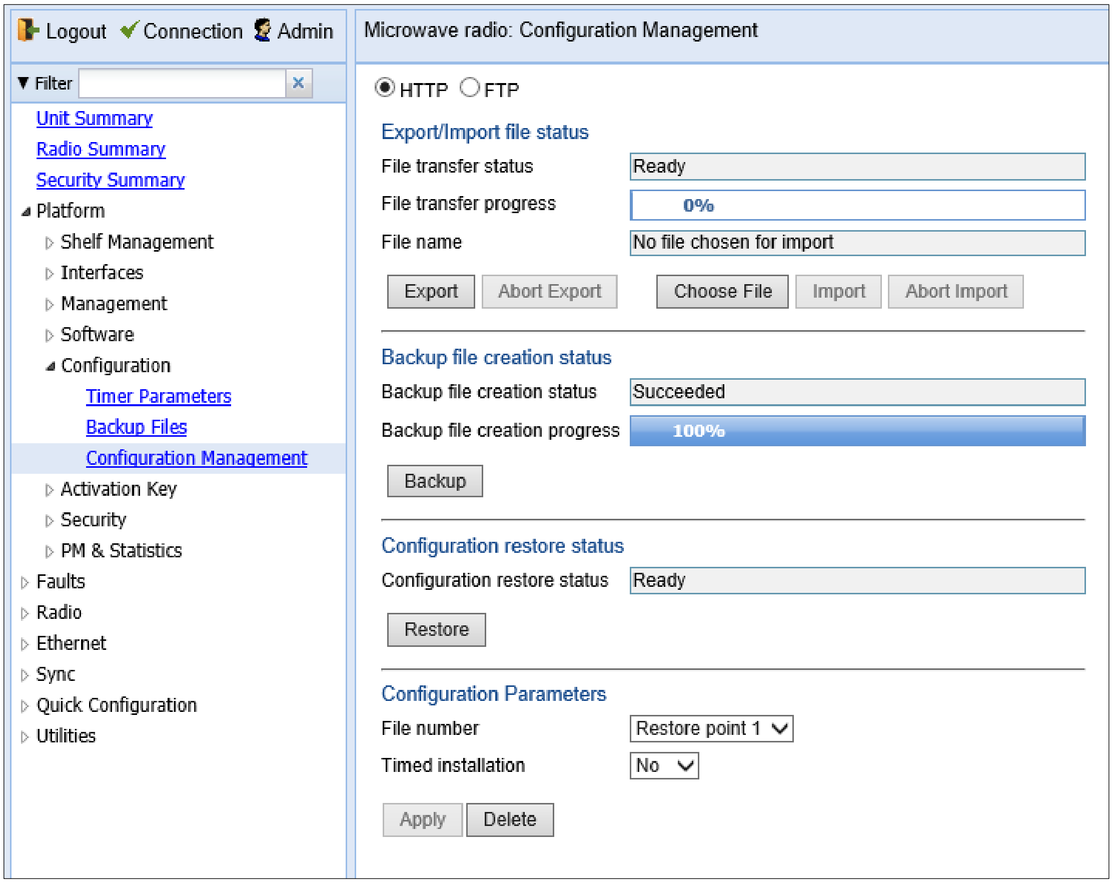
To export a configuration file:

Exporting a Configuration File Via HTTP or HTTPS

To export a configuration file using HTTP or HTTPS:

4 Select Platform > Configuration > Configuration Management. The Configuration Management page opens.

5 Select **HTTP**.



Microwave radio: Configuration Management

● HTTP ○ FTP

Export/Import file status

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

Backup file creation status

Backup file creation status	Succeeded
Backup file creation progress	100%

Configuration restore status

Configuration restore status	Ready

Configuration Parameters

File number	Restore point 1
Timed installation	No

Figure 124 Configuration Management Page – HTTP/HTTPS

6 In the **File number** field, select the restore point from which to export the file.

Note: The Timed installation field is reserved for future use.

7 Click **Export**. The export begins. You can view the status of the export in the **File Transfer status** field in the Export/Import file status section. Possible values are:

◦ **Ready** - The default value, which appears when no import or export is in progress.

- **File-in-Transfer** – The file export is in progress.
- If an error occurs during the import or export, an appropriate error message is displayed in this field.

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

- Succeeded
- Failure

The next time the system is reset, the File Transfer status field returns to Ready.

8 To abort the export, click Abort Export.

Exporting a Configuration File Via FTP or SFTP

To export a configuration file via FTP or SFTP:

7 Verify that you have followed all the steps in *Setting the FTP/SFTP Configuration Management Parameters*.

8 Select Platform > Configuration > Configuration Management. The Configuration Management page opens (*Figure 116*).

9 Select **FTP**.

10 In the File Number field, select the restore point from which you want to export the file.

Note: The Timed installation field is reserved for future use.

11 Click Apply to save your settings.

12 Click Export. The export begins. You can view the status of the export in the File Transfer status field in the Export/Import file status section. Possible values are:

- Ready – The default value, which appears when no import or export is in progress.
- File-in-Transfer – The file export is in progress.
- If an error occurs during the import or export, an appropriate error message is displayed in this field.

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

- Succeeded
- Failure

The next time the system is reset, the File Transfer status field returns to Ready.

Importing a Configuration File

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

Importing a Configuration File Via HTTP or HTTPS

1. Select **Platform > Configuration > Configuration Management**. The Configuration Management page opens (Figure 122).
2. In the **File Number** field, select the restore point to which you want to import the file.
3. Click **Apply** to save your settings.
4. Click **Import**. The import begins. You can view the status of the import in the **File Transfer status** field in the Export/Import file status section. Possible values are:
   - **Ready** – The default value, which appears when no import or export is in progress.
   - **File-in-Transfer** – The file import is in progress.
   - If an **error** occurs during the import or export, an appropriate error message is displayed in this field.
   - When the import or export is complete, one of the following status indications appears:
   - Succeeded
   - Failure
   - The next time the system is reset, the File Transfer status field returns to
   - Ready.

After importing the configuration file, you can apply the configuration by restoring the file from the restore point to which you saved it. See Restoring a Saved Configuration.

Importing a Configuration File Via FTP or SFTP

To import a configuration file using FTP or SFTP:

- Verify that you have followed all the steps in Setting the FTP/SFTP Configuration Management Parameters.
- Select Platform > Configuration > Configuration Management. The Configuration Management page opens (Figure 202).
- Select FTP.
- In the File Number field, select the restore point to which you want to import the file. The imported file will be saved to the selected restore point, and will overwrite whatever file was previously held in that restore point.
- Click Apply to save your settings.
- Click Import. The import begins. You can view the status of the import in the File Transfer status field in the Export/Import file status section. Possible values are:
- Ready – The default value, which appears when no import or export is in progress.
- File-in-Transfer – The file import is in progress.
- If an error occurs during the import or export, an appropriate error message is displayed in this field.
- When the import or export is complete, one of the following status indications appears:
- Succeeded
- Failure
- The next time the system is reset, the File Transfer status field returns to Ready.

- After importing the configuration file, you can apply the configuration by restoring the file from the restore point to which you saved it.

Deleting a Configuration File

You can delete a saved configuration file from any of the system's three restore points:

To delete a configuration file:

1. Select **Platform > Configuration > Configuration Management**. The Configuration Management page opens (Figure 122).
2. In the **File Number** field, select the restore point that holds the configuration file you want to delete.
3. Click **Delete**. The file is deleted.

Backing Up the Current Configuration

You can back up the current configuration file to one of the system's three restore points.

To back up a configuration file:

1. Select **Platform > Configuration > Configuration Management**. The Configuration Management page opens (Figure 122).
2. In the **File Number** field, select the restore point to which you want to back up the file. If another configuration file is already saved to that restore point, it will be overwritten by the file you back up.
3. Click **Backup**. The backup begins. You can view the status of the backup in the **Backup file creation status** field. Possible values in the status field are:
   - **Ready** – The default value, which appears when no backup is in progress.
   - **Generating file** – The system is verifying the files to be backed up.

If an error occurs during the backup, an appropriate error message is displayed in this field.

When the backup is complete, one of the following status indications appears:

- **Succeeded**
- **Failure**

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

Restoring a Saved Configuration

You can replace the current configuration with any configuration file saved to one of the system's three restore points by restoring the configuration file from the restore point.

To restore a configuration file:

1. Select **Platform > Configuration > Configuration Management**. The Configuration Management page opens (Figure 122 Configuration Management Page).
2. In the **File Number** field, select the restore point that holds the configuration you want to restore.

3. Click **Restore**. The configuration restoration begins. You can view the status of the restoration in the **Configuration restore status** field.

Note

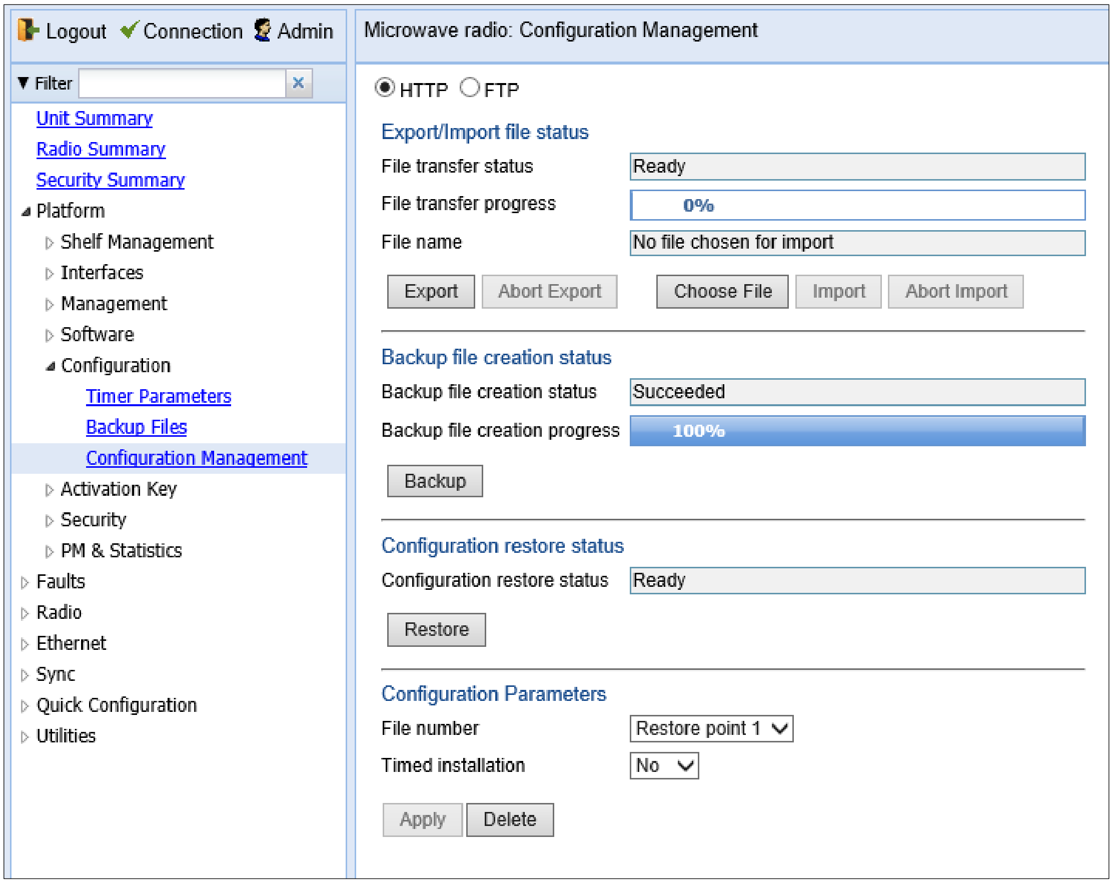
While a configuration restoration is taking place, no user can make any changes to the configuration. All system configuration parameters are read-only during the configuration restoration.

Editing CLI Scripts

The configuration file package includes a text file that enables you to write CLI scripts in a backed-up configuration that are executed after restoring the configuration.

To edit a CLI script:

1. Back up the current configuration to one of the restore points. See Backing Up the Current Configuration.
2. Export the configuration from the restore point to a PC or laptop. See Exporting a Configuration File.
3. On the PC or laptop, unzip the file *Configuration_files.zip*.
4. Edit *the cli_script.txt* file using clish commands, one per line.
5. Save and close the *cli_script.txt* file, and add it back into the *Configuration_files.zip* file.
6. Import the updated *Configuration_files.zip* file back into the unit. See



Microwave radio: Configuration Management

● HTTP ○ FTP

Export/Import file status

File transfer status: Ready

File transfer progress: 0%

File name: No file chosen for import

Backup file creation status

Backup file creation status: Succeeded

Backup file creation progress: 100%

Configuration restore status

Configuration restore status: Ready

Configuration Parameters

File number: Restore point 1

Timed installation: No

7.

8. Figure 124 Configuration Management Page – HTTP/HTTPS

9 In the **File number** field, select the restore point from which to export the file.

Note: The Timed installation field is reserved for future use.

10 Click **Export**. The export begins. You can view the status of the export in the **File Transfer status** field in the Export/Import file status section. Possible values are:

- **Ready** - The default value, which appears when no import or export is in progress.
- **File-in-Transfer** – The file export is in progress.
- If an error occurs during the import or export, an appropriate error message is displayed in this field.

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

- Succeeded
- Failure

The next time the system is reset, the File Transfer status field returns to

Ready.

11 To abort the export, click Abort Export.

Exporting a Configuration File Via FTP or SFTP

To export a configuration file via FTP or SFTP:

13 Verify that you have followed all the steps in *Setting the FTP/SFTP Configuration Management Parameters*.

14 Select Platform > Configuration > Configuration Management. The Configuration Management page opens (*Figure 116*).

15 Select **FTP**.

16 In the File Number field, select the restore point from which you want to export the file.

Note: The Timed installation field is reserved for future use.

17 Click Apply to save your settings.

18 Click Export. The export begins. You can view the status of the export in the File Transfer status field in the Export/Import file status section. Possible values are:

- Ready – The default value, which appears when no import or export is in progress.
- File-in-Transfer – The file export is in progress.
- If an error occurs during the import or export, an appropriate error message is displayed in this field.

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

- Succeeded
- Failure

The next time the system is reset, the File Transfer status field returns to Ready.

9. Importing a Configuration File.
10. Restore the imported configuration file. See Restoring a Saved Configuration. The unit is automatically reset. During initialization, the CLI script is executed, line by line.

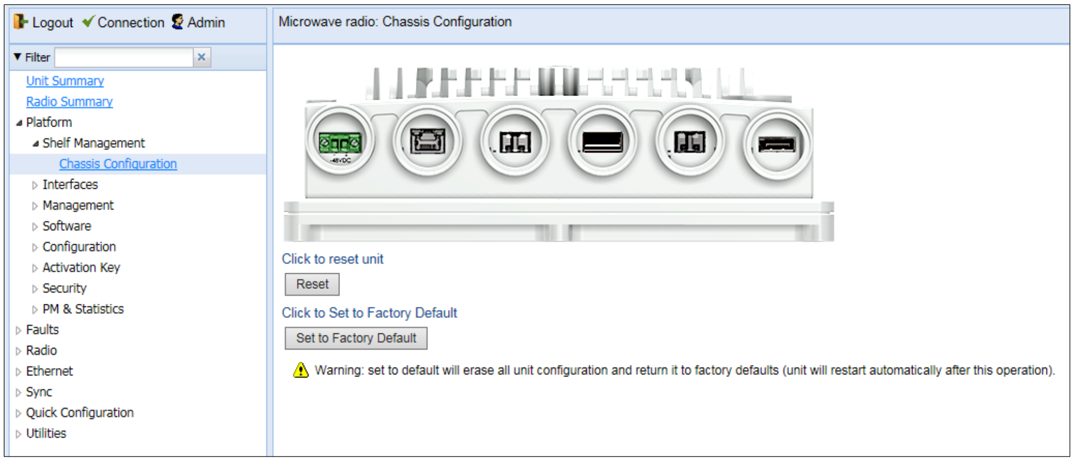
> **Note**
>
> If any specific command in the CLI script requires reset, the unit is reset when that that command is executed. During initialization following the reset, execution of the CLI script continues from the following command.

Setting the Unit to the Factory Default Configuration

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

To restore the factory default settings:

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



Click to reset unit

Click to Set to Factory Default

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

Figure 125: Chassis Configuration Page

2. Click **Set to Factory Default**. The unit is restored to its factory default settings. This does not change the unit's IP address.

Performing a Hard (Cold) Reset

To initiate a hard (cold) reset on the unit:

1. Select **Platform > Shelf Management > Chassis Configuration**. The Chassis Configuration page opens (*Figure 125*).
2. Click **Reset**.
3. A prompt appears asking if you want to proceed with the reset. Click **Yes** to initiate the reset.

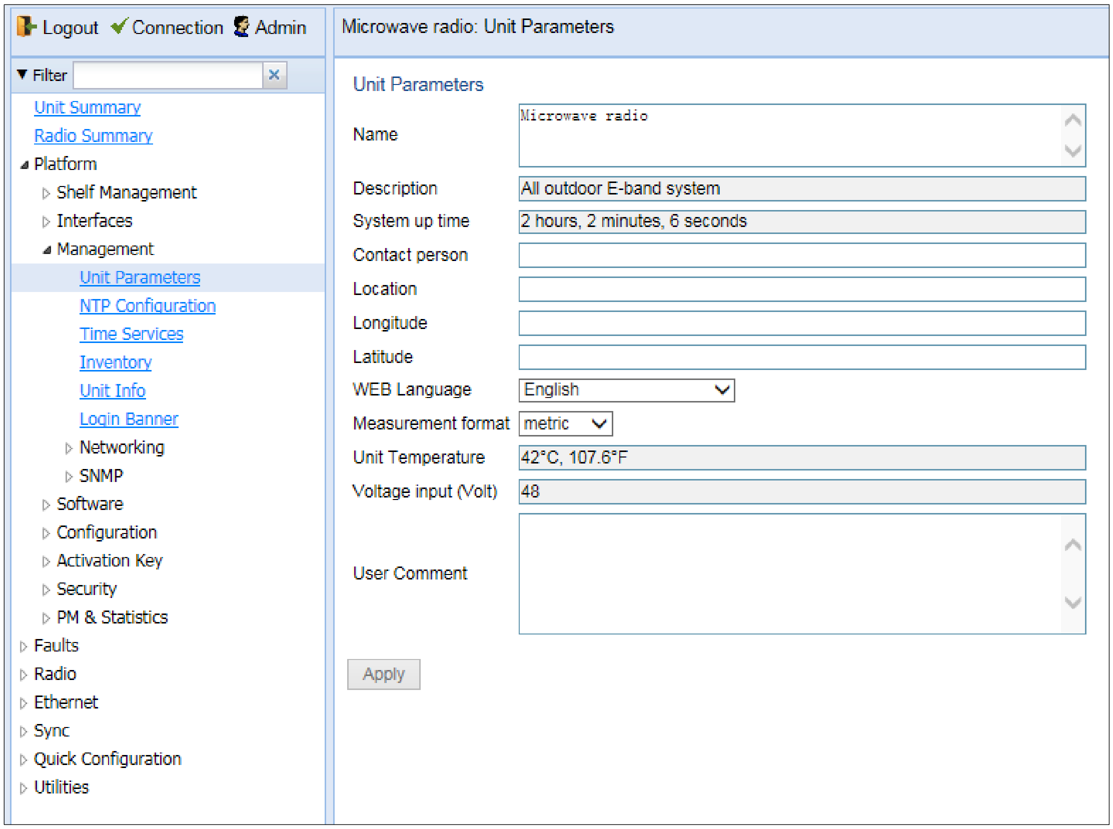
The unit is reset.

Configuring Unit Parameters

To view and configure system information:

1. Select **Platform > Management > Unit Parameters.** The Unit Parameters page opens.
2. Table 25 describes the fields in the Unit Parameters page.

Figure 126 Unit Parameters Page



Microwave radio: Unit Parameters

Unit Parameters

Name: Microwave radio
Description: All outdoor E-band system
System up time: 2 hours, 2 minutes, 6 seconds
Contact person:
Location:
Longitude:
Latitude:
WEB Language: English
Measurement format: metric
Unit Temperature: 42°C, 107.6°F
Voltage input (Volt): 48
User Comment:

Table 25 Unit Parameters

Parameter	Definition
Name	A name for the unit (optional, up to 128 characters). This name appears at the top of every Web EMS page.
Description	Descriptive information about the unit. This information is used for debugging, and should include information such as the unit type.
System up time	The time since the system was last reinitialized.
Contact person	The name of the person to be contacted if and when a problem with the system occurs (optional).
Location	The actual physical location of the node or agent (optional).

Parameter	Definition
Longitude	The unit's longitude coordinates.
Latitude	The unit's latitude coordinates.
Web Language	Enables you to select the language in which the Web EMS is displayed. In release 11.1, the following languages are available: • English (default) • Russian
Measurement format	The type of measurement you want the system to use: **Metric** or **Imperial**.
Unit Temperature	The current temperature of the unit. If the unit temperature goes lower than -40°C or higher than 90°C, the unit raises an extreme temperature alarm (Alarm ID 25). This alarm is cleared when the unit temperature rises above -37°C or goes below 87°C.
Voltage input (Volt)	The voltage input of the unit.
User Comment	A free text field for any information you want to record (up to 500 characters).

Configuring NTP

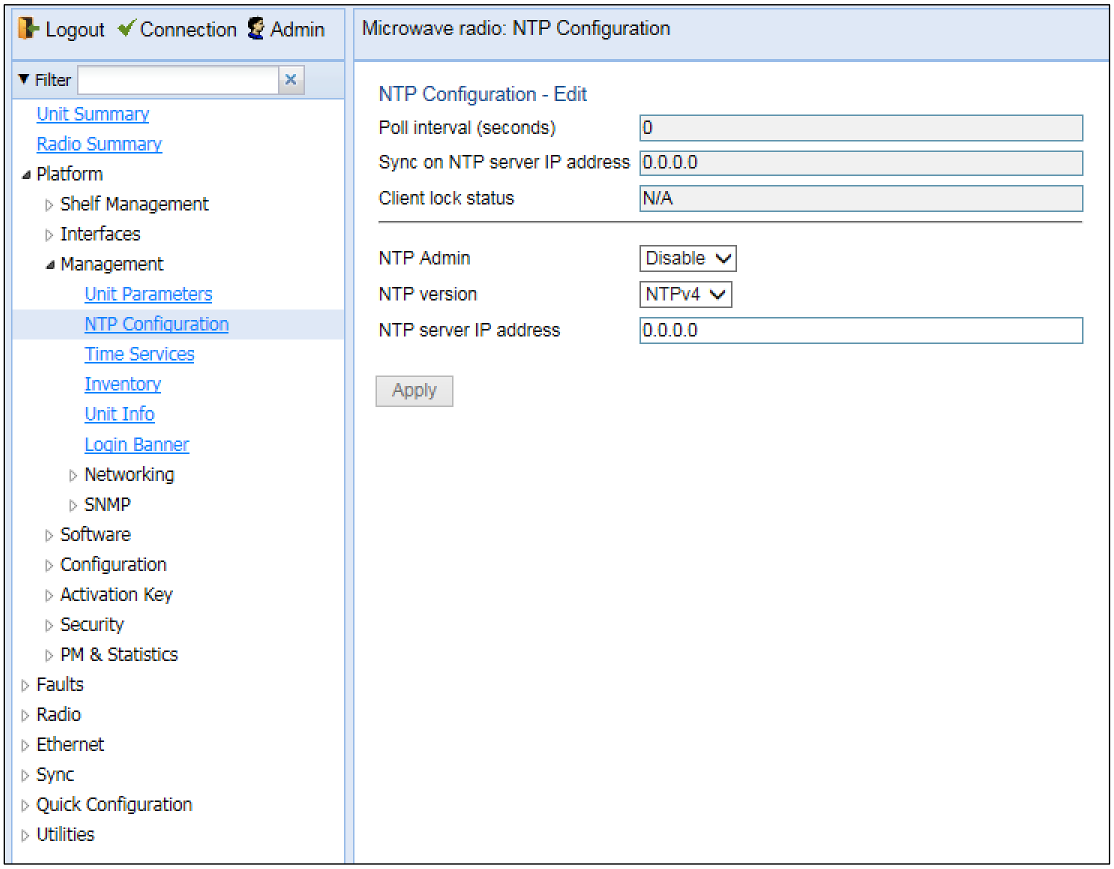
PTP 850E supports Network Time Protocol (NTP). NTP distributes Coordinated Universal Time (UTC) throughout the system, using a jitter buffer to neutralize the effects of variable latency.

You can configure up to four NTP servers. Each server can be configured using IPv4 or IPv6. When multiple servers are configured, the unit chooses the best server according to the implementation of Version 4.2.6p1 of the NTPD (Network Time Protocol Daemon). The servers are continually polled. The polling interval is determined by the NTPD, to achieve maximum accuracy consistent with minimum network overhead.

To view and configure the NTP Parameters:

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

Figure 127 NTP Configuration Page



Microwave radio: NTP Configuration

NTP Configuration - Edit

Poll interval (seconds)	0
Sync on NTP server IP address	0.0.0.0
Client lock status	N/A
NTP Admin	Disable
NTP version	NTPv4
NTP server IP address	0.0.0.0

2. In the **NTP Admin** field, select **Enable**.
3. In the **NTP version** field, select the NTP version you want to use. Options are **NTPv3** and **NTPv4**. NTPv4 provides interoperability with NTPv3 and with SNTP.
4. In the **NTP server IP address** field, enter the IP address of the NTP server.
5. Click **Apply**.

Table 26 describes the status parameters that appear in the NTP Configuration page.

Table 26 NTP Status Parameters

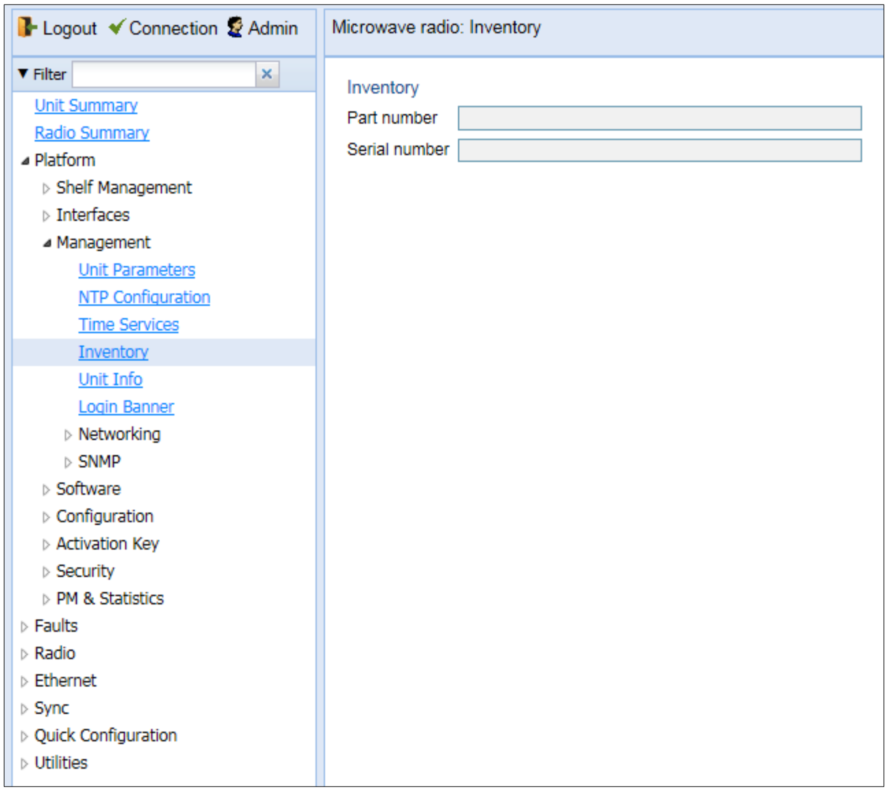
Parameter	Definition
Lock status	Indicates the NTP status of the unit. Possible values are: • **LOCK** – The NTP client is locked on a remote server. • **LOCAL** – The NTP client is locked on the local system clock (free running clock). • **CANDIDATE** – The server is next in line to be selected if the currently locked server is discarded. **N/A** – The NTP client is not locked on any clock or NTP is disabled.
IPv4 address	The IPv4 address of the NTP server (if configured).
IPv6 address	The IPv6 address of the NTP server (if configured).
Refid	The NTP client time server.
Stratum	The NTP client statum..
Peer type	The server peer type.
Reach	The result of the last 8 polls in octal form.
Delay	The round trip delay to peer in milliseconds.
Offset	Offset to the client in milliseconds.
Jitter	Variance in latency on the network.

Displaying Unit Inventory

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

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

Figure 128 Inventory Page



Displaying SFP DDM and Inventory Information

Static and dynamic monitoring is available for SFP, SFP+, and QSFP modules used in ports P3 (Eth2), P4 (Eth3, Eth4, Eth5, Eth6), and P5 (Eth7).

Dynamic monitoring (DDM) PMs are also available.

> Note
>
> DDM parameters are not relevant for electrical SFPs.

The following alarms are available in connection with SFP DDM and inventory monitoring. The polling interval for these alarms is one minute.

- Alarm #803- SFP port RX power level is too low.
- Alarm #804 – SFP port RX power level is too high.
- Alarm #805- SFP port TX power level is too low.
- Alarm #806 – SFP port TX power level is too high.

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

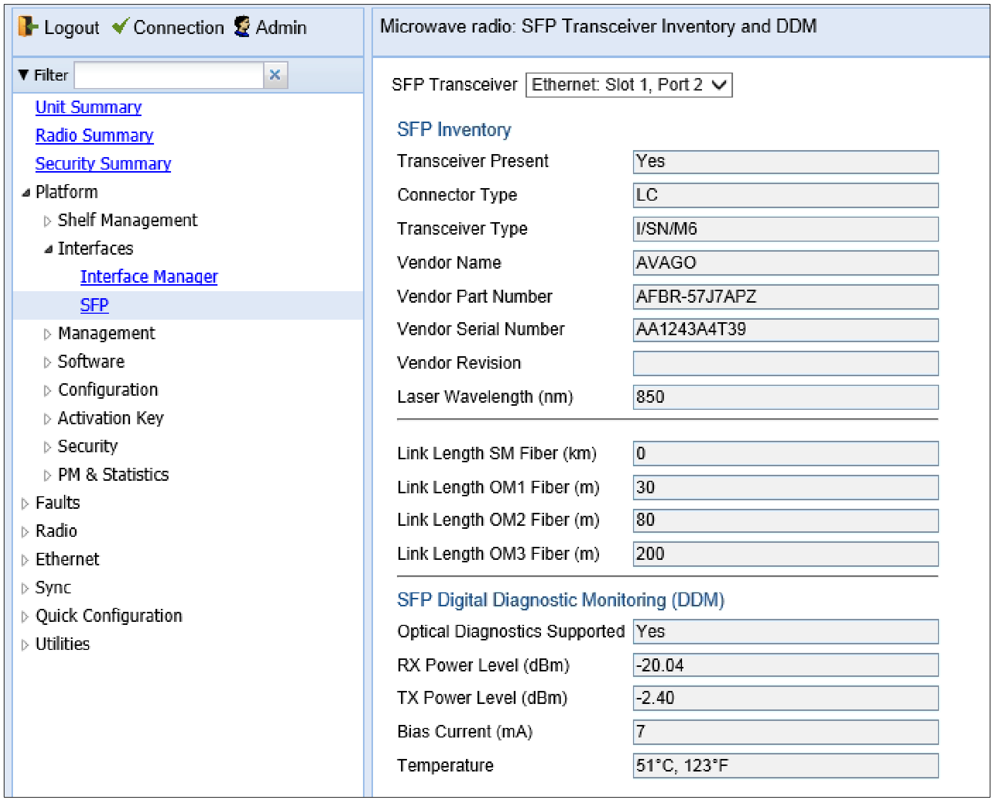
If there is no signal on the interface, a Loss of Carrier alarm (LOC) is raised, and this alarm masks the DDM alarms.

Displaying Information about an SFP Module

To display information about an SFP module:

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

Figure 129 SFP Transceiver Inventory and DDM Page



Microwave radio: SFP Transceiver Inventory and DDM

SFP Transceiver: Ethernet: Slot 1, Port 2

SFP Inventory

Transceiver Present	Yes
Connector Type	LC
Transceiver Type	I/SN/M6
Vendor Name	AVAGO
Vendor Part Number	AFBR-57J7APZ
Vendor Serial Number	AA1243A4T39
Vendor Revision	
Laser Wavelength (nm)	850
Link Length SM Fiber (km)	0
Link Length OM1 Fiber (m)	30
Link Length OM2 Fiber (m)	80
Link Length OM3 Fiber (m)	200

SFP Digital Diagnostic Monitoring (DDM)

Optical Diagnostics Supported	Yes
RX Power Level (dBm)	-20.04
TX Power Level (dBm)	-2.40
Bias Current (mA)	7
Temperature	51°C, 123°F

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

Table 27 SFP Inventory Parameters

Parameter	Description
Transceiver Present	Indicates whether an SFP module is attached to the interface.
Connector Type	Always displays LC.
Transceiver Type	Displays a description of the SFP module.
Vendor Name	Displays the name of the SFP's vendor.
Vendor Part Number	Displays the vendor's part number for the SFP module.
Vendor Serial Number	Displays the vendor's serial number for the SFP module.
Vendor Revision	Displays the revision number of the serial number provided by the vendor for the SFP module.

Parameter	Description
Laser Wavelength (nm)	Display's the SFP module's laser wavelength. This parameters is not relevant for copper SFPs.
Link Length SM Fiber (km)	The maximum length of the cable (in km) for single mode fiber cables.
Link Length OM1 Fiber (m)	The maximum length of the cable (in meters) for OM1 multi-mode fiber cables.
Link Length OM2 Fiber (m)	The maximum length of the cable (in meters) for OM2 multi-mode fiber cables.
Link Length OM3 Fiber (m)	The maximum length of the cable (in meters) for OM3 multi-mode fiber cables.

Table 28 SFP Digital Diagnostic Monitoring (DDM) Parameters

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

Note

Tx Power level DDM is not supported for QSFP (P4) – not part of the standard.

If no signal is being received, RX Power Level is displayed as -40 dBm.

If the Admin status of the port is Down, the TX Power Level is displayed as -40 DBm and the Bias Current is displayed as 0 mA.

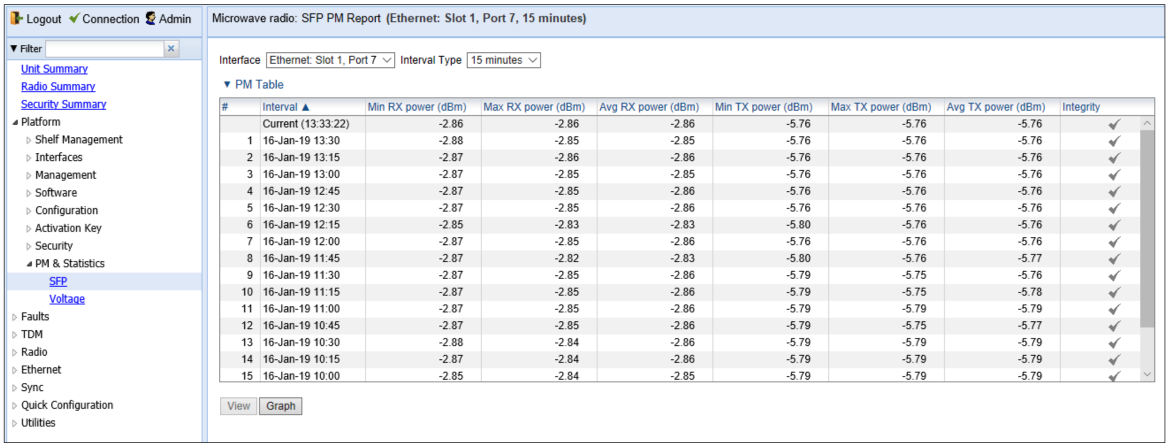
The Temperature is always shown as long as the SFP module is inserted in the port.

Displaying PMs about an SFP Module

To display DDM PMs:

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

Figure 130 SFP PM Report Page



Microwave radio: SFP PM Report (Ethernet: Slot 1, Port 7, 15 minutes)

Interface: Ethernet: Slot 1, Port 7 Interval Type: 15 minutes

#	Interval ▲	Min RX power (dBm)	Max RX power (dBm)	Avg RX power (dBm)	Min TX power (dBm)	Max TX power (dBm)	Avg TX power (dBm)	Integrity
	Current (13:33:22)	-2.86	-2.86	-2.86	-5.76	-5.76	-5.76	✓
1	16-Jan-19 13:30	-2.88	-2.85	-2.85	-5.76	-5.76	-5.76	✓
2	16-Jan-19 13:15	-2.87	-2.86	-2.86	-5.76	-5.76	-5.76	✓
3	16-Jan-19 13:00	-2.87	-2.85	-2.85	-5.76	-5.76	-5.76	✓
4	16-Jan-19 12:45	-2.87	-2.85	-2.86	-5.76	-5.76	-5.76	✓
5	16-Jan-19 12:30	-2.87	-2.85	-2.86	-5.76	-5.76	-5.76	✓
6	16-Jan-19 12:15	-2.85	-2.83	-2.83	-5.80	-5.76	-5.76	✓
7	16-Jan-19 12:00	-2.87	-2.85	-2.86	-5.76	-5.76	-5.76	✓
8	16-Jan-19 11:45	-2.87	-2.82	-2.83	-5.80	-5.76	-5.77	✓
9	16-Jan-19 11:30	-2.87	-2.85	-2.86	-5.79	-5.75	-5.76	✓
10	16-Jan-19 11:15	-2.87	-2.85	-2.86	-5.79	-5.75	-5.78	✓
11	16-Jan-19 11:00	-2.87	-2.85	-2.86	-5.79	-5.79	-5.79	✓
12	16-Jan-19 10:45	-2.87	-2.85	-2.86	-5.79	-5.75	-5.77	✓
13	16-Jan-19 10:30	-2.88	-2.84	-2.86	-5.79	-5.79	-5.79	✓
14	16-Jan-19 10:15	-2.87	-2.84	-2.86	-5.79	-5.79	-5.79	✓
15	16-Jan-19 10:00	-2.85	-2.84	-2.85	-5.79	-5.79	-5.79	✓

2. In the **Interface** field, select the interface for which you want to display PMs.
3. In the **Interval Type** field:
   - To display reports for the past 24 hours, in 15 minute intervals, select **15 minutes**.
   - To display reports for the past month, in daily intervals, select **24 hours**.

Note

No entries are displayed if the SFP device does not support DDM, or if the Admin status of the interface is Down.

DDM PMs are not persistent, which means they are not saved in the event of unit reset. RX and TX power levels are collected five times per 15-minute interval. 15-minute PM data is saved for 24 hours. 24-hour PM data, which is updated every 15 minutes, is saved for 30 days.

Table 29 DDM PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Min RX Power (dBm)	The minimum RX power during the interval (dBm).
Max RX Power (dBm)	The maximum RX power during the interval (dBm).
Avg RX Power (dBm)	The average RX power during the interval (dBm).
Min TX Power (dBm)	The minimum TX power during the interval (dBm).
Max TX Power (dBm)	The maximum TX power during the interval (dBm).
Avg TX Power (dBm)	The average TX power during the interval (dBm).
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable. Possible causes are (i) an LOC alarm, (ii) changing the Admin status of the interface, or (iii) unit reset.

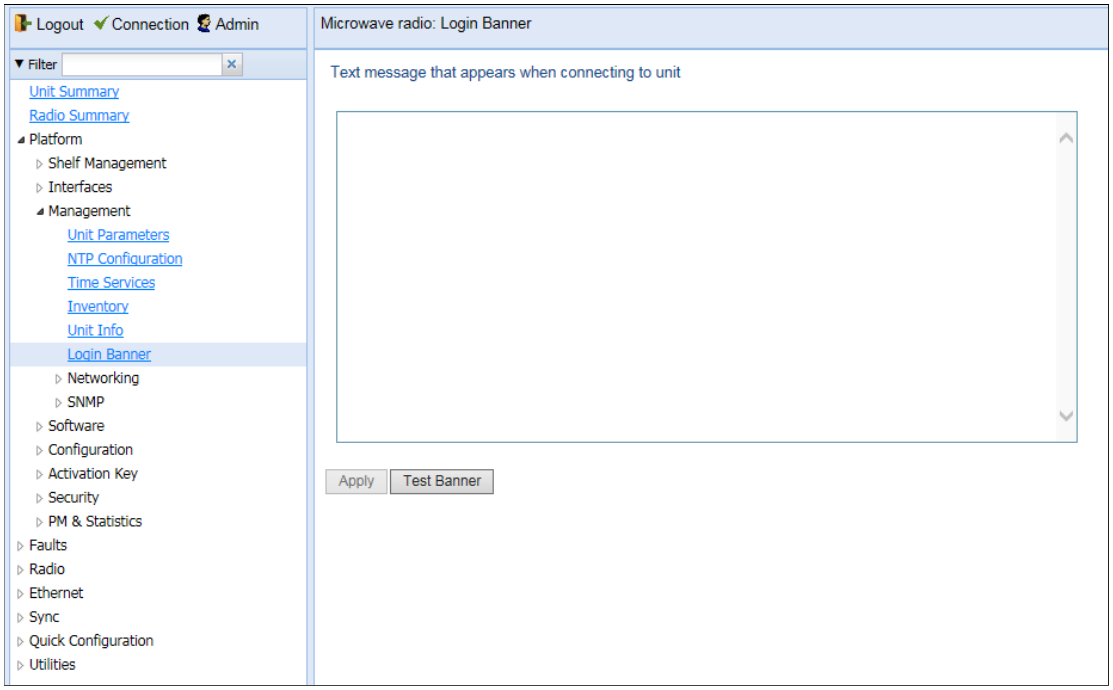
Defining a Login Banner

You can define a login banner of up to 2,000 bytes. This banner will appear every time a user establishes a connection with the Web EMS. The banner appears before the login prompt, so that users will always see the login banner and must manually close the banner before logging in to the Web EMS.

To define a login banner:

1 Select **Platform > Management > Login Banner**. The Login Banner page opens.

Figure 131 Login Banner Page



Text message that appears when connecting to unit

2 Enter a text message of up to 2,000 bytes.

3 To display a test banner as it will appear to users, click **Test Banner**.

4 Click **Apply**.

Chapter 8: Radio Configuration

This section includes:

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

Related topics:

- Configuring the Radio Parameters
- Configuring the Radio (MRMC) Script(s)
- Configuring XPIC
- Configuring 1+1 HSB Unit Protection
- Performing Radio Loopback

Viewing the Radio Status and Settings

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

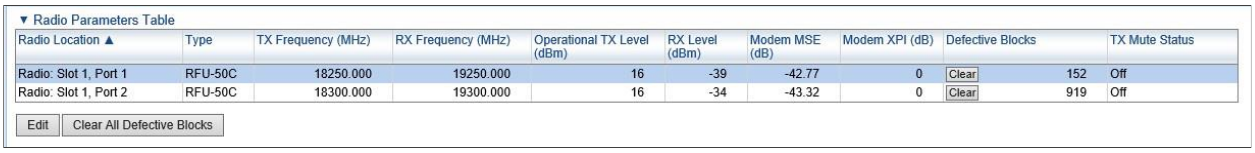
Note

For instructions how to configure the radio parameters, see Error! Reference source not found..

To display the radio parameters:

1. Select **Radio > Radio Parameters.** The Radio Parameters page opens.

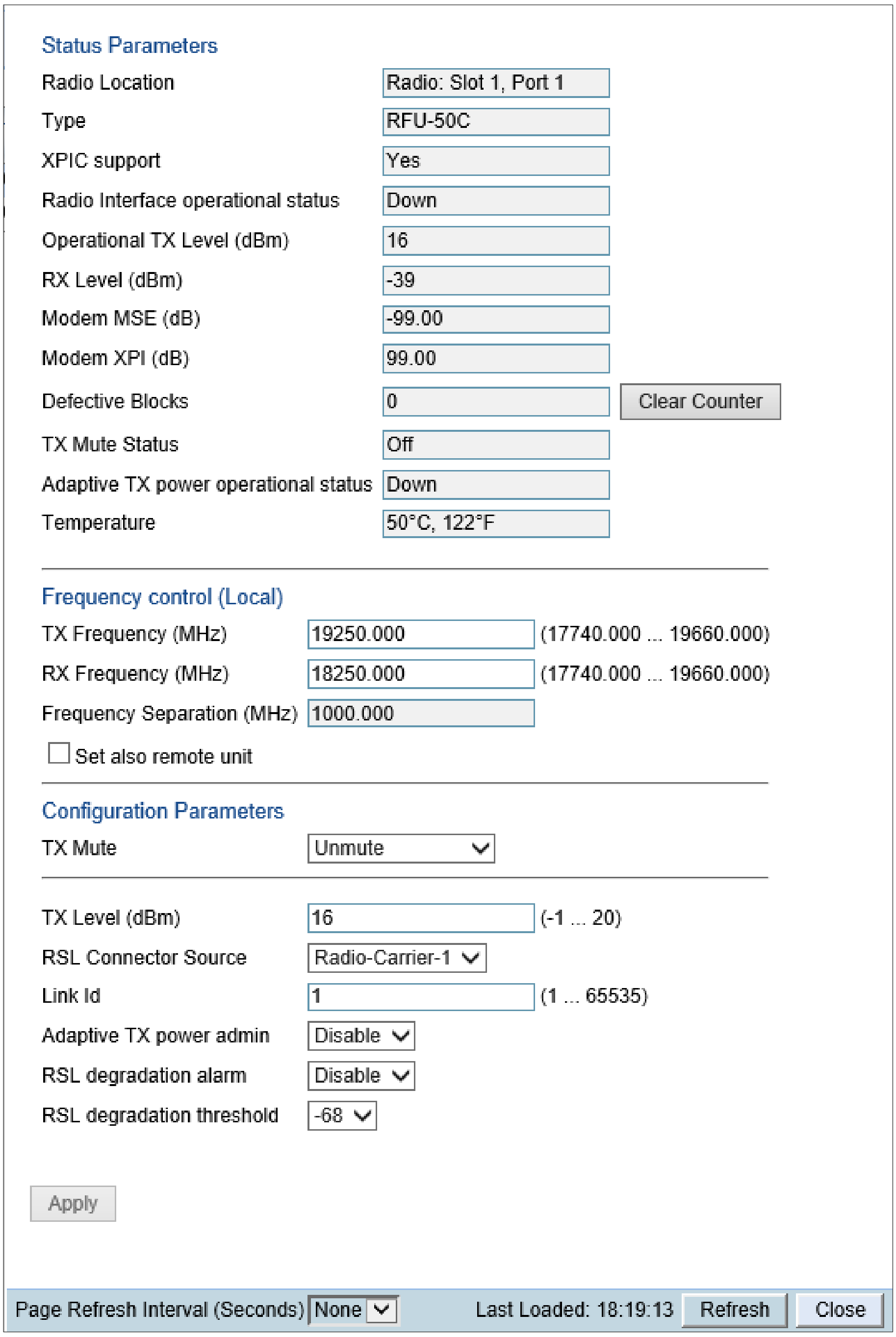
Figure 132 Radio Parameters Page



▼ Radio Parameters Table

Radio Location ▲	Type	TX Frequency (MHz)	RX Frequency (MHz)	Operational TX Level (dBm)	RX Level (dBm)	Modem MSE (dB)	Modem XPI (dB)	Defective Blocks	TX Mute Status
Radio: Slot 1, Port 1	RFU-50C	18250.000	19250.000	16	-39	-42.77	0	Clear 152	Off
Radio: Slot 1, Port 2	RFU-50C	18300.000	19300.000	16	-34	-43.32	0	Clear 919	Off

Figure 133 Radio Parameters Page – PTP 850C



Status Parameters

Radio Location	Radio: Slot 1, Port 1
Type	RFU-50C
XPIC support	Yes
Radio Interface operational status	Down
Operational TX Level (dBm)	16
RX Level (dBm)	-39
Modem MSE (dB)	-99.00
Modem XPI (dB)	99.00
Defective Blocks	0
TX Mute Status	Off
Adaptive TX power operational status	Down
Temperature	50°C, 122°F

Frequency control (Local)

TX Frequency (MHz)	19250.000	(17740.000 ... 19660.000)
RX Frequency (MHz)	18250.000	(17740.000 ... 19660.000)
Frequency Separation (MHz)	1000.000	

□ Set also remote unit

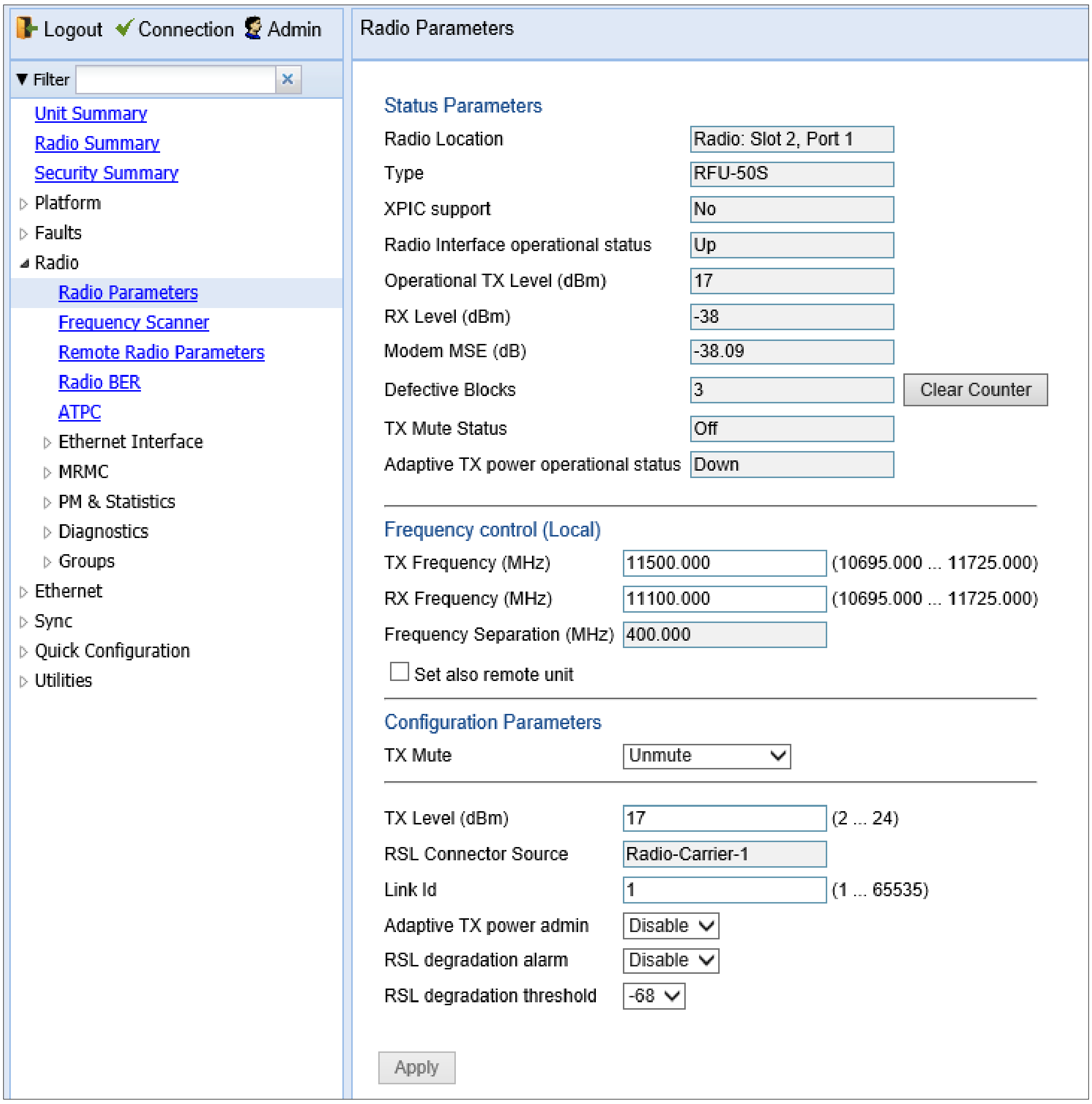
Configuration Parameters

TX Mute	Unmute	
TX Level (dBm)	16	(-1 ... 20)
RSL Connector Source	Radio-Carrier-1	
Link Id	1	(1 ... 65535)
Adaptive TX power admin	Disable	
RSL degradation alarm	Disable	
RSL degradation threshold	-68	

Page Refresh Interval (Seconds) None

Last Loaded: 18:19:13

Figure 134 Radio Parameters Page – PTP 850S



Radio Parameters

Status Parameters

Radio Location	Radio: Slot 2, Port 1
Type	RFU-50S
XPIC support	No
Radio Interface operational status	Up
Operational TX Level (dBm)	17
RX Level (dBm)	-38
Modem MSE (dB)	-38.09
Defective Blocks	3
TX Mute Status	Off
Adaptive TX power operational status	Down

Frequency control (Local)

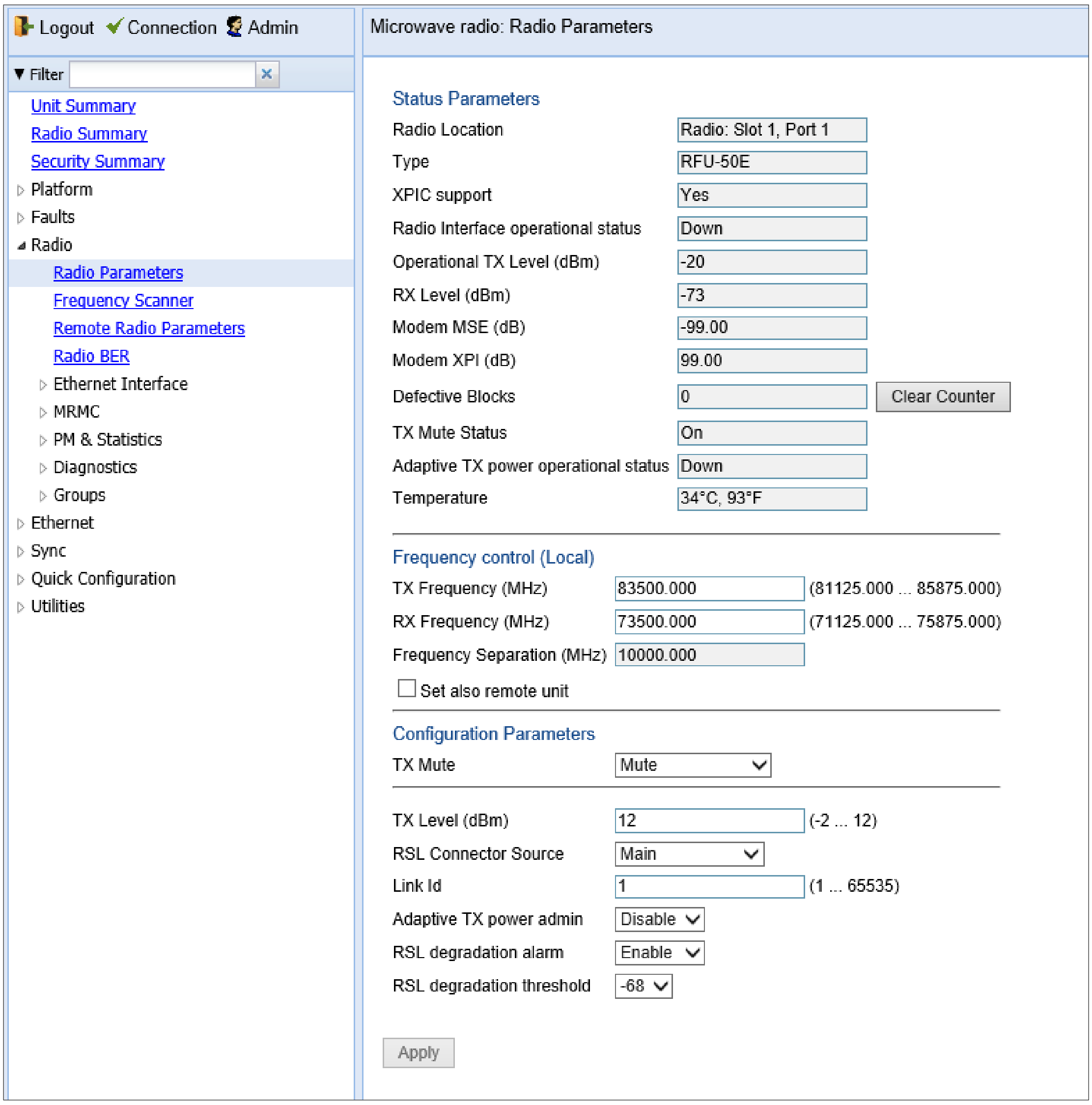
TX Frequency (MHz)	11500.000	(10695.000 ... 11725.000)
RX Frequency (MHz)	11100.000	(10695.000 ... 11725.000)
Frequency Separation (MHz)	400.000	

□ Set also remote unit

Configuration Parameters

TX Mute	Unmute	
TX Level (dBm)	17	(2 ... 24)
RSL Connector Source	Radio-Carrier-1	
Link Id	1	(1 ... 65535)
Adaptive TX power admin	Disable	
RSL degradation alarm	Disable	
RSL degradation threshold	-68	

Figure 135 Radio Parameters Page – PTP 850E



Microwave radio: Radio Parameters

Status Parameters

Radio Location	Radio: Slot 1, Port 1
Type	RFU-50E
XPIC support	Yes
Radio Interface operational status	Down
Operational TX Level (dBm)	-20
RX Level (dBm)	-73
Modem MSE (dB)	-99.00
Modem XPI (dB)	99.00
Defective Blocks	0
TX Mute Status	On
Adaptive TX power operational status	Down
Temperature	34°C, 93°F

Frequency control (Local)

TX Frequency (MHz)	83500.000	(81125.000 ... 85875.000)
RX Frequency (MHz)	73500.000	(71125.000 ... 75875.000)
Frequency Separation (MHz)	10000.000	

□ Set also remote unit

Configuration Parameters

TX Mute	Mute	
TX Level (dBm)	12	(-2 ... 12)
RSL Connector Source	Main	
Link Id	1	(1 ... 65535)
Adaptive TX power admin	Disable	
RSL degradation alarm	Enable	
RSL degradation threshold	-68	

Table 30 lists and describes the parameters displayed in the **Status parameters** section of the Radio Parameters page. The configurable parameters are described in ***Error! Reference source not found.***.

Table 30 Radio Status Parameters

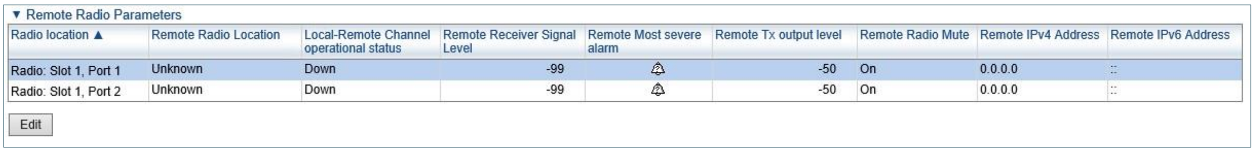
Parameter	Description
Type	The RF module type.
XPIC Support	Reserved for future use.
Radio Interface operational status	Indicates whether the carrier is operational (Up) or not operational (Down).
Operational TX Level (dBm)	The actual TX signal level (TSL) of the carrier (in dBm).
RX Level (dBm)	The actual measured RX signal level (RSL) of the carrier (in dBm).
Modem MSE (dB)	The MSE (Mean Square Error) of the RX signal, measured in dB. A value of 0 means that the modem is not locked.
Modem XPI (dB)	The XPI (Cross Polarization Interference) level, measured in dB.
Defective Blocks	The number of defective radio blocks that have been counted. Click **Clear Counter** to reset this counter.
TX Mute Status	Indicates whether radio transmission is muted.
Adaptive TX power operational status	Indicates whether Adaptive TX power is currently operational.
Temperature	The internal temperature of the unit.
TX Frequency	The configured TX radio frequency (MHz). The TX radio frequency is configured in the Frequency control (Local) section of the Radio Parameters page. See ***Error! Reference source not found.***.
RX Frequency	The configured RX radio frequency (MHz). The RX radio frequency is configured in the Frequency control (Local) section of the Radio Parameters page. See ***Error! Reference source not found.***.
Frequency Separation	The frequency separation, based on the configured TX and RX frequencies.

Configuring the Remote Radio Parameters

You can view and configure the parameters of the carrier or carriers at the remote side of the link in the Remote Radio Parameters page.

To display the remote radio parameters:

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

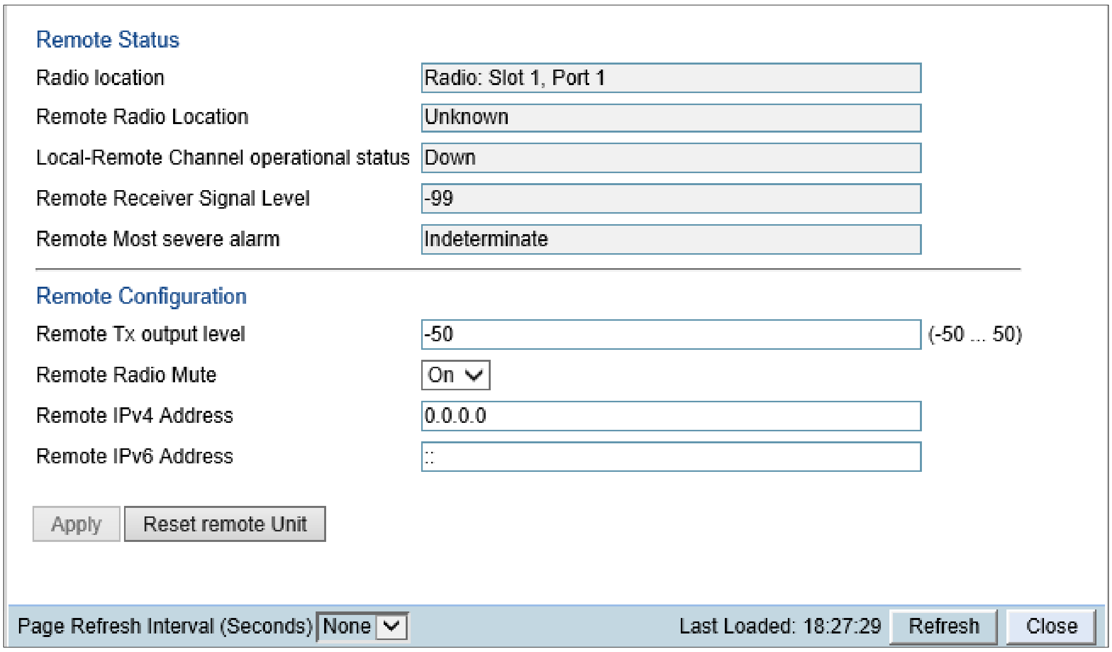


▼ Remote Radio Parameters

Radio location ▲	Remote Radio Location	Local-Remote Channel operational status	Remote Receiver Signal Level	Remote Most severe alarm	Remote Tx output level	Remote Radio Mute	Remote IPv4 Address	Remote IPv6 Address
Radio: Slot 1, Port 1	Unknown	Down	-99	🔔	-50	On	0.0.0.0	::
Radio: Slot 1, Port 2	Unknown	Down	-99	🔔	-50	On	0.0.0.0	::

    b. For other PTP 850 products, the Remote Radio Parameters page opens right away.

Figure 136 Remote Radio Parameters Page



Remote Status

Radio location	Radio: Slot 1, Port 1
Remote Radio Location	Unknown
Local-Remote Channel operational status	Down
Remote Receiver Signal Level	-99
Remote Most severe alarm	Indeterminate

Remote Configuration

Remote Tx output level	-50	(-50 ... 50)
Remote Radio Mute	On	
Remote IPv4 Address	0.0.0.0	
Remote IPv6 Address	::	

2. Configure the remote radio parameters. For a description of these parameters, see Table 31 Remote Radio Parameters.
3. Click **Apply**.

To reset the remote unit, click **Reset Remote Unit**.

Table 31 Remote Radio Parameters

Parameter	Definition
Radio Location	Read-only. Identifies the carrier.

Parameter	Definition
Remote Radio Location	Read-only. Identifies the location of the remote radio.
Local Remote Channel Operational Status	Read-only. The operational status of the local-remote channel.
Remote Receiver Signal Level	Read-only. The Rx level of the remote radio, in dBm.
Remote Most Severe Alarm	Read-only. The level of the most severe alarm currently active on the remote unit.
Remote Tx Output Level	Set the remote unit's Tx output level (in dBm).
Remote Radio Mute	To mute the TX output of the remote radio, select **On**. To unmute the TX output of the remote radio, select **Off**.
Remote IP Address	The IPv4 IP address of the remote unit.
Remote IPv6 Address	The IPv6 IP address of the remote unit.

Configuring ATPC and ATPC Override Timer

Note

This section is only relevant for PTP 850S.

ATPC is a closed-loop mechanism by which each carrier changes the TX power according to the indication received across the link, in order to achieve a desired RSL on the other side of the link.

With ATPC, if the radio increases its TX power up to the configured TX power, it can lead to a period of sustained transmission at maximum power, resulting in unacceptable interference with other systems.

In order to minimize interference, PTP 850 provides an ATPC override mechanism. When ATPC override is enabled, a timer begins when ATPC raises the TX power to its maximum. When the timer expires, the radio enters ATPC override state. In ATPC override state, the radio transmits no higher than the pre-determined ATPC override TX level, and an ATPC override alarm is raised. The radio remains in ATPC override state until the ATPC override state is manually cancelled by the user (or until the unit is reset). The radio then returns to normal ATPC operation.

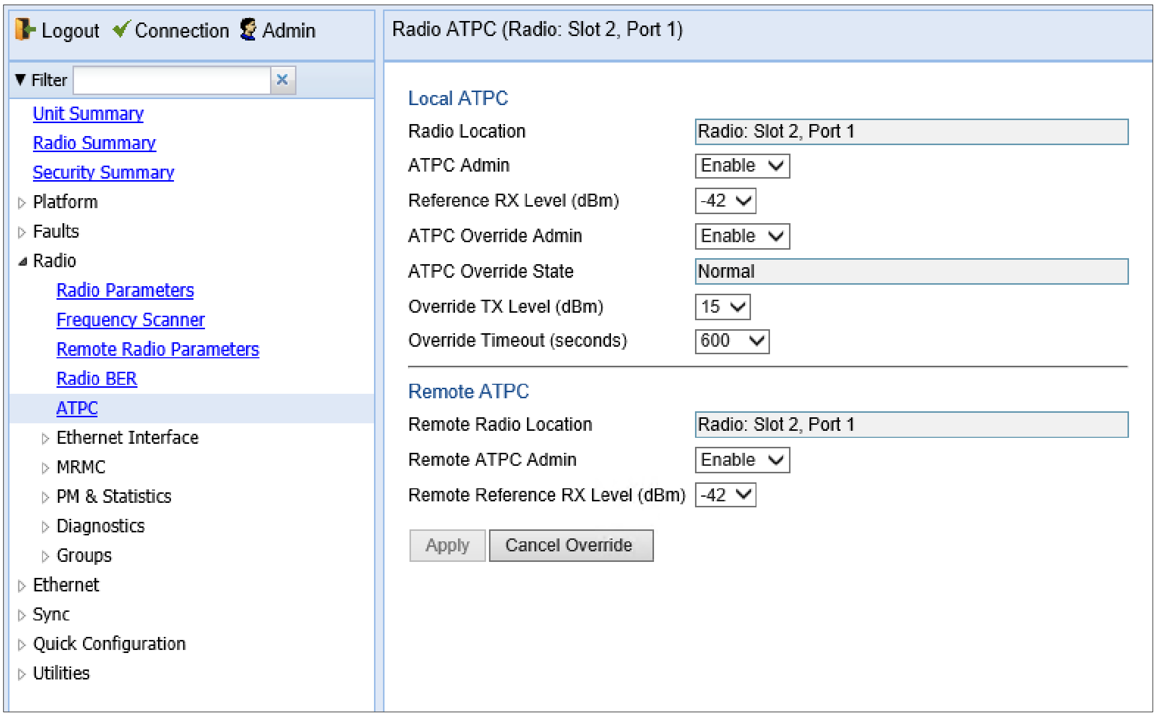
In a configuration with unit protection, the ATPC override state is propagated to the standby unit in the event of switchover.

Note

When canceling an ATPC override state, you should ensure that the underlying problem has been corrected. Otherwise, ATPC may be overridden again.

To enable and configure ATPC and display ATPC settings:

1 Select **Radio > ATPC**. The ATPC page opens.



Radio ATPC (Radio: Slot 2, Port 1)

Local ATPC

Radio Location	Radio: Slot 2, Port 1
ATPC Admin	Enable
Reference RX Level (dBm)	-42
ATPC Override Admin	Enable
ATPC Override State	Normal
Override TX Level (dBm)	15
Override Timeout (seconds)	600

Remote ATPC

Remote Radio Location	Radio: Slot 2, Port 1
Remote ATPC Admin	Enable
Remote Reference RX Level (dBm)	-42

Figure 137 ATPC Page

In the **ATPC Admin** field, select **Enable** to enable ATPC or **Disable** to disable

2 Click **Apply**. If you selected **ATPC -Admin** – **Enable**, the **Reference RX Level (dBm)** and **ATPC Override Admin** fields are now displayed.

3 In the Reference RX Level (dBm) field, enter a number between -70 and -30 as the reference value for the ATPC mechanism. When ATPC is enabled, it adjusts the TX power dynamically to preserve this RSL level. The range of values depends on the frequency, MRMC script, and RFU type.

4 In the **ATPC Override Admin** field, select **Enable** to enable ATPC override or **Disable** to disable ATPC override. You can only enable ATPC override if ATPC itself is enabled.

Note

Make sure to set an appropriate value in the Override Timeout field before enabling ATPC override. Failure to do so can lead to unexpected reduction of the TX power with corresponding loss of capacity if TX override is enabled with the timer set to a lower-than- desired value.

5 Click **Apply**. If you selected **ATPC Override Admin** – **Enable**, the **ATPC Override State**, **Override TX Level,** and **ATPC Override Admin** fields are now displayed.

6 In the Override TX Level field, select the TX power, in dBm, to be used when the unit is in an ATPC override state. The range of values depends on the frequency, MRMC script, and RFU type.

7 In the **Override Timeout** field, select the amount of time, in seconds, the timer counts from the moment the radio reaches its maximum configured TX power until ATPC override goes into effect. You can select from 0 to 1800 seconds.

8 In the **Remote ATPC Admin** field, select **Enable** to enable ATPC or **Disable** to disable ATPC on the remote radio carrier.

9 Click **Apply**. If you selected **Remote ATPC Admin** – **Enable**, the **Remote Reference RX Level (dBm)** field is now displayed.

10 In the **Remote Reference RX Level (dBm)** field, enter a number between -70 and -30 as the reference value for the ATPC mechanism on the remote radio carrier.

11 Click **Apply**.

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

Configuring Header De-Duplication and Frame Cut-Through

Note

This section is only relevant for PTP 850S.

Header De-Duplication enables operators to significantly improve Ethernet throughout over the radio link without affecting user traffic. Header

De-Duplication can be configured to operate on various layers of the protocol stack, saving bandwidth by reducing unnecessary header overhead. Header De- duplication is also sometimes known as header compression.

Note

The Header De-Duplication and Frame Cut-Through configuration must be identical on both sides of the link.

If Frame Cut-Through is used together with 1588 Transparent Clock, the 1588 packets must be given a CoS that is not assigned to the fourth priority queue.

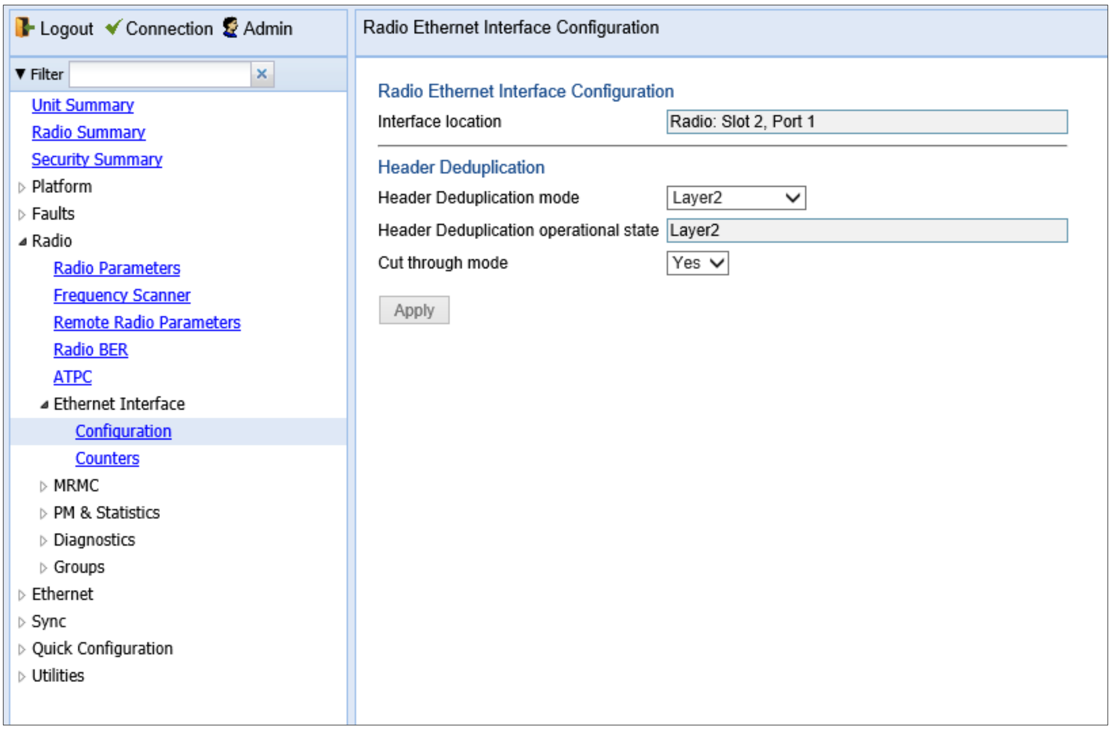
Using the Frame Cut-Through feature, frames assigned to queues with 4th priority pre-empt frames already in transmission over the radio from other queues. After the 4th queue frames have been transmitted, transmission of the pre-empted frames resumes.

Note

Frame Cut-Through cannot be used together with 1588 Transparent Clock.

To configure Header De-Duplication and Frame Cut-Through:

1 Select **Radio > Ethernet Interface > Configuration**. The Radio Ethernet Interface Configuration page opens.



Radio Ethernet Interface Configuration

Radio Ethernet Interface Configuration

Interface location: Radio: Slot 2, Port 1

Header Deduplication

Header Deduplication mode: Layer2

Header Deduplication operational state: Layer2

Cut through mode: Yes

Figure 138 Radio Ethernet Interface Configuration Page

2 In the **Cut through mode** field, select **Yes** to enable Frame Cut-Through or **No** to disable Frame Cut-Through.

3 In the **Header Deduplication mode** field, select from the following options:

- **Disabled** – Header De-Duplication is disabled.
- **Layer2** – Header De-Duplication operates on the Ethernet level.
- **MPLS** – Header De-Duplication operates on the Ethernet and MPLS levels.
- **Layer3** – Header De-Duplication operates on the Ethernet and IP levels.
- **Layer4** – Header De-Duplication operates on all supported layers up to Layer 4.
- **Tunnel** – Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel layer for packets carrying GTP or GRE frames.
- **Tunnel-Layer3** – Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel and T-3 layers for packets carrying GTP or GRE frames.
- **Tunnel-Layer4** – Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel, T-3, and T-4 layers for packets carrying GTP or GRE frames.

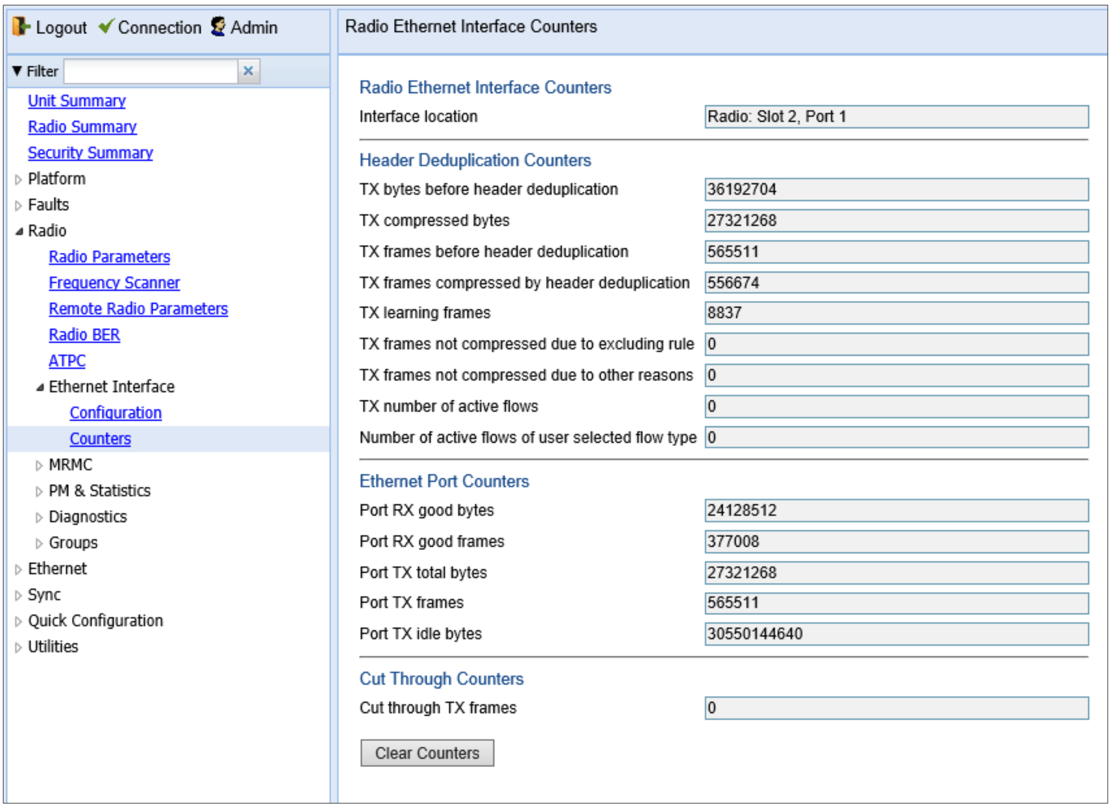
4 Click Apply, then Close

> Note
>
> The **Utilization threshold** field is not applicable.

Viewing Header De-Duplication and Frame Cut-Through Counters

You can view PMs on the usage of Header De-Duplication and Frame Cut-Through. To view Header De-Duplication and Frame Cut-Through counters:

1 Select **Radio > Ethernet Interface > Counters**. The Radio Ethernet Interface Configuration page opens.



Radio Ethernet Interface Counters

Radio Ethernet Interface Counters

Interface location	Radio: Slot 2, Port 1

Header Deduplication Counters

TX bytes before header deduplication	36192704
TX compressed bytes	27321268
TX frames before header deduplication	565511
TX frames compressed by header deduplication	556674
TX learning frames	8837
TX frames not compressed due to excluding rule	0
TX frames not compressed due to other reasons	0
TX number of active flows	0
Number of active flows of user selected flow type	0

Ethernet Port Counters

Port RX good bytes	24128512
Port RX good frames	377008
Port TX total bytes	27321268
Port TX frames	565511
Port TX idle bytes	30550144640

Cut Through Counters

Cut through TX frames	0

Figure 139 Radio Ethernet Interface Counters Page

Below table lists and describes the fields in the Radio Ethernet Interface Counters page.

Table 32 Radio Ethernet Interface Counters Fields

Parameter	Description
Interface Location	Identifies the radio interface.
Header Compression Counters	
TX bytes before header deduplication	Bytes on the TX side before Header De-Duplication.
TX compressed bytes	Bytes on the TX side that were compressed by Header De-Duplication.
TX frames before header deduplication	Frames on the TX side before Header De-Duplication.

TX frames compressed by header deduplication	Frames on the TX side that were compressed by Header De-Duplication.
TX learning frames	The number of frames that have been used to learn unique data flows. Once a particular flow type has been learned, subsequent frames with that flow type are compressed by Header De-Duplication.
TX frames not compressed due to excluding rule	Frames on the TX side that were not compressed due to exclusion rules. **Note**: The use of exclusion rules for Header De-Duplication is planned for future release.
TX frames not compressed due to other reasons	Frames on the TX side that were not compressed for reasons other than the use of exclusion rules.
TX number of active flows	The number of Header De-Duplication flows that are active on the TX side.
Number of active flows of user selected flow type	Not supported.
Ethernet Port Counters	
Port RX good bytes	The number of good bytes received on the port since the last time the Radio Ethernet Interface counters were cleared.
Port RX good frames	The number of good frames received on the port since the last time the Radio Ethernet Interface counters were cleared.
Port TX total bytes	The number of bytes transmitted since the last time the Radio Ethernet Interface counters were cleared.
Port TX frames	The number of frames transmitted since the last time the Radio Ethernet Interface counters were cleared.
Port TX idle bytes	The number of idle bytes transmitted since the last time the Radio Ethernet Interface counters were cleared.
Cut Through Counters	
Cut through TX frames	The number of frames that have been transmitted via Frame Cut-Through since the last time the Radio Ethernet Interface counters were cleared.

Configuring AES-256 Payload Encryption

> Note
>
> This feature is only relevant for PTP 850E units.
>
> This feature is not supported with 2+0 XPIC and Multiband links.

This feature requires:

- Requires an activation key. If no valid AES activation key has been applied to the unit, AES will not operate on the unit. See *Configuring the Activation Key*.

> Note
>
> In order for the AES activation key to become active, you must reset
>
> the unit after configuring a valid AES activation key. Until the unit is reset, an alarm will be present if you enable AES. This is not the case for other activation keys.

PTP 850E supports AES-256 payload encryption, using a dual-key encryption mechanism:

- The user provides a master key. The master key can also be generated by the system upon user command. The master key is a 32-byte symmetric encryption key. The same master key must be manually configured on both ends of the encrypted link.
- The session key is a 32-byte symmetric encryption key used to encrypt the actual data. Each link uses two session keys, one for each direction. For each direction, the session key is generated by the transmit side unit and propagated automatically, via a Key Exchange Protocol, to the other side of the link. The Key Exchange Protocol exchanges session keys by encrypting them with the master key, using the AES-256 encryption algorithm. Session keys are regenerated at user-configured intervals.

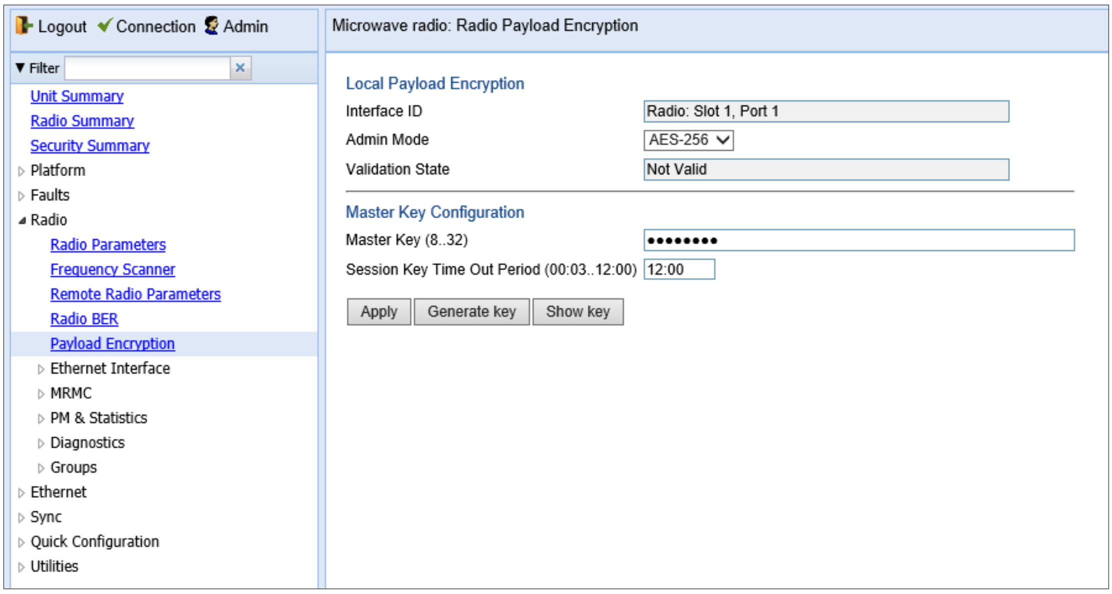
The first KEP exchange that takes place after a new master key is configured causes traffic to be blocked for up to one minute, until the Crypto Validation State becomes Valid. Subsequent KEP exchanges that take place when a session key expires do not affect traffic. KEP exchanges have no effect upon ACM, RSL, and MSE.

To configure payload encryption:

1 Verify that both the local and remote units are running with no alarms. If any alarm is present, take corrective actions to clear the alarms before proceeding.

2 If the link is using in-band management, identify which unit is local and which unit is remote from the management point of view.

3 On the remote unit, select **Radio > Payload Encryption**. The Payload Encryption page opens.



Microwave radio: Radio Payload Encryption

Local Payload Encryption

Interface ID: Radio: Slot 1, Port 1

Admin Mode: AES-256

Validation State: Not Valid

Master Key Configuration

Master Key (8..32): ••••••••

Session Key Time Out Period (00:03..12:00): 12:00

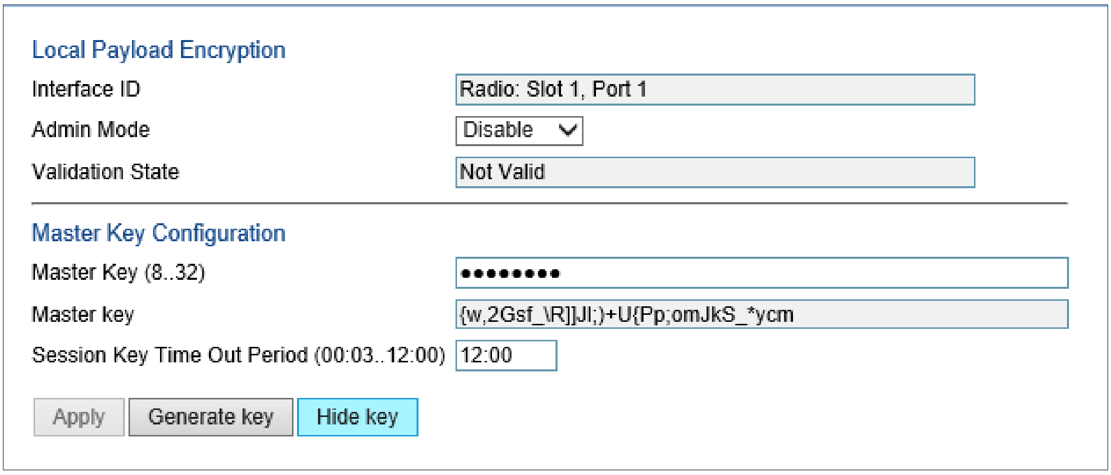
Figure 140 Payload Encryption Page

4 Configure the master key by doing one of the following:

- Enter a master key in the **Master Key** field. You must enter between 8 and 32 ASCII characters.
- Click **Generate key** to generate a master key automatically.

You must use the same master key on both sides of the link. This means that if you generate a master key automatically on one side of the link, you must copy that key and for use on the other side of the link. Once payload encryption has been enabled on both sides of the link, the Key Exchange Protocol periodically verifies that both ends of the link have the same master key. If a mismatch is detected, an alarm is raised and traffic transmission is stopped for the mismatched carrier at both sides of the link. The link becomes non-valid and traffic stops being forwarded.

When you enter a master key, or when the master key is automatically generated, the key is hidden behind dots. To copy the master key, you must display the key. To display the master key, click **Show Key**. A new **Master key** field appears, displaying the master key. You can copy the key to the clipboard from this field.



Local Payload Encryption

Interface ID: Radio: Slot 1, Port 1

Admin Mode: Disable

Validation State: Not Valid

Master Key Configuration

Master Key (8..32): •••••••••

Master key: {w,2Gsf_\R]]Jl;)+U{Pp;omJkS_*ycm

Session Key Time Out Period (00:03..12:00): 12:00

Figure 141 Radio Payload Encryption Page with Master Key Displayed

5 Record and save the master key generated in Step 4.

6 On the local unit, follow Steps 3 through 4 to configure the same master key configured on the remote unit also on the local unit.

7 Enable payload encryption on the remote unit:

i In the Admin **Mode** field, select **AES-256** to enable payload encryption.

ii In the Session **Key Period** field, configure a time interval in hours and minutes (HH:MM). This is the interval at which the session key is automatically regenerated. The Session Key Period can be from 3 minutes (00:03) to 12 hours (12:00).

iii When you are finished, click **Apply**.

This step will cause the link status to be Down until payload encryption is successfully enabled on the local unit. However, the RSL measured on the link should remain at an acceptable level.

> Note
>
> The **Validation State** field indicates whether the interface is functioning properly, with AES-256 encryption. In order for this field to display **Valid**, both the interface itself and AES-256 encryption must be enabled, the hardware must be in place and functioning properly, initialization must be finished, and AES-256 encryption must be functioning properly, with no loopback on the interface.

8 Enable payload encryption on the local unit by following the procedure described in Step 7. Verify that on both the local and remote active units, the link status returns to Up and user traffic is restored. In links using in-band management, verify also that in-band management returns.

9 Verify that there are no alarms on the link.

Configuring and Viewing Radio PMs and Statistics

This section includes:

Note

The **Radio > PM & Statistics > Diversity** and **Radio > PM & Statistics > Combined** pages are reserved for future use.

Configuring BER Thresholds and Displaying Current BER

You can configure PM thresholds, BER thresholds, and Excessive BER Administration. This enables you to define the levels at which certain PMs are counted, such as the number of seconds in which the configured threshold RX and TX levels are exceeded. This also enables you to define the levels at which certain alarms are triggered.

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

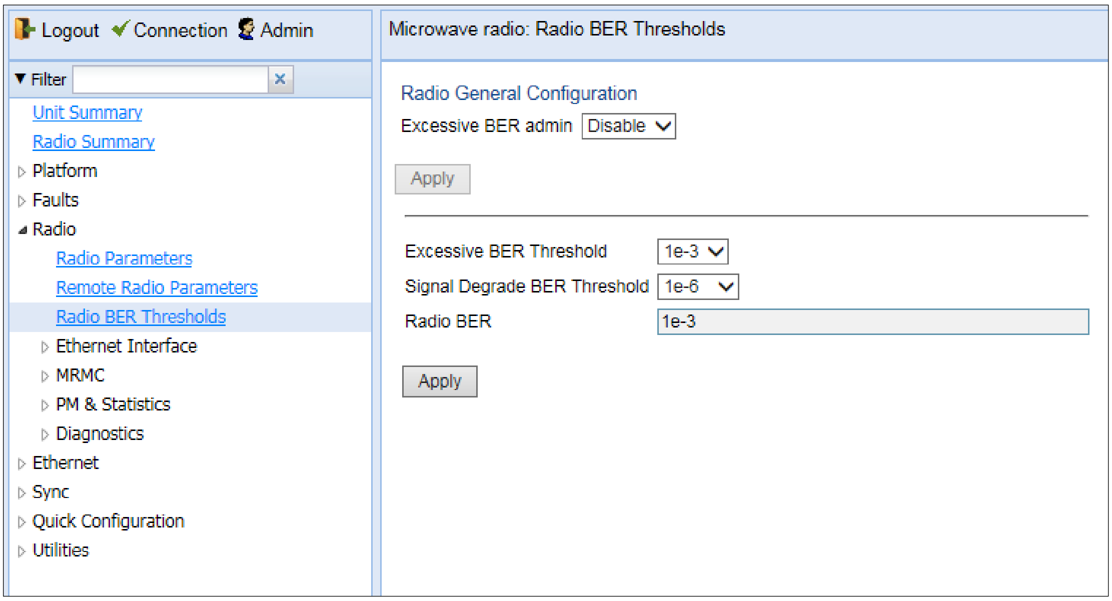
MSE PM Thresholds are configured from the MSE PM Report page. See Displaying MSE PMs and Configuring MSE PM Thresholds.

You can also display the current BER level.

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

1. Select **Radio > Radio BER Thresholds**. The Radio BER Thresholds page opens. The current BER level is displayed, per radio, in the Radio BER column.

Figure 142 Radio BER Thresholds Page



Microwave radio: Radio BER Thresholds

Radio General Configuration

Excessive BER admin: Disable

Excessive BER Threshold: 1e-3

Signal Degrade BER Threshold: 1e-6

Radio BER: 1e-3

2. In the **Excessive BER admin** field, select **Enable** to enable excessive BER administration or **Disable** to disable excessive BER administration. Excessive BER administration determines whether or not excessive BER is propagated as a fault and considered a system event. For example, if excessive BER administration is enabled, excessive BER can trigger a protection switchover and can cause a synchronization source to go into a failure status. Excessive BER administration is enabled or disabled for the entire unit rather than for specific radios.
3. In the **Excessive BER Threshold field**, select the level above which an excessive BER alarm is issued for errors detected over the radio link.
4. In the **Signal Degrade BER Threshold** field, select the level above which a Signal Degrade alarm is issued for errors detected over the radio link.
5. Click **Apply**, then **Close**.

Displaying MRMC Status

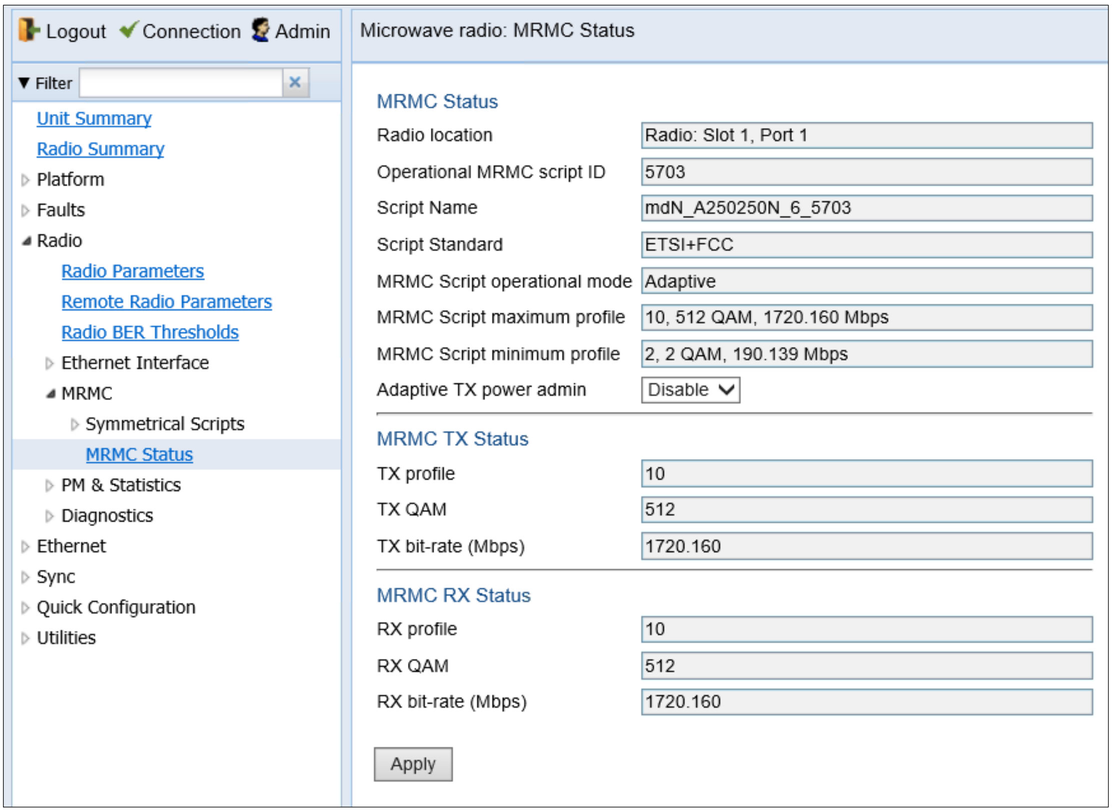
Related Topics:

Configuring the Radio (MRMC) Script(s)

To display the current modulation and bit rate per radio:

1. Select **Radio > MRMC > MRMC Status**. The MRMC Status page opens.

Figure 143 MRMC Status Page



Microwave radio: MRMC Status

MRMC Status

Radio location	Radio: Slot 1, Port 1
Operational MRMC script ID	5703
Script Name	mdN_A250250N_6_5703
Script Standard	ETSI+FCC
MRMC Script operational mode	Adaptive
MRMC Script maximum profile	10, 512 QAM, 1720.160 Mbps
MRMC Script minimum profile	2, 2 QAM, 190.139 Mbps
Adaptive TX power admin	Disable

MRMC TX Status

TX profile	10
TX QAM	512
TX bit-rate (Mbps)	1720.160

MRMC RX Status

RX profile	10
RX QAM	512
RX bit-rate (Mbps)	1720.160

Table 33 describes the MRMC status parameters.

Note

To display the same parameters for an individual radio in a separate page, select the radio in the MRMC script status table and click **Edit**.

Table 33 MRMC Status Parameters

Parameter	Definition
Radio Location	Displays the location of the radio.
Operational MRMC Script ID	The current MRMC script.
Script Name	The name of the script.
Script Standard	Indicates whether the script is compatible with ETSI or FCC (ANSI) standards, or both.
MRMC Script operational mode	The ACM mode: **Fixed** or **Adaptive**. Fixed ACM mode applies constant TX and RX rates. However, unlike regular scripts, with a Fixed ACM script you can specify a maximum profile to inhibit inefficient transmission levels. In Adaptive ACM mode, TX and RX rates are dynamic. An ACM-enabled radio system automatically chooses which profile to use according to the channel fading conditions.
MRMC Script profile	Fixed ACM mode only: The profile in which the system will operate.
MRMC Script maximum profile	Adaptive ACM mode only: The maximum profile for the script. For example, if you select a maximum profile of 5, the system will not climb above profile 5, even if channel fading conditions allow it.
MRMC Script minimum profile	Adaptive ACM mode only: The minimum profile for the script. For example, if you select a minimum profile of 3, the system will not go below profile 3 regardless of the channel fading conditions. The minimum profile cannot be greater than the maximum profile, but it can be equal to it. **Note:** The default minimum profile is 2.
Adaptive Tx Power Admin	Enables or disables Adaptive TX Power. When Adaptive TX Power is enabled, the radio adjusts its TX power dynamically based on the current modulation. When the modulation is at a high level, the TX power is adjusted to the level required with the high modulation. If the modulation goes down to a lower level, the TX power increases to compensate for the lower modulation. The TX level configured in the **TX Level (dBm)** field of the Radio Parameters page determines the maximum TX level, but the actual TX level as shown in the **Operational TX Level (dBm)** field of the Radio Parameters page can be expected to be lower when the radio is operating at high modulations requiring less TX power. See ***Error! Reference source not found.***.
TX profile	The current TX profile.
TX QAM	The current TX modulation.
TX bit-rate	The current TX bit-rate (Mbps).
RX profile	The current RX profile.
RX QAM	The current RX modulation.
RX bit-rate	The current RX bit-rate (Mbps).

Displaying MRMC PMs and Configuring ACM Profile Thresholds

Related Topics:

Configuring the Radio (MRMC) Script(s)

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

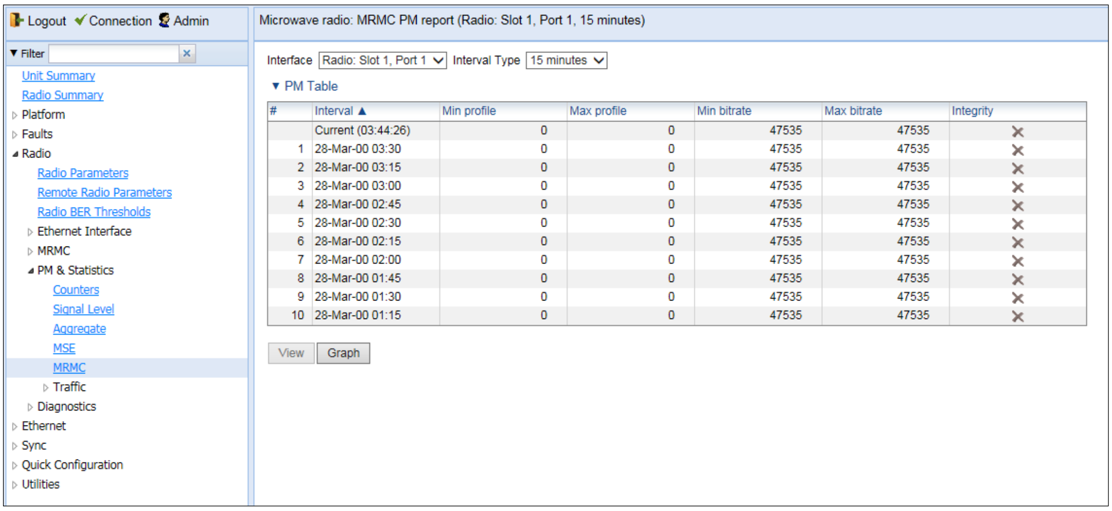
For each radio carrier, you can display the minimum and maximum ACM profile and the minimum and maximum bitrate (throughput) per 15-minute or daily intervals.

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

- Threshold 1 – When the ACM profile goes beneath this threshold, Alarm ID 1313 (Major) is raised. The alarm is cleared when the ACM profile is at or above this threshold.
- Threshold 2 – When the ACM profile goes beneath this threshold, Alarm ID 1314 (Critical) is raised. The alarm is cleared when the ACM profile is at or above this threshold.

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

Figure 144 MRMC PM Report Page



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

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

▼ PM Table

#	Interval ▲	Min profile	Max profile	Min bitrate	Max bitrate	Integrity
	Current (03:44:26)	0	0	47535	47535	✕
1	28-Mar-00 03:30	0	0	47535	47535	✕
2	28-Mar-00 03:15	0	0	47535	47535	✕
3	28-Mar-00 03:00	0	0	47535	47535	✕
4	28-Mar-00 02:45	0	0	47535	47535	✕
5	28-Mar-00 02:30	0	0	47535	47535	✕
6	28-Mar-00 02:15	0	0	47535	47535	✕
7	28-Mar-00 02:00	0	0	47535	47535	✕
8	28-Mar-00 01:45	0	0	47535	47535	✕
9	28-Mar-00 01:30	0	0	47535	47535	✕
10	28-Mar-00 01:15	0	0	47535	47535	✕

2. In the **Interval Type** field:

To display reports in 15-minute intervals, select **15 minutes**.

To display reports in daily intervals, select **24 hours**.

Table 34 describes the MRMC PMs.

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

Table 34 MRMC PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Min profile	Displays the minimum ACM profile that was measured during the interval.
Max profile	Displays the maximum ACM profile that was measured during the interval.
Min bitrate	Displays the minimum total radio throughput (Mbps) delivered during the interval.
Max bitrate	Displays the maximum total radio throughput (Mbps) delivered during the interval.
Seconds above Threshold 1	Displays the number of seconds the radio was above both ACM profile thresholds during the interval.
Seconds below Threshold 1	Displays the number of seconds the radio was below ACM profile threshold 1 during the interval.
Seconds below Threshold 2	Displays the number of seconds the radio was below ACM profile threshold 2 during the interval.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.

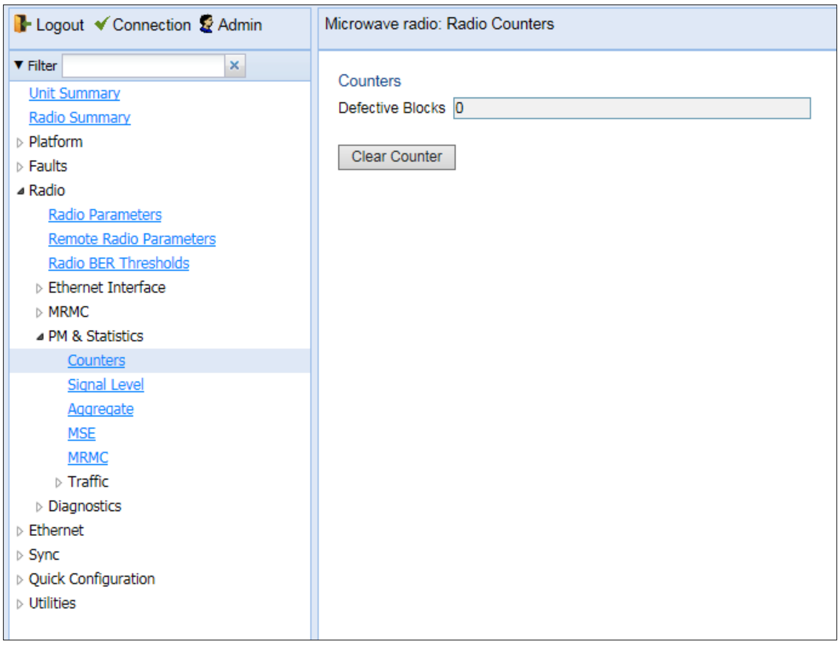
Displaying and Clearing Defective Block Counters

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

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

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

Figure 145 Counters Page



Microwave radio: Radio Counters

Counters

Defective Blocks: 0

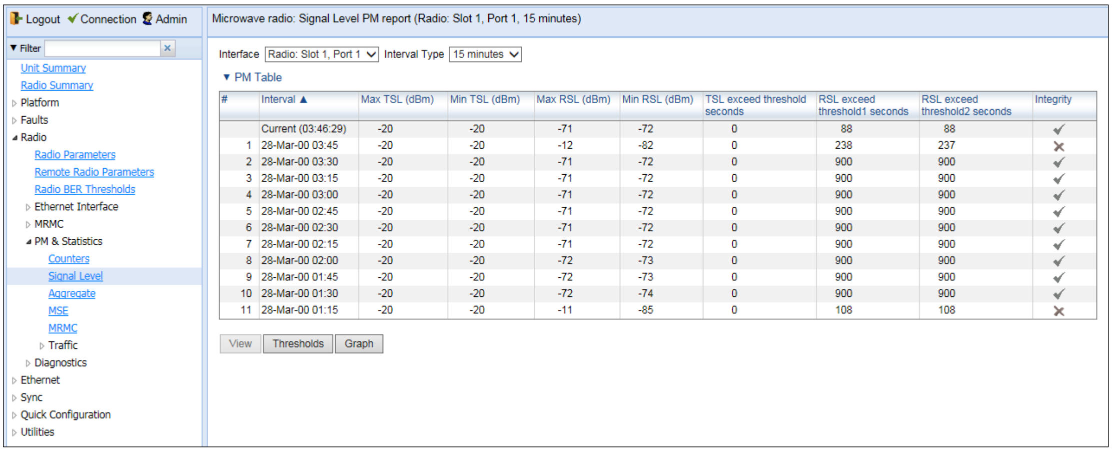
2. To clear the counters, click **Clear Counters**.

Displaying Signal Level PMs and Configuring Signal Level PM Thresholds

To display signal level PMs per radio:

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

Figure 146 Signal Level PM Report Page



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

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

PM Table

#	Interval ▲	Max TSL (dBm)	Min TSL (dBm)	Max RSL (dBm)	Min RSL (dBm)	TSL exceed threshold seconds	RSL exceed threshold1 seconds	RSL exceed threshold2 seconds	Integrity
	Current (03:46:29)	-20	-20	-71	-72	0	88	88	✓
1	28-Mar-00 03:45	-20	-20	-12	-82	0	238	237	✗
2	28-Mar-00 03:30	-20	-20	-71	-72	0	900	900	✓
3	28-Mar-00 03:15	-20	-20	-71	-72	0	900	900	✓
4	28-Mar-00 03:00	-20	-20	-71	-72	0	900	900	✓
5	28-Mar-00 02:45	-20	-20	-71	-72	0	900	900	✓
6	28-Mar-00 02:30	-20	-20	-71	-72	0	900	900	✓
7	28-Mar-00 02:15	-20	-20	-71	-72	0	900	900	✓
8	28-Mar-00 02:00	-20	-20	-72	-73	0	900	900	✓
9	28-Mar-00 01:45	-20	-20	-72	-73	0	900	900	✓
10	28-Mar-00 01:30	-20	-20	-72	-74	0	900	900	✓
11	28-Mar-00 01:15	-20	-20	-11	-85	0	108	108	✗

2. In the **Interval Type** field:
   - To display reports in 15-minute intervals, select **15 minutes**.
   - To display reports in daily intervals, select **24 hours**.

Table 35 describes the Signal Level PMs.

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

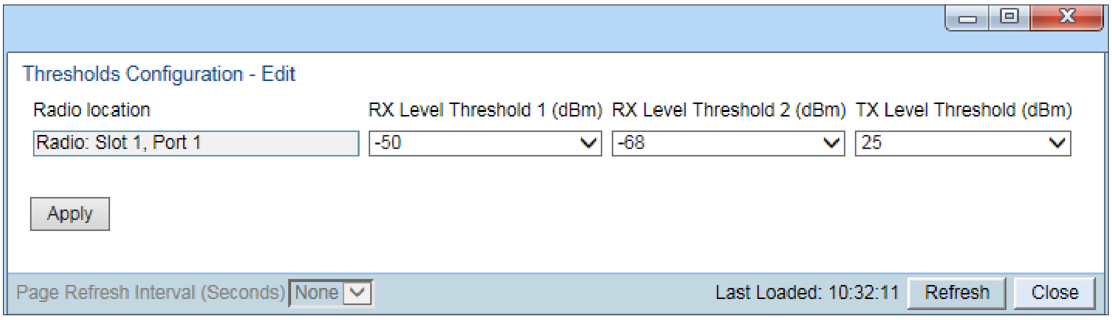
Table 35 Signal Level PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Max TSL (dBm)	The maximum TSL (Transmit Signal Level) that was measured during the interval.
Min TSL (dBm)	The minimum TSL (Transmit Signal Level) that was measured during the interval.
Max RSL (dBm)	The maximum RSL (Received Signal Level) that was measured during the interval.
Min RSL (dBm)	The minimum RSL (Received Signal Level) that was measured during the interval.

Parameter	Definition
TSL exceed threshold seconds	The number of seconds the measured TSL exceeded the threshold during the interval. TSL thresholds are configured in the Radio Thresholds page. See Configuring BER Thresholds and Displaying Current BER
RSL exceed threshold1 seconds	The number of seconds the measured RSL exceeded RSL threshold 1 during the interval. RSL thresholds are configured in the Radio Thresholds page. See Configuring BER Thresholds and Displaying Current BER.
RSL exceed threshold2 seconds	The number of seconds the measured RSL exceeded RSL threshold 2 during the interval. RSL thresholds are configured in the Radio Thresholds page. See Configuring BER Thresholds and Displaying Current BER
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.

To set the Signal Level PM thresholds, click **Thresholds**. The Signal Level Thresholds Configuration – Edit Page opens. Set the thresholds, described in Table 36, and click **Apply**.

Figure 147 Signal Level Thresholds Configuration - Edit Page



Thresholds Configuration - Edit

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

Table 36 Signal Level Thresholds

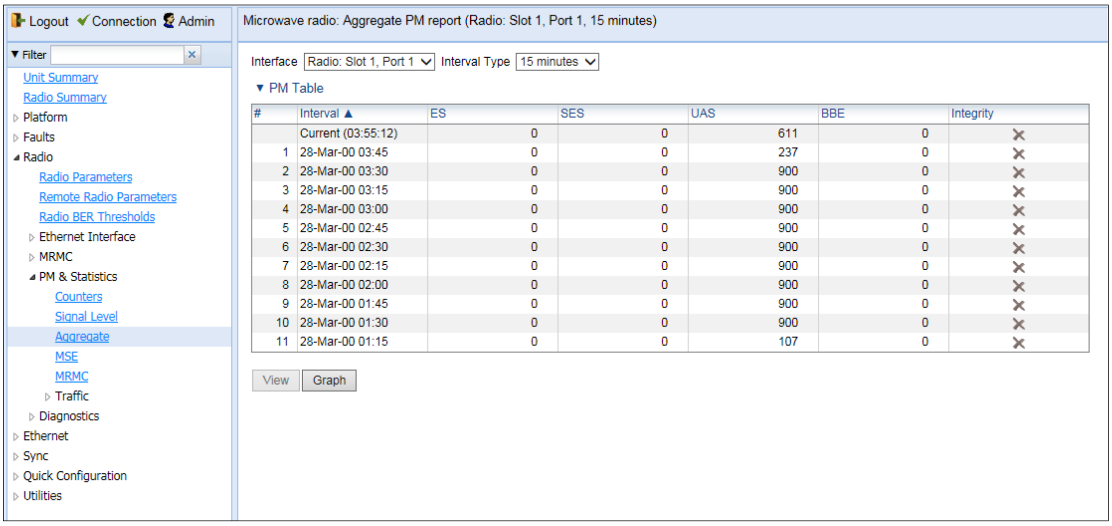
Parameter	Definition
RX Level Threshold 1 (dBm)	Specify the threshold for counting exceeded seconds if the RSL is below this level.
RX Level Threshold 2 (dBm)	Specify a second threshold for counting exceeded seconds if the RSL is below this level.
TX Level Threshold (dBm)	Specify the threshold for counting exceeded seconds if the TSL is below this level.

Displaying Modem BER (Aggregate) PMs

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

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

Figure 148 Aggregate PM Report Page



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

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

#	Interval ▲	ES	SES	UAS	BBE	Integrity
	Current (03:55:12)	0	0	611	0	✕
1	28-Mar-00 03:45	0	0	237	0	✕
2	28-Mar-00 03:30	0	0	900	0	✕
3	28-Mar-00 03:15	0	0	900	0	✕
4	28-Mar-00 03:00	0	0	900	0	✕
5	28-Mar-00 02:45	0	0	900	0	✕
6	28-Mar-00 02:30	0	0	900	0	✕
7	28-Mar-00 02:15	0	0	900	0	✕
8	28-Mar-00 02:00	0	0	900	0	✕
9	28-Mar-00 01:45	0	0	900	0	✕
10	28-Mar-00 01:30	0	0	900	0	✕
11	28-Mar-00 01:15	0	0	107	0	✕

2. In the **Interval Type** field:
   - To display reports in 15-minute intervals, select **15 minutes**.
   - To display reports in daily intervals, select **24 hours**.

Table 37 describes the Modem BER (Aggregate) PMs.

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

Table 37 Modem BER (Aggregate) PMs

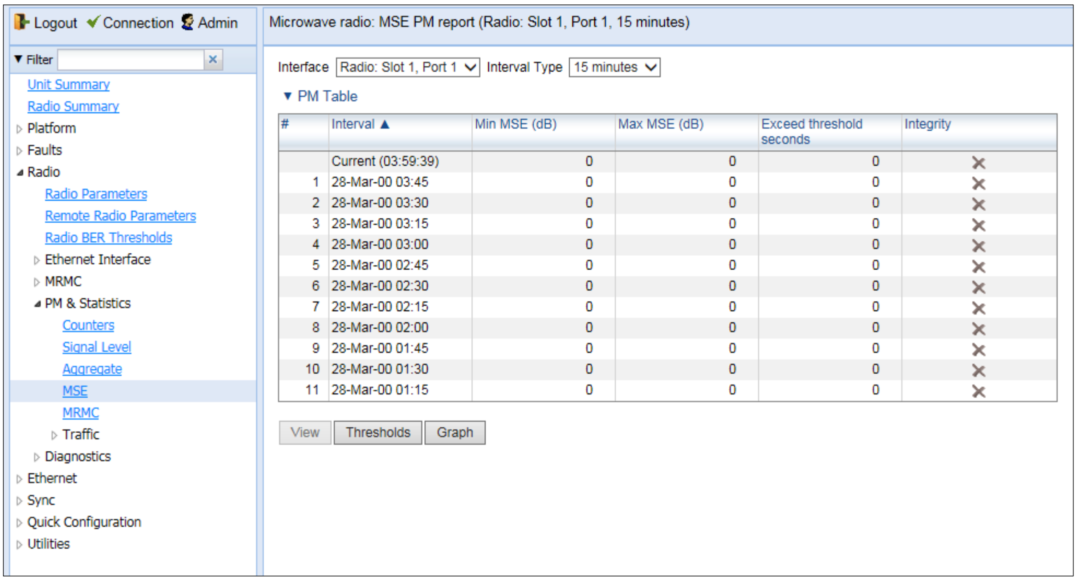
Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
ES	Displays the number of seconds in the measuring interval during which errors occurred.
SES	Displays the number of severe error seconds in the measuring interval.
UAS	Displays the Unavailable Seconds value of the measured interval. The value can be between 0 and 900 seconds (15 minutes).
BBE	Displays the number of background block errors during the measured interval.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.

Displaying MSE PMs and Configuring MSE PM Thresholds

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

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

Figure 149 MSE PM Report Page



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

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

PM Table

#	Interval ▲	Min MSE (dB)	Max MSE (dB)	Exceed threshold seconds	Integrity
	Current (03:59:39)	0	0	0	✕
1	28-Mar-00 03:45	0	0	0	✕
2	28-Mar-00 03:30	0	0	0	✕
3	28-Mar-00 03:15	0	0	0	✕
4	28-Mar-00 03:00	0	0	0	✕
5	28-Mar-00 02:45	0	0	0	✕
6	28-Mar-00 02:30	0	0	0	✕
7	28-Mar-00 02:15	0	0	0	✕
8	28-Mar-00 02:00	0	0	0	✕
9	28-Mar-00 01:45	0	0	0	✕
10	28-Mar-00 01:30	0	0	0	✕
11	28-Mar-00 01:15	0	0	0	✕

2. In the **Interval Type** field:
   - To display reports in 15-minute intervals, select **15 minutes**.
   - To display reports in daily intervals, select **24 hours**.

Table 38 describes the Modem MSE PMs.

Note

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

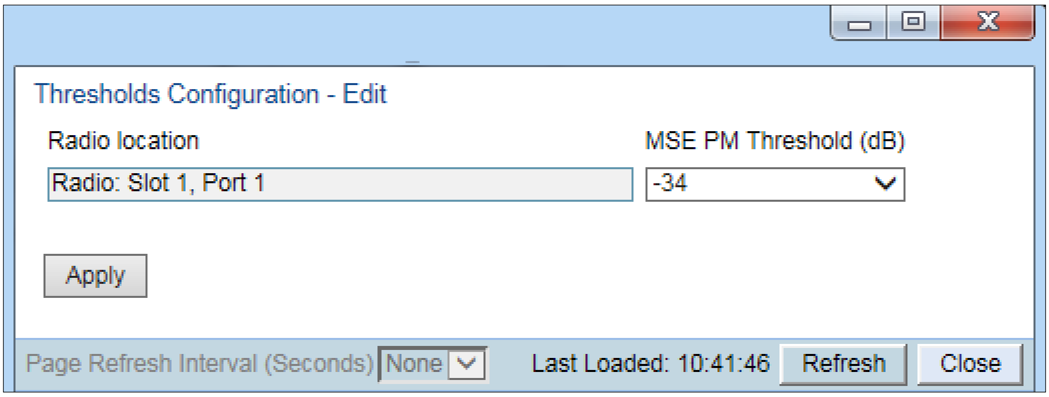
Table 38 Modem MSE PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Min MSE (dB)	Displays the minimum MSE in dB, measured during the interval. A 0 in this field and an X in the **Integrity** field may also indicate that the modem was unlocked during the entire interval.
Max MSE (dB)	Displays the maximum MSE in dB, measured during the interval. A 0 in this field and an X in the **Integrity** field may also indicate that the modem was unlocked.

Parameter	Definition
Exceed threshold seconds	Displays the number of seconds the MSE exceeded the MSE PM threshold during the interval. The MSE PM is configured in the Radio Thresholds page. See Configuring BER Thresholds AND Displaying Cureent BER.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time. An X and a 0 value in the **Max MSE** field may also indicate that the modem was unlocked.

To set the Modem MSE PM thresholds, click **Thresholds**. The Modem MSE Thresholds Configuration–Edit Page opens. For each radio, specify the modem MSE (Mean Square Error) threshold for calculating MSE Exceed Threshold seconds, and click **Apply**.

Figure 150 Modem MSE Thresholds Configuration – Edit Page



Thresholds Configuration - Edit

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

Page Refresh Interval (Seconds): None

Last Loaded: 10:41:46

Displaying XPI PMs and Configuring XPI PM Thresholds

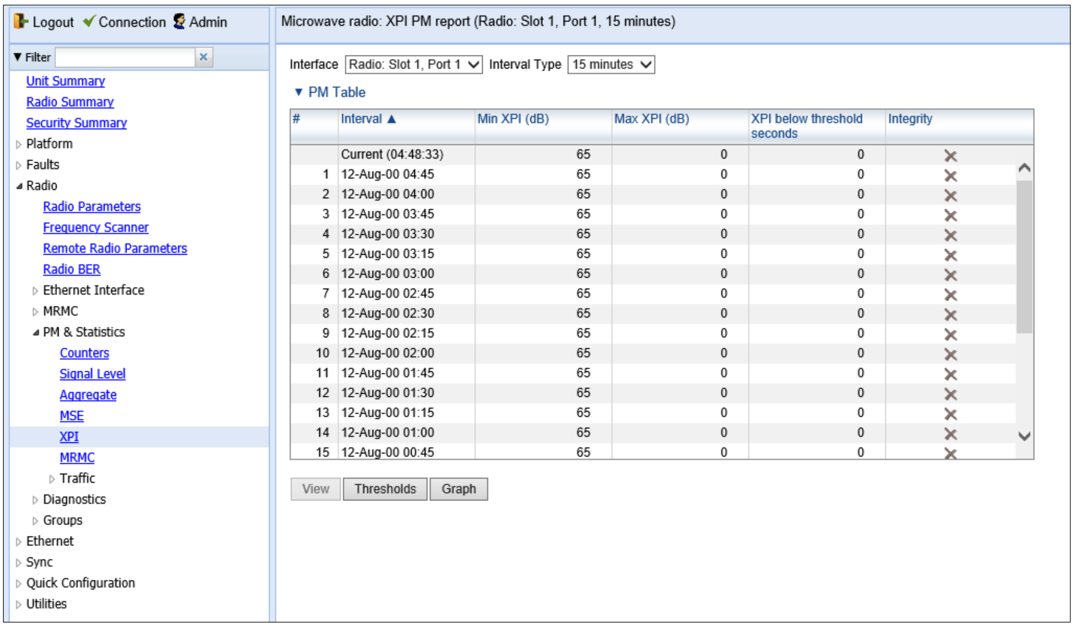
Related topics:

- Configuring XPIC

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

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

Figure 151 XPI PM Report Page



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

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

▼ PM Table

#	Interval ▲	Min XPI (dB)	Max XPI (dB)	XPI below threshold seconds	Integrity
	Current (04:48:33)	65	0	0	✕
1	12-Aug-00 04:45	65	0	0	✕
2	12-Aug-00 04:00	65	0	0	✕
3	12-Aug-00 03:45	65	0	0	✕
4	12-Aug-00 03:30	65	0	0	✕
5	12-Aug-00 03:15	65	0	0	✕
6	12-Aug-00 03:00	65	0	0	✕
7	12-Aug-00 02:45	65	0	0	✕
8	12-Aug-00 02:30	65	0	0	✕
9	12-Aug-00 02:15	65	0	0	✕
10	12-Aug-00 02:00	65	0	0	✕
11	12-Aug-00 01:45	65	0	0	✕
12	12-Aug-00 01:30	65	0	0	✕
13	12-Aug-00 01:15	65	0	0	✕
14	12-Aug-00 01:00	65	0	0	✕
15	12-Aug-00 00:45	65	0	0	✕

2. In the **Interval Type** field:
   - To display reports in 15-minute intervals, select 15 minutes.
   - To display reports in daily intervals, select 24 hours.

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

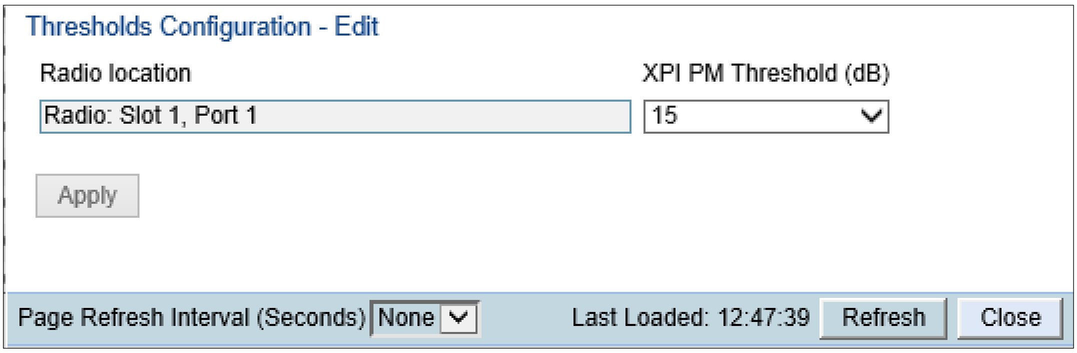
Table 39 XPI PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Min XPI (dB)	The minimum XPI level that was measured during the interval.
Max XPI (dB)	The maximum XPI level that was measured during the interval.
XPI below threshold seconds	The number of seconds the measured XPI level was below the threshold during the interval.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the

Parameter	Definition
	values are not reliable due to a possible power surge or power failure that occurred at that time.

To set the XPI PM thresholds, click **Thresholds**. The XPI Thresholds Configuration– Edit Page opens. Specify the modem XPI threshold for calculating XPI Exceed Threshold seconds and click **Apply**.

Figure 152 XPI Thresholds Configuration – Edit Page



Thresholds Configuration - Edit

Radio location: Radio: Slot 1, Port 1

XPI PM Threshold (dB): 15

Page Refresh Interval (Seconds): None

Last Loaded: 12:47:39

Displaying Traffic PMs

This section includes:

- Displaying Capacity and Throughput PMs
- Displaying Utilization PMs

Displaying Capacity and Throughput PMs

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

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

You can also configure thresholds for capacity and throughput PMs. The number of seconds during which these thresholds are exceeded are among the displayed PMs.

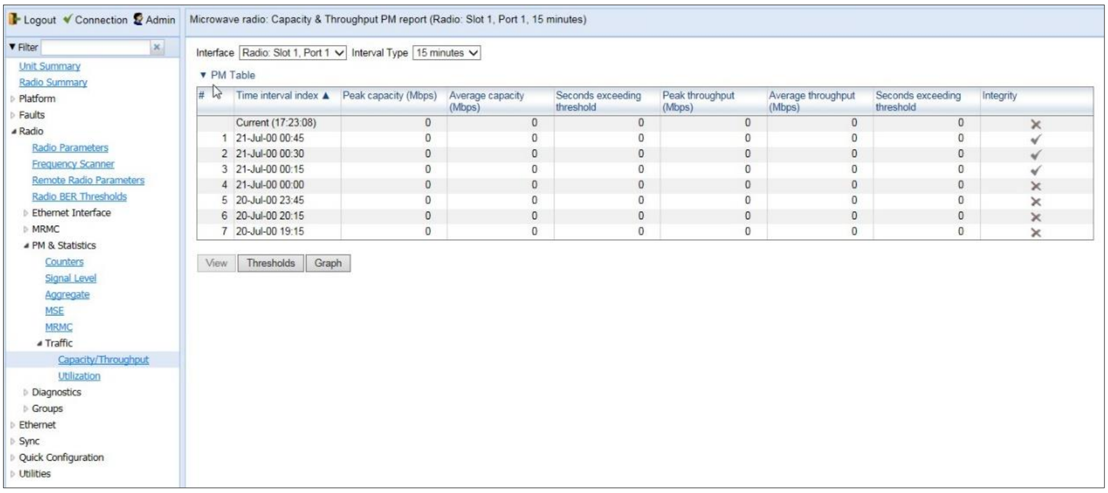
Peak counters display the maximum data rate for each interval, with a resolution of one second. This means the PM mechanism records the number of bytes sent during each second of the interval and displays the number of bytes for the highest one-second period during that interval. So, for example, when measuring 15-minute intervals, the PM mechanism chooses the peak value from 900 recorded values in that interval (60 seconds multiplied by 15 60-second record periods).

Average counters display the average number of bytes received on the interface measured with a resolution of one second. This means the PM mechanism divides the total number of bytes received during the interval by the total number of seconds in the interval. So, for example, when measuring 15-minute intervals, the PM mechanism divides the total number of bytes received during the 15-minute interval by 900.

To display capacity and throughput PMs per radio:

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

Figure 153 Capacity PM Report Page



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

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

PM Table

#	Time interval index ▲	Peak capacity (Mbps)	Average capacity (Mbps)	Seconds exceeding threshold	Peak throughput (Mbps)	Average throughput (Mbps)	Seconds exceeding threshold	Integrity
	Current (17:23:08)	0	0	0	0	0	0	✗
1	21-Jul-00 00:45	0	0	0	0	0	0	✓
2	21-Jul-00 00:30	0	0	0	0	0	0	✓
3	21-Jul-00 00:15	0	0	0	0	0	0	✓
4	21-Jul-00 00:00	0	0	0	0	0	0	✗
5	20-Jul-00 23:45	0	0	0	0	0	0	✗
6	20-Jul-00 20:15	0	0	0	0	0	0	✗
7	20-Jul-00 19:15	0	0	0	0	0	0	✗

2 In the **Interface** field, select the radio or, if Multiband is configured, select the Multiband group.

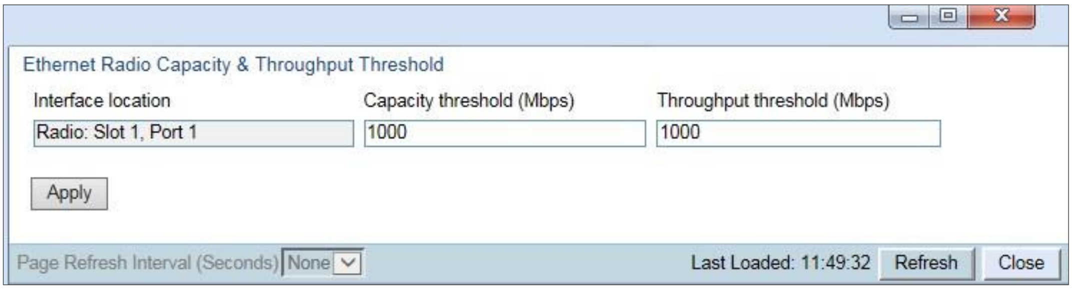
3 In the Interval Type field:

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

To set the thresholds for capacity and throughput PMs:

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

Figure 154 Ethernet Radio Capacity and Throughput Threshold Page



Ethernet Radio Capacity & Throughput Threshold

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

Page Refresh Interval (Seconds): None
Last Loaded: 11:49:32

2 Enter the capacity and throughput thresholds you want, in Mbps. The range of values is 0 to 4294967295. The default value for is 1000.

3 Click Apply, then Close.

Note

To display the same parameters for a specific interval in a separate page, select the interval in the PM table and click View

Table 40 Capacity/Throughput PMs

Parameter	Definition
Time interval index	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Peak capacity (Mbps)	Displays the highest L1 bandwidth, in Mbps, sent through the selected radio during the measured time interval.
Average capacity	Displays the average L1 bandwidth, in Mbps, during the measured time interval.
Seconds exceeding	Displays the number of seconds during the measured time interval during which the L1 bandwidth exceeded the configured capacity
Peak throughput	Displays the highest throughput, in Mbps, that occurred for the selected radio during the measured time interval.
Average throughput	Displays the average throughput, in Mbps, for the selected radio during the measured time interval.
Seconds exceeding	Displays the number of seconds during the measured time interval during which the throughput exceeded the configured throughput
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the

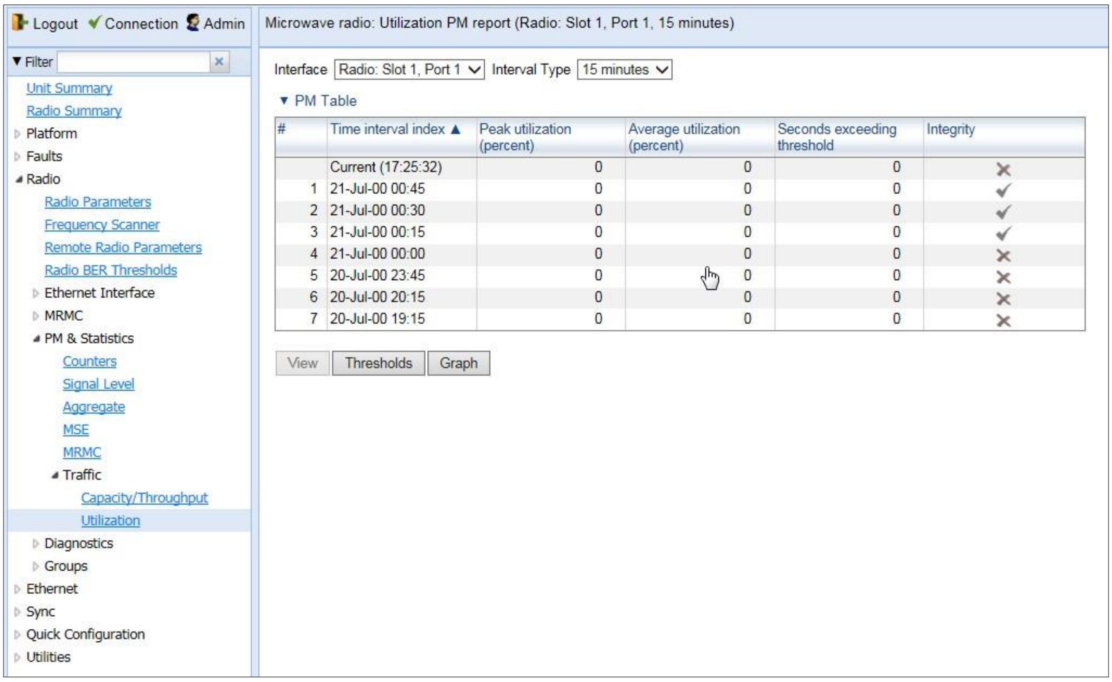
Displaying Utilization PMs and Configuring Utilization Thresholds

You can configure three radio capacity utilization thresholds, in percentage. The Utilization PM Report displays, for each radio carrier and Multi-Carrier ABC group, the number of seconds in which the radio or group exceeded each threshold in each interval. It also displays the peak and average utilization, in percentage, per interval.

To display radio capacity utilization PMs per radio:

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

Figure 155 Utilization PM Report Page



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

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

PM Table

#	Time interval index ▲	Peak utilization (percent)	Average utilization (percent)	Seconds exceeding threshold	Integrity
	Current (17:25:32)	0	0	0	✗
1	21-Jul-00 00:45	0	0	0	✓
2	21-Jul-00 00:30	0	0	0	✓
3	21-Jul-00 00:15	0	0	0	✓
4	21-Jul-00 00:00	0	0	0	✗
5	20-Jul-00 23:45	0	0	0	✗
6	20-Jul-00 20:15	0	0	0	✗
7	20-Jul-00 19:15	0	0	0	✗

2 In the **Interface** field, select the radio or, if Multiband is configured, select the Multiband group.

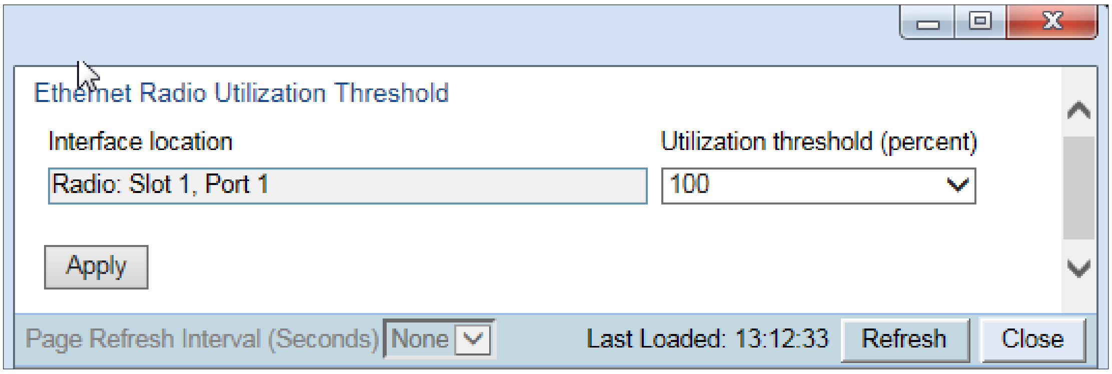
3 In the Interval Type field:

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

To display reports in daily intervals, select 24 hours. To set the thresholds for utilization PMs:

1 Select **Threshold**. The Utilization Threshold page opens.

Figure 156 Ethernet Radio Utilization Threshold Page



Ethernet Radio Utilization Threshold

Interface location: Radio: Slot 1, Port 1

Utilization threshold (percent): 100

Page Refresh Interval (Seconds): None

Last Loaded: 13:12:33

2 Select the utilization threshold you want, in % (1-100). The default value for is 100.

3 Click Apply, then Close.

Note

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

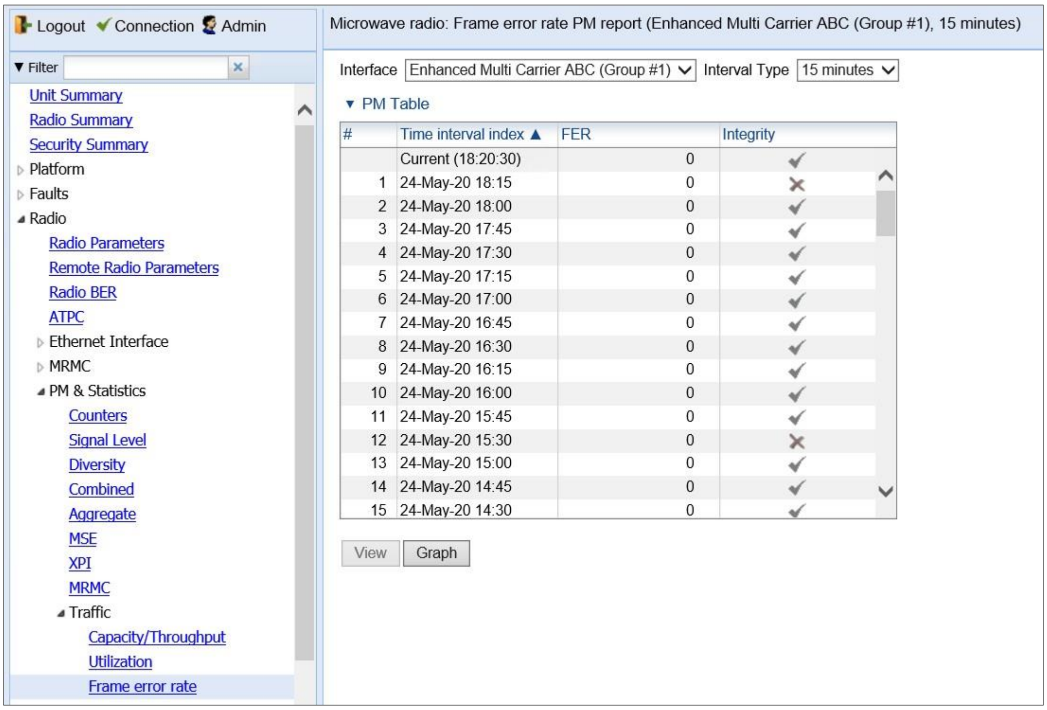
Table 41 Utilization PMs

Parameter	Definition
Time interval index	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of
Peak utilization (%)	Indicates the highest utilization of the radio capacity that occurred for the selected radio or group during the
Average utilization (%)	Indicates the average utilization of the radio capacity for the selected radio or group during the measured time
Seconds exceeding Threshold 1	Displays the number of seconds during the measured time interval during which the L1 bandwidth exceeded the configured utilization threshold.
Seconds exceeding Threshold 2	Displays the number of seconds during the measured time interval during which the L1 bandwidth exceeded Threshold 2.
Seconds exceeding Threshold 3	Displays the number of seconds during the measured time interval during which the L1 bandwidth exceeded Threshold 3 (the lowest threshold).
Seconds below Threshold 3	Displays the number of seconds during the measured time interval during which the L1 bandwidth was less than Threshold 3 (the lowest threshold).
Integrity	Indicates whether the values received at time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.

Displaying Frame Error Rate PMs

To display frame error rate PMs per radio or Multi-Carrier ABC group:

1 Select **Radio > PM & Statistics > Traffic > Frame error rate**. The Frame error rate PM report page opens.



Microwave radio: Frame error rate PM report (Enhanced Multi Carrier ABC (Group #1), 15 minutes)

Interface: Enhanced Multi Carrier ABC (Group #1) Interval Type: 15 minutes

▼ PM Table

#	Time interval index ▲	FER	Integrity
	Current (18:20:30)	0	✓
1	24-May-20 18:15	0	✗
2	24-May-20 18:00	0	✓
3	24-May-20 17:45	0	✓
4	24-May-20 17:30	0	✓
5	24-May-20 17:15	0	✓
6	24-May-20 17:00	0	✓
7	24-May-20 16:45	0	✓
8	24-May-20 16:30	0	✓
9	24-May-20 16:15	0	✓
10	24-May-20 16:00	0	✓
11	24-May-20 15:45	0	✓
12	24-May-20 15:30	0	✗
13	24-May-20 15:00	0	✓
14	24-May-20 14:45	0	✓
15	24-May-20 14:30	0	✓

Figure 157 Frame Error PM Report Page

2 In the **Interface** field, select the radio or, if Multi-Carrier ABC (PTP 850C) or Multiband (PTP 850E) is configured, select the ABC or Multiband group.

Note: For PTP 850C, only radio carrier 1 and the Multi-Carrier ABC group (if configured) is available.

3 In the Interval Type field:

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

Table 45 describes the capacity and throughput PMs.

Table 42 Frame Error Rate PMs

Parameter	Definition
Time interval index	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
FER	Displays the frame error rate (%) during the measured time interval.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.

Displaying Ethernet Interface Counters

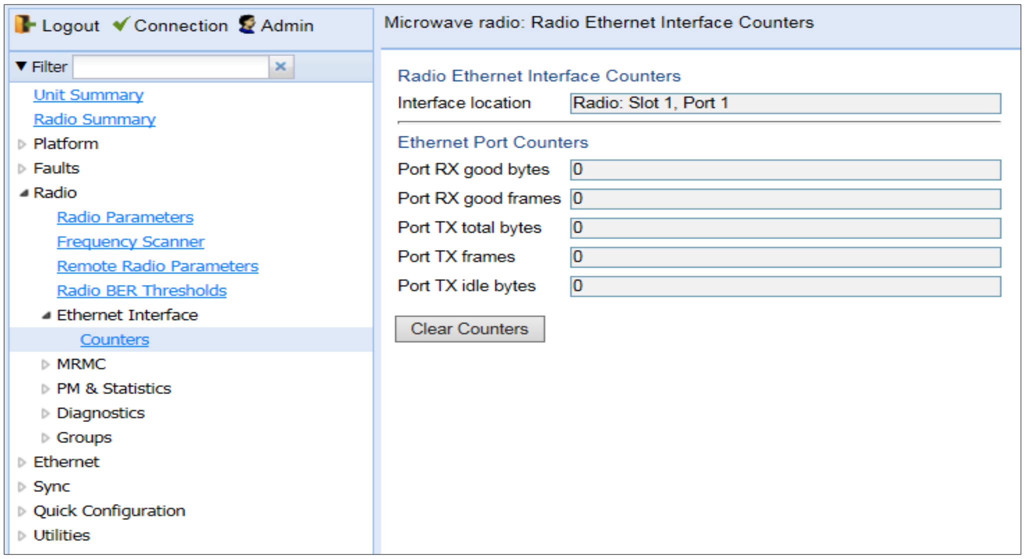
You can view PMs on Ethernet frames entering the radio interface.

> Note
>
> In a Multiband configuration, this page displays PMs for the Multiband group rather than the individual interface.

To view Ethernet interface counters:

1 Select **Radio > Ethernet Interface > Counters**. The Radio Ethernet Interface Counters page opens.

Figure 158 Radio Ethernet Interface Counters Page



Microwave radio: Radio Ethernet Interface Counters

Radio Ethernet Interface Counters

Interface location: Radio: Slot 1, Port 1

Ethernet Port Counters

Port RX good bytes: 0

Port RX good frames: 0

Port TX total bytes: 0

Port TX frames: 0

Port TX idle bytes: 0

Table 43 Ethernet Interface Counter Fields

Parameter	Description
Port RX good bytes	The number of good bytes received on the port since the last time the Ethernet Interface counters were cleared.
Port RX good frames	The number of good frames received on the port since the last time the Ethernet Interface counters were cleared.
Port TX total bytes	The number of bytes transmitted since the last time the Ethernet Interface counters were cleared.

Port TX frames	The number of frames transmitted since the last time the Radio Ethernet Interface counters were cleared.
Port TX idle bytes	The number of idle bytes transmitted since the last time the Radio Ethernet Interface counters were cleared.

Chapter 9: Ethernet Services and Interfaces

This section includes:

Related topics:

Quality of Service (QoS)

Performing Ethernet Loopback

Configuring Ethernet Service(s)

This section includes:

Ethernet Services Overview

Users can define the following number of Ethernet services.

- PTP 850C and PTP 850E: Up to 1024.
- PTP 850S: Up to 64.

Each service constitutes a virtual bridge that defines the connectivity between logical ports in the PTP 850 network element.

This version of PTP 850 supports the following service types:

Multipoint (MP)

Point-to-Point (P2P)

Management (MNG)

In addition to user-defined services, PTP 850 contains a pre-defined management service (Service ID 1025). By default, this service is operational.

Note

You can use the management service for in-band management. For instructions on configuring in-band management, see Configuring In-Band Management.

A service point is a logical entity attached to a physical or logical interface. Service points define the movement of frames through the service. Each service point includes both ingress and egress attributes. A Point-to-Point or Multipoint service can hold up to 32 service points. A Management service can hold up 30 service points.

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

General Guidelines for Provisioning Ethernet Services

When provisioning Ethernet services, it is recommended to follow these guidelines:

Use the same Service ID for all service fragments along the path of the service.

Do not re-use the same Service ID within the same region. A region is defined as consisting of all PTP 850 devices having Ethernet connectivity between them.

Use meaningful EVC IDs.

Give the same EVC ID (service name) to all service fragments along the path of the service.

Do not reuse the same EVC ID within the same region.

It is recommended to follow these guidelines for creating service points:

Always use SNP service points on NNI ports and SAP service points on UNI ports.

For each logical interface associated with a specific service, there should never be more than a single service point.

The transport VLAN ID should be unique per service within a single region. That is, no two services should use the same transport VLAN ID.

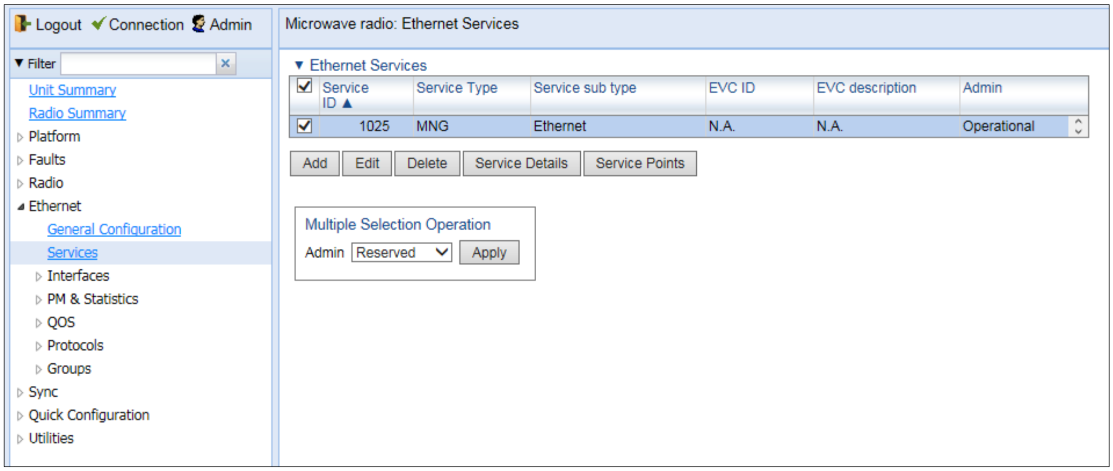
The Ethernet Services Page

The Ethernet Services page is the starting point for defining Ethernet services on the PTP 850.

To open the Ethernet Services page:

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

Figure 159 Ethernet Services Page



Microwave radio: Ethernet Services

▼ Ethernet Services

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

Multiple Selection Operation

Admin: Reserved

Table 44 Ethernet Services Page Parameters

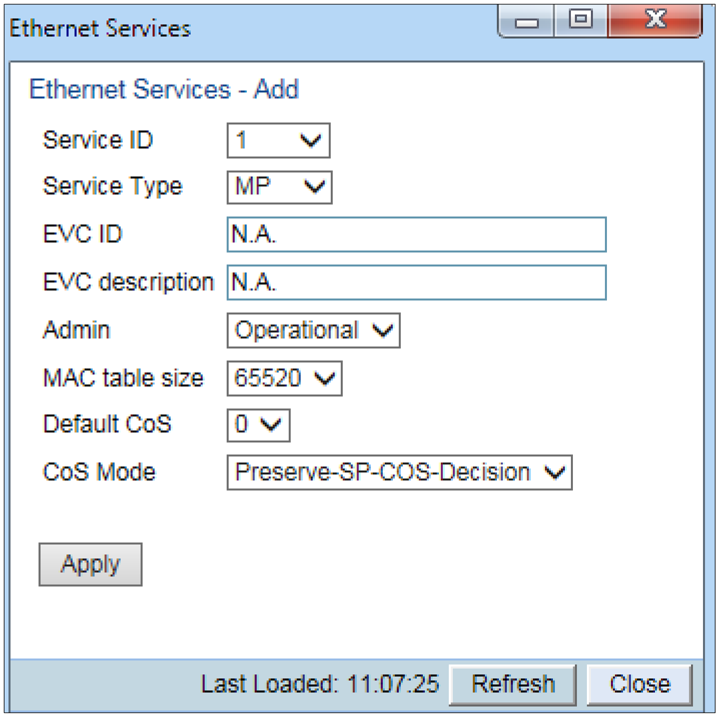
Parameter	Definition
Services ID	A unique ID for the service.
Service Type	The service type: • **MP** – Multipoint • **P2P** – Point-to-Point • **MNG** – Management
Service sub type	Indicates the type of service (**Ethernet**).
EVC ID	The Ethernet Virtual Connection (EVC) ID. This parameter does not affect the network element's behavior, but is used by the NMS for topology management.
EVC description	The Ethernet Virtual Connection (EVC) description. This parameter does not affect the network element's behavior, but is used by the NMS for topology management.
Admin	Indicates whether the service is enabled (**Operational**) or disabled (**Reserved**). You can configure services for later use by defining the service as **Reserved**. In Reserved mode, the service occupies system resources but is unable to transmit and receive data.

Adding an Ethernet Service

To add an Ethernet service:

1. Select **Ethernet** > **Services**. The Ethernet Services page opens (Figure 159).
2. In the Ethernet Services page, click **Add**. The Ethernet Services – Add page opens.

Figure 160 Ethernet Services - Add page



Ethernet Services

Ethernet Services - Add

Service ID	1
Service Type	MP
EVC ID	N.A.
EVC description	N.A.
Admin	Operational
MAC table size	65520
Default CoS	0
CoS Mode	Preserve-SP-COS-Decision

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

Note

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

9. In the **Default CoS** field, enter a default Class of Service (CoS) value (0-7). This value is assigned to frames at the service level if CoS Mode is set to Default-CoS. Otherwise, this value is not used, and frames retain whatever CoS value they were assigned at the service point or logical interface level.
10. In the **CoS Mode** field, select one of the following options. This parameter determines whether or not frames passing through the service have their CoS modified at the service level. The CoS determines the priority queue to which frames are assigned.
    - **Default CoS** – Frames passing through the service are assigned the default CoS defined above. This CoS value overrides whatever CoS may have been assigned at the service point or interface level.
    - **Preserve-SP-COS-Decision** – The CoS of frames passing through the service is not modified by the service's default CoS.
11. Click **Apply**, then **Close** to close the Ethernet Services - Add page.
12. Add service points. You must add service points to the service in order for the service to carry traffic. See Configuring Service Points.

Editing a Service

To edit a service:

1. Select **Ethernet** > **Services**. The Ethernet Services page opens (Figure 159).
2. Select the service in the Service Configuration Table.
3. In the Ethernet Services page, click **Edit**. The Ethernet Services - Edit page opens.
4. This page is identical to the Ethernet Services - Add page (Figure 160). You can edit any parameter that can be configured in the Add page, except the **Service ID**.

Deleting a Service

Before deleting a service, you must first delete any service points attached to the service.

To delete a service:

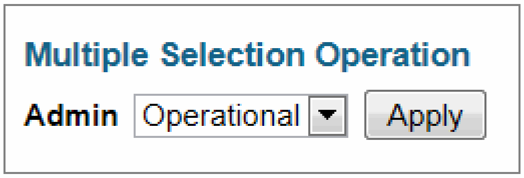
1. Delete all service points attached to the service you wish to delete, as described in Deleting a Service Point*.*
2. Select **Ethernet** > **Services**. The Ethernet Services page opens (Figure 159).
3. Select the service in the Ethernet Service Configuration Table.
4. Click **Delete.** The service is deleted.

Enabling, Disabling, or Deleting Multiple Services

To enable, disable, or delete multiple services:

1. Select **Ethernet** > **Services**. The Ethernet Services page opens (Figure 159).
2. Select the services in the Ethernet Services Configuration table, or select all the services by selecting the check box in the top row.
    - To enable the selected services, in the Multiple Selection Operation section underneath the Ethernet Services Configuration Table, select **Operational** and click **Apply**.
    - To disable the selected services, in the Multiple Selection Operation section underneath the Ethernet Services Configuration Table, select **Reserved** and click **Apply**.
    - To delete the selected services, select **Delete** underneath the Ethernet Services Configuration Table. Before deleting a service, you must delete any service points attached to the service, as described in Deleting a Service Point.

Figure 161 Multiple Selection Operation Section (Ethernet Services)



Multiple Selection Operation

Admin Operational ▾ Apply

Note

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

When setting multiple services to **Reserve** state, make sure to avoid setting the management service to **Reserve** state

Viewing Service Details

To view the full service parameters:

1. Select **Ethernet > Services**. The Ethernet Services page opens (Figure 159).
2. Select the service in the Ethernet Services Configuration table.
3. In the Ethernet Services page, click **Service Details**. The Ethernet Services – Service Details page opens. The Service Details page contains the same fields as the Add page (Figure 159). However, in the Service Details page, these fields are read-only.

Configuring Service Points

This section includes:

Ethernet Services Points Overview

Ethernet Services Points Overview

Service points are logical interfaces within a service. A service point is a logical entity attached to a physical or logical interface. Service points define the movement of frames through the service. Each service point includes both ingress and egress attributes.

Each service point for a Point-to-Point or Multipoint service can be either a Service Access Point (SAP) or a Service Network Point (SNP). A Point-to-Point service can also use Pipe service points.

An SAP is equivalent to a UNI in MEF terminology and defines the connection of the user network with its access points. SAPs are used for Point-to-Point and Multipoint traffic services.

An SNP is equivalent to an NNI or E-NNI in MEF terminology and defines the connection between the network elements in the user network. SNPs are used for Point-to-Point and Multipoint traffic services.

A Pipe service point is used to create traffic connectivity between two ports in a port-based manner (Smart Pipe). In other words, all the traffic from one port passes to the other port.

Management services utilize Management (MNG) service points.

A Point-to-Point or Multipoint service can hold up to 32 service points. A management service can hold up to 30 service points.

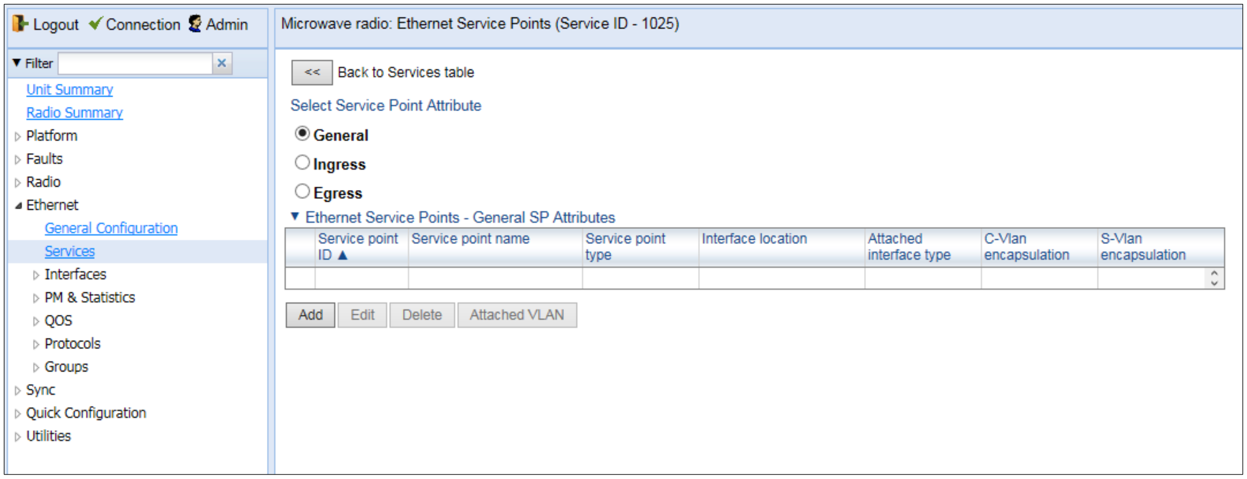
The Ethernet Service Points Page

The Ethernet Service Points page is the starting point for configuring Ethernet service points.

To open the Ethernet Service Points page:

1. Select **Ethernet > Services**. The Ethernet Services page opens (Figure 159).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens.

Figure 162 Ethernet Service Points Page



Microwave radio: Ethernet Service Points (Service ID - 1025)

Select Service Point Attribute

● General

○ Ingress

○ Egress

▼ Ethernet Service Points - General SP Attributes

	Service point ID ▲	Service point name	Service point type	Interface location	Attached interface type	C-Vlan encapsulation	S-Vlan encapsulation

You can choose to display the following sets of attributes by selecting the appropriate button above the SP Attributes table:

General – See Ethernet Service Points – General SP Attributes Table

Ingress – See 2. Ethernet Service Points – Ingress Attributes

Egress – See 3. Ethernet Service Points – Egress Attributes

To return to the Ethernet Services page at any time, click **Back to Services table** at the top of the Ethernet Service Points page.

1. Ethernet Service Points – General SP Attributes Table

The General SP Attributes table is shown in Figure 162 Ethernet Service Points Page. Table 45 describes the parameters displayed in the General SP Attributes table.

Table 45 General Service Point Attributes

Parameter	Definition
Service point ID	This ID is unique within the service. For Point-to-Point and Multipoint services, the range of values is 1-32. For Management services, the range of values is 1-30. When adding a service point, you can select a service point ID from the available options in the **Service point ID** drop-down list in the Ethernet Service Points – Add page. Once you have added the service point, you cannot change the service point ID.
Service point name	A descriptive name for the service point (optional). The Service Point Name can be up to 20 characters.

Parameter	Definition
Service point type	The service point type. Options are: • **SAP** – Service Access Point. • **SNP** – Service Network Point. • **MNG** – Management service point. • **PIPE** – Pipe service point. The following rules apply to the mixing of different types of service points on a single logical interface: You cannot configure both SAPs and SNPs on the same logical interface. • You can configure both SAPs or SNPs on the same logical interface as a MNG service point. • If you configure a Pipe service point on an interface, you cannot configure an SAP, SNP, or another Pipe service point on the same interface. You can, however, configure an MNG service point on the same interface. • You cannot configure more than one MNG service point on a single logical interface. • Once you have added the service point, you cannot change this parameter.
Interface location	The physical or logical interface on which the service point is located. Once you have added the service point, you cannot change this parameter.
Attached interface type	The encapsulation type (Ethertype) for frames entering the service point. Once you have added the service point, you cannot change this parameter. The Attached Interface Type determines which frames enter the service via this service point, based on the frame's VLAN tagging. Since more than one service point may be associated with a single interface, frames are assigned to the earliest defined service point in case of conflict. For a list of available Attached Interface Types, the types of frames to which each one applies, and the service point types for which each one is available, see Table 46.
C-Vlan encapsulation	The C-VLAN classified into the service point. Options are 1-4094, **Untagged**, or **N.A.** (Not Applicable). Once you have added the service point, you cannot change this parameter. If you selected **Bundle-C** in the **Attached Interface Type** field, select **Untagged** or **N.A.** You can then add multiple C-VLANs via the **Attach VLAN** option. See Attaching VLANs.

Parameter	Definition
S-Vlan encapsulation	The S-VLAN classified into the service point. Options are 1-4094, **Untagged**, or **N.A.** (Not Applicable). Once you have added the service point, you cannot change this parameter. If you selected **Bundle-S** in the **Attached Interface Type** field, select the S-VLAN value to classify into the service point (1-4094), or select **Untagged**. You can then add multiple C-VLANs via the **Attach VLAN** option. See Attaching VLANs.

Table 46 describes the available Attached Interface Types.

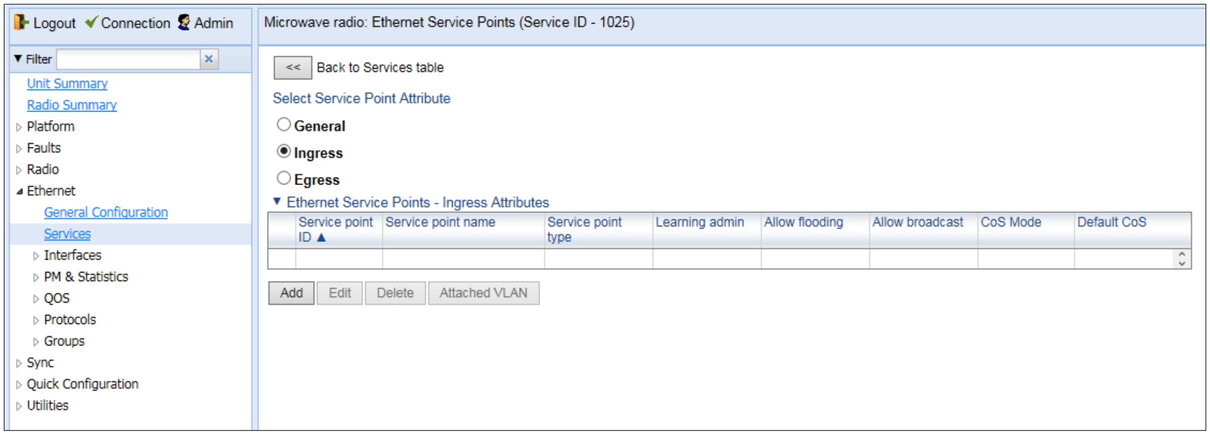
Table 46 Attached Interface Types

Attached Interface Type	Types of Frames	Available for Service Point Types
dot1q	A single C-VLAN is classified into the service point.	All
s-tag	A single S-VLAN is classified into the service point.	SNP, PIPE, and MNG
Bundle-C	A set of C-VLANs is classified into the service point.	SAP
Bundle-S	A single S-VLAN and a set of C-VLANs are classified into the service point.	SAP
All-to-One	All C-VLANs and untagged frames that enter the interface are classified into the service point.	SAP
Q-in-Q	A single S-VLAN and C-VLAN combination is classified into the service point.	SAP and MNG

2. Ethernet Service Points – Ingress Attributes

Select **Ingress** in the Ethernet Service Points page to display the Ethernet Service Points – Ingress Attributes table. Table 47 describes the parameters displayed in the Ingress SP Attributes table.

Figure 163 Ethernet Service Points Page – Ingress Attributes



Microwave radio: Ethernet Service Points (Service ID - 1025)

Select Service Point Attribute

○ General

● Ingress

○ Egress

▼ Ethernet Service Points - Ingress Attributes

	Service point ID ▲	Service point name	Service point type	Learning admin	Allow flooding	Allow broadcast	CoS Mode	Default CoS

Table 47 Service Point Ingress Attributes

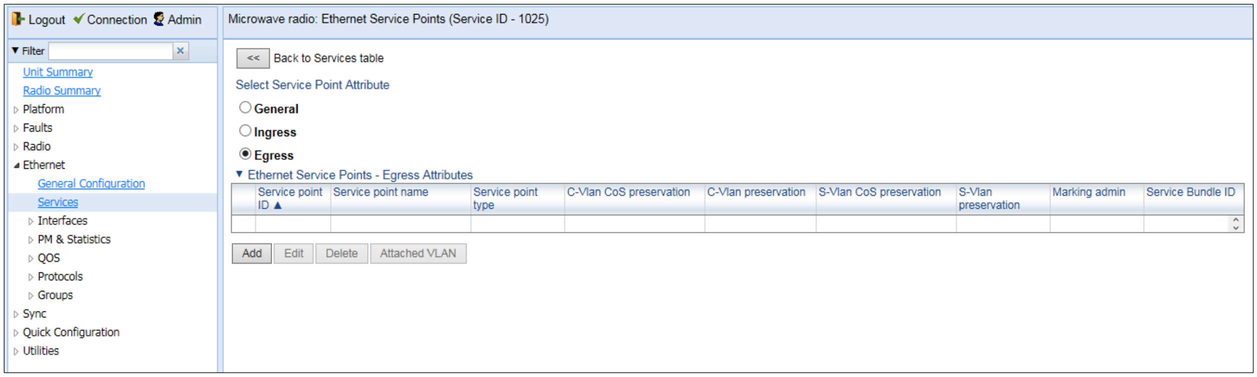
Parameter	Definition
Service point ID	This ID is unique within the service. For Point-to-Point and Multipoint services, the range of values is 1-32. For Management services, the range of values is 1-30.
Service point name	A descriptive name for the service point (optional). The Service Point Name can be up to 20 characters.
Service point type	The service point type. Options are: **SAP** – Service Access Point. **SNP** – Service Network Point. **MNG** – Management service point. **PIPE** – Pipe service point.
Learning admin	Determines whether MAC address learning for incoming frames is enabled (**Enable**) or disabled (**Disable**). When enabled, the service point learns the source MAC addresses of incoming frames and adds them to a MAC address forwarding table.
Allow flooding	Determines whether incoming frames with unknown MAC addresses are forwarded to other service points via flooding. Select **Allow** to allow flooding or **Disable** to disable flooding.
Allow broadcast	Indicates whether frames with a broadcast destination MAC address are allowed to ingress the service via this service point. Select **Allow** to allow broadcast or **Disable** to disable broadcast.

Parameter	Definition
CoS Mode	Indicates how the service point handles the CoS of frames that pass through the service point. Options are: **sp-def-cos** – The service point re-defines the CoS of frames that pass through the service point, according to the Default CoS (below). This decision can be overwritten on the service level. **Interface-Decision** – The service point preserves the CoS decision made at the interface level. The decision can still be overwritten at the service level. **PCL** – Reserved for future use. **TCAM** – Reserved for future use.
Default CoS	The default CoS. If the **CoS Mode** is **sp-def-cos**, this is the CoS assigned to frames that pass through the service point. This decision can be overwritten at the service level. Possible values are 0 to 7.

3. Ethernet Service Points – Egress Attributes

Select **Egress** in the Ethernet Service Points page to display the Ethernet Service Points – Egress Attributes table. Table 48 `describes the parameters displayed in the General SP Attributes table.

Figure 164 Ethernet Service Points Page – Egress Attributes



Microwave radio: Ethernet Service Points (Service ID - 1025)

Back to Services table

Select Service Point Attribute

○ General

○ Ingress

● Egress

Ethernet Service Points - Egress Attributes

Service point ID ▲	Service point name	Service point type	C-Vlan CoS preservation	C-Vlan preservation	S-Vlan CoS preservation	S-Vlan preservation	Marking admin	Service Bundle ID

Table 48 Service Point Egress Attributes

Parameter	Definition
Service point ID	This ID is unique within the service. For Point-to-Point and Multipoint services, the range of values is 1-32. For Management services, the range of values is 1-30.
Service point name	A descriptive name for the service point (optional). The Service Point Name can be up to 20 characters.

Parameter	Definition
Service point type	The service point type. Options are: **SAP** – Service Access Point. **SNP** – Service Network Point. **MNG** – Management service point. **PIPE** – Pipe service point.
C-Vlan CoS preservation	Determines whether the original C-VLAN CoS value is preserved or restored for frames egressing from the service point. If C-VLAN CoS preservation is enabled, the C-VLAN CoS value of frames egressing the service point is the same as the value when the frame entered the service. If C-VLAN CoS preservation is disabled, the C-VLAN CoS value of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking.
C-Vlan preservation	Determines whether the original C-VLAN ID is preserved or restored for frames egressing from the service point. If C-VLAN preservation is enabled, the C-VLAN ID of frames egressing the service point is the same as the C-VLAN ID when the frame entered the service. If C-VLAN preservation is disabled, the C-VLAN ID of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking
S-Vlan CoS preservation	Determines whether the original S-VLAN CoS value is preserved or restored for frames egressing from the service point. If S-VLAN CoS preservation is enabled, the S-VLAN CoS value of frames egressing the service point is the same as the value when the frame entered the service. If S-VLAN CoS preservation is disabled, the C-VLAN CoS value of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking

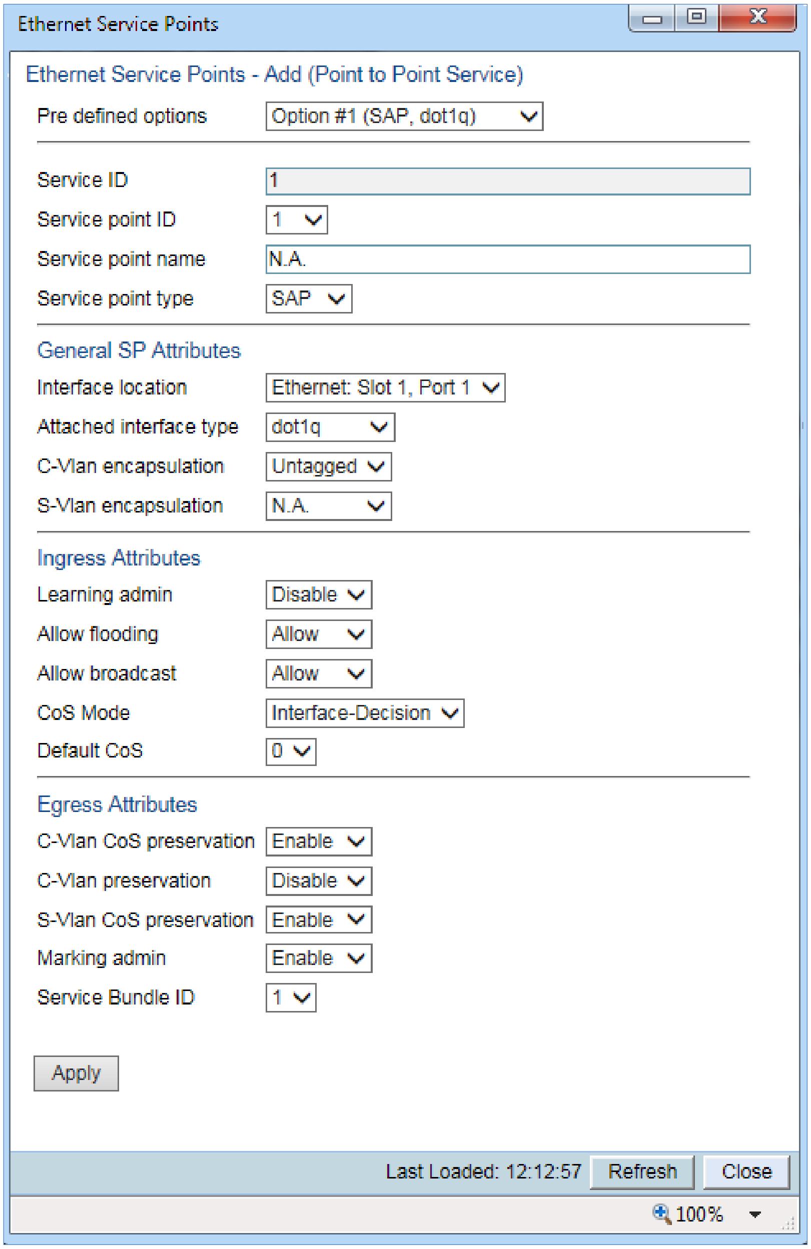
Parameter	Definition
S-Vlan preservation	Read-only. Indicates whether the original S-VLAN ID is preserved or restored for frames egressing from the service point. If S-VLAN preservation is enabled, the S-VLAN ID of frames egressing the service point is the same as the S-VLAN ID when the frame entered the service. If S-VLAN preservation is disabled, the S-VLAN ID of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking
Marking admin	Determines whether re-marking of the outer VLAN (C-VLAN or S-VLAN) of tagged frames that pass through the service point is enabled. If **Marking admin** is set to **Enable**, and CoS preservation for the relevant outer VLAN is set to **Disable**, the SAP re-marks the C-VLAN or S-VLAN 802.1p UP bits of egress frames according to the calculated CoS and Color, and the user-configurable 802.1Q and 802.1AD marking tables. You can configure these tables by selecting **Ethernet > QoS > Marking** from the menu on the left side of the Web EMS. If **Marking admin** and CoS preservation for the relevant outer VLAN are both set to **Enable**, re-marking is not performed. If **Marking admin** and CoS preservation for the relevant outer VLAN are both set to **Disable**, re-marking is applied, but only according to the values defined for Green frames in the 802.1Q and 802.1AD marking tables.
Service Bundle ID	This can be used to assign one of the available service bundles from the H-QoS hierarchy queues to the service point. This enables you to personalize the QoS egress path. Permitted values are 1-63.

Adding a Service Point

To add a service point:

1. Select **Ethernet > Services**. The Ethernet Services page opens (Figure 159).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens (Figure 162).
4. Select the relevant service point in the Ethernet Services Points – General SP Attributes table.
5. Click **Add**. The Ethernet Service Points – Add page opens.

Figure 165 Ethernet Service Points - Add Page



Ethernet Service Points

Ethernet Service Points - Add (Point to Point Service)

Pre defined options	Option #1 (SAP, dot1q)
Service ID	1
Service point ID	1
Service point name	N.A.
Service point type	SAP

General SP Attributes

Interface location	Ethernet: Slot 1, Port 1
Attached interface type	dot1q
C-Vlan encapsulation	Untagged
S-Vlan encapsulation	N.A.

Ingress Attributes

Learning admin	Disable
Allow flooding	Allow
Allow broadcast	Allow
CoS Mode	Interface-Decision
Default CoS	0

Egress Attributes

C-Vlan CoS preservation	Enable
C-Vlan preservation	Disable
S-Vlan CoS preservation	Enable
Marking admin	Enable
Service Bundle ID	1

6. Configure the service point attributes, as described in Table 45, Table 47, and Table 48.

Note

Optionally, you can select from a list of pre-defined service point options in the **Pre defined options** field at the top of the Ethernet Service Points - Add page. The system automatically populates the remaining service point parameters according to the system-defined parameters. However, you can manually change these parameter values. The pre-defined options are customized to the type of service to which you are adding the service point.

7. Click **Apply**, then **Close**.

Editing a Service Point

To edit a service point:

1. Select **Ethernet > Services**. The Ethernet Services page opens (Figure 159).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens (Figure 162).
4. Select the relevant service point in the Ethernet Services Points – General SP Attributes table.
5. Click **Edit**. The Ethernet Service Points– Edit page opens. The Ethernet Service Points – Edit page is similar to the Ethernet Service Points - Add page (Figure 165). You can edit any parameter that can be configured in the Add Service Point page, except **Service Point ID**, **Service Point Type**, and the **General SP Attributes**.
6. Edit the service point attributes, as described in Table 45, Table 47, and Table 48.
7. Click **Apply**, then **Close**.

Deleting a Service Point

You can only delete a service point with an **Attached Interface Type** of **Bundle-C** or **Bundle-S** if no VLANs are attached to the service point. See *Attaching VLANs*.

To delete a service point:

1. Select **Ethernet > Services**. The Ethernet Services page opens (Figure 159).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens (Figure 162).
4. Select the relevant service point in the Ethernet Services Points – General SP Attributes table.
5. Click **Delete**. The service point is deleted.

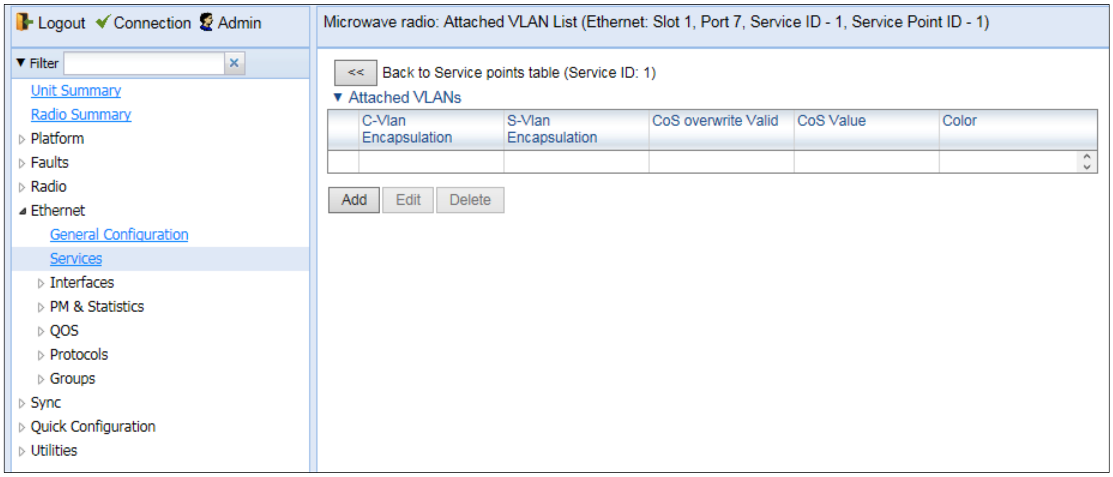
Attaching VLANs

When the Attached Interface Type for a service point is set to Bundle-C or Bundle-S, you can add multiple C-VLANs to the service point.

To add multiple C-VLANs:

1. Select **Ethernet > Services**. The Ethernet Services page opens (Figure 159).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens (Figure 162).
4. Select the relevant service point in the Ethernet Services Points – General SP Attributes table.
5. Click **Attached VLAN**. The Attached VLAN List page opens.

Figure 166 Attached VLAN List Page



Microwave radio: Attached VLAN List (Ethernet: Slot 1, Port 7, Service ID - 1, Service Point ID - 1)

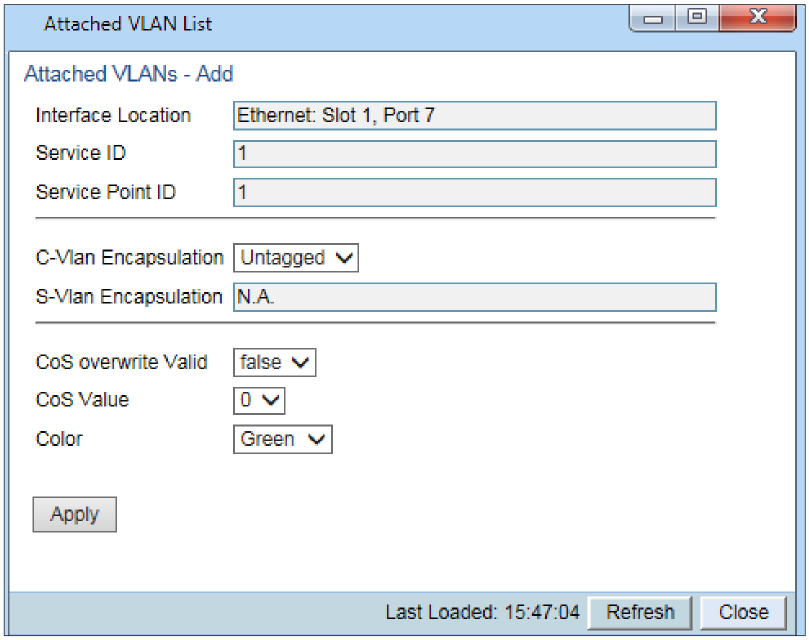
Back to Service points table (Service ID: 1)

Attached VLANs

	C-Vlan Encapsulation	S-Vlan Encapsulation	CoS overwrite Valid	CoS Value	Color

6. Click **Add.** The Attached VLAN List - Add page opens.

Figure 167 Attached VLAN List - Add Page



Attached VLANs - Add

Interface Location	Ethernet: Slot 1, Port 7
Service ID	1
Service Point ID	1
C-Vlan Encapsulation	Untagged
S-Vlan Encapsulation	N.A.
CoS overwrite Valid	false
CoS Value	0
Color	Green

Last Loaded: 15:47:04

7. Configure the VLAN Classification parameters, described in *Table 49*.
8. Click **Apply**, then **Close**.

Table 49 VLAN Classification Parameters

Parameter	Definition
Interface Location	Read-only. The physical or logical interface on which the service point is located.
Service ID	Read-only. The ID of the service to which the service point belongs.
Service Point ID	Read-only. The ID of the service point.

Parameter	Definition
C-Vlan Encapsulation	Select the C-VLAN you want to add to the service point.
S-Vlan Encapsulation	Read-only. If the **Attached Interface Type** for the service point is **Bundle-S**, this field displays the S-VLAN encapsulation selected when the service point was created. If the **Attached Interface Type** for the service point is **Bundle-C**, this field is inactive.
CoS Overwrite Valid	If you want to assign a specific CoS and Color to frames with the C-VLAN or S-VLAN defined in the **C-VLAN Encapsulation** field, select **true**. This CoS and Color values defined below override the CoS and Color decisions made at the interface level. However, if the service point or service are configured to apply their own CoS and Color decisions, those decisions override the decision made here.
CoS Value	If **CoS Overwrite Valid** is set to **true**, the CoS value defined in this field is applied to frames with the C-VLAN defined in the **C-VLAN Encapsulation** field. This CoS overrides the CoS decision made at the interface level. However, if the service point or service are configured to apply their own CoS, that decision overrides the decision made here. If CoS Overwrite Valid is set to false, this parameter has no effect.
Color	If **CoS Overwrite Valid** is set to **true**, the Color value defined in this field is applied to frames with the C-VLAN defined in the **C-VLAN Encapsulation** field. This Color overrides the Color decision made at the interface level. However, if the service point or service are configured to apply their own Color, that decision overrides the decision made here. If **CoS Overwrite Valid** is set to **false**, this parameter has no effect.

To edit a VLAN Classification table entry, select the entry in the VLAN Classification table and click **Edit**. You can edit all the fields that can be configured in the Attached VLAN List – Add page, except the **C-VLAN Encapsulation** field.

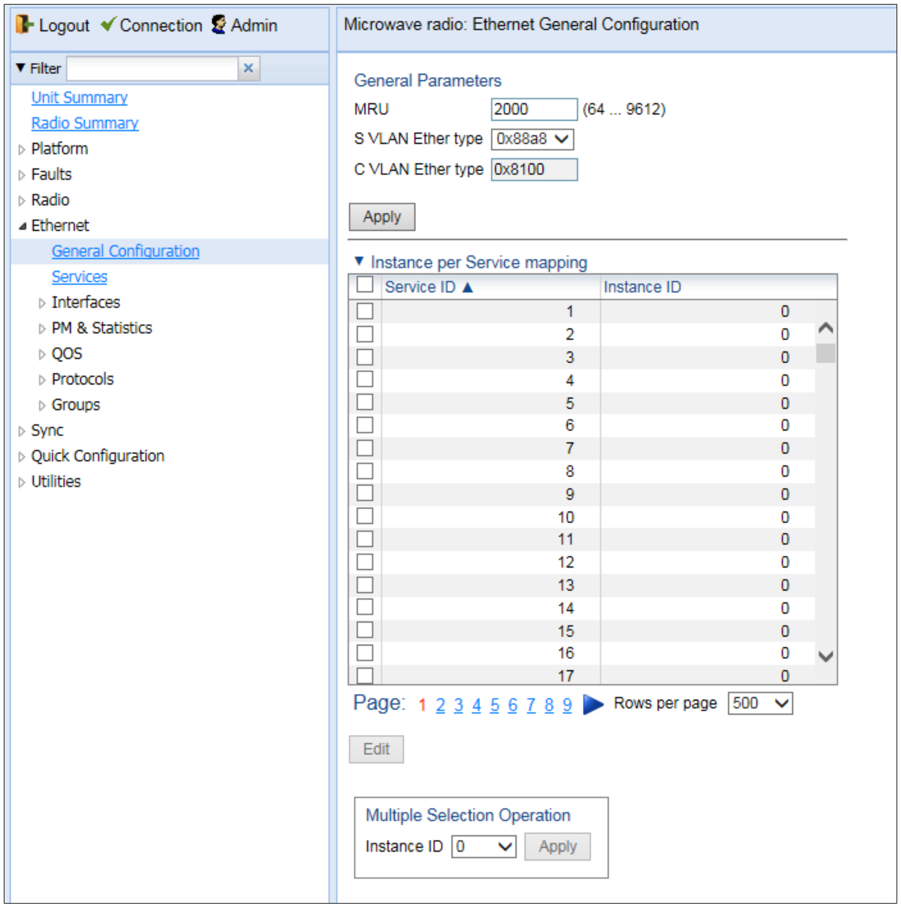
To delete a VLAN Classification table entry, select the entry in the VLAN Classification table and click **Delete**.

Setting the MRU Size and the S-VLAN Ethertype

To configure the size of the MRU (Maximum Receive Unit) and the S-VLAN Ethertype:

1. Select **Ethernet > General Configuration**. The Ethernet General Configuration page opens.

Figure 168 Ethernet General Configuration Page



Microwave radio: Ethernet General Configuration

General Parameters

MRU: 2000 (64 ... 9612)

S VLAN Ether type: 0x88a8

C VLAN Ether type: 0x8100

□	Service ID ▲	Instance ID
□	1	0
□	2	0
□	3	0
□	4	0
□	5	0
□	6	0
□	7	0
□	8	0
□	9	0
□	10	0
□	11	0
□	12	0
□	13	0
□	14	0
□	15	0
□	16	0
□	17	0

Page: 1 2 3 4 5 6 7 8 9 ▶ Rows per page 500

Multiple Selection Operation

Instance ID: 0

2. In the **MRU** field, enter the global size (in bytes) of the Maximum Receive Unit (MRU). Permitted values are 64 to 9612. The default value is 2000. Frames that are larger than the global MRU will be discarded.

3. In the **S VLAN Ether type** field, select the S-VLAN Ethertype. This defines the ethertype recognized by the system as the S-VLAN ethertype. Options are: 0x8100, 0x88A8, 0x9100, and 0x9200. The default value is 0x88A8.

> **Note**
>
> The C-VLAN Ethertype is set at 0x8100 and cannot be modified.

4. Click **Apply**.

Configuring Ethernet Interfaces

Related Topics:

Enabling the Interfaces (Interface Manager)

Performing Ethernet Loopback

Configuring Ethernet Service(s)

Quality of Service (QoS)

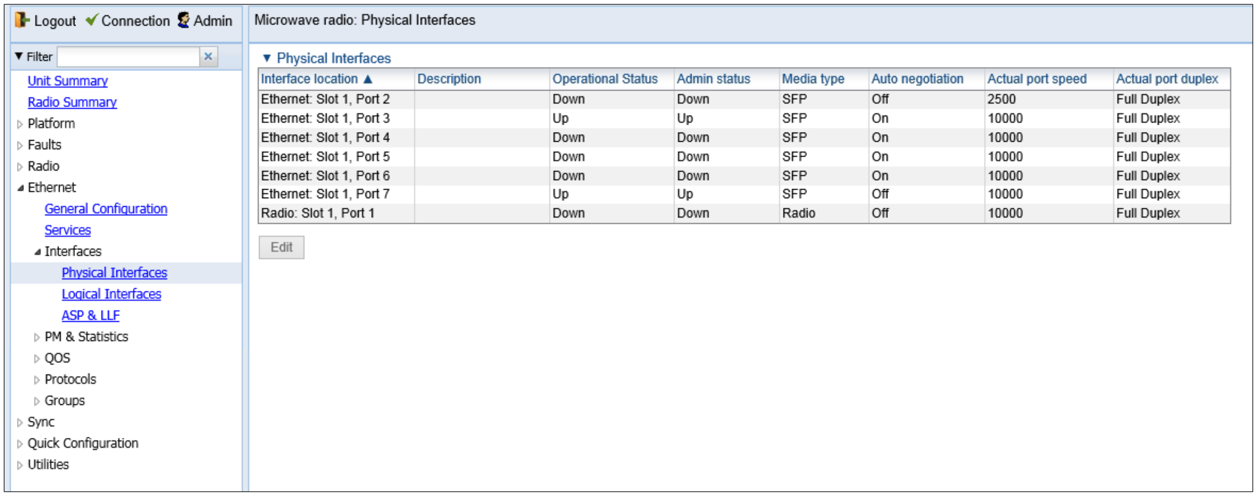
The PTP 850's switching fabric distinguishes between physical interfaces and logical interfaces. Physical and logical interfaces serve different purposes in the switching fabric. In some cases, a physical interface corresponds to a logical interface on a one-to-one basis. For some features, such as LAG, a group of physical interfaces can be joined into a single logical *interface.*

The basic interface characteristics, such as media type, port speed, duplex, and auto-negotiation, are configured for the physical interface via the Physical Interfaces page. Ethernet services, QoS, and OAM characteristics are configured on the logical interface level.

To configure the physical interface parameters:

1. Select **Ethernet > Interfaces > Physical Interfaces**. The Physical Interfaces page opens.

Figure 169 Physical Interfaces Page



Microwave radio: Physical Interfaces

▼ Physical Interfaces

Interface location ▲	Description	Operational Status	Admin status	Media type	Auto negotiation	Actual port speed	Actual port duplex
Ethernet: Slot 1, Port 2		Down	Down	SFP	Off	2500	Full Duplex
Ethernet: Slot 1, Port 3		Up	Up	SFP	On	10000	Full Duplex
Ethernet: Slot 1, Port 4		Down	Down	SFP	On	10000	Full Duplex
Ethernet: Slot 1, Port 5		Down	Down	SFP	On	10000	Full Duplex
Ethernet: Slot 1, Port 6		Down	Down	SFP	On	10000	Full Duplex
Ethernet: Slot 1, Port 7		Up	Up	SFP	Off	10000	Full Duplex
Radio: Slot 1, Port 1		Down	Down	Radio	Off	10000	Full Duplex

If an alarm is currently raised on an interface, an alarm icon appears to the left of the interface location. For example, in *Figure 169*, an alarm is raised on the Radio interface. To display details about the alarm or alarms in tooltip format, hover the mouse over the alarm icon.

Note

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

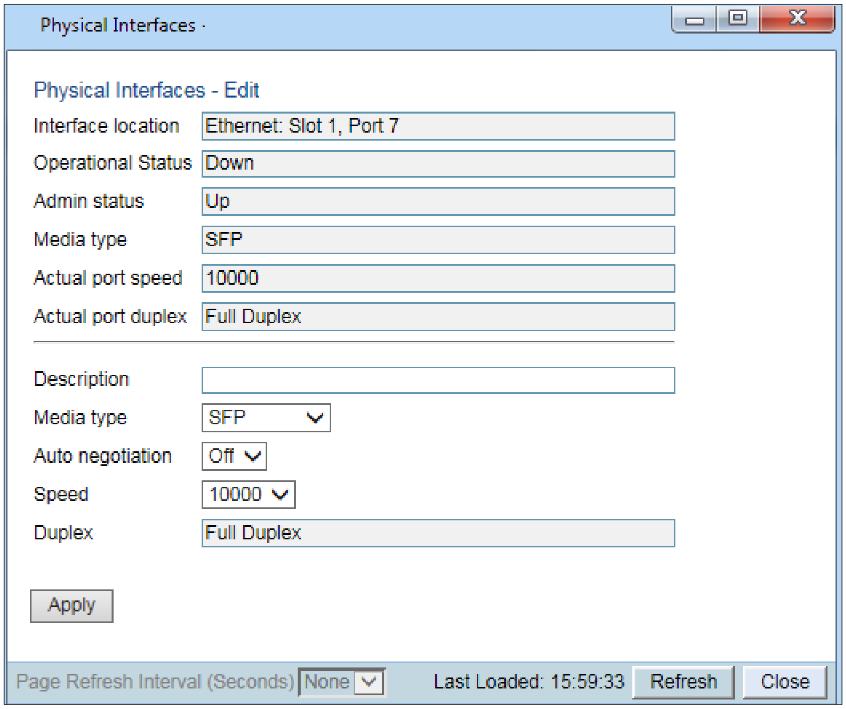
The QSFP port (Port 4) is displayed as follows.

In a 4x1/10G configuration the QSFP port can provide four Ethernet interfaces: Eth3, Eth4, Eth 5, and Eth6. In this configuration, a QSFP transceiver is attached to the QSFP port, and an MPO-MPO cable is connected between the transceiver and a splitter on the other side of the link. The splitter splits the traffic between four Ethernet cables connecting the splitter to the customer equipment.

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

7. Select the interface you want to configure and click **Edit**. The Physical Interfaces - Edit page opens.

Figure 170 Physical Interfaces - Edit Page



Physical Interfaces - Edit

Interface location	Ethernet: Slot 1, Port 7
Operational Status	Down
Admin status	Up
Media type	SFP
Actual port speed	10000
Actual port duplex	Full Duplex
Description	
Media type	SFP
Auto negotiation	Off
Speed	10000
Duplex	Full Duplex

8. Optionally, in the **Description** field, enter a description of the interface.
9. In the **Media type** field, select the physical interface layer 1 media type. Options are:
   - ○ **Auto-Type** – NA.
   - ○ **RJ45** – An electrical (RJ-45) Ethernet interface.
   - ○ **SFP** – An optical (SFP) Ethernet interface.
   - ○ **Radio** – A radio interface.
10. In the **Auto negotiation** field, select **On** to enable or **Off** to disable Auto-Negotiation. When the Media-Type is **Radio**, Auto Negotiation is always **Off**.
    a. For Ethernet interfaces, the default value is **Off**:
       i. For Ports 3 to 6 (the QSFP ports), **Off** is the only supported value.
       ii. For Port 7 if the Speed is set to 10000 (10G), Auto Negotiation is not available, and the setting must remain **Off**. If the speed is set to 1000 (1G), **Auto negotiation** can be set to **Off** (default) or **On**.
11. In the **Speed** field, select the maximum speed of the interface in Mbps. Options are:

- Ethernet RJ-45 interfaces –**100** and **1000.**
- Ethernet SFP interfaces – Only **1000**is supported.
- Ethernet SFP+ and QSFP interfaces – Only **1000** and **10000** are supported.
- Radio interfaces – The parameter is read-only and set by the system to **1000FD**.

> **Note**
>
> After changing the speed of an SFP+ interface, you must reset the unit in order for the change to take effect.

12. In the **Duplex** field, select the interface's duplex setting (**Full-Duplex** or **Half-Duplex**). Only Full-Duplex is available in this release.
13. Click **Apply**, then **Close**.

The following tables summarize the Speed and Auto-Negotiation options for the Ethernet traffic ports.

Table 50 Ethernet Interface Speed and Auto-Negotiation Options – PTP 850C

Interface	Physical Port Number	Notes	Speed (Mbps)	Auto-Negotiation
Eth 1	P2	RJ-45	1000/2500/10000	On
Eth 2	P3	SFP	2500	Depends on speed.
Eth 3	P4	SFP+	1000/10000	Off

Table 51 Ethernet Interface Speed and Auto-Negotiation Options – PTP 850S

Interface	Physical Port Number	Notes	Speed (Mbps)	Auto-Negotiation
Eth 1	P3	SFP+	1000/10000	On/Off
Eth2	P2	SFP/CSFP	100/1000	Off only
Eth3	P3	Only available with CSFP.	100/1000	Off only

Table 52 Ethernet Interface Speed and Auto-Negotiation Options – PTP 850E

Interface	Physical Port Number	Notes	Speed (Mbps)	Auto-Negotiation
Eth 2	P3	P3. Multiband interface (SFP). Only supported for PTP 850E.	1000	Off only
Eth3	P4	QSFP.	1000/10000/40000	Off only
Eth4	P4	QSFP. Only available with QSFP transceiver in P4.	1000/10000	Off only

Eth5	P4	QSFP. Only available with QSFP transceiver in P4.	1000/10000	Off only

Table 53 describes the status parameters that appear in the Physical Interfaces page.

Table 53 Physical Interface Status Parameters

Parameter	Definition
Interface location	The location of the interface.
Operational Status	Indicates whether the interface is currently operational (**Up**) or non-operational (**Down**).
Admin Status	Indicates whether the interface is currently enabled (**Up**) or disabled (**Down**). You can enable or disable an interface from the Interface Manager page. See *Enabling the Interfaces (Interface Manager)*.
Media Type	The physical interface layer 1 media type.
Actual port speed	Displays the actual speed of the interface for the link as agreed by the two sides of the link after the auto negotiation process.
Actual port duplex	Displays the actual duplex status of the interface for the link as agreed by the two sides of the link after the auto negotiation process.

Configuring Automatic State Propagation and Link Loss Forwarding

Automatic state propagation enables propagation of radio failures back to the Ethernet port. You can also configure Automatic State Propagation to close the Ethernet port based on a radio failure at the remote carrier.

Automatic state propagation is configured as pairs of interfaces. Each interface pair includes one Monitored Interface and one Controlled Interface. You can create multiple pairs using the same monitored interface and multiple controlled interfaces.

The Monitored Interface is a radio interface, or a radio protection or Multi-Carrier ABC group. The Controlled Interface is an Ethernet interface or LAG. An Ethernet interface can only be assigned to one Monitored interface.

Each Controlled Interface is assigned an LLF ID. If **ASP trigger by remote fault** is enabled on the remote side of the link, the ASP state of the Controlled Interface is propagated to the Controlled Interface with the same LLF ID at the remote side of the link. This means if ASP is triggered locally, it is propagated to the remote side of the link, but only to Controlled Interfaces with LLF IDs that match the LLF IDs of the affected Controlled Interfaces on the local side of the link.

Note

LLF requires an activation key (SL-LLF). Without this activation key, only LLF ID 1 is available.

The following events in the Monitored Interface trigger ASP:

Radio LOF

Radio Excessive BER

Radio LOC

Remote Radio LOF

Remote Excessive BER

Remote LOC

The user can also configure the ASP pair so that Radio LOF, Radio Excessive BER, or loss of the Ethernet connection at the remote side of the link will also trigger ASP.

In addition, ASP is triggered if the Controlled Interface is a LAG, and the physical interfaces that belong to the LAG are set to **Admin = Down** in the Interface Manager.

When a triggering event takes place:

If the Controlled Interface is an electrical GbE port, the port is closed.

If the Controlled Interface is an optical GbE port, the port is muted.

The Controlled Interface remains closed or muted until all triggering events are cleared.

In addition, when a local triggering event takes place, the ASP mechanism sends an indication to the remote side of the link. Even when no triggering event has taken place, the ASP mechanism sends periodic update messages indicating that no triggering event has taken place.

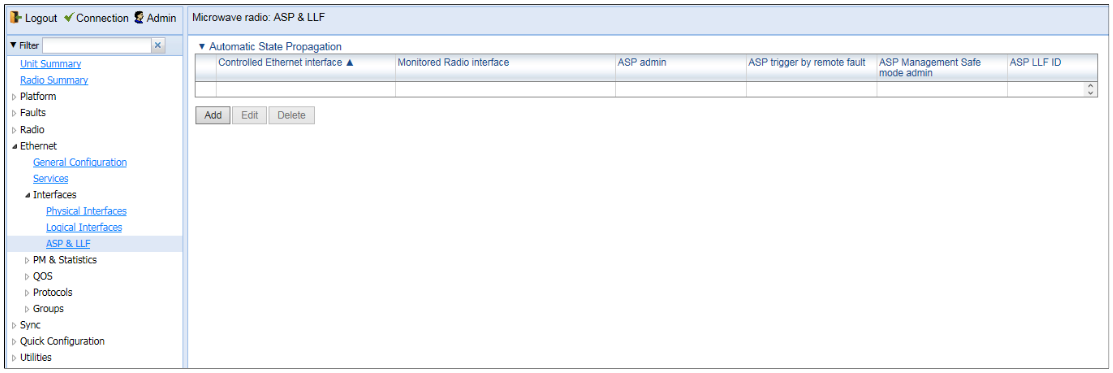
A trigger delay time can be configured, so that when a triggering event takes place, the ASP mechanism does not propagate the event until this delay time has elapsed. A trigger delay from 0 to 10,000 ms can be set per LLD ID. The delay time must be configured via CLI. See Configuring Automatic State Propogation and Link Loss Forwarding (CLI).

It is recommended to configure both ends of the link to the same Automatic State Propagation configuration.

To configure an Automatic State Propagation interface pair:

1. Select **Ethernet > Interfaces > Automatic State Propagation**. The Automatic State Propagation page opens.

Figure 171 Automatic State Propagation Page



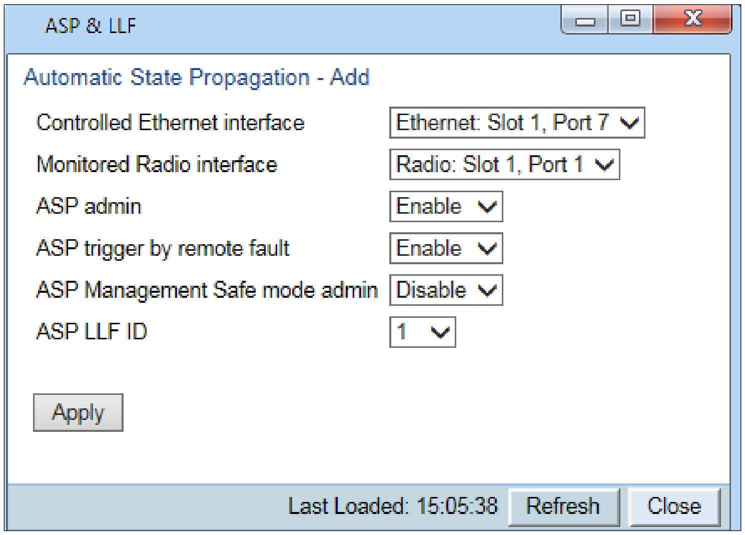
Microwave radio: ASP & LLF

Automatic State Propagation

Controlled Ethernet interface ▲	Monitored Radio interface	ASP admin	ASP trigger by remote fault	ASP Management Safe mode admin	ASP LLF ID

2. Click **Add**. The Automatic State Propagation - Add page opens.

Figure 172 Automatic State Propagation - Add Page



Automatic State Propagation - Add

Controlled Ethernet interface	Ethernet: Slot 1, Port 7
Monitored Radio interface	Radio: Slot 1, Port 1
ASP admin	Enable
ASP trigger by remote fault	Enable
ASP Management Safe mode admin	Disable
ASP LLF ID	1

Last Loaded: 15:05:38

3. In the **Controlled Ethernet interface** field, select an interface that will be disabled upon failure of the Monitored Radio Interface, defined below.

4. In the **Monitored Radio interface** field, select the Monitored Radio Interface. The Controlled Ethernet Interface, defined above, is disabled upon a failure indication on the Monitored Radio Interface.
5. In the **ASP admin** field, select **Enable** to enable Automatic State Propagation on the interface pair, or **Disable** to disable Automatic State Propagation on the pair.
6. Optionally, in the**ASP trigger by remote fault** field, select **Enable** if you want to configure the system to disable the Controlled Ethernet Interface upon a radio failure at the remote side of the link from the Monitored Radio Interface. ASP events will only be propagated to Controlled Interfaces with LLF IDs that match LLF IDs of affected Controlled Interfaces at the other side of the link.
7. Optionally, in the **ASP Management Safe mode admin** field, select **Enable** or **Disable** to enable or disable ASP Management Safe mode. In ASP Management Safe mode, the ASP mechanism does not physically shut down the Controlled Interface when ASP is triggered. Instead, the ASP mechanism sends a failure indication message. This message is used to propagate the failure indication to external equipment.
8. In the **ASP LLF ID** field, select an ID for Link Loss Forwarding (LLF). When **ASP trigger by remote fault** is set to **Enable**, ASP events at the other side of the link are propagated to Controlled Interfaces with LLF IDs that match the LLF IDs of affected Controlled Interfaces at the other side of the link. LLF IDs are unique per Monitored Interface. That is, if LLF ID 1 has been used for a Controlled Interface that is grouped with radio interface 1, that ID cannot be used again for another Controlled Interface grouped fixed radio interface 1. However, it *can* be used for Controlled Interface grouped with radio interface 2. You can select an LLF ID between 1 and 30.
9. Repeat this procedure to assign additional Controlled Interfaces to the Monitored Interface, or to set up additional ASP pair with other interfaces. Controlled Interfaces can only be assigned to one ASP pair. Monitored Interfaces can be assigned to multiple ASP pairs.

To edit an Automatic State Propagation interface pair:

1. Select the interface pair in the Automatic state propagation configuration table.
2. Click **Edit**. The Automatic State Propagation – Edit page opens. The Edit page is similar to the Add page (Figure 172), but the **Controlled Ethernet Interface** and **Monitored Radio Interface** parameters are read-only.

To delete an Automatic State Propagation interface pair:

1. Select the interface pair in the Automatic state propagation configuration table.
2. Click **Delete.** The interface pair is removed from the Automatic state propagation configuration table.

To delete multiple interface pairs:

1. Select the interface pairs in the Automatic state propagation configuration table or select all the interfaces by selecting the check box in the top row.
2. Click **Delete.** The interface pairs are removed from the Automatic state propagation configuration table.

Viewing Ethernet PMs and Statistics

PTP 850 stores and displays statistics in accordance with RMON and RMON2 standards. You can display various peak TX and RX rates (per second) and average TX and RX rates (per second), both in bytes and in packets, for each measured time interval. You can also display the number of seconds in the interval during which TX and RX rates exceeded the configured threshold.

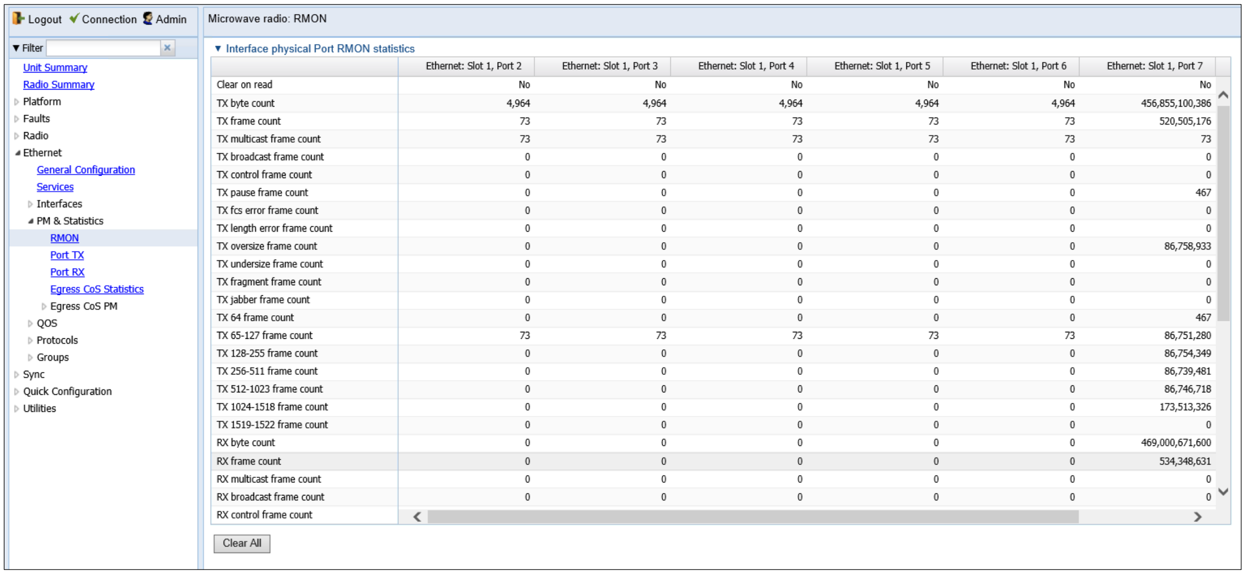
This section includes:

RMON Statistics

To view and reset RMON statistics:

1. Select **Ethernet > PM & Statistics > RMON**. The RMON page opens.

Figure 173 RMON Page



Microwave radio: RMON

▼ Interface physical Port RMON statistics

	Ethernet: Slot 1, Port 2	Ethernet: Slot 1, Port 3	Ethernet: Slot 1, Port 4	Ethernet: Slot 1, Port 5	Ethernet: Slot 1, Port 6	Ethernet: Slot 1, Port 7
Clear on read	No	No	No	No	No	No
TX byte count	4,964	4,964	4,964	4,964	4,964	456,855,100,386
TX frame count	73	73	73	73	73	520,505,176
TX multicast frame count	73	73	73	73	73	73
TX broadcast frame count	0	0	0	0	0	0
TX control frame count	0	0	0	0	0	0
TX pause frame count	0	0	0	0	0	467
TX fcs error frame count	0	0	0	0	0	0
TX length error frame count	0	0	0	0	0	0
TX oversize frame count	0	0	0	0	0	86,758,933
TX undersize frame count	0	0	0	0	0	0
TX fragment frame count	0	0	0	0	0	0
TX jabber frame count	0	0	0	0	0	0
TX 64 frame count	0	0	0	0	0	467
TX 65-127 frame count	73	73	73	73	73	86,751,280
TX 128-255 frame count	0	0	0	0	0	86,754,349
TX 256-511 frame count	0	0	0	0	0	86,739,481
TX 512-1023 frame count	0	0	0	0	0	86,746,718
TX 1024-1518 frame count	0	0	0	0	0	173,513,326
TX 1519-1522 frame count	0	0	0	0	0	0
RX byte count	0	0	0	0	0	469,000,671,600
RX frame count	0	0	0	0	0	534,348,631
RX multicast frame count	0	0	0	0	0	0
RX broadcast frame count	0	0	0	0	0	0
RX control frame count						

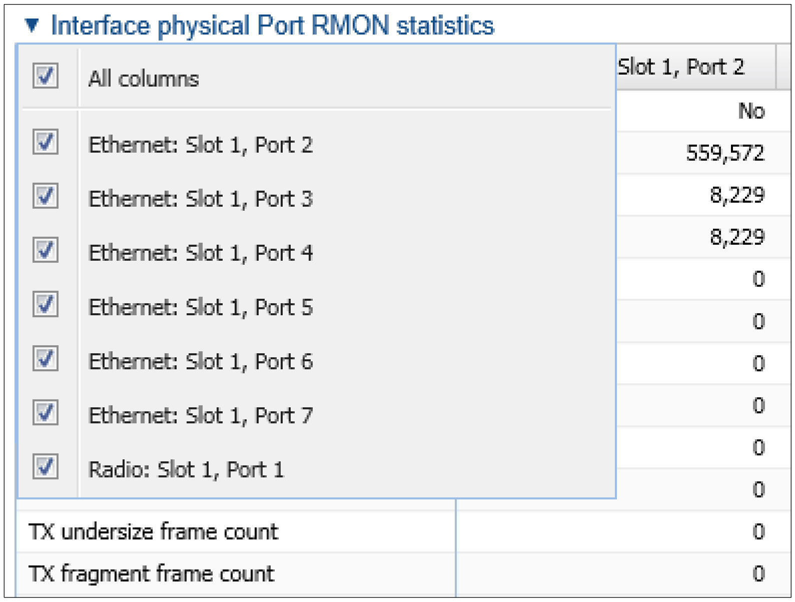
To clear the statistics, click **Clear All** at the bottom of the page.

To refresh the statistics, click **Refresh** at the bottom of the page.

Each column in the RMON page displays RMON statistics for one of the unit's interfaces. To hide or display columns:

1. Click the arrow next to the table title (**Interface Physical Port RMON Statistics**).
2. Mark the interfaces you want to display and clear the interfaces you do not want to display.

Figure 174 RMON Page – Hiding and Displaying Columns



▼ Interface physical Port RMON statistics

☑ All columns

☑ Ethernet: Slot 1, Port 2

☑ Ethernet: Slot 1, Port 3

☑ Ethernet: Slot 1, Port 4

☑ Ethernet: Slot 1, Port 5

☑ Ethernet: Slot 1, Port 6

☑ Ethernet: Slot 1, Port 7

☑ Radio: Slot 1, Port 1

	Slot 1, Port 2
	No
	559,572
	8,229
	8,229
	0
	0
	0
	0
	0
	0
TX undersize frame count	0
TX fragment frame count	0

Note

If you click the table title itself, all columns are hidden. To un-hide the columns, click the table title again.

Egress CoS Statistics

You can display packet egress statistics per CoS value. For each CoS value, the following statistics are displayed per Color (Green and Yellow):

Number of packets transmitted

Number of packets dropped

Number of bytes transmitted

Number of bytes dropped

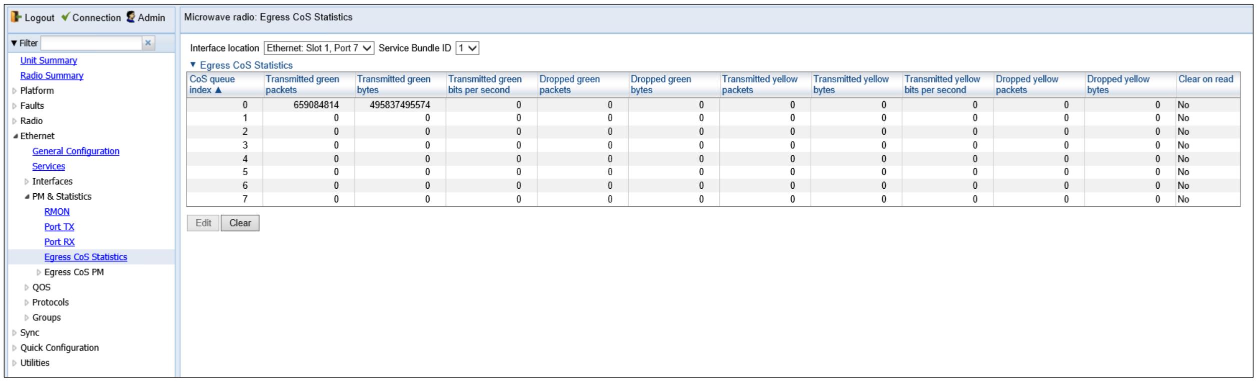
Note

Transmitted bits per second are not supported in the current release.

To display egress CoS statistics:

1. Select **Ethernet > PM & Statistics > Egress CoS Statistics**. The Egress CoS Statistics page opens.

Figure 175 Egress Cos Statistics Page



Microwave radio: Egress CoS Statistics

Interface location Ethernet: Slot 1, Port 7 Service Bundle ID 1

▼ Egress CoS Statistics

CoS queue index ▲	Transmitted green packets	Transmitted green bytes	Transmitted green bits per second	Dropped green packets	Dropped green bytes	Transmitted yellow packets	Transmitted yellow bytes	Transmitted yellow bits per second	Dropped yellow packets	Dropped yellow bytes	Clear on read
0	659084814	495837495574	0	0	0	0	0	0	0	0	No
1	0	0	0	0	0	0	0	0	0	0	No
2	0	0	0	0	0	0	0	0	0	0	No
3	0	0	0	0	0	0	0	0	0	0	No
4	0	0	0	0	0	0	0	0	0	0	No
5	0	0	0	0	0	0	0	0	0	0	No
6	0	0	0	0	0	0	0	0	0	0	No
7	0	0	0	0	0	0	0	0	0	0	No

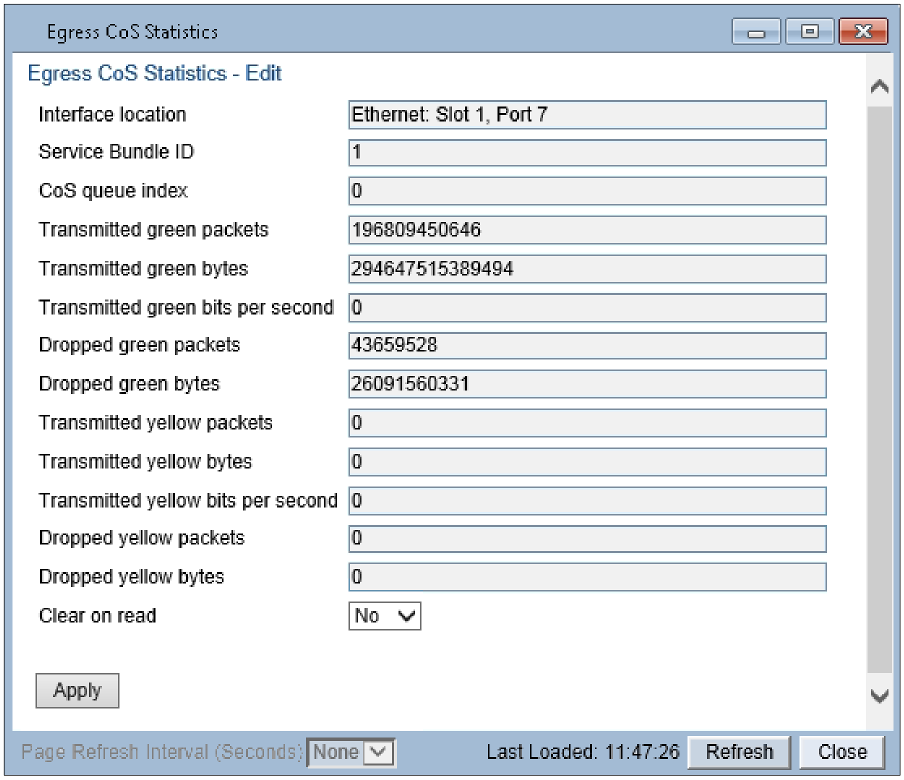
2. In the **Show Service bundle ID** field, select 1.

> **Note**
>
> Service Bundles are bundles of queues, grouped together in order to configure common egress characteristics for specific services. In the current release, only Service Bundle 1 is supported.

By default, the egress CoS statistics are cumulative. That is, they are not automatically cleared. You can set each individual CoS number to be cleared whenever the Egress CoS Statistics page is opened by changing the Clear on read value to **Yes.**

1. To change the clear on read value, select the CoS number in the CoS queue index column and click **Edit.** The Egress CoS Statistics – Edit page opens.

Figure 176 Egress CoS Statistics – Edit Page



Egress CoS Statistics - Edit

Interface location	Ethernet: Slot 1, Port 7
Service Bundle ID	1
CoS queue index	0
Transmitted green packets	196809450646
Transmitted green bytes	294647515389494
Transmitted green bits per second	0
Dropped green packets	43659528
Dropped green bytes	26091560331
Transmitted yellow packets	0
Transmitted yellow bytes	0
Transmitted yellow bits per second	0
Dropped yellow packets	0
Dropped yellow bytes	0
Clear on read	No

Page Refresh Interval (Seconds): None

Last Loaded: 11:47:26

2. In the **Clear on read** field, select **Yes** to have statistics for the CoS value cleared every time you open the page.
3. Click **Apply**.

Port TX Statistics

The Ethernet Port TX PM report page displays PMs that measure various peak transmission rates (per second) and average transmission rates (per second), both in bytes and in packets, for each measured time interval.

The page also displays the number of seconds in the interval during which transmission rates exceeded the configured threshold.

This section includes:

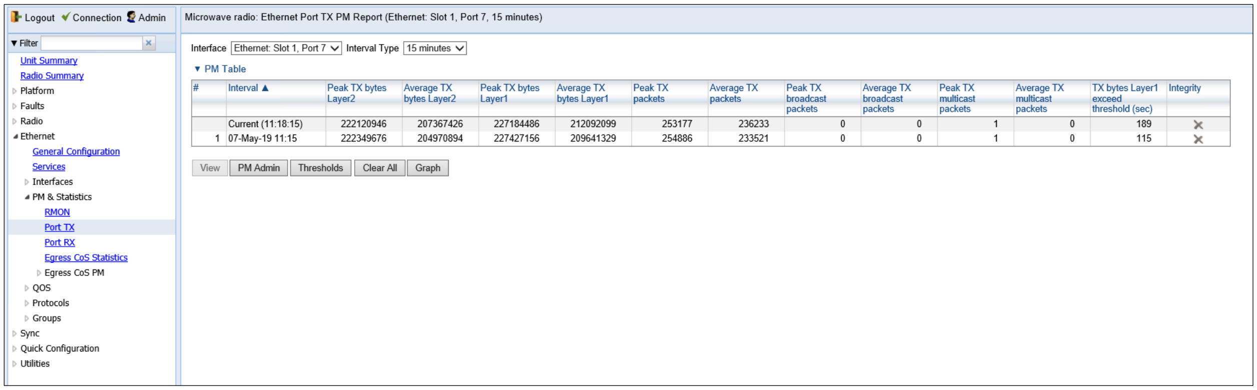
- Displaying Ethernet Port TX PMs
- Enabling or Disabling Gathering of Port TX PM Statistics per Interface
- Setting the Ethernet Port TX Threshold

Displaying Ethernet Port TX PMs

To display Ethernet Port TX PMs:

1. Select **Ethernet > PM & Statistics > Port TX**. The Ethernet Port TX PM Report page opens.

Figure 177 Ethernet Port TX PM Report Page



Microwave radio: Ethernet Port TX PM Report (Ethernet: Slot 1, Port 7, 15 minutes)

Interface: Ethernet: Slot 1, Port 7 Interval Type: 15 minutes

PM Table

#	Interval ▲	Peak TX bytes Layer2	Average TX bytes Layer2	Peak TX bytes Layer1	Average TX bytes Layer1	Peak TX packets	Average TX packets	Peak TX broadcast packets	Average TX broadcast packets	Peak TX multicast packets	Average TX multicast packets	TX bytes Layer1 exceed threshold (sec)	Integrity
	Current (11:18:15)	222120946	207367426	227184486	212092099	253177	236233	0	0	1	0	189	✕
1	07-May-19 11:15	222349676	204970894	227427156	209641329	254886	233521	0	0	1	0	115	✕

2. In the **Interface** field, select the interface for which you want to display PMs.
3. In the **Interval Type** field:
   - To display reports for the past 24 hours, in 15 minute intervals, select **15 minutes**.
   - To display reports for the past month, in daily intervals, select **24 hours**.

Table 54 describes the Ethernet TX port PMs.

Table 54 Ethernet TX Port PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Peak... Average... bytes... Packets...	Various peak transmission rates (per second) and average transmission rates (per second), both in bytes and in packets, for each measured time interval.
TX bytes Layer 1 exceed threshold (sec)	The number of seconds the TX bytes exceeded the specified threshold during the interval. For instructions on setting the threshold, see Setting the Ethernet Port TX Threshold.
Invalid data flag	Indicates whether the values received during the measured interval are valid. An x in the column indicates that the values are not valid (for example, because of a power surge or power failure that occurred during the interval).

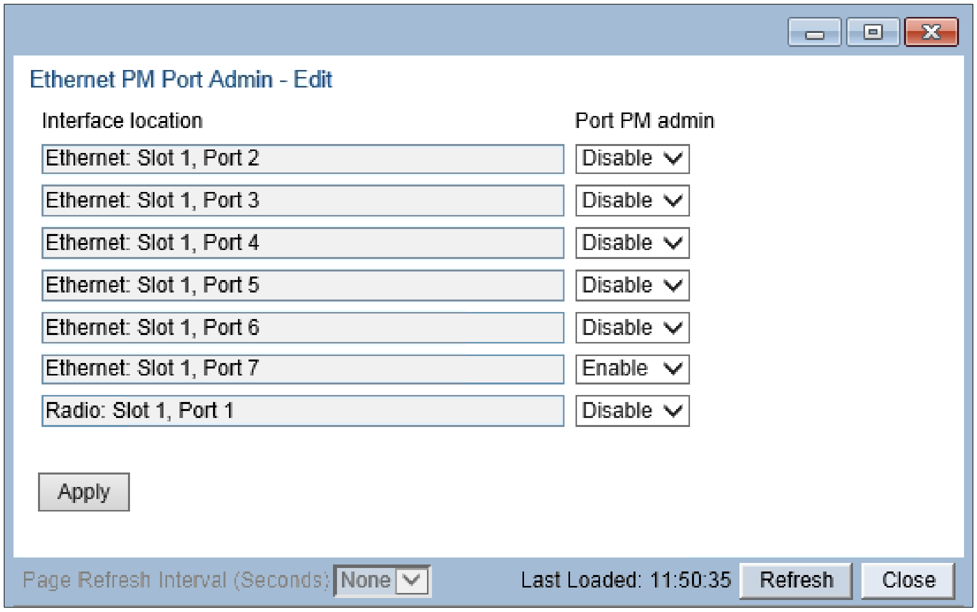
To clear the PMs, click **Clear All**.

Enabling or Disabling Gathering of Port TX PM Statistics per Interface

To select the interfaces for which to gather and display Port TX PMs:

1. In the Ethernet Port TX PM Report page, click **PM Admin**. The Ethernet PM Port Admin page opens.

Figure 178 Ethernet PM Port Admin Page



Ethernet PM Port Admin - Edit

Interface location	Port PM admin
Ethernet: Slot 1, Port 2	Disable
Ethernet: Slot 1, Port 3	Disable
Ethernet: Slot 1, Port 4	Disable
Ethernet: Slot 1, Port 5	Disable
Ethernet: Slot 1, Port 6	Disable
Ethernet: Slot 1, Port 7	Enable
Radio: Slot 1, Port 1	Disable

Page Refresh Interval (Seconds): None

Last Loaded: 11:50:35

2. Select the interface.
3. Click **Enable Port PM** or **Disable Port PM** to enable or disable the gathering of Port TX PMs on the selected interface.
4. Click **Close**.

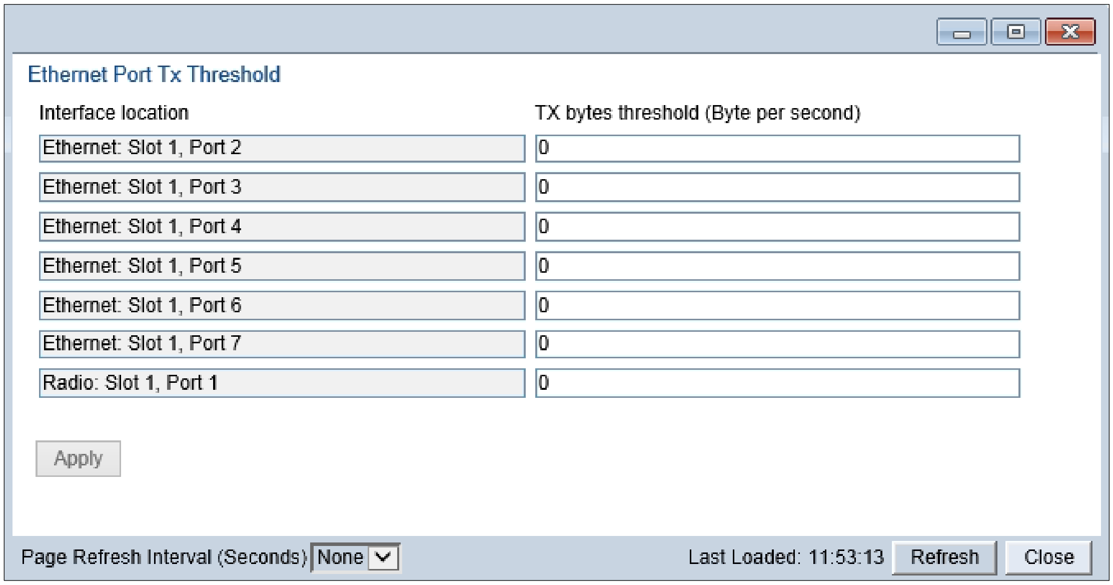
Setting the Ethernet Port TX Threshold

The **TX bytes Layer 1 exceed threshold (sec)** column shows, for each interval, the number of seconds the TX bytes exceeded the specified threshold during the interval:

To view and set this threshold:

1. In the Ethernet Port TX PM Report page, click **Threshold**. The Ethernet Port Tx Threshold page opens.

Figure 179 Ethernet Port Tx Threshold Page



Ethernet Port Tx Threshold

Interface location	TX bytes threshold (Byte per second)
Ethernet: Slot 1, Port 2	0
Ethernet: Slot 1, Port 3	0
Ethernet: Slot 1, Port 4	0
Ethernet: Slot 1, Port 5	0
Ethernet: Slot 1, Port 6	0
Ethernet: Slot 1, Port 7	0
Radio: Slot 1, Port 1	0

Page Refresh Interval (Seconds) None

Last Loaded: 11:53:13

2. Enter a threshold, between 0 and 4294967295.
3. Click **Apply**, then **Close**.

Port RX Statistics

The Ethernet Port RX PM report page displays PMs that measure various peak transmission rates (per second) and average RX rates (per second), both in bytes and in packets, for each measured time interval.

The page also displays the number of seconds in the interval during which RX rates exceeded the configured threshold.

This section includes:

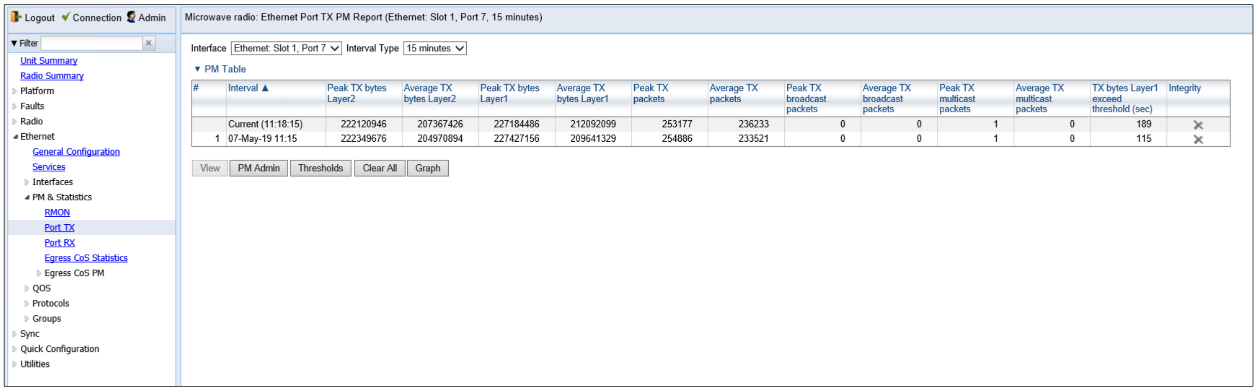
- Displaying Ethernet Port RX PMs
- Enabling or Disabling Gathering of Port RX PM Statistics per Interface
- Setting the Ethernet Port RX Threshold

Displaying Ethernet Port RX PMs

To display Ethernet Port RX PMs:

1. Select **Ethernet > PM & Statistics > Port RX**. The Ethernet Port RX PM Report page opens.

Figure 180: Ethernet Port RX PM Report Page



Microwave radio: Ethernet Port TX PM Report (Ethernet: Slot 1, Port 7, 15 minutes)

Interface: Ethernet: Slot 1, Port 7 Interval Type: 15 minutes

PM Table

#	Interval ▲	Peak TX bytes Layer2	Average TX bytes Layer2	Peak TX bytes Layer1	Average TX bytes Layer1	Peak TX packets	Average TX packets	Peak TX broadcast packets	Average TX broadcast packets	Peak TX multicast packets	Average TX multicast packets	TX bytes Layer1 exceed threshold (sec)	Integrity
	Current (11:18:15)	222120946	207367426	227184486	212092099	253177	236233	0	0	1	0	189	✕
1	07-May-19 11:15	222349676	204970894	227427156	209641329	254886	233521	0	0	1	0	115	✕

2. In the **Interface** field, select the interface for which you want to display PMs.
3. In the **Interval Type** field:
   - To display reports for the past 24 hours, in 15 minute intervals, select **15 minutes**.
   - To display reports for the past month, in daily intervals, select **24 hours**.

Table 55 describes the Ethernet RX port PMs.

Table 55 Ethernet RX Port PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Peak... Average... bytes... Packets...	Various peak transmission rates (per second) and average RX rates (per second), both in bytes and in packets, for each measured time interval.
RX bytes Layer 1 exceed threshold (sec)	The number of seconds the RX bytes exceeded the specified threshold during the interval. For instructions on setting the threshold, see Setting the Ethernet Port RX Threshold.
Invalid data flag	Indicates whether the values received during the measured interval are valid. An x in the column indicates that the values are not valid (for example, because of a power surge or power failure that occurred during the interval).

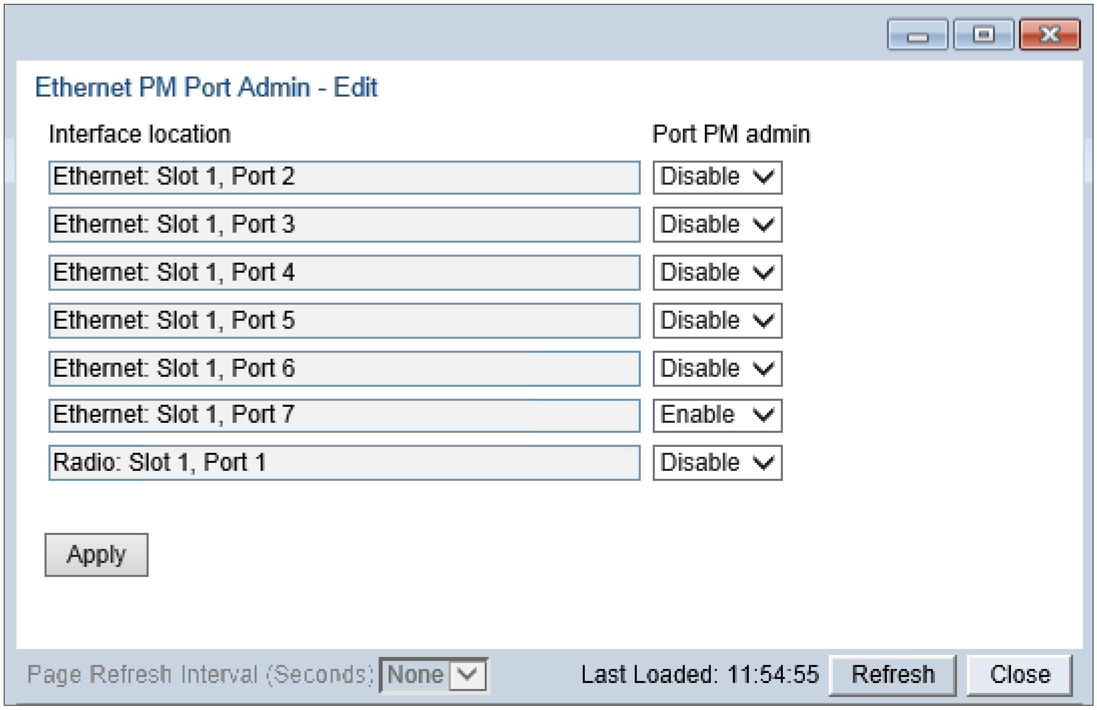
To clear the PMs, click **Clear All**.

Enabling or Disabling Gathering of Port RX PM Statistics per Interface

To select the interfaces for which to gather and display Port RX PMs:

1. In the Ethernet Port RX PM Report page, click **PM Admin**. The Ethernet PM Port Admin page opens.

Figure 181 Ethernet PM Port Admin Page



Ethernet PM Port Admin - Edit

Interface location	Port PM admin
Ethernet: Slot 1, Port 2	Disable
Ethernet: Slot 1, Port 3	Disable
Ethernet: Slot 1, Port 4	Disable
Ethernet: Slot 1, Port 5	Disable
Ethernet: Slot 1, Port 6	Disable
Ethernet: Slot 1, Port 7	Enable
Radio: Slot 1, Port 1	Disable

Page Refresh Interval (Seconds): None

Last Loaded: 11:54:55

2. In the field to the right of the interface, select **Enable** or **Disable** to enable or disable the gathering of Port PMs on the interface.
3. Click **Close**.

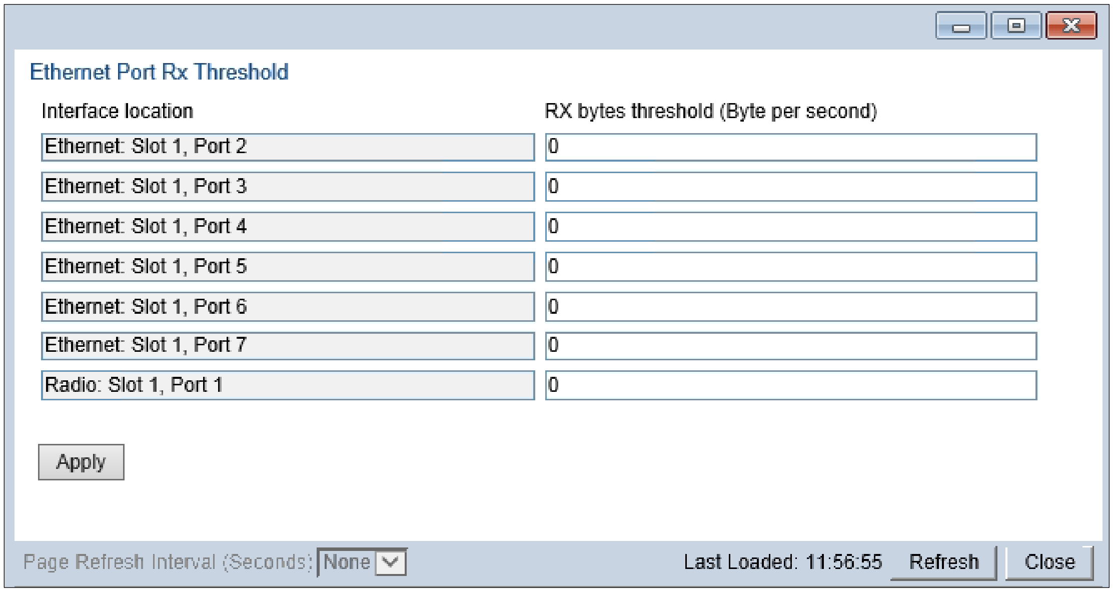
Setting the Ethernet Port RX Threshold

The **RX bytes Layer 1 exceed threshold (sec)** column shows for each interval, the number of seconds the RX bytes exceeded the specified threshold during the interval:

To view and set this threshold:

1. In the Ethernet Port RX PM Report page, click **Threshold**. The Ethernet Port Rx Threshold page opens.

Figure 182 Ethernet Port Rx Threshold Page



Ethernet Port Rx Threshold

Interface location	RX bytes threshold (Byte per second)
Ethernet: Slot 1, Port 2	0
Ethernet: Slot 1, Port 3	0
Ethernet: Slot 1, Port 4	0
Ethernet: Slot 1, Port 5	0
Ethernet: Slot 1, Port 6	0
Ethernet: Slot 1, Port 7	0
Radio: Slot 1, Port 1	0

2. For each interface, you can enter a threshold, in bytes per second, between 0 and 4294967295.
3. Click **Apply**, then **Close**.

Chapter 10: Quality of Service (QoS)

This section includes:

- QoS Overview
- Configuring Classification
- Configuring Policers (Rate Metering)
-

- Configuring Marking
- Configuring WRED
- Configuring Scheduling
- Configuring and Displaying Queue-Level PMs

QoS Overview

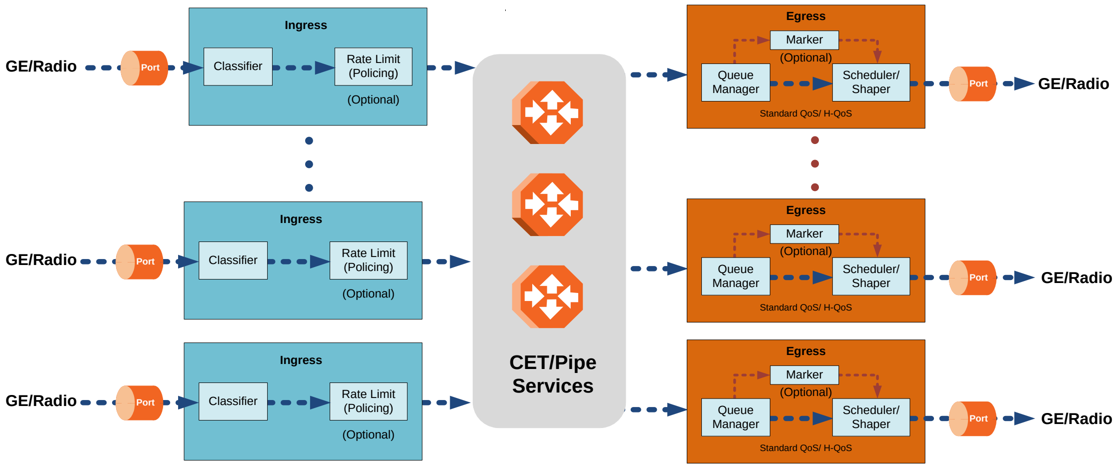
Quality of Service (QoS) deals with the way frames are handled within the switching fabric. QoS is required in order to deal with many different network scenarios, such as traffic congestion, packet availability, and delay restrictions.

PTP 850's personalized QoS enables operators to handle a wide and diverse range of scenarios. PTP 850's smart QoS mechanism operates from the frame's ingress into the switching fabric until the moment the frame egresses via the destination port.

QoS capability is very important due to the diverse topologies that exist in today's network scenarios. These can include, for example, streams from two different ports that egress via single port, or a port-to-port connection that holds hundreds of services. In each topology, a customized approach to handling QoS will provide the best results.

Figure 183 shows the basic flow of PTP 850's QoS mechanism. Traffic ingresses (left to right) via the Ethernet or radio interfaces, on the "ingress path." Based on the services model, the system determines how to route the traffic. Traffic is then directed to the most appropriate output queue via the "egress path."

Figure 183 QoS Block Diagram



The ingress path consists of the following QoS building blocks:

Ingress Classifier – A hierarchical mechanism that deals with ingress traffic on three different levels: interface, service point, and service. The classifier determines the exact traffic stream and associates it with the appropriate service. It also calculates an ingress frame CoS and Color. CoS and Color classification can be performed on three levels, according to the user's configuration.

Ingress Rate Metering – A hierarchical mechanism that deals with ingress traffic on three different levels: interface, service point, and service point CoS. The rate metering mechanism enables the system to measure the incoming frame rate on different levels using a TrTCM standard MEF rate meter, and to determine whether to modify the color calculated during the classification stage.

Note

Ingress rate meters can be configure per service point or per service point CoS, but not on both.

The egress path consists of the following QoS building blocks:

Queue Manager – This is the mechanism responsible for managing the transmission queues, utilizing smart WRED per queue and per packet color (Green or Yellow).

Scheduling and Shaping – A hierarchical mechanism that is responsible for scheduling the transmission of frames from the transmission queues, based on priority among queues, Weighted Fair Queuing (WFQ) in bytes per each transmission queue, and eligibility to transmit based on required shaping on several different levels (per queue, per service bundle, and per port).

Marker – This mechanism provides the ability to modify priority bits in frames based on the calculated CoS and Color.

For a more detailed description of QoS in the PTP 850, refer to the Technical Description for the PTP 850 product type you are using.

Configuring Classification

The hierarchical classifier consists of the following levels:

Logical interface-level classification

Service point-level classification

Service level classification

This section explains how to configure classification at the logical interface level.

For instructions how to configure classification at the service point level, see 2. Ethernet Service Points – Ingress Attributes.

For instructions how to configure classification at the service level, see Adding an Ethernet Service.

This section includes:

- Classification Overview
- Configuring Ingress Path Classification on a Logical Interface
- Modifying the C-VLAN 802.1Q UP and CFI Bit Classification Table
- Modifying the S-VLAN 802.1 UP and DEI Bit Classification Table
- Modifying the DSCP Classification Table
- Modifying the MPLS EXP Bit Classification Table

In addition to the procedures described in this section, you can specify a specific CoS and Color for a specific VLAN ID. This is the highest classification priority on the logical interface level, and overrides any other classification criteria at the logical interface level. Classification by VLAN ID can only be configured via CLI. See Configuring VLAN Classification and Override (CLI).

Classification Overview

PTP 850 supports a hierarchical classification mechanism. The classification mechanism examines incoming frames and determines their CoS and Color. The benefit of hierarchical classification is that it provides the ability to “zoom in” or “zoom out”, enabling classification at higher or lower levels of the hierarchy. The nature of each traffic stream defines which level of the hierarchical classifier to apply, or whether to use several levels of the classification hierarchy in parallel.

Classification takes place on the logical interface level according to the following priorities:

- VLAN ID (CLI-only – see Configuring VLAN Classification and Override (CLI))
- 802.1p bits
- DSCP bits (only considered if MPLS is not present, regardless of trust setting)
- MPLS EXP field
- Default interface CoS

For PTP 850S, classification is performed according to the following priorities:

- VLAN ID (CLI-only – see Configuring VLAN Classification and Override (CLI))
- 802.1p bits
- DSCP bits

PTP 850 performs the classification on each frame ingressing the system via the logical interface. Classification is performed step by step from the highest priority to the lowest priority classification method. Once a match is found, the classifier determines the CoS and Color decision for the frame for the logical interface-level.

You can disable some of these classification methods by configuring them as un-trusted. For example, if 802.1p classification is configured as un-trusted for a specific interface, the classification mechanism does not perform classification by UP bits. This is useful, for example, if classification is based on DSCP priority bits.

If no match is found at the logical interface level, the default CoS is applied to incoming frames at this level. In this case, the Color of the frame is assumed to be Green.

For PTP 850S, classification may also be performed by Destination MAC Address (MAC DA) at the service point level. When MAC DA classification is enabled on a service point, the classification mechanism checks each frame ingressing the interface on which the service point is defined against a list of user-defined MAC DAs. If there is a match, the mechanism applies to the frame the CoS and Color defined for that MAC DA. Classification by MAC DA overrides the other classification criteria at the service point level.

Up to 64 MAC addresses can be defined per device, including four predefined MAC addresses. You can assign each of these MAC addresses a CoS value and a Color.

The following MAC addresses are predefined, with a high priority (CoS=7, Color=Green). You can edit or delete these MAC addresses:

- 09:00:2B:00:00:04
- 09:00:2B:00:00:05
- 01:80:C2:00:00:14
- 01:80:C2:00:00:15

These are protocol MAC addresses used to transport IS-IS frames as defined in ISO 9542 and ISO/IEC 10589.

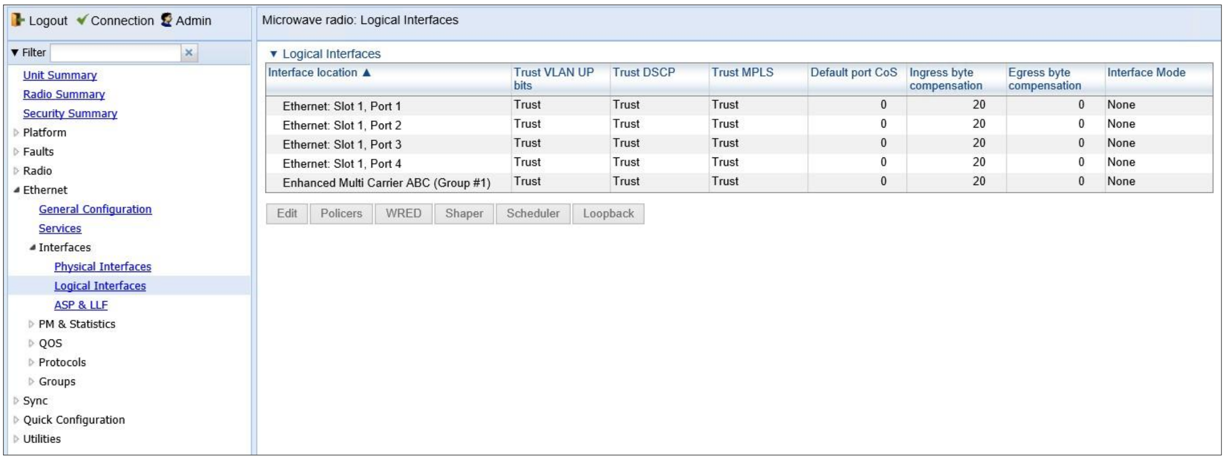
Configuring Ingress Path Classification on a Logical Interface

This section explains how to configure the classification criteria per each logical interface. The following sections explain how to modify the classification tables per bit type.

To configure the classification criteria for a logical interface:

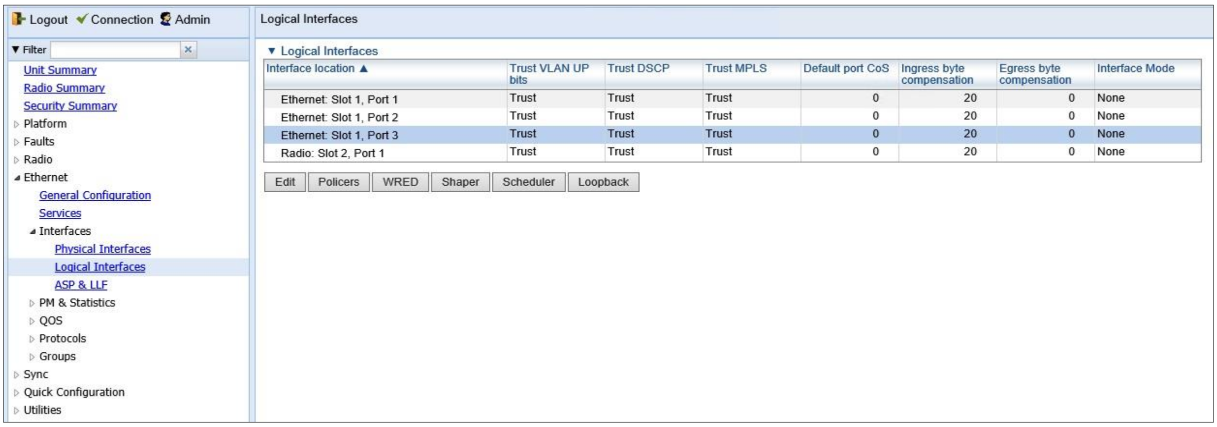
1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens.

Figure 184 Logical Interfaces Page-PTP 850C



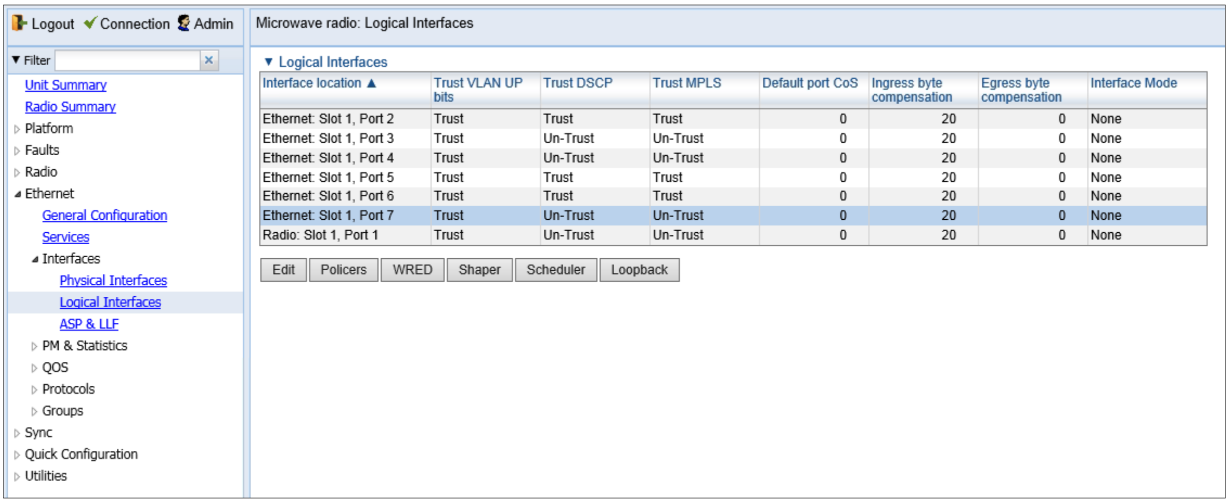
Interface location ▲	Trust VLAN UP bits	Trust DSCP	Trust MPLS	Default port CoS	Ingress byte compensation	Egress byte compensation	Interface Mode
Ethernet: Slot 1, Port 1	Trust	Trust	Trust	0	20	0	None
Ethernet: Slot 1, Port 2	Trust	Trust	Trust	0	20	0	None
Ethernet: Slot 1, Port 3	Trust	Trust	Trust	0	20	0	None
Ethernet: Slot 1, Port 4	Trust	Trust	Trust	0	20	0	None
Enhanced Multi Carrier ABC (Group #1)	Trust	Trust	Trust	0	20	0	None

Table 56 Logical Interfaces Page-PTP 850S



Interface location ▲	Trust VLAN UP bits	Trust DSCP	Trust MPLS	Default port CoS	Ingress byte compensation	Egress byte compensation	Interface Mode
Ethernet: Slot 1, Port 1	Trust	Trust	Trust	0	20	0	None
Ethernet: Slot 1, Port 2	Trust	Trust	Trust	0	20	0	None
Ethernet: Slot 1, Port 3	Trust	Trust	Trust	0	20	0	None
Radio: Slot 2, Port 1	Trust	Trust	Trust	0	20	0	None

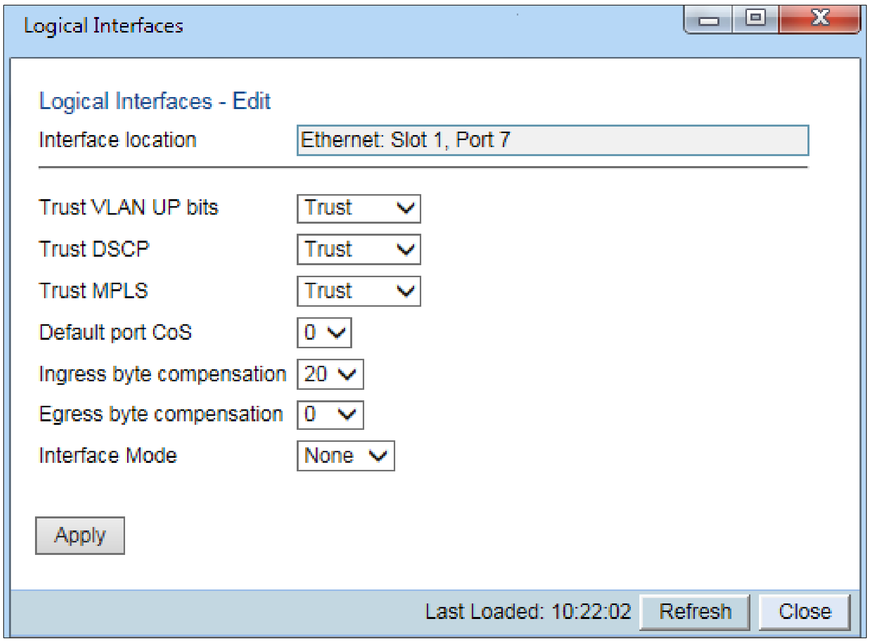
Table 57 Logical Interfaces Page-PTP 850E



Interface location ▲	Trust VLAN UP bits	Trust DSCP	Trust MPLS	Default port CoS	Ingress byte compensation	Egress byte compensation	Interface Mode
Ethernet: Slot 1, Port 2	Trust	Trust	Trust	0	20	0	None
Ethernet: Slot 1, Port 3	Trust	Un-Trust	Un-Trust	0	20	0	None
Ethernet: Slot 1, Port 4	Trust	Un-Trust	Un-Trust	0	20	0	None
Ethernet: Slot 1, Port 5	Trust	Trust	Trust	0	20	0	None
Ethernet: Slot 1, Port 6	Trust	Trust	Trust	0	20	0	None
Ethernet: Slot 1, Port 7	Trust	Un-Trust	Un-Trust	0	20	0	None
Radio: Slot 1, Port 1	Trust	Un-Trust	Un-Trust	0	20	0	None

2. Select the interface you want to configure and click **Edit**. The Logical Interfaces - Edit page opens.

Figure 185 Logical Interfaces - Edit Page



Logical Interfaces

Logical Interfaces - Edit

Interface location	Ethernet: Slot 1, Port 7
Trust VLAN UP bits	Trust
Trust DSCP	Trust
Trust MPLS	Trust
Default port CoS	0
Ingress byte compensation	20
Egress byte compensation	0
Interface Mode	None

3. Configure the parameters described in Table 58.
4. Click **Apply**, then **Close**.

Note

The **Ingress byte compensation** and **Egress byte compensation** fields are described in Configuring the Ingress and Egress Byte Compensation.

Table 58 Logical Interface Classification Parameters

Parameter	Definition
Trust VLAN UP bits	Select the interface's trust mode for user priority (UP) bits: Trust – The interface performs QoS and color classification according to UP and CFI/DEI bits according to user-configurable tables for 802.1q UP bits (C-VLAN frames) or 802.1AD UP bits (S-VLAN frames). MPLS and DSCP classification has priority over 802.1p Trust Mode, so that if a match is found with the MPLS or DSCPI, 802.1p bits are not considered. Un-Trust – The interface does not consider 802.1 UP bits during classification.

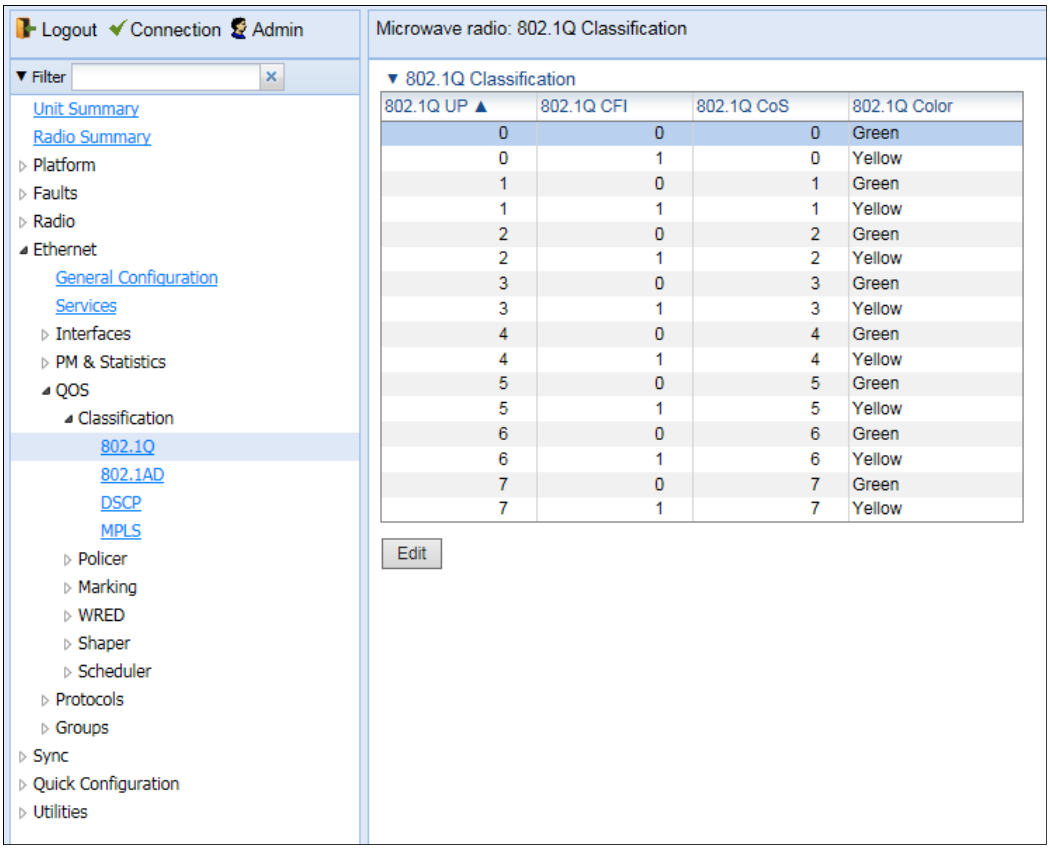
Parameter	Definition
Trust DSCP	Select the interface's trust mode for DSCP: **Trust** – The interface performs QoS and color classification according to a user-configurable table for DSCP to CoS and color classification. DSCP classification has priority over MPLS classification, so that if a match is found with the DSCP value of the ingressing frame, MPLS bits are not considered. **Un-Trust** – The interface does not consider DSCP during classification. **Note:** If you change the trust mode for DSCP, the trust mode for MPLS is automatically changed to the same setting.
Trust MPLS	Select the interface's trust mode for MPLS bits: **Trust** – The interface performs QoS and color classification according to a user-configurable table for MPLS EXP to CoS and color classification. **Un-Trust** – The interface does not consider MPLS bits during classification. **Note:** If you change the trust mode for MPLS, the trust mode for DSCP is automatically changed to the same setting.
Default port CoS	Select the default CoS value for frames passing through the interface (0 to 7). This value can be overwritten on the service point and service level.
Ingress Byte Compensation	See Configuring the Ingress and Egress Byte Compensation.
Egress Byte Compensation	See Configuring the Ingress and Egress Byte Compensation.
Interface Mode	Reserved for future use.

Modifying the C-VLAN 802.1Q UP and CFI Bit Classification Table

To modify the classification criteria for 802.1Q User Priority (UP) bits:

1. Select **Ethernet > QoS > Classification > 802.1Q**. The 802.1Q Classification page opens.

Figure 186 802.1Q Classification Page



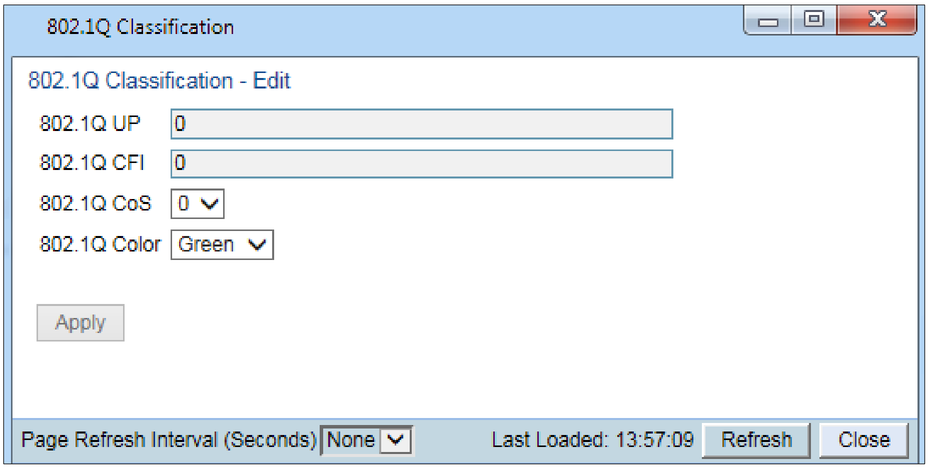
Microwave radio: 802.1Q Classification

▼ 802.1Q Classification

802.1Q UP ▲	802.1Q CFI	802.1Q CoS	802.1Q Color
0	0	0	Green
0	1	0	Yellow
1	0	1	Green
1	1	1	Yellow
2	0	2	Green
2	1	2	Yellow
3	0	3	Green
3	1	3	Yellow
4	0	4	Green
4	1	4	Yellow
5	0	5	Green
5	1	5	Yellow
6	0	6	Green
6	1	6	Yellow
7	0	7	Green
7	1	7	Yellow

2. Select the row you want to modify and click **Edit**. The 802.1Q Classification – Edit page opens.

Figure 187 802.1Q Classification - Edit Page



802.1Q Classification - Edit

802.1Q UP: 0

802.1Q CFI: 0

802.1Q CoS: 0

802.1Q Color: Green

Page Refresh Interval (Seconds): None

Last Loaded: 13:57:09

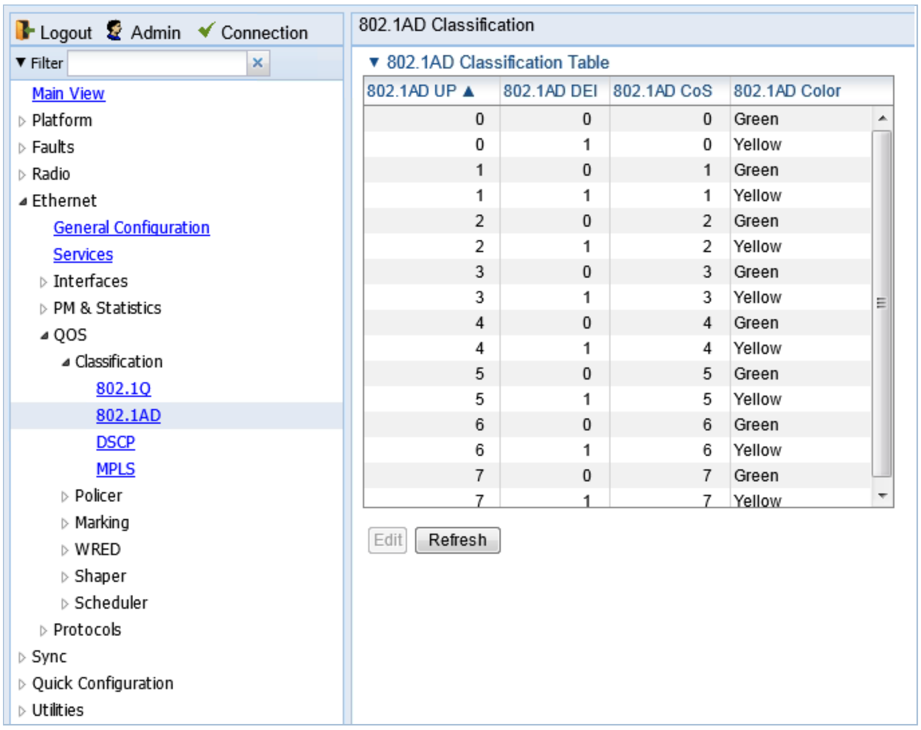
3. Modify the parameters you want to change:
   - **802.1Q UP** – Read-only. The User Priority (UP) bit to be mapped.
   - **802.1Q CFI** – Read-only. The CFI bit to be mapped.
   - **802.1Q CoS** – The CoS assigned to frames with the designated UP and CFI.
   - **802.1Q Color** – The Color assigned to frames with the designated UP and CFI.
4. Click **Apply**, then **Close.**

Modifying the S-VLAN 802.1 UP and DEI Bit Classification Table

To modify the classification criteria for 802.1AD User Priority (UP) bits:

1. Select **Ethernet > QoS > Classification > 802.1AD**. The 802.1AD Classification page opens.

Figure 188 802.1AD Classification Page



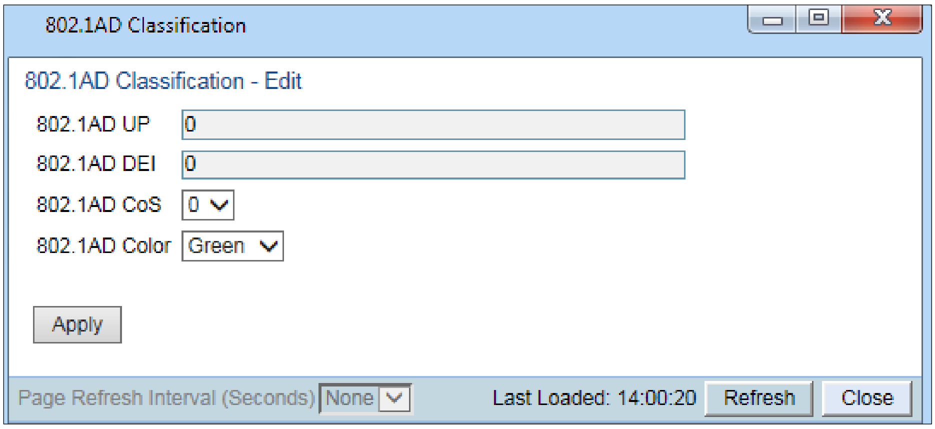
802.1AD Classification

▼ 802.1AD Classification Table

802.1AD UP ▲	802.1AD DEI	802.1AD CoS	802.1AD Color
0	0	0	Green
0	1	0	Yellow
1	0	1	Green
1	1	1	Yellow
2	0	2	Green
2	1	2	Yellow
3	0	3	Green
3	1	3	Yellow
4	0	4	Green
4	1	4	Yellow
5	0	5	Green
5	1	5	Yellow
6	0	6	Green
6	1	6	Yellow
7	0	7	Green
7	1	7	Yellow

2. Select the row you want to modify and click **Edit**. The 802.1AD Classification - Edit page opens.

Figure 189 802.1Q Classification - Edit Page



802.1AD Classification

802.1AD Classification - Edit

802.1AD UP	0
802.1AD DEI	0
802.1AD CoS	0
802.1AD Color	Green

Page Refresh Interval (Seconds) None

Last Loaded: 14:00:20

3. Modify the parameters you want to change:
   - **802.1AD UP** – Read-only. The User Priority (UP) bit to be mapped.
   - **802.1ADQ DEI** – Read-only. The DEI bit to be mapped.
   - **802.1AD CoS** – The CoS assigned to frames with the designated UP and DEI.
   - **802.1AD Color** – The Color assigned to frames with the designated UP and DEI.

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

Modifying the DSCP Classification Table

You can configure the classification criteria for Differentiated Service Code Point (DSCP) priority values. The DSCP is a 6-bit length field inside the IP datagram header carrying priority information. Classification by DSCP can be used for untagged frames, as well as 802.1Q tagged or provider VLAN tagged frames.

PTP 850 units have a DSCP classification table with 24 pre-defined entries. Each entry includes the following criteria:

- DSCP – The DSCP value to be mapped.
- Binary – The binary representation of the DSCP value.
- Description – A description of the DSCP value.
- CoS – The CoS assigned to frames with the designated DSCP value.
- Color – The Color assigned to frames with the designated DSCP value.

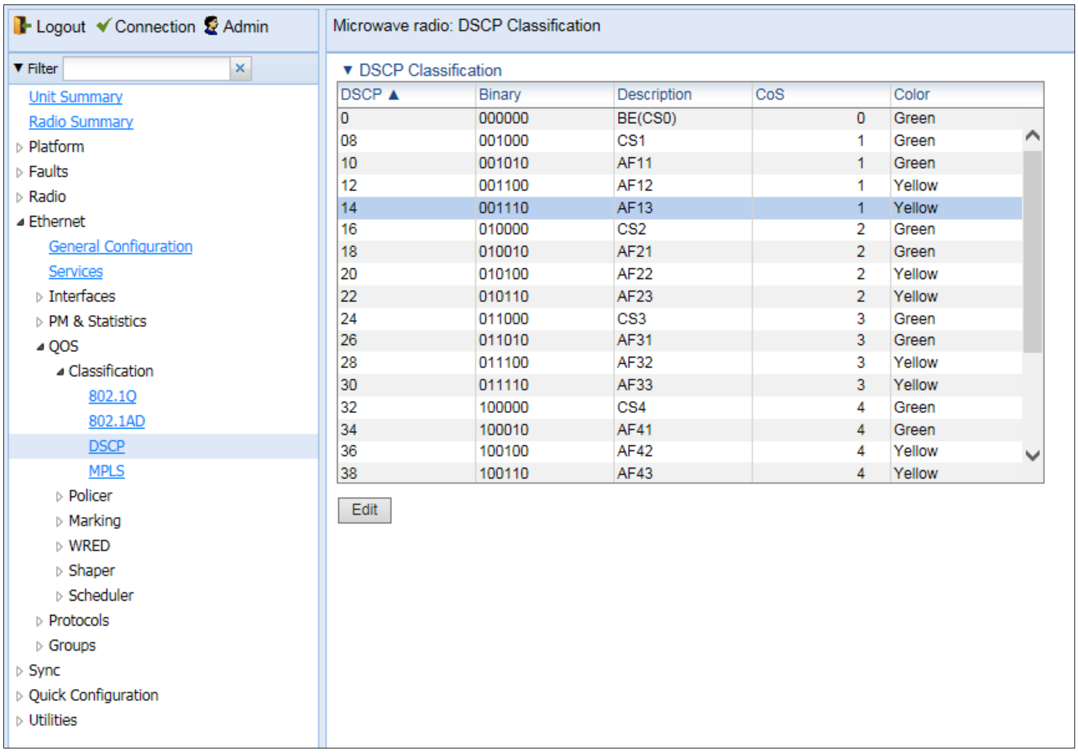
You can modify the Description, CoS, and Color for any of the pre-defined entries. You can also add and delete entries. The maximum number of entries is:

- PTP 850C and PTP 850E: 64.
- PTP 850S: 32

To modify the classification criteria for DSCPs:

1. Select **Ethernet > QoS > Classification > DSCP**. The DSCP Classification page opens.

Figure 190 DSCP Classification Page



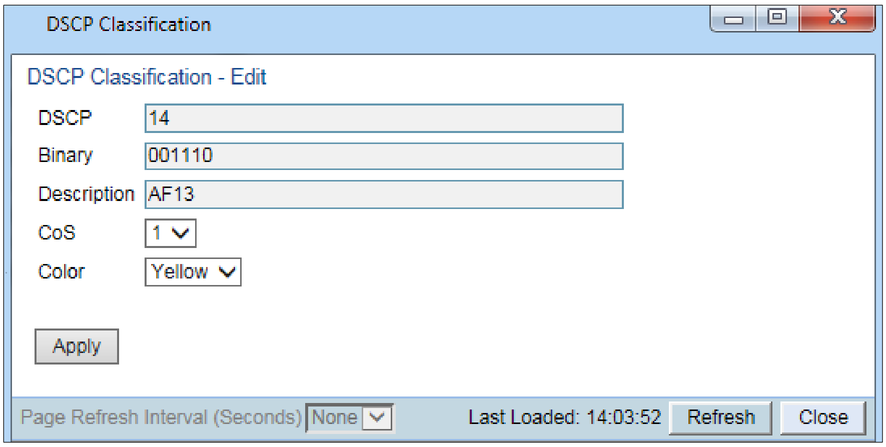
Microwave radio: DSCP Classification

▼ DSCP Classification

DSCP ▲	Binary	Description	CoS	Color
0	000000	BE(CS0)	0	Green
08	001000	CS1	1	Green
10	001010	AF11	1	Green
12	001100	AF12	1	Yellow
14	001110	AF13	1	Yellow
16	010000	CS2	2	Green
18	010010	AF21	2	Green
20	010100	AF22	2	Yellow
22	010110	AF23	2	Yellow
24	011000	CS3	3	Green
26	011010	AF31	3	Green
28	011100	AF32	3	Yellow
30	011110	AF33	3	Yellow
32	100000	CS4	4	Green
34	100010	AF41	4	Green
36	100100	AF42	4	Yellow
38	100110	AF43	4	Yellow

2. Select the row you want to modify and click **Edit**. The DSCP Classification - Edit page opens.

Figure 191 DSCP Classification - Edit Page



DSCP Classification

DSCP Classification - Edit

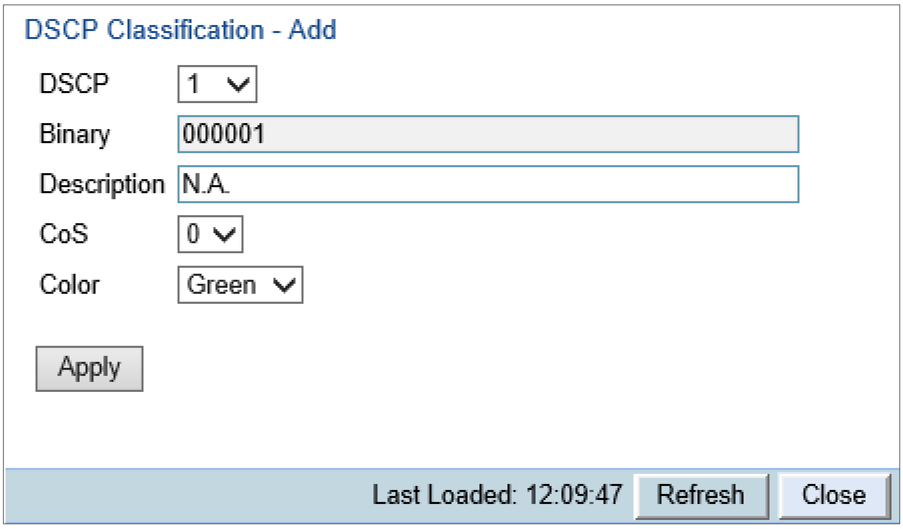
DSCP	14
Binary	001110
Description	AF13
CoS	1
Color	Yellow

3. Modify the parameters you want to change:
   - **DSCP** – Read-only. The DSCP value to be mapped.
   - **Binary** – Read-only. The binary representation of the DSCP value.
   - **Description** – Read-only. The description of the DSCP value.
   - **CoS** – The CoS assigned to frames with the designated DSCP value.
   - **Color** – The Color assigned to frames with the designated DSCP value.
4. Click **Apply**, then **Close**.

To add an entry to the DSCP Classification table:

1 Select **Ethernet > QoS > Classification > DSCP**. The DSCP Classification page opens (*Figure 259*).

2 Click **Add**. The DSCP Classification - Add page opens.



DSCP Classification - Add

DSCP	1
Binary	000001
Description	N.A.
CoS	0
Color	Green

Figure 261: DSCP Classification - Add Page

3 In the **DSCP** field, select the DSCP value you want to add. The **Binary** field is automatically adjusted to display the binary representation of the DSCP value you selected.

4 In the **Description** field, enter a description of the DSCP entry.

5 In the **CoS** field, select a CoS value to assign to frames with the designated DSCP value.

6 In the **Color** field, select a Color to assign to frames with the designated DSCP value.

7 Click **Apply**.

To delete an entry from the DSCP Classification table:

1 Select **Ethernet > QoS > Classification > DSCP**. The DSCP Classification page opens (*Figure 259*).

2 Select the row you want to modify and click **Delete**. A confirmation window opens.

3 Click **OK**. The entry is deleted.

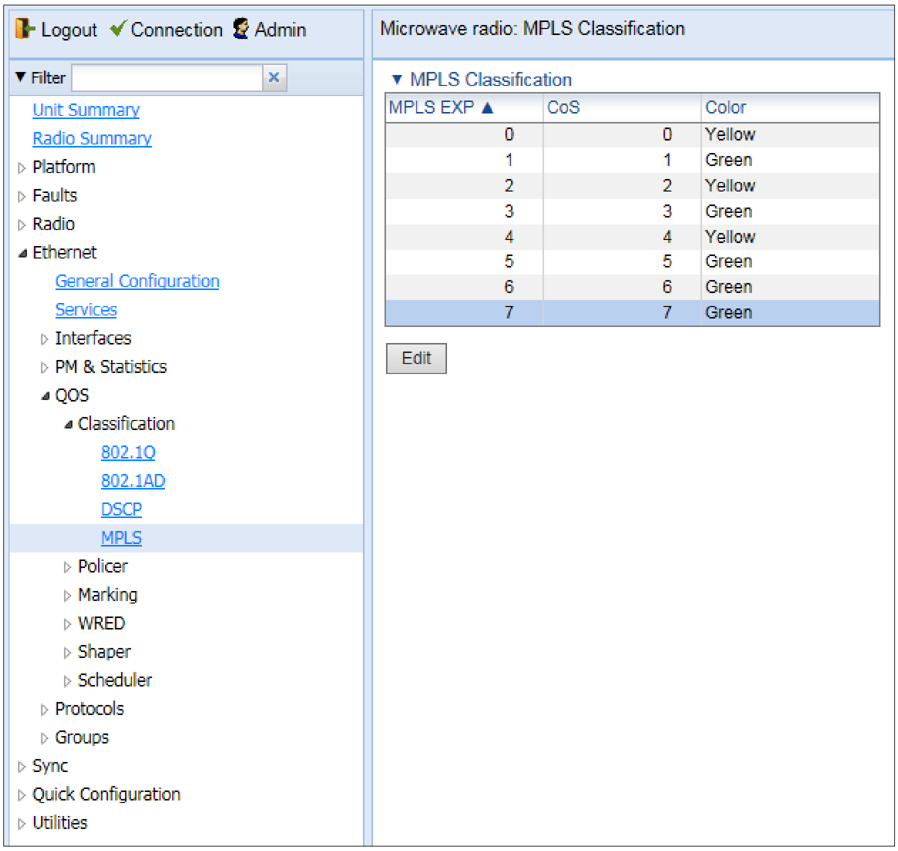
Modifying the MPLS EXP Bit Classification Table

MPLS bits are used to provide QoS capabilities by utilizing the bits set in the MPLS labels. Classification by MPLS bits is supported in both untagged and 802.1Q provider-tagged frames.

To modify the classification criteria for MPLS EXP bits:

1. Select **Ethernet > QoS > Classification > MPLS**. The MPLS Classification page opens.

Figure 192 MPLS Classification Page



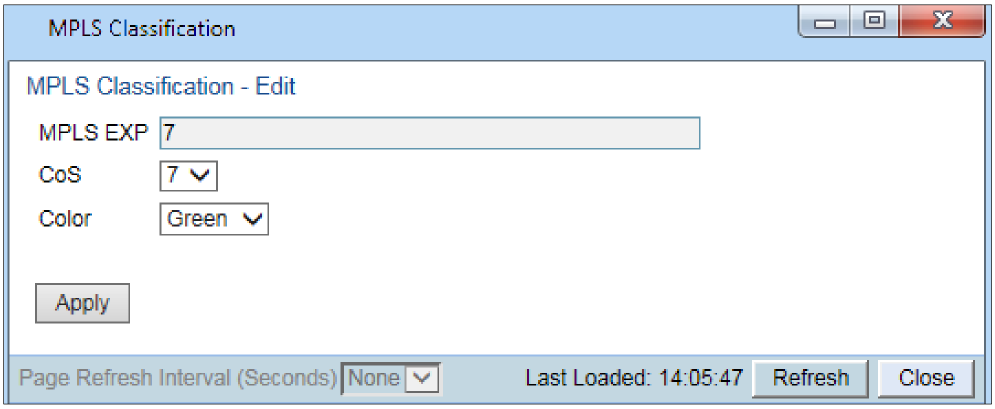
Microwave radio: MPLS Classification

▼ MPLS Classification

MPLS EXP ▲	CoS	Color
0	0	Yellow
1	1	Green
2	2	Yellow
3	3	Green
4	4	Yellow
5	5	Green
6	6	Green
7	7	Green

2. Select the row you want to modify and click **Edit**. The MPLS Classification - Edit page opens.

Figure 193 MPLS Classification - Edit Page



MPLS Classification

MPLS Classification - Edit

MPLS EXP: 7

CoS: 7

Color: Green

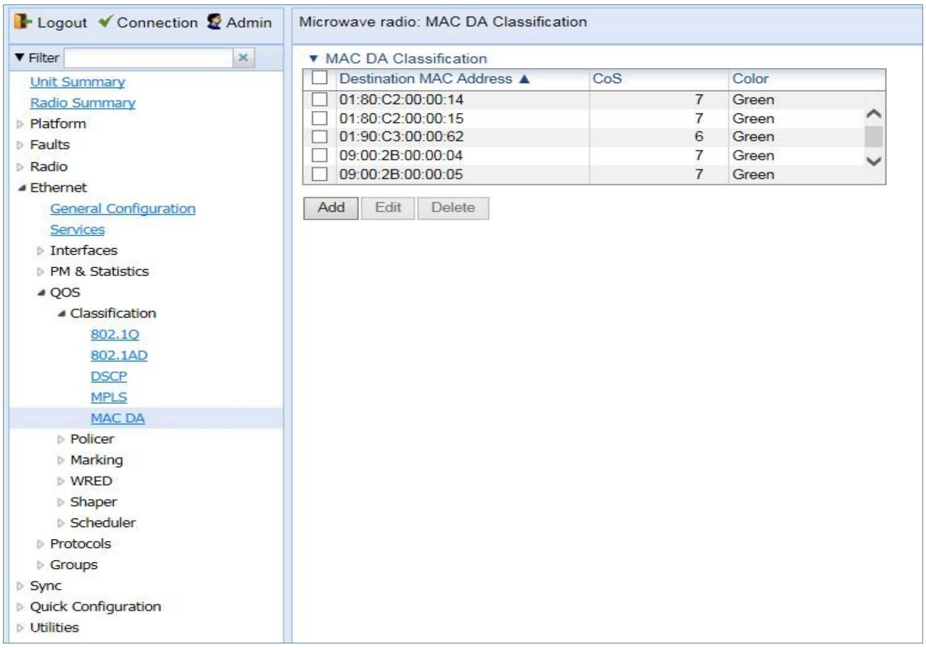
3. Modify the parameters you want to change:
   - **MPLS EXP** – Read-only. The MPLS (experimental) bit to be mapped.
   - **CoS** – The CoS assigned to frames with the designated MPLS EXP value.
   - **Color** – The Color assigned to frames with the designated MPLS EXP value.
4. Click **Apply**, then **Close**.

Modifying the MAC DA Classification Table

You can determine whether classification is performed by MAC DA in the **CoS Mode** field of the service point's Ingress Parameters page. See *Classification Overview*.

To add an entry to the MAC DA Classification Table:

1 Select **Ethernet > QoS > Classification > MAC DA**. The MAC DA Classification page opens.



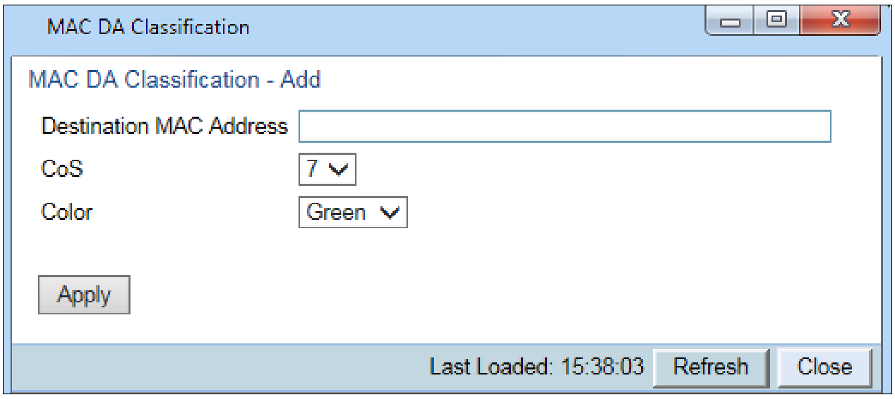
Microwave radio: MAC DA Classification

MAC DA Classification

□	Destination MAC Address ▲	CoS	Color
□	01:80:C2:00:00:14	7	Green
□	01:80:C2:00:00:15	7	Green
□	01:90:C3:00:00:62	6	Green
□	09:00:2B:00:00:04	7	Green
□	09:00:2B:00:00:05	7	Green

Figure 264: MAC DA Classification Page

2 Click **Add**. The MAC DA Classification – Add page opens.



MAC DA Classification

MAC DA Classification - Add

Destination MAC Address

CoS 7

Color Green

Figure 194 MAC DA Classification – Add Page

In the **Destination MAC Address** field, enter the MAC address.

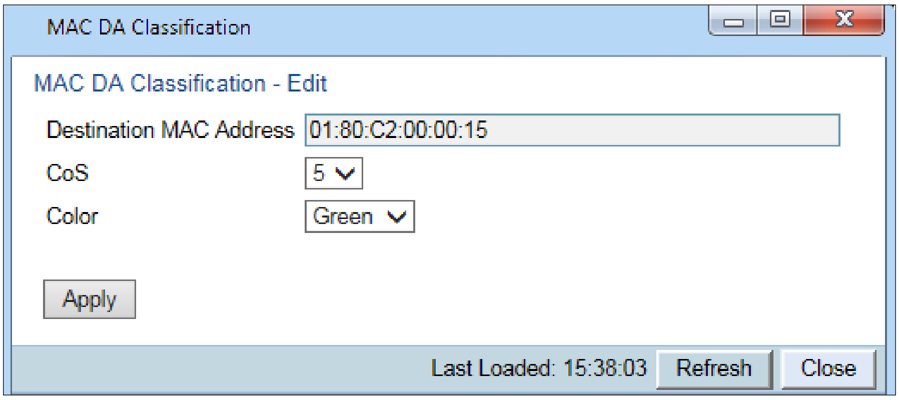
3 In the **CoS** field, enter the CoS to be assigned to frames with this MAC DA.

4 In the **Color** field, enter the Color to be assigned to frames with this MAC DA.

5 Click Apply, then Close.

To modify an entry in the MAC DA Classification Table:

1 In the MAC DA Classification page, select the row you want to modify and click **Edit**. The MAC DA Classification – Edit page opens.



MAC DA Classification

MAC DA Classification - Edit

Destination MAC Address 01:80:C2:00:00:15

CoS 5

Color Green

Figure 195 MAC DA Classification – Edit Page

2 Modify the parameters you want to change:

- **CoS** – The CoS assigned to frames with this MAC DA.
- **Color** – The Color assigned to frames with this MAC DA.

3 Click Apply, then Close.

To delete an entry from the MAC DA Classification Table:

1 In the MAC DA Classification page, select the row you want to delete and click **Delete**. A confirmation window opens.

2 Click OK.

Configuring Policers (Rate Metering)

This section includes:

- Policer (Rate Metering) Overview
- Configuring Policer Profiles
- Assigning Policers to Interfaces
- Configuring the Ingress and Egress Byte Compensation

Policer (Rate Metering) Overview

The PTP 850 switching fabric supports hierarchical policing on the logical interface level. You can define up to 250 rate meter (policer) profiles.

Note

Policing on the service point level, and the service point and CoS level, is planned for future release.

PTP 850's policer mechanism is based on a dual leaky bucket mechanism (TrTCM). The policers can change a frame's color and CoS settings based on CIR/EIR + CBS/EBS, which makes the policer mechanism a key tool for implementing bandwidth profiles and enabling operators to meet strict SLA requirements.

The output of the policers is a suggested color for the inspected frame. Based on this color, the queue management mechanism decides whether to drop the frame or to pass it to the queue.

Configuring Policer Profiles

This section includes:

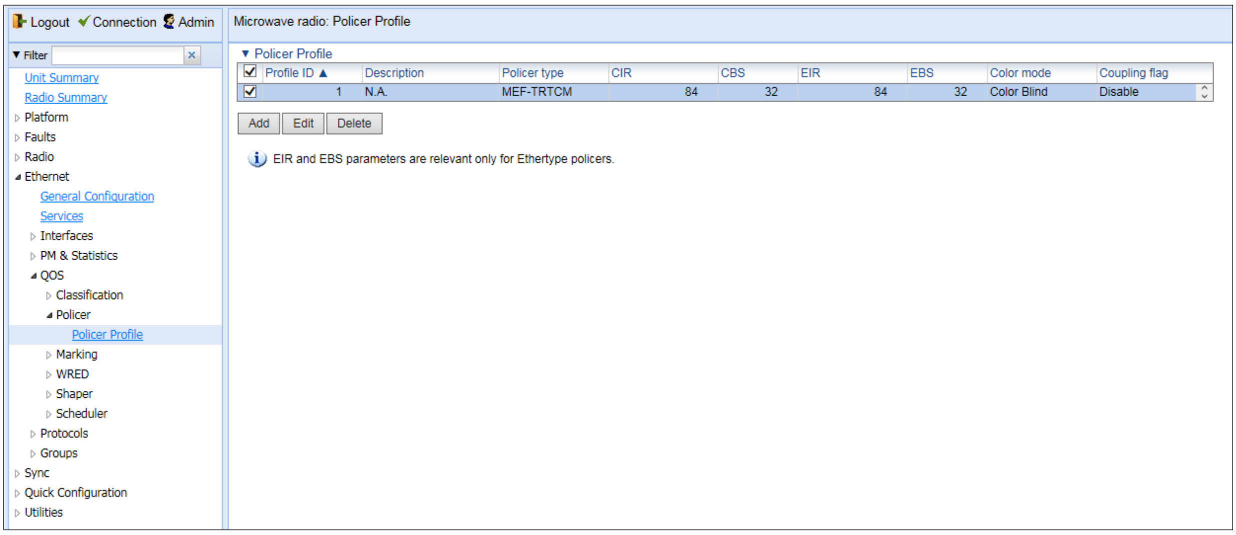
- Adding a Policer Profile
- Editing a Policer Profile
- Deleting a Policer Profile

Adding a Policer Profile

To add a policer profile:

1. Select **Ethernet > QoS > Policer > Policer Profile**. The Policer Profile page opens.

Figure 196 Policer Profile Page

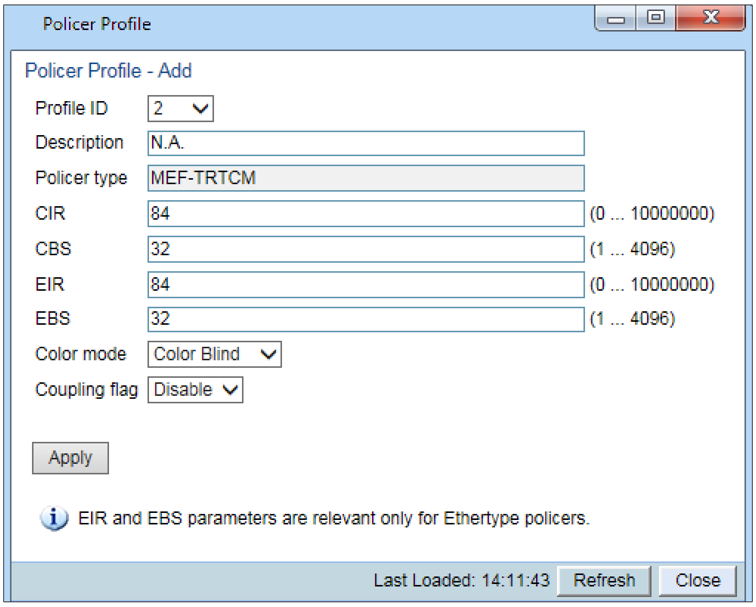


☑	Profile ID ▲	Description	Policer type	CIR	CBS	EIR	EBS	Color mode	Coupling flag
☑	1	N.A.	MEF-TRTCM	84	32	84	32	Color Blind	Disable

EIR and EBS parameters are relevant only for Ethertype policers.

2. Click **Add**. The Policer Profile - Add page opens.

Figure 197 Policer Profile - Add Page



Policer Profile - Add

Profile ID	2	
Description	N.A.	
Policer type	MEF-TRTCM	
CIR	84	(0 ... 10000000)
CBS	32	(1 ... 4096)
EIR	84	(0 ... 10000000)
EBS	32	(1 ... 4096)
Color mode	Color Blind	
Coupling flag	Disable	

EIR and EBS parameters are relevant only for Ethertype policers.

Last Loaded: 14:11:43

3. Configure the profile's parameters. See Table 59 Policer Profile Parameters for a description of the policer profile parameters.
4. Click **Apply**, then **Close**.

Table 59 Policer Profile Parameters

Parameter	Definition
Profile ID	A unique ID for the policer profile. You can choose from any unused value from 1 to 250. Once you have added the profile, you cannot change the Profile ID.
Description	A description of the policer profile.
Policer type	Read-only. The type of policer. Always set to MEF-TRTCM.
CIR	Enter the Committed Information Rate (CIR) for the policer, in bits per second. Permitted values are 0, or 64,000 through 1,000,000,000 bps. If the value is 0, all incoming CIR traffic is dropped.
CBS	Enter the Committed Burst Rate (CBR) for the policer, in Kbytes. Permitted values are 0 through 4096 Kbytes.
EIR	Enter the Excess Information Rate (EIR) for the policer, in bits per second. Permitted values are 0, or 64,000 through 1,000,000,000 bps. If the value is 0, all incoming EIR traffic is dropped.
EBS	Enter the Excess Burst Rate (EBR) for the policer, in Kbytes. Permitted values are 0 through 4096 Kbytes.
Color mode	Select how the policer treats packets that ingress with a CFI or DEI field set to 1 (yellow). Options are: **Color Aware** – All packets that ingress with a CFI/DEI field set to 1 (yellow) are treated as EIR packets, even if credits remain in the CIR bucket. **Color Blind** – All ingress packets are treated as green regardless of their CFI/DEI value. A color-blind policer discards any former color decisions.
Coupling flag	Select **Enable** or **Disable**. When enabled, frames that ingress as yellow may be converted to green when there are no available yellow credits in the EIR bucket. **Coupling Flag** is only relevant in Color Aware mode.

Editing a Policer Profile

To edit a policer profile, select the profile in the Police Profile table and click **Edit**. The Policer Profile Table Edit page opens.

The Policer Profile Table - Edit page is identical to the Policer Profile Table - Add page (Figure 197). You can edit any parameter that can be configured in the Policer Profile Table Add page, except the **Profile ID**.

Deleting a Policer Profile

You cannot delete a policer profile that is attached to a logical interface. You must first remove the profile from the logical interface, then delete the profile. See Assigning Policers to Interfaces.

To delete a policer profile, select the profile in the Police Profile table and click **Delete**. The profile is deleted.

To delete multiple policer profiles:

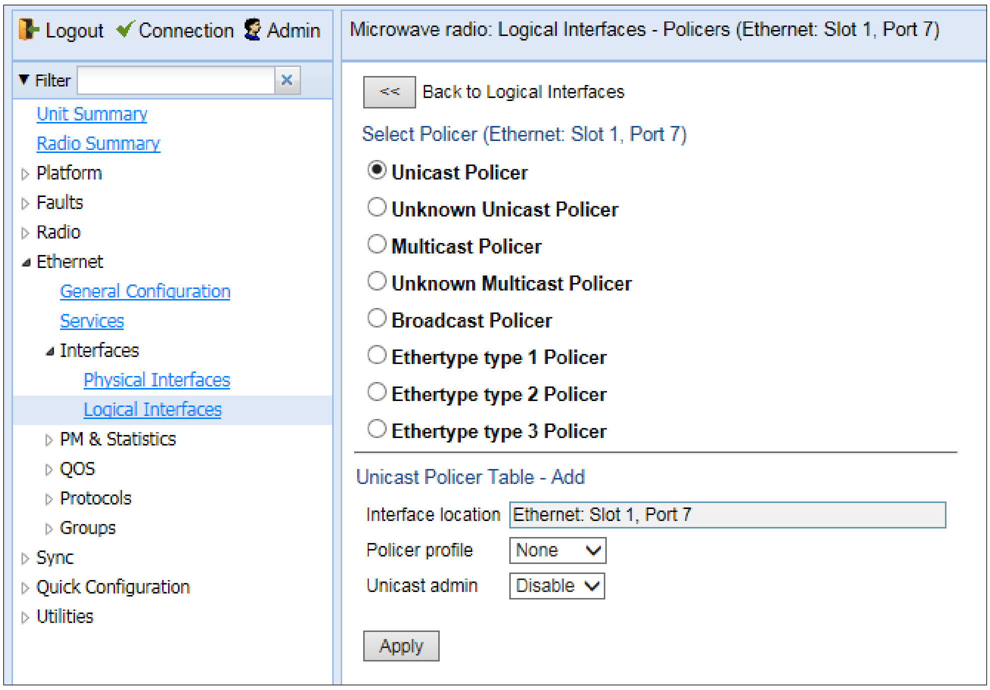
1. Select the profiles in the Policer Profile table or select all the profiles by selecting the check box in the top row.
2. Click **Delete**. The profiles are deleted.

Assigning Policers to Interfaces

To assign policers to a logical interface:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 184).
2. Select the interface in the Ethernet Logical Port Configuration table and click **Policers**. The Policers page opens.

Figure 198 Logical Interfaces – Policers Page – Unicast Policer (Default)



Microwave radio: Logical Interfaces - Policers (Ethernet: Slot 1, Port 7)

Select Policer (Ethernet: Slot 1, Port 7)

● Unicast Policer
○ Unknown Unicast Policer
○ Multicast Policer
○ Unknown Multicast Policer
○ Broadcast Policer
○ Ethertype type 1 Policer
○ Ethertype type 2 Policer
○ Ethertype type 3 Policer

Unicast Policer Table - Add

Interface location: Ethernet: Slot 1, Port 7
Policer profile: None
Unicast admin: Disable

For a logical interface, you can assign policers to the following traffic flows:

Unicast Policer

Unknown Unicast Policer

Multicast Policer

Unknown Multicast Policer

Broadcast Policer

Ethertype Policers

Assigning Unicast Policers

To assign a policer for unicast traffic to a logical interface:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 184).
2. Select the interface in the Ethernet Logical Port Configuration Table and click **Policers**. The Policers page opens. By default, the Policers page opens to the Unicast Policer table (Figure 198).

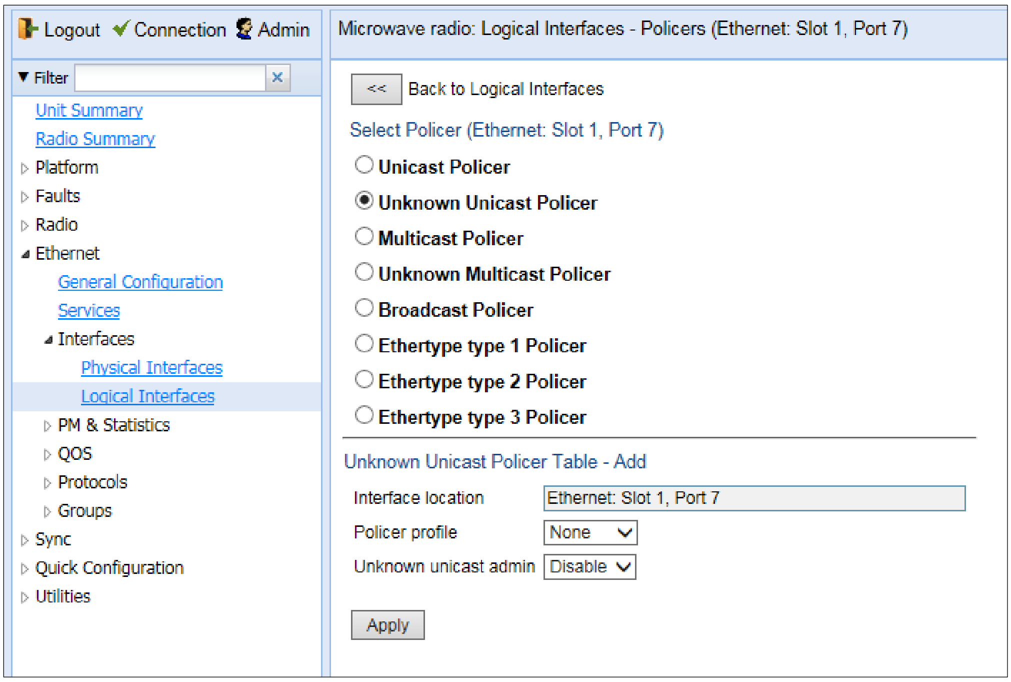
3. In the **Policer profile** field, select a profile from the policer profiles defined in the system. The **Policer profile** drop-down list includes the ID and description of all defined profiles.
4. In the **Unicast admin** field, select **Enable** to enable policing on unicast traffic flows from the logical interface, or **Disable** to disable policing on unicast traffic flows from the logical interface.
5. Click **Apply**.

Assigning Unknown Unicast Policers

Unknown unicast packets are unicast packets with unknown destination MAC addresses. To assign a policer for unknown unicast traffic to a logical interface:

1. Select Ethernet > Interfaces > Logical Interfaces. The Logical Interfaces page opens (Figure 184).
2. Select the interface in the Ethernet Logical Port Configuration table and click Policers. The Policers page opens. By default, the Policers page opens to the Unicast Policer table (Figure 198).
3. Select Unknown Unicast Policer. The Unknown Unicast Policer table appears.

Figure 199 Logical Interfaces – Policers Page – Multicast Policer



Microwave radio: Logical Interfaces - Policers (Ethernet: Slot 1, Port 7)

Select Policer (Ethernet: Slot 1, Port 7)

○ Unicast Policer
● Unknown Unicast Policer
○ Multicast Policer
○ Unknown Multicast Policer
○ Broadcast Policer
○ Ethertype type 1 Policer
○ Ethertype type 2 Policer
○ Ethertype type 3 Policer

Unknown Unicast Policer Table - Add

Interface location	Ethernet: Slot 1, Port 7
Policer profile	None
Unknown unicast admin	Disable

4. In the Policer profile field, select a profile from the policer profiles defined in the system. The Policer profile drop-down list includes the ID and description of all defined profiles.
5. In the Multicast admin field, select Enable to enable policing on multicast traffic flows from the logical interface, or Disable to disable policing on multicast traffic flows from the logical interface.
6. Click Apply.

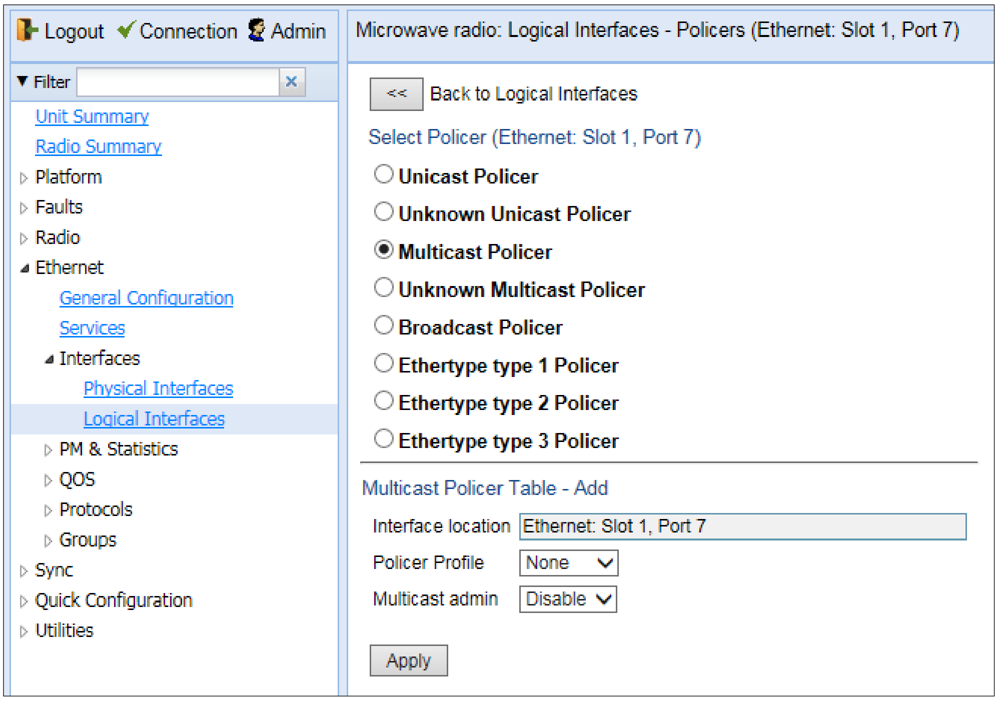
Assigning Multicast Policers

To assign a policer for multicast traffic to a logical interface:

1 Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (*Figure 184*).

2 Select the interface in the Ethernet Logical Port Configuration table and click **Policers**. The Policers page opens. By default, the Policers page opens to the Unicast Policer table (*Figure 198*).

3 Select **Multicast Policer**. The Multicast Policer table appears.



Microwave radio: Logical Interfaces - Policers (Ethernet: Slot 1, Port 7)

Select Policer (Ethernet: Slot 1, Port 7)

○ Unicast Policer
○ Unknown Unicast Policer
● Multicast Policer
○ Unknown Multicast Policer
○ Broadcast Policer
○ Ethertype type 1 Policer
○ Ethertype type 2 Policer
○ Ethertype type 3 Policer

Multicast Policer Table - Add

Interface location: Ethernet: Slot 1, Port 7
Policer Profile: None
Multicast admin: Disable

Figure 200: Logical Interfaces – Policers Page – Multicast Policer

4 In the **Policer profile** field, select a profile from the policer profiles defined in the system. The **Policer profile** drop-down list includes the ID and description of all defined profiles.

5 In the **Multicast admin** field, select **Enable** to enable policing on multicast traffic flows from the logical interface, or **Disable** to disable policing on multicast traffic flows from the logical interface.

6 Click **Apply**.

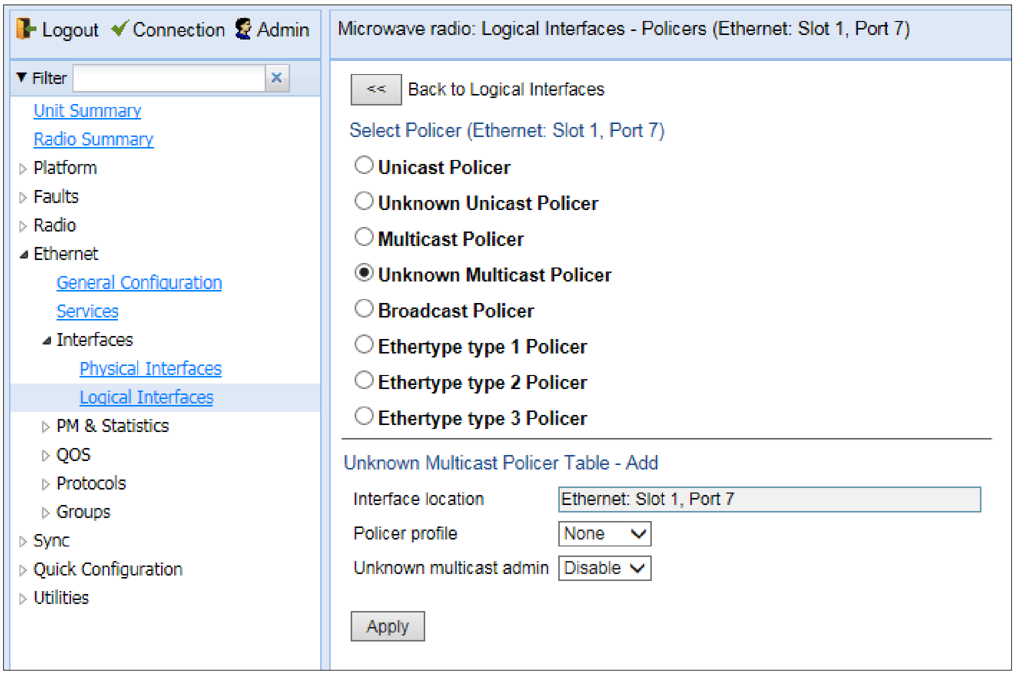
Assigning Unknown Multicast Policers

Unknown multicast packets are multicast packets with unknown destination MAC addresses. To assign a policer for unknown multicast traffic to a logical interface:

1 Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (*Figure 184*).

2 Select the interface in the Ethernet Logical Port Configuration table and click **Policers**. The Policers page opens. By default, the Policers page opens to the Unicast Policer table (*Figure 198*).

3 Select **Unknown Multicast Policer**. The Unknown Multicast Policer table appears.



Microwave radio: Logical Interfaces - Policers (Ethernet: Slot 1, Port 7)

Select Policer (Ethernet: Slot 1, Port 7)

○ Unicast Policer
○ Unknown Unicast Policer
○ Multicast Policer
● Unknown Multicast Policer
○ Broadcast Policer
○ Ethertype type 1 Policer
○ Ethertype type 2 Policer
○ Ethertype type 3 Policer

Unknown Multicast Policer Table - Add

Interface location: Ethernet: Slot 1, Port 7
Policer profile: None
Unknown multicast admin: Disable

Figure 201: Logical Interfaces – Policers Page – Unknown Multicast Policer

4 In the **Policer profile** field, select a profile from the policer profiles defined in the system. The **Policer profile** drop-down list includes the ID and description of all defined profiles.

5 In the **Unknown multicast admin** field, select **Enable** to enable policing on unknown multicast traffic flows from the logical interface, or **Disable** to disable policing on unknown multicast traffic flows from the logical interface.

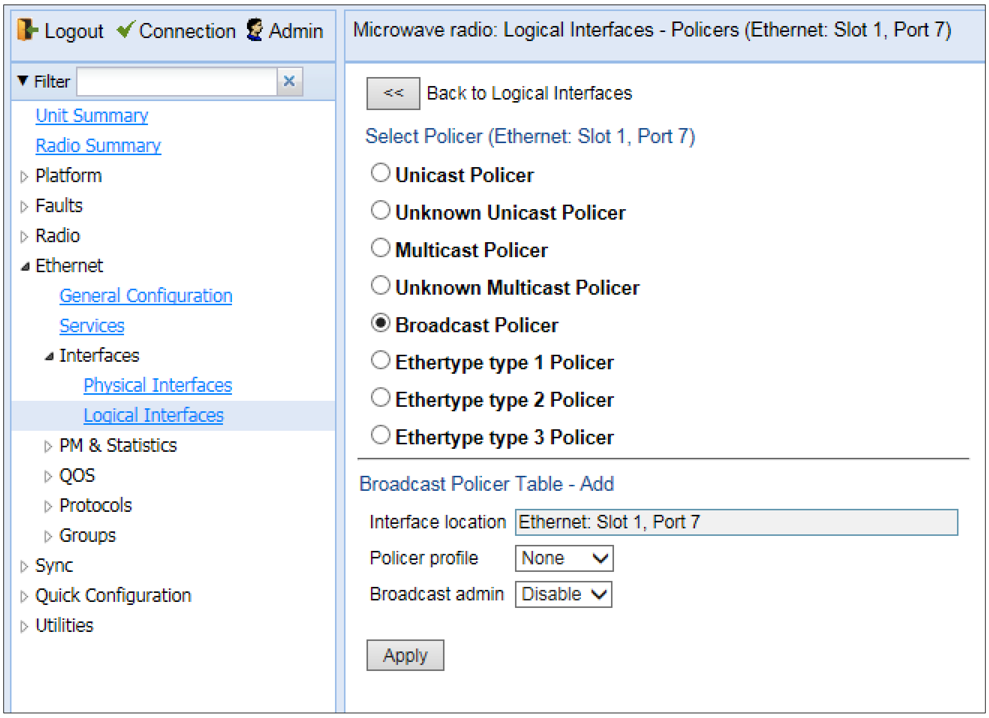
6 Click **Apply**.

Assigning Broadcast Policers

To assign a policer for broadcast traffic to a logical interface:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 184).
2. Select the interface in the Ethernet Logical Port Configuration table and click **Policers**. The Policers page opens. By default, the Policers page opens to the Unicast Policer table (Figure 198).
3. Select **Broadcast Policer**. The Broadcast Policer table appears.

Figure 202 Logical Interfaces – Policers Page – Broadcast Policer



Microwave radio: Logical Interfaces - Policers (Ethernet: Slot 1, Port 7)

Select Policer (Ethernet: Slot 1, Port 7)

○ Unicast Policer

○ Unknown Unicast Policer

○ Multicast Policer

○ Unknown Multicast Policer

● Broadcast Policer

○ Ethertype type 1 Policer

○ Ethertype type 2 Policer

○ Ethertype type 3 Policer

Broadcast Policer Table - Add

Interface location	Ethernet: Slot 1, Port 7
Policer profile	None
Broadcast admin	Disable

4. In the **Policer profile** field, select a profile from the policer profiles defined in the system. The **Policer profile** drop-down list includes the ID and description of all defined profiles.
5. In the **Broadcast admin** field, select **Enable** to enable policing on broadcast traffic flows from the logical interface, or **Disable** to disable policing on broadcast traffic flows from the logical interface.
6. Click **Apply**.

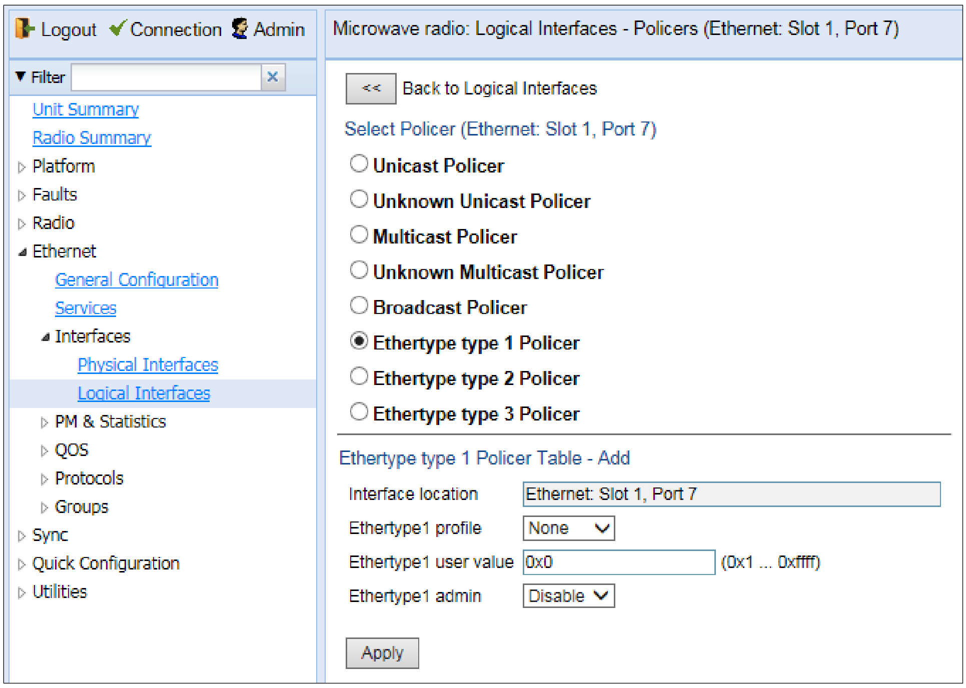
Assigning Ethertype Policers

You can define up to three policers per Ethertype value.

To assign a policer to an Ethertype:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 184).
2. Select the interface in the Ethernet Logical Port Configuration Table and click **Policers**. The Policers page opens. By default, the Policers page opens to the Unicast Policer table (Figure 198).
3. Select **Ethertype type 1 Policer**. The Ethertype type 1 Policer table appears.

Figure 203 Logical Interfaces – Policers Page – Ethertype Policer



Microwave radio: Logical Interfaces - Policers (Ethernet: Slot 1, Port 7)

Select Policer (Ethernet: Slot 1, Port 7)

○ Unicast Policer
○ Unknown Unicast Policer
○ Multicast Policer
○ Unknown Multicast Policer
○ Broadcast Policer
● Ethertype type 1 Policer
○ Ethertype type 2 Policer
○ Ethertype type 3 Policer

Ethertype type 1 Policer Table - Add

Interface location	Ethernet: Slot 1, Port 7
Ethertype1 profile	None
Ethertype1 user value	0x0 (0x1 ... 0xffff)
Ethertype1 admin	Disable

4. In the **Ethertype 1 profile** field, select a profile from the policer profiles defined in the system. The **Ethertype 1 profile** drop-down list includes the ID and description of all defined profiles.
5. In the **Ethertype 1 user value** field, enter the Ethertype value to which you want to apply this policer. The field length is 4 nibbles (for example, 0x0806 - ARP).
6. In the **Ethertype 1 admin** field, select **Enable** to enable policing on the logical interface for the specified ethertype, or **Disable** to disable policing on the logical interface for the specified ethertype.
7. Click **Apply**.
8. To assign policers to additional Ethertypes, select **Ethertype type 2 Policer** and **Ethertype type 3 Policer** and repeat the steps above.

Configuring the Ingress and Egress Byte Compensation

You can define the ingress and egress byte compensation value per logical interface. The policer attached to the interface uses these values to compensate for Layer 1 non-effective traffic bytes.

To define the ingress byte compensation value for a logical interface:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 184).
2. Select the interface you want to configure and click **Edit**. The Logical Interfaces - Edit page opens (Figure 185).
3. In the **Ingress byte compensation** field, enter the ingress byte compensation value, in bytes. Permitted values are 0 to 32 bytes. The default value is 20 bytes.
4. In the **Egress byte compensation** field, enter the egress byte compensation value, in bytes. Permitted values are 0 to 32 bytes. The default value is 0 bytes. Only even values are permitted.
5. Click **Apply**, then **Close**.

Configuring Marking

This section includes:

- Marking Overview
- Enabling Marking
- Modifying the 802.1Q Marking Table
- Modifying the 802.1AD Marking Table

Marking Overview

When enabled, PTP 850's marking mechanism modifies each frame's 802.1p UP bit and CFI/DEI bits according to the classifier decision. The CFI/DEI (color) field is modified according to the classifier and policer decision. The color is first determined by a classifier and may be later overwritten by a policer. Green color is represented by a CFI/DEI value of 0, and Yellow color is represented by a CFI/DEI value of 1. Marking is performed on egress frames that are VLAN-tagged.

The marking is performed according to global mapping tables that describe the 802.1p UP bits and the CFI bits (for C-VLAN tags) or DEI bits (for S VLAN tags). The marking bit in the service point egress attributes determines whether the frame is marked as green or according to the calculated color.

Note

The calculated color is sent to the queue manager regardless of whether the marking bit is set.

Regular marking is only performed when:

The outer frame is S-VLAN, and S-VLAN CoS preservation is disabled, or

The outer frame is C-VLAN, and C-VLAN CoS preservation is disabled.

If marking and CoS preservation for the relevant outer VLAN are both disabled, special marking is applied. Special marking means that marking is performed, but only according to the values defined for Green frames in the 802.1Q and 802.1AD marking tables.

When marking is performed, the C-VLAN or S-VLAN 802.1p UP bits are re-marked according to the calculated CoS and color, and the mapping table for C-VLAN or S-VLAN.

Enabling Marking

Marking is enabled and disabled on the service point level. See 3. Ethernet Service Points – Egress Attributes.

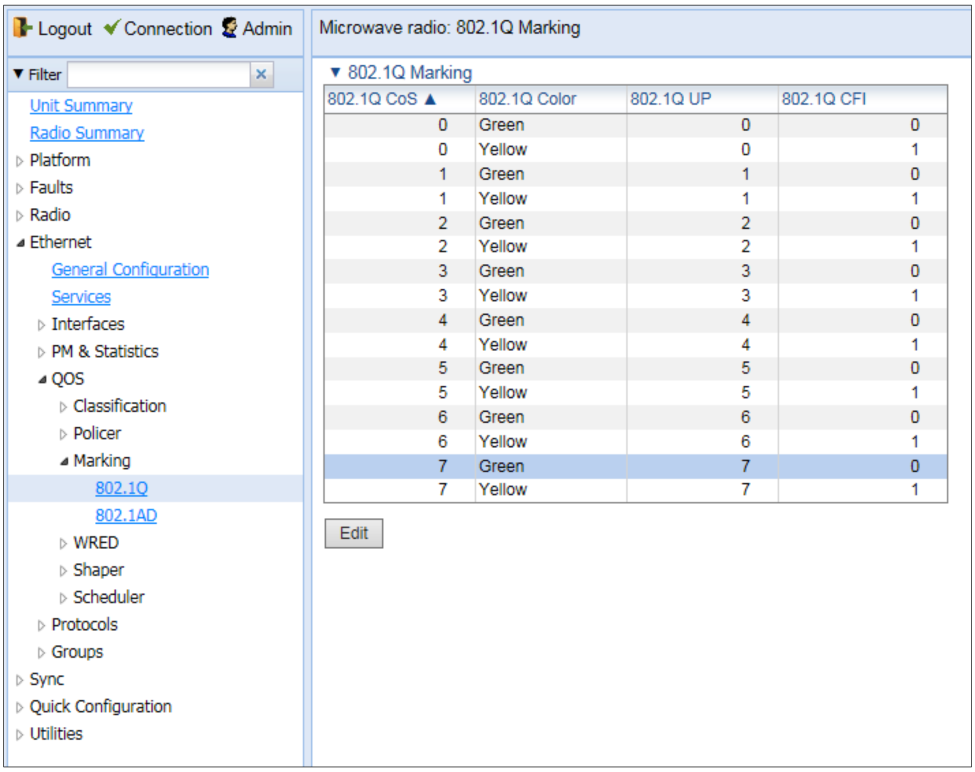
Modifying the 802.1Q Marking Table

The 802.1Q Marking table enables you to modify the CoS to UP and CFI bit mapping that is implemented when marking is enabled.

To modify the 802.1Q Marking table:

1. Select **Ethernet > QoS > Marking > 802.1Q**. The 802.1Q Marking page opens. Each row in the 802.1Q Marking page represents a CoS and color combination.

Figure 204 802.1Q Marking Page

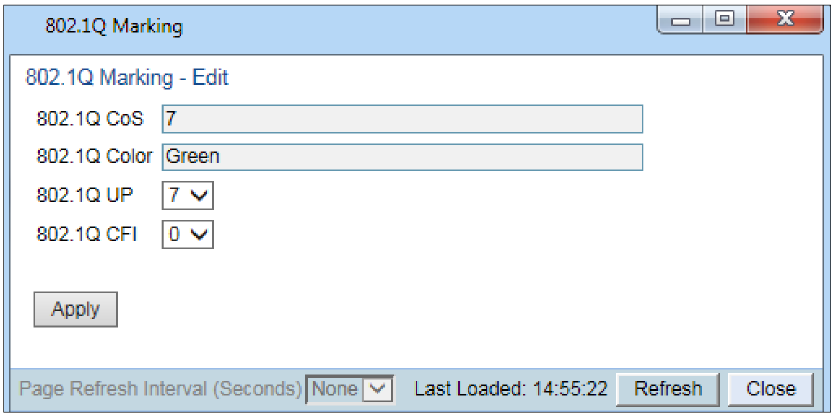


Microwave radio: 802.1Q Marking

802.1Q Marking

802.1Q CoS ▲	802.1Q Color	802.1Q UP	802.1Q CFI
0	Green	0	0
0	Yellow	0	1
1	Green	1	0
1	Yellow	1	1
2	Green	2	0
2	Yellow	2	1
3	Green	3	0
3	Yellow	3	1
4	Green	4	0
4	Yellow	4	1
5	Green	5	0
5	Yellow	5	1
6	Green	6	0
6	Yellow	6	1
7	Green	7	0
7	Yellow	7	1

2. Select the row you want to modify and click **Edit**. The 802.1Q Marking - Edit page opens.



802.1Q Marking

802.1Q Marking - Edit

802.1Q CoS	7
802.1Q Color	Green
802.1Q UP	7
802.1Q CFI	0

Page Refresh Interval (Seconds) None

Last Loaded: 14:55:22

Figure 205 802.1Q Marking - Edit Page

3. Enter the new 802.1Q UP and 802.1Q CFI values.
4. Click **Apply**, then **Close**.

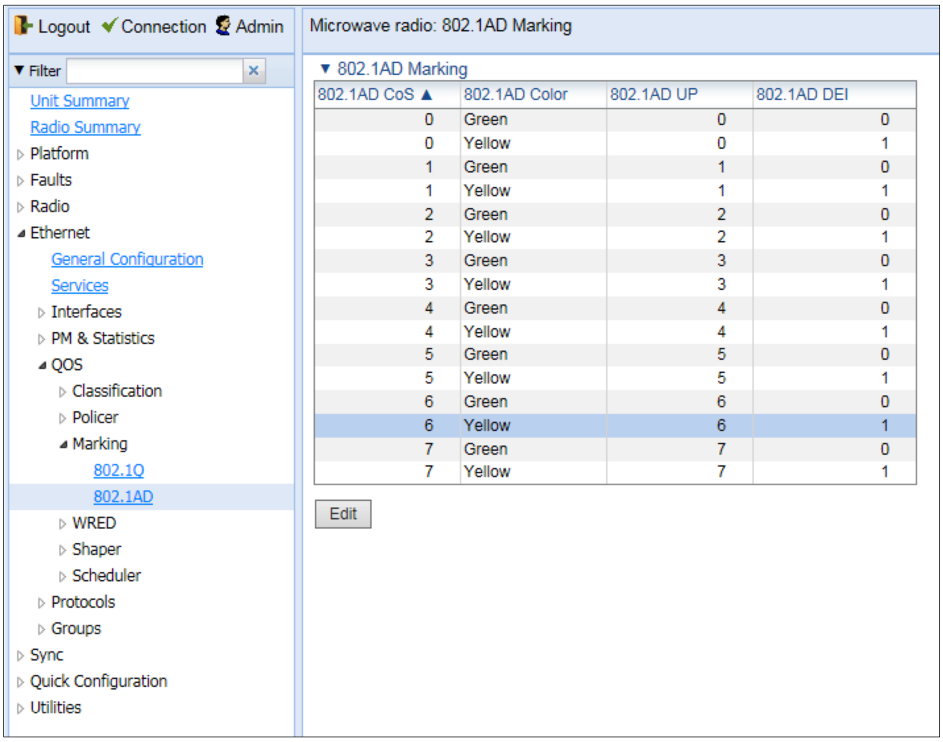
Modifying the 802.1AD Marking Table

The 802.1AD Marking table enables you to modify the CoS to UP and DEI bit mapping that is implemented when marking is enabled.

To modify the 802.1AD Marking table:

1. Select **Ethernet > QoS > Marking > 802.1AD**. The 802.1AD Marking page opens. Each row in the 802.1AD Marking page represents a CoS and color combination.

Figure 206 802.1AD Marking Page



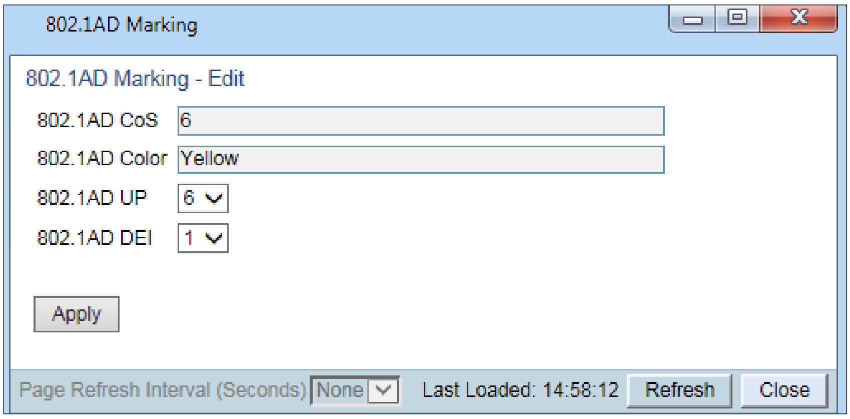
Microwave radio: 802.1AD Marking

802.1AD Marking

802.1AD CoS ▲	802.1AD Color	802.1AD UP	802.1AD DEI
0	Green	0	0
0	Yellow	0	1
1	Green	1	0
1	Yellow	1	1
2	Green	2	0
2	Yellow	2	1
3	Green	3	0
3	Yellow	3	1
4	Green	4	0
4	Yellow	4	1
5	Green	5	0
5	Yellow	5	1
6	Green	6	0
6	Yellow	6	1
7	Green	7	0
7	Yellow	7	1

2. Select the row you want to modify and click **Edit**. The 802.1AD Marking - Edit page opens.

Figure 207 802.1AD Marking - Edit Page



802.1AD Marking

802.1AD Marking - Edit

802.1AD CoS: 6

802.1AD Color: Yellow

802.1AD UP: 6

802.1AD DEI: 1

3. Enter the new 802.1AD UP and 802.1AD DEI values.

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

Configuring WRED

This section includes:

- WRED Overview
- Configuring WRED Profiles
- Assigning WRED Profiles to Queues

WRED Overview

Weighted Random Early Detection (WRED) enables differentiation between higher and lower priority traffic based on CoS. You can define up to 30 WRED profiles. Each profile contains a green traffic curve and a yellow traffic curve. This curve describes the probability of randomly dropping frames as a function of queue occupancy.

The system also includes two pre-defined read-only profiles. These profiles are assigned profile IDs 31 and 32.

Profile number 31 defines a tail-drop curve and is configured with the following values:

- ○ 100% Yellow traffic drop after 64kbytes occupancy.
- ○ 100% Green traffic drop after 128kbytes occupancy.
- ○ Yellow maximum drop is 100%
- ○ Green maximum drop is 100%

Profile number 32 defines a profile in which all will be dropped. It is for internal use and should not be applied to traffic.

A WRED profile can be assigned to each queue. The WRED profile assigned to the queue determines whether or not to drop incoming packets according to the occupancy of the queue. As the queue occupancy grows, the probability of dropping each incoming frame increases as well. As a consequence, statistically more TCP flows will be restrained before traffic congestion occurs.

Configuring WRED Profiles

This section includes:

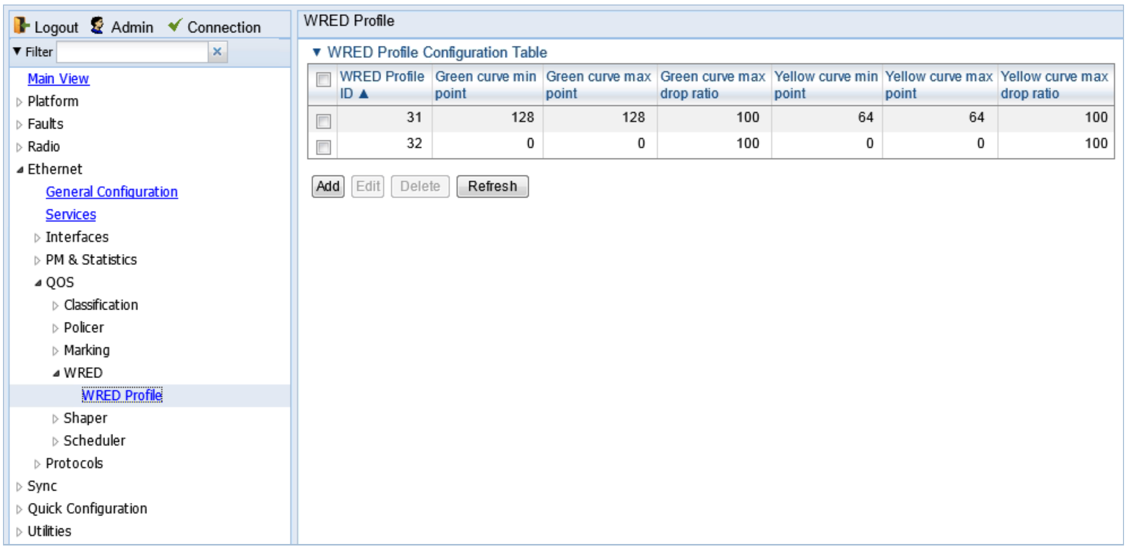
- Adding a WRED Profile
- Editing a WRED Profile
- Deleting a WRED Profile

Adding a WRED Profile

To add a WRED profile:

1. Select **Ethernet > QoS > WRED > WRED Profile**. The WRED Profile page opens.

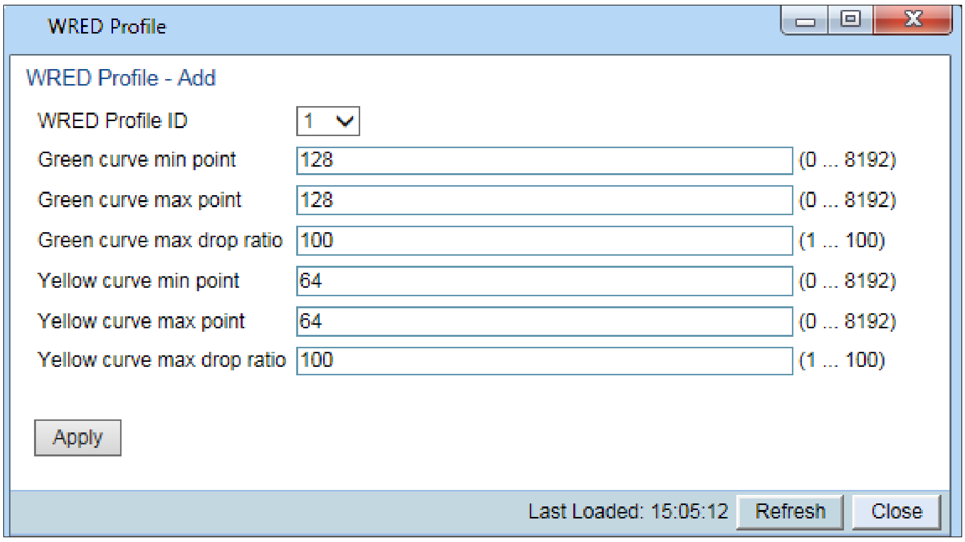
Figure 208 WRED Profile Page



□	WRED Profile ID ▲	Green curve min point	Green curve max point	Green curve max drop ratio	Yellow curve min point	Yellow curve max point	Yellow curve max drop ratio
□	31	128	128	100	64	64	100
□	32	0	0	100	0	0	100

2. Click **ADD**. The WRED Profile - Add page opens, with default values displayed.

Figure 209 WRED Profile - Add Page



WRED Profile ID	1	
Green curve min point	128	(0 ... 8192)
Green curve max point	128	(0 ... 8192)
Green curve max drop ratio	100	(1 ... 100)
Yellow curve min point	64	(0 ... 8192)
Yellow curve max point	64	(0 ... 8192)
Yellow curve max drop ratio	100	(1 ... 100)

3. In the **WRED Profile ID** field, select a unique ID to identify the profile. Permitted values are 1-30.
4. In the **Green curve min point** field, enter the minimum throughput of green packets for queues with this profile, in Kbytes (24-8192). When this value is reached, the system begins dropping green packets in the queue.
5. In the **Green curve max point** field, enter the maximum throughput of green packets for queues with this profile, in Kbytes (24-8192). When this value is reached, all green packets in the queue are dropped.
6. In the **Green curve max drop ratio** field, enter the maximum percentage (1-100) of dropped green packets for queues with this profile.
7. In the **Yellow curve min point** field, enter the minimum throughput of yellow packets for queues with this profile, in Kbytes (24-8192). When this value is reached, the system begins dropping yellow packets in the queue.
8. In the **Yellow curve max point** field, enter the maximum throughput of yellow packets for queues with this profile, in Kbytes (24-8192). After this value is reached, all yellow packets in the queue are dropped.

9. In the **Yellow curve max drop ratio** field, enter the maximum percentage (1-100) of dropped yellow packets for queues with this profile.
10. Click **Apply**, then **Close**.

Editing a WRED Profile

To edit a WRED profile:

1. Select **Ethernet > QoS > WRED > WRED Profile**. The WRED Profile page opens ().
2. Select the profile you want to edit and click Edit. The WRED Profile – Edit page opens. This page is similar to the WRED Profile – Add page (Figure 209). You can edit any parameter except the **WRED Profile ID**.
3. Modify the profile.
4. Click **Apply**, then **Close**.

Deleting a WRED Profile

You cannot delete a WRED profile that is assigned to a queue. You must first remove the WRED profile from the queue, then delete the WRED profile. See Assigning WRED Profiles to Queues.

To delete a WRED profile, select the profile in the WRED Profile Configuration table (Figure 208) and click **Delete**. The profile is deleted.

To delete multiple WRED profiles:

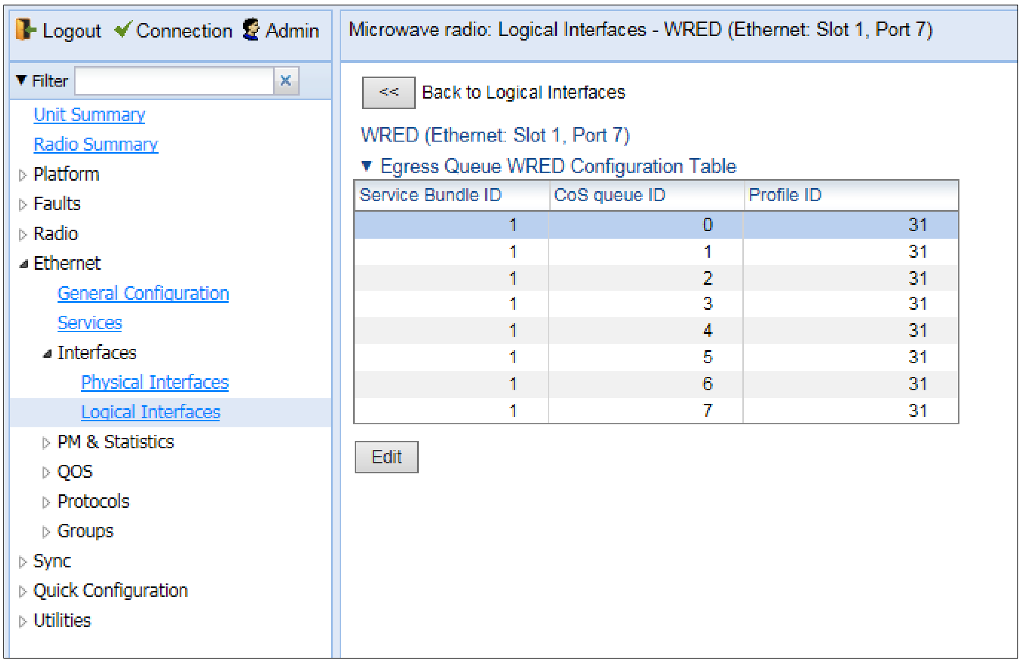
1. Select the profiles in the WRED Profile Configuration table or select all the profiles by selecting the check box in the top row.
2. Click **Delete**. The profiles are deleted.

Assigning WRED Profiles to Queues

To assign a WRED profile to a queue:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 184).
2. Select an interface in the Ethernet Logical Port Configuration table and click **WRED**. The WRED page opens.

Figure 210 Logical Interfaces – WRED Page



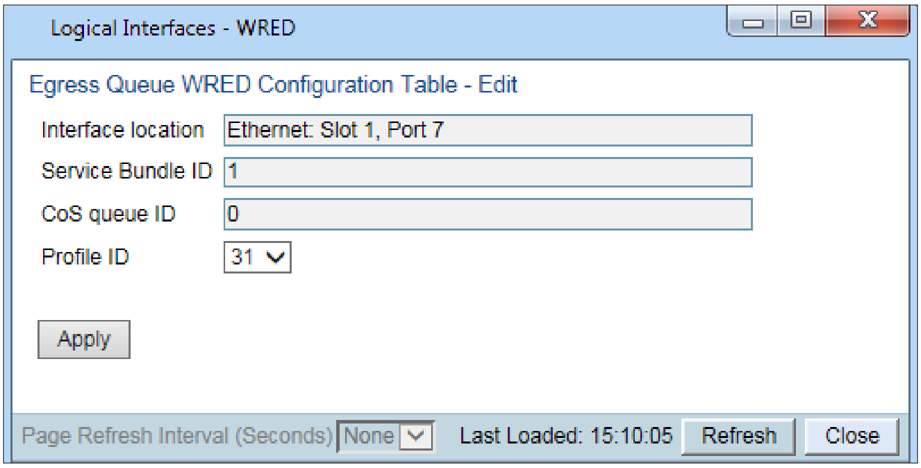
Microwave radio: Logical Interfaces - WRED (Ethernet: Slot 1, Port 7)

WRED (Ethernet: Slot 1, Port 7)

▼ Egress Queue WRED Configuration Table

Service Bundle ID	CoS queue ID	Profile ID
1	0	31
1	1	31
1	2	31
1	3	31
1	4	31
1	5	31
1	6	31
1	7	31

3. Select a CoS Queue ID and click **Edit**. The Logical Interfaces – WRED – Edit page opens.



Logical Interfaces - WRED

Egress Queue WRED Configuration Table - Edit

Interface location	Ethernet: Slot 1, Port 7
Service Bundle ID	1
CoS queue ID	0
Profile ID	31

Page Refresh Interval (Seconds) None

Last Loaded: 15:10:05

Figure 211: Logical Interfaces – WRED - Edit Page

4. In the **Profile ID** field, select the WRED profile you want to assign to the selected queue.
5. Click **Apply**, then **Close**.

Configuring Egress Shaping

This section includes:

Egress Shaping Overview

Egress shaping determines the traffic profile for each queue. PTP 850E can perform queue shaping on the queue level, using dual leaky bucket shaping. On the queue level, you can configure up to 31 single leaky bucket shaper profiles. If no profile is attached to the queue, no egress shaping is performed on that queue.

Configuring Queue Shaper Profiles

This section includes:

Table 60 Queue Shaper **Profile Parameters**

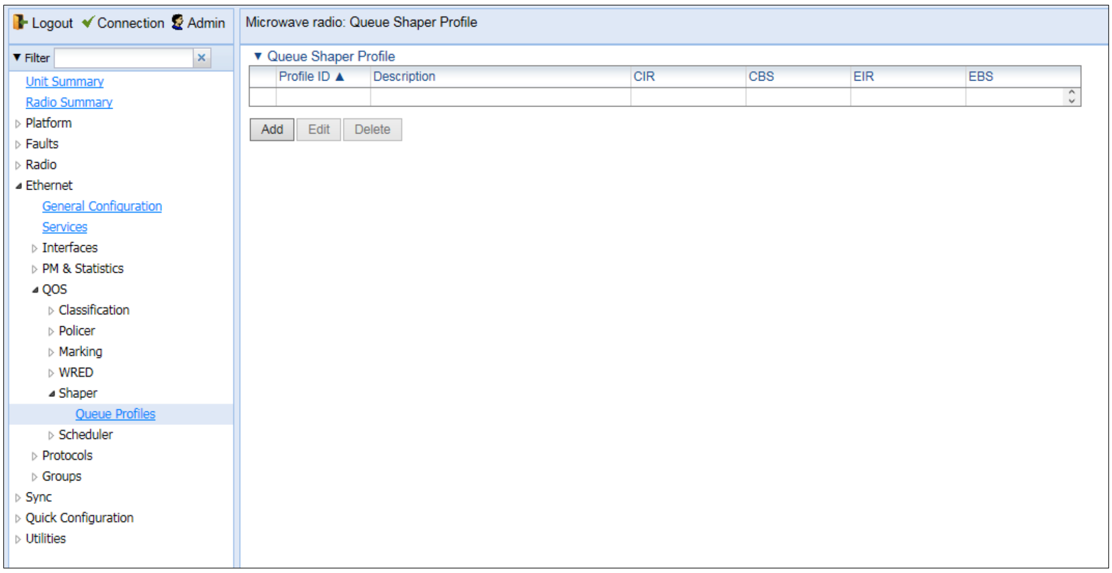
Parameter	Definition
Profile ID	A unique ID for the queue shaper profile. You can choose any unused value from 1 to 32. Once you have added the profile, you cannot change the Profile ID.
Description	A description of the queue shaper profile.
CIR	Enter the Committed Information Rate (CIR) for the shaper, in Kbits per second. Permitted values are 0-40000000 kbps (40 Gbps). If the value is 0, all incoming CIR traffic is dropped. Granularity is 81 kbps. The default value is 40000000 kbps.
CBS	Enter the Committed Burst Rate (CBR) for the shaper, in Kbytes. Permitted values are 1-32 KB. The default value is 16 KB.
EIR	Enter the Excess Information Rate (EIR) for the shaper, in Kbits per second. Permitted values are 0-40000000 kbps (40 Gbps). If the value is 0, all incoming EIR traffic is dropped. Granularity is 162 kbps. The default value is 40000000 kbps.
EBS	Enter the Excess Burst Rate (EBR) for the shaper, in Kbytes. Permitted values are 1-32 KB. The default value is 16 KB.

Adding a Queue Shaper Profile

To add a queue shaper profile:

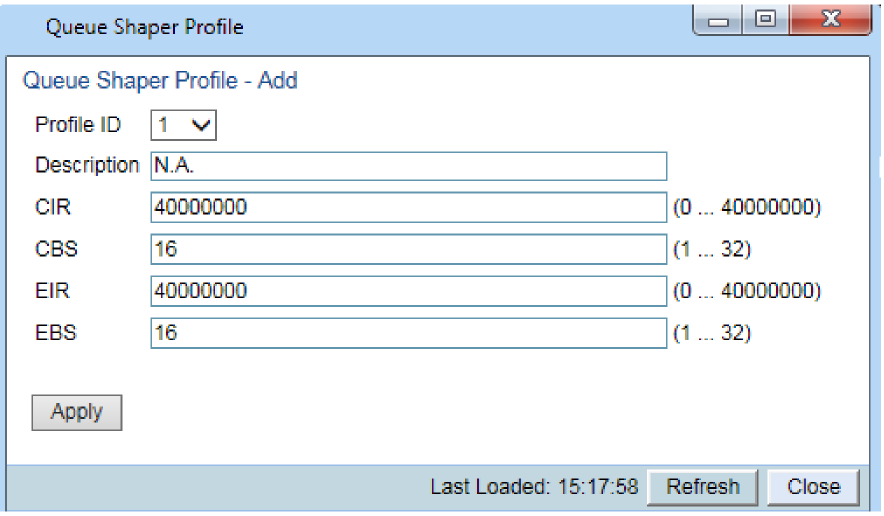
1. Select **Ethernet > QoS > Shaper > Queue Profiles**. The Queue Shaper Profile page opens.

Figure 212 Queue Shaper Profile Page



2. Click **Add**. The Queue Shaper – Add page opens, with default values displayed.

Figure 213 Queue Shaper Profile – Add Page



Profile ID 1

Description N.A.

CIR 40000000 (0 ... 40000000)

CBS 16 (1 ... 32)

EIR 40000000 (0 ... 40000000)

EBS 16 (1 ... 32)

3. Configure the profile's parameters. See Table 60 Queue Shaper Profile **Parameters** for a description of the queue shaper profile parameters.
4. Click **Apply**, then **Close**.

Note

EIR and EBS are only relevant for policers assigned to logical interfaces.

Table 60 Queue Shaper Profile Parameters

Parameter	Definition
Profile ID	A unique ID for the queue shaper profile. You can choose any unused value from 1 to 32. Once you have added the profile, you cannot change the Profile ID.
Description	A description of the queue shaper profile.

Parameter	Definition
CIR	Enter the Committed Information Rate (CIR) for the shaper, in Kbits per second. Permitted values are 0-40000000 kbps (40 Gbps). If the value is 0, all incoming CIR traffic is dropped. Granularity is 81 kbps. The default value is 40000000 kbps.
CBS	Enter the Committed Burst Rate (CBR) for the shaper, in Kbytes. Permitted values are 1-32 KB. The default value is 16 KB.
EIR	Enter the Excess Information Rate (EIR) for the shaper, in Kbits per second. Permitted values are 0-40000000 kbps (40 Gbps). If the value is 0, all incoming EIR traffic is dropped. Granularity is 162 kbps. The default value is 40000000 kbps.
EBS	Enter the Excess Burst Rate (EBR) for the shaper, in Kbytes. Permitted values are 1-32 KB. The default value is 16 KB.

Editing a Queue Shaper Profile

To edit a queue shaper profile:

1. Select **Ethernet > QoS > Shaper > Queue Profiles**. The Queue Shaper Profile page opens (Figure 212).
2. Select the profile you want to edit and click **Edit**. The Queue Shaper Profile – Edit page opens. This page is similar to the Queue Shaper Profile – Add page (Figure 213). You can edit any parameter except the **Profile ID**.
3. Modify the profile.
4. Click **Apply**, then **Close**.

Deleting a Queue Shaper Profile

You cannot delete a queue shaper profile that is assigned to a queue. You must first remove the profile from the queue, then delete the profile. See Assigning a Queue Shaper Profile to a Queue.

To delete a queue shaper profile, select the profile in the Queue Shaper Profiles Configuration table (Figure 212) and click **Delete**. The profile is deleted.

To delete multiple queue shaper profiles:

1. Select the profiles in the Queue Shaper Profiles Configuration table or select all the profiles by selecting the check box in the top row.
2. Click **Delete**. The profiles are deleted.

Configuring Service Bundle Shaper Profiles

Note: This section is only relevant for PTP 850S.

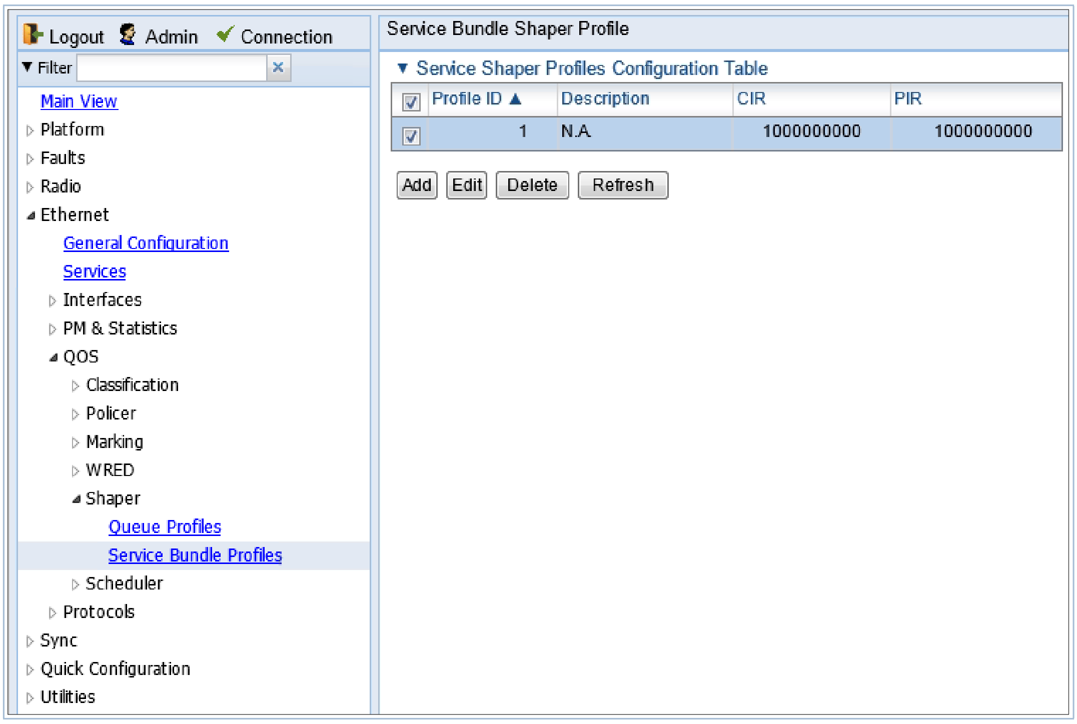
This section includes:

- Adding a Service Bundle Shaper Profile
- Editing a Service Bundle Shaper Profile
- Deleting a Service Bundle Shaper Profile

Adding a Service Bundle Shaper Profile

To add a service bundle shaper profile:

1 Select **Ethernet > QoS > Shaper > Service Bundle Profiles.** The Service Bundle Shaper Profile page opens.



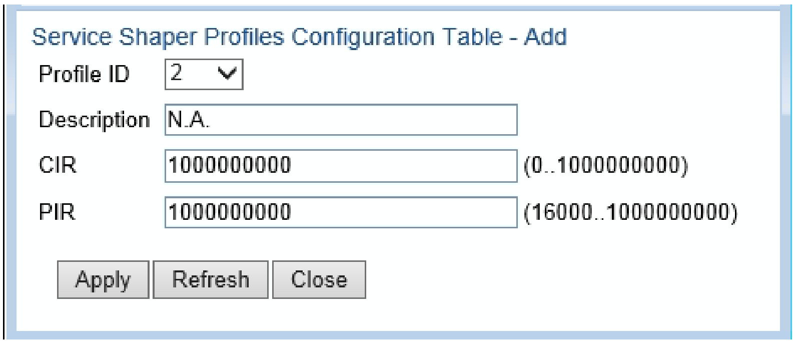
Service Bundle Shaper Profile

Service Shaper Profiles Configuration Table

☑	Profile ID ▲	Description	CIR	PIR
☑	1	N.A	1000000000	1000000000

Figure 214 Service Bundle Shaper Profile Page

2 Click **Add**. The Service Bundle Shaper Profile – Add page opens, with default values displayed.



Service Shaper Profiles Configuration Table - Add

Profile ID	2	
Description	N.A.	
CIR	1000000000	(0..1000000000)
PIR	1000000000	(16000..1000000000)

Figure 289: Service Bundle Shaper Profile – Add Page

3 In the **Profile ID** field, select a unique ID to identify the profile. Permitted values are 1-31.

4 Optionally, in the **Description** field, enter a description of the profile.

5 In the **CIR** field, enter the Committed Information Rate (CIR) assigned to the profile, in bits per second. Permitted values are:

- 0 – 32,000,000 bps, with granularity of 16,000.
- 32,000,000 – 1,000,000,000 bps, with granularity of 64,000.

6 In the **PIR** field, enter the Peak Information Rate (PIR) assigned to the profile, in bits per second. Permitted values are:

- 16,000 – 32,000,000 bps, with granularity of 16,000.
- 32,000,000 – 1,000,000,000 bps, with granularity of 64,000.

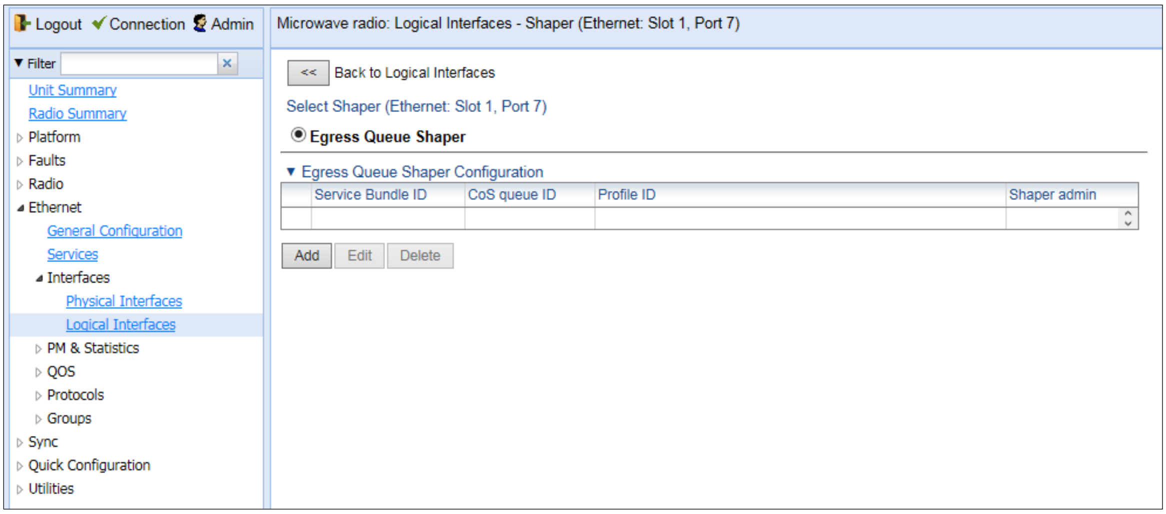
7 Click **Apply**, then **Close**.

Assigning a Queue Shaper Profile to a Queue

To assign a queue shaper profile to a queue:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 184).
2. Select an interface in the Ethernet Logical Port Configuration table and click **Shaper**. The Logical Interfaces – Shaper page opens, with the Egress Queue Shaper Configuration table open by default. All queue shaper profiles defined in the system are listed in the table.

Figure 215 Logical Interfaces – Shaper – Egress Queue Shaper

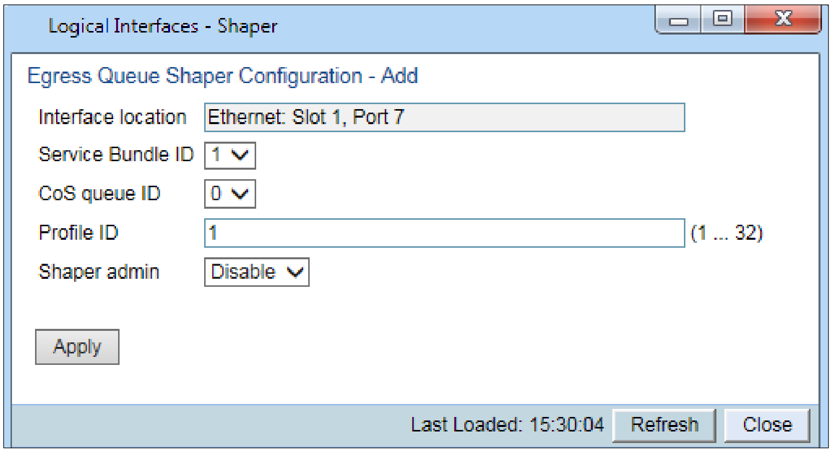


● Egress Queue Shaper

Service Bundle ID	CoS queue ID	Profile ID	Shaper admin

3. Click **Add**. The Egress Queue Shaper Configuration – Add page opens.

Figure 216 Logical Interfaces – Egress Queue Shaper Configuration – Add Page



Egress Queue Shaper Configuration - Add

Interface location: Ethernet: Slot 1, Port 7

Service Bundle ID: 1

CoS queue ID: 0

Profile ID: 1 (1 ... 32)

Shaper admin: Disable

Note

In this release, only one service bundle (Service Bundle ID 1) is supported.

4. In the **CoS queue ID** field, select the CoS queue ID of the queue to which you want to assign the shaper. Queues are numbered according to CoS value, from 0 to 7.
5. In the **Profile ID** field, select from a list of configured queue shaper profiles. See Configuring Queue Shaper Profiles.
6. In the **Shaper Admin** field, select **Enable** to enable egress queue shaping for the selected queue, or **Disable** to disable egress queue shaping for the selected queue.
7. Click **Apply**, then **Close**.

To assign a different queue shaper profile to a queue:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 184).
2. Select an interface in the Ethernet Logical Port Configuration table and click **Shaper**. The Logical Interfaces – Shaper page opens, with the Egress Queue Shaper Configuration table open by default (Figure 215).
3. Select an interface in the Ethernet Logical Port Configuration table and click **Shaper**. The Logical Interfaces – Shaper page opens, with the Egress Queue Shaper Configuration table open by default (Figure 215).
4. Select the row you want to edit and click **Edit**. The Egress Queue Shaper Configuration – Edit page opens. This page is similar to the Egress Queue Shaper Configuration – Add page (Figure 216).
5. To assign a different egress queue shaper profile, select the profile in the **Profile ID** field.
6. To enable or disable egress queue shaping for the selected queue, select **Enable** to enable egress queue shaping for the queue, or **Disable** to disable egress queue shaping for the queue.
7. Click **Apply**, then **Close**.

Configuring Scheduling

This section includes:

- Scheduling Overview
- Configuring Priority Profiles
- Configuring WFQ Profiles
- Assigning a Priority Profile to an Interface
- Assigning a WFQ Profile to an Interface

Scheduling Overview

Scheduling determines the priority among the queues. PTP 850 provides a unique hierarchical scheduling model that includes four priorities, with Weighted Fair Queuing (WFQ) within each priority, and shaping per port and per queue.

The scheduler scans the queues and determines which queue is ready to transmit. If more than one queue is ready to transmit, the scheduler determines which queue transmits first based on:

Queue Priority – A queue with higher priority is served before lower-priority queues.

Weighted Fair Queuing (WFQ) – If two or more queues have the same priority and are ready to transmit, the scheduler transmits frames from the queues based on a WFQ algorithm that determines the ratio of frames per queue based on a predefined weight assigned to each queue.

Configuring Priority Profiles

Scheduling priority profiles determine the queue priority. Each profile contains eight CoS-based priorities, corresponding to eight queues in an interface to which the profile is assigned. You can configure up to eight priority profiles. A ninth profile, Profile ID 9, is pre-configured. You can configure Green priorities from 4 (highest) to 1 (lowest). An additional four Yellow priority profiles are defined automatically.

This section includes:

Adding a Scheduler Priority Profile

Editing a Service Scheduler Priority Profile

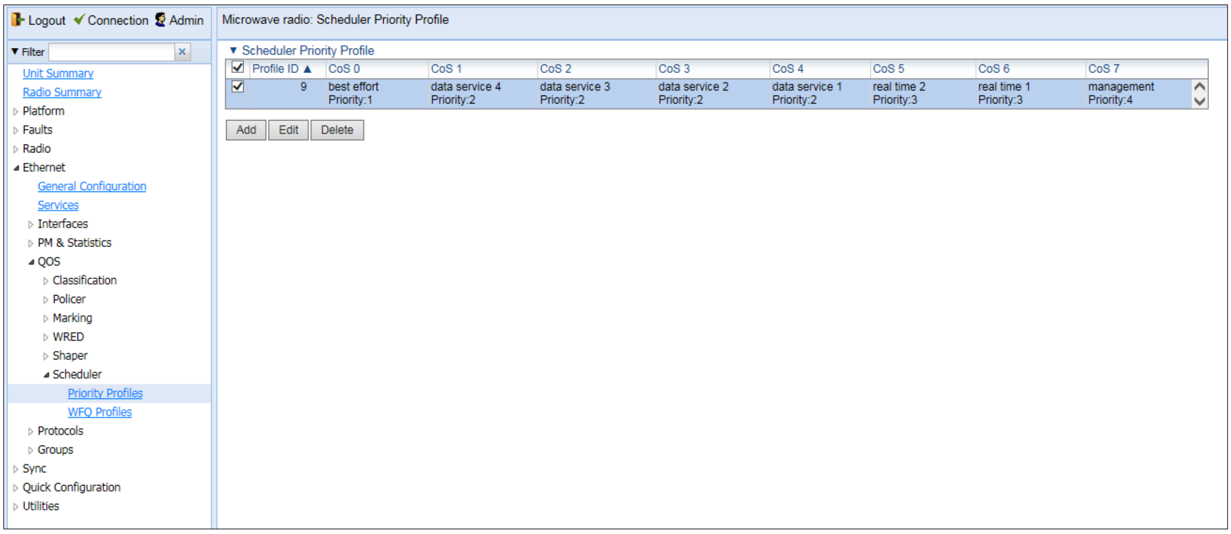
Deleting a Scheduler Priority Profile

Adding a Scheduler Priority Profile

To add a scheduler priority profile:

1. Select **Ethernet > QoS > Scheduler > Priority Profiles**. The Scheduler Priority Profile page opens.

Figure 217 Scheduler Priority Profile Page



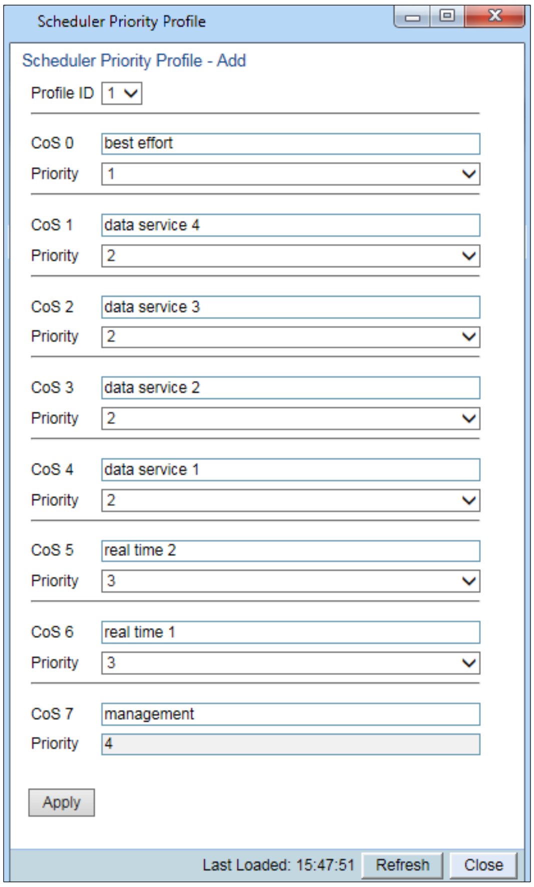
Microwave radio: Scheduler Priority Profile

▼ Scheduler Priority Profile

☑	Profile ID ▲	CoS 0	CoS 1	CoS 2	CoS 3	CoS 4	CoS 5	CoS 6	CoS 7
☑	9	best effort Priority:1	data service 4 Priority:2	data service 3 Priority:2	data service 2 Priority:2	data service 1 Priority:2	real time 2 Priority:3	real time 1 Priority:3	management Priority:4

2. Click **Add**. The Scheduler Priority Profile – Add page opens, with default values displayed.

Figure 218 Scheduler Priority Profile – Add Page



Scheduler Priority Profile - Add

Profile ID	1
CoS 0	best effort
Priority	1
CoS 1	data service 4
Priority	2
CoS 2	data service 3
Priority	2
CoS 3	data service 2
Priority	2
CoS 4	data service 1
Priority	2
CoS 5	real time 2
Priority	3
CoS 6	real time 1
Priority	3
CoS 7	management
Priority	4

Last Loaded: 15:47:51

3. In the **Profile ID** field, select a unique Profile ID between 1 and 8.
4. For each CoS value, enter the Green priority, from 4 (highest) to 1 (lowest) (1-4). This priority is applied to Green frames with that CoS egressing a queue to which the profile is assigned.
5. Optionally, you can enter a description of up to 20 characters in the field to the right of each CoS value.
6. Click **Apply**, then **Close**.

Note

The Yellow priority values are assigned automatically by the system.

Editing a Service Scheduler Priority Profile

To edit a scheduler priority profile:

1. Select **Ethernet > QoS > Scheduler > Priority Profiles**. The Scheduler Priority Profile page opens (Figure 217).
2. Select the profile you want to edit and click **Edit**. The Scheduler Priority Profile – Edit page opens. This page is similar to the Scheduler Priority Profile – Add page (Figure 218). You can edit any parameter except the **Profile ID**.
3. Modify the profile.
4. Click **Apply**, then **Close**.

Deleting a Scheduler Priority Profile

To delete a scheduler priority profile, select the profile in the Scheduler Priority Profiles page (Figure 217) and click **Delete**. The profile is deleted.

To delete multiple scheduler priority profiles:

1. Select the profiles in the Scheduler Priority Profiles page or select all the profiles by selecting the check box in the top row.
2. Click **Delete**. The profiles are deleted.

Configuring WFQ Profiles

WFQ profiles determine the relative weight per queue. Each profile contains eight CoS-based weight values, corresponding to eight queues in an interface to which the profile is assigned. You can configure up to five WFQ profiles. A sixth profile, Profile ID 1, is pre-configured.

This section includes:

WFQ Overview

The scheduler serves the queues based on their priority, but when two or more queues have data to transmit and their priority is the same, the scheduler uses Weighted Fair Queuing (WFQ) to determine the weight within each priority. WFQ defines the transmission ratio between the queues.

For each WFQ profile, you can determine the relative weights for both CIR and EIR traffic.

The system supports up to six WFQ profiles. Profile ID 1 is a pre-defined read-only profile, and is used as the default profile. Profiles 2 to 6 are user-defined profiles.

The following table provides an example of a WFQ profile.

Table 61 WFQ Profile Example

Profile ID (1-7) CoS	Queue Weight - CIR	Queue Weight - EIR
0	15	20
1	15	20
2	15	20
3	15	20
4	15	20
5	15	20
6	15	20
7	20	20

You can attach one of the configured WFQ profiles to each interface. By default, the interface is assigned Profile ID 1, the pre-defined system profile. Profile ID 1 assigns 20 to each CoS for both CIR and EIR traffic.

Adding a WFQ Profile

Editing a WFQ Priority Profile

Deleting a WFQ Profile

WFQ Overview

The scheduler serves the queues based on their priority, but when two or more queues have data to transmit and their priority is the same, the scheduler uses Weighted Fair Queuing (WFQ) to determine the weight within each priority. WFQ defines the transmission ratio between the queues.

For each WFQ profile, you can determine the relative weights for both CIR and EIR traffic.

The system supports up to six WFQ profiles. Profile ID 1 is a pre-defined read-only profile, and is used as the default profile. Profiles 2 to 6 are user-defined profiles.

The following table provides an example of a WFQ profile.

Table 61 WFQ Profile Example

Profile ID (1-7) CoS	Queue Weight - CIR	Queue Weight - EIR
0	15	20
1	15	20
2	15	20
3	15	20
4	15	20
5	15	20
6	15	20
7	20	20

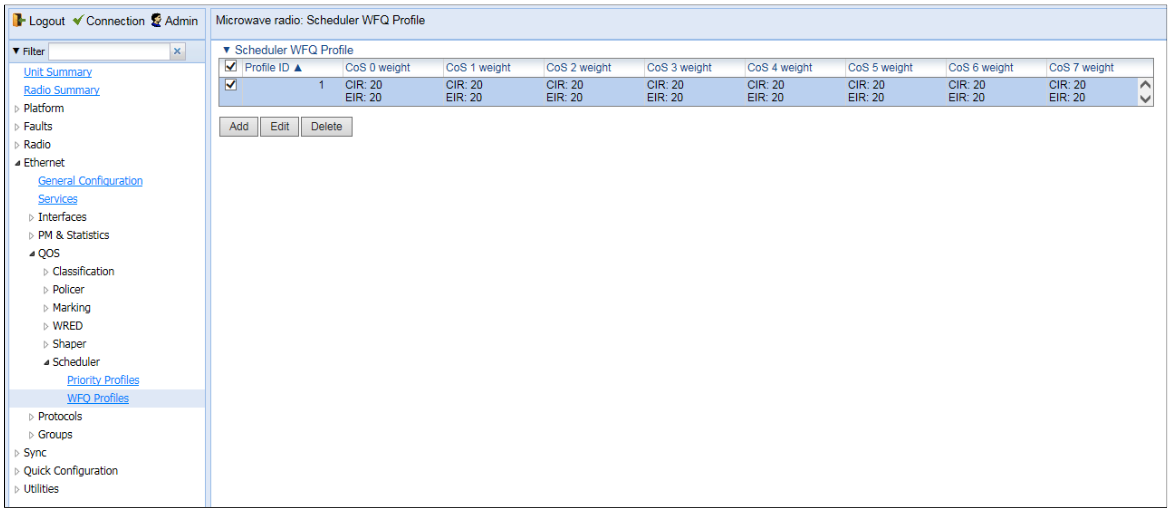
You can attach one of the configured WFQ profiles to each interface. By default, the interface is assigned Profile ID 1, the pre-defined system profile. Profile ID 1 assigns 20 to each CoS for both CIR and EIR traffic.

Adding a WFQ Profile

To add a WFQ profile:

1. Select **Ethernet > QoS > Scheduler > WFQ Profiles**. The Scheduler WFQ Profile page opens.

Figure 219 Scheduler WFQ Profile Page



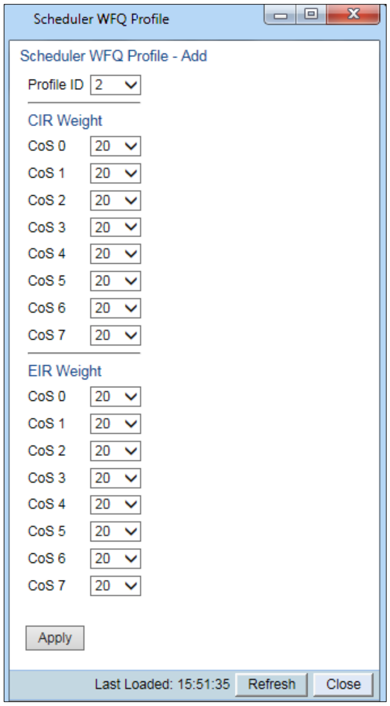
Microwave radio: Scheduler WFQ Profile

Scheduler WFQ Profile

☑	Profile ID ▲	CoS 0 weight	CoS 1 weight	CoS 2 weight	CoS 3 weight	CoS 4 weight	CoS 5 weight	CoS 6 weight	CoS 7 weight
☑	1	CIR: 20 EIR: 20	CIR: 20 EIR: 20	CIR: 20 EIR: 20	CIR: 20 EIR: 20	CIR: 20 EIR: 20	CIR: 20 EIR: 20	CIR: 20 EIR: 20	CIR: 20 EIR: 20

2. Click **Add**. The Scheduler WFQ Profile – Add page opens, with default values displayed.

Figure 220 Scheduler WFQ Profile – Add Page



Scheduler WFQ Profile - Add

Profile ID 2

CIR Weight

CoS 0	20
CoS 1	20
CoS 2	20
CoS 3	20
CoS 4	20
CoS 5	20
CoS 6	20
CoS 7	20

EIR Weight

CoS 0	20
CoS 1	20
CoS 2	20
CoS 3	20
CoS 4	20
CoS 5	20
CoS 6	20
CoS 7	20

Last Loaded: 15:51:35

3. In the **Profile ID** field, select a unique Profile ID between 2 and 7. Profile ID 1 is used for a pre-defined WFQ profile.
4. For each CoS value, enter the CIR weight and the EIR weight for that CoS, from 1 to 20.
5. Click **Apply**, then **Close**.

Editing a WFQ Priority Profile

To edit a scheduler WFQ profile:

1. Select **Ethernet > QoS > Scheduler > WFQ Profiles**. The Scheduler WFQ Profile page opens (Figure 219).
2. Select the profile you want to edit and click **Edit.** The Scheduler WFQ Profile – Edit page opens. This page is similar to the Scheduler WFQ Profile – Add page (Figure 212). You can edit any parameter except the **Profile ID**.
3. Modify the profile.
4. Click **Apply**, then **Close**.

Deleting a WFQ Profile

To delete a scheduler WFQ profile, select the profile in the Scheduler WFQ Profiles page (Figure 219) and click **Delete**. The profile is deleted.

To delete multiple scheduler WFQ profiles:

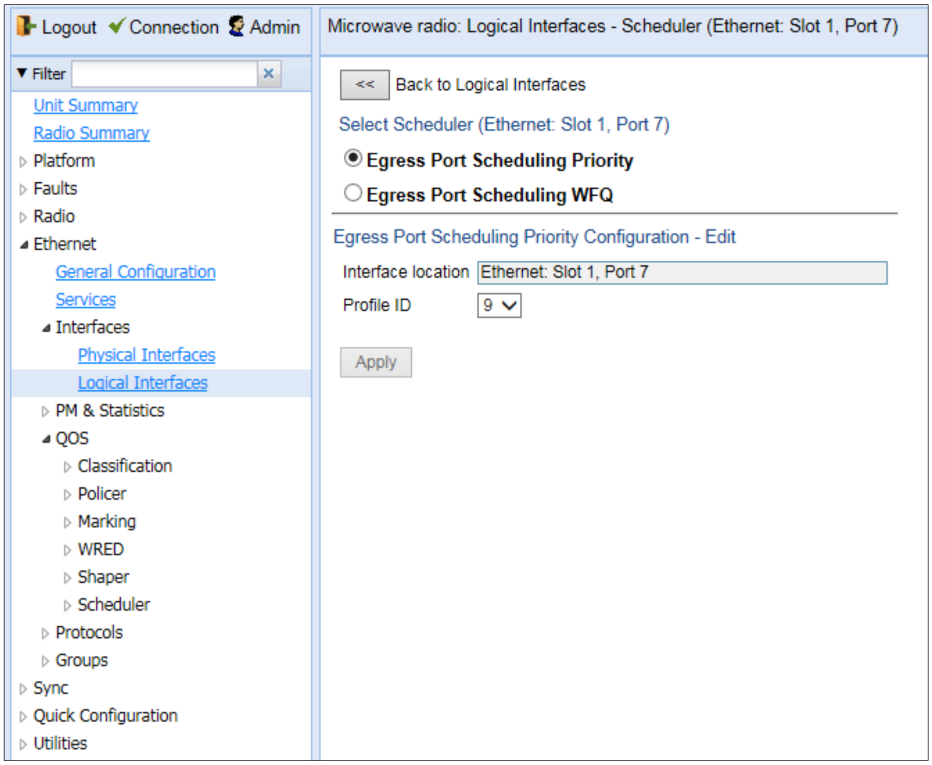
1. Select the profiles in the Scheduler WFQ Profiles page or select all the profiles by selecting the check box in the top row.
2. Click **Delete.** The profiles are deleted.

Assigning a Priority Profile to an Interface

To assign a priority profile to an interface:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 184).
2. Select an interface in the Ethernet Logical Port Configuration table and click **Scheduler.** The Logical Interfaces – Scheduler page opens, with the Egress Port Scheduling Priority Configuration – Edit page open by default.

Figure 221 Logical Interfaces – Scheduler – Egress Port Scheduling Priority



Microwave radio: Logical Interfaces - Scheduler (Ethernet: Slot 1, Port 7)

Select Scheduler (Ethernet: Slot 1, Port 7)

● Egress Port Scheduling Priority

○ Egress Port Scheduling WFQ

Egress Port Scheduling Priority Configuration - Edit

Interface location: Ethernet: Slot 1, Port 7

Profile ID: 9

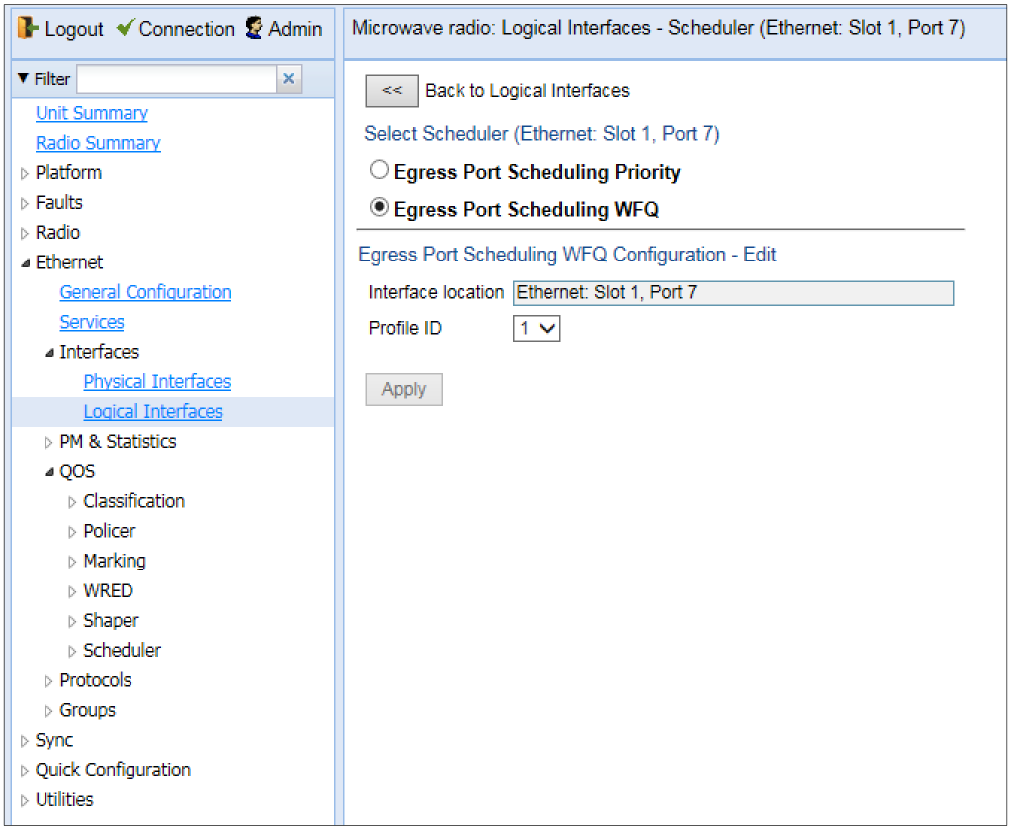
3. In the **Profile ID** field, select from a list of configured scheduling priority profiles. See *Configuring Priority Profiles*.
4. Click **Apply**, then **Close**.

Assigning a WFQ Profile to an Interface

To assign a WFQ profile to an interface:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 184).
2. Select an interface in the Ethernet Logical Port Configuration table and click **Scheduler.** The Logical Interfaces – Scheduler page opens, with the Egress Port Scheduling Priority Configuration – Edit page open by default (Figure 221).
3. Select **Egress Port Scheduling WFQ.** The Egress Port Scheduling WFQ Configuration – Edit page opens.

Figure 222 Logical Interfaces – Scheduler – Egress Port Scheduling WFQ



Microwave radio: Logical Interfaces - Scheduler (Ethernet: Slot 1, Port 7)

Select Scheduler (Ethernet: Slot 1, Port 7)

○ **Egress Port Scheduling Priority**

● **Egress Port Scheduling WFQ**

Egress Port Scheduling WFQ Configuration - Edit

Interface location: Ethernet: Slot 1, Port 7

Profile ID: 1

4. In the **Profile ID** field, select from a list of configured scheduling priority profiles. See Configuring WFQ Profiles.

5. Click **Apply**, then **Close**.

Configuring and Displaying Queue-Level PMs

PTP 850 devices support advanced traffic PMs per CoS queue and service bundle. For each logical interface, you can configure thresholds for Green and Yellow traffic per queue. You can then display the following PMs for 15-minute and 24-hour intervals, per queue and color:

- Maximum bytes passed per second
- Minimum bytes passed per second
- Average bytes passed per second
- Maximum bytes dropped per second
- Minimum bytes dropped per second
- Average bytes dropped per second
- Maximum packets passed per second
- Minimum packets passed per second
- Average packets passed per second
- Maximum packets dropped per second
- Minimum packets dropped per second
- Average packets dropped per second
- Seconds bytes per second were over the configured threshold per interval

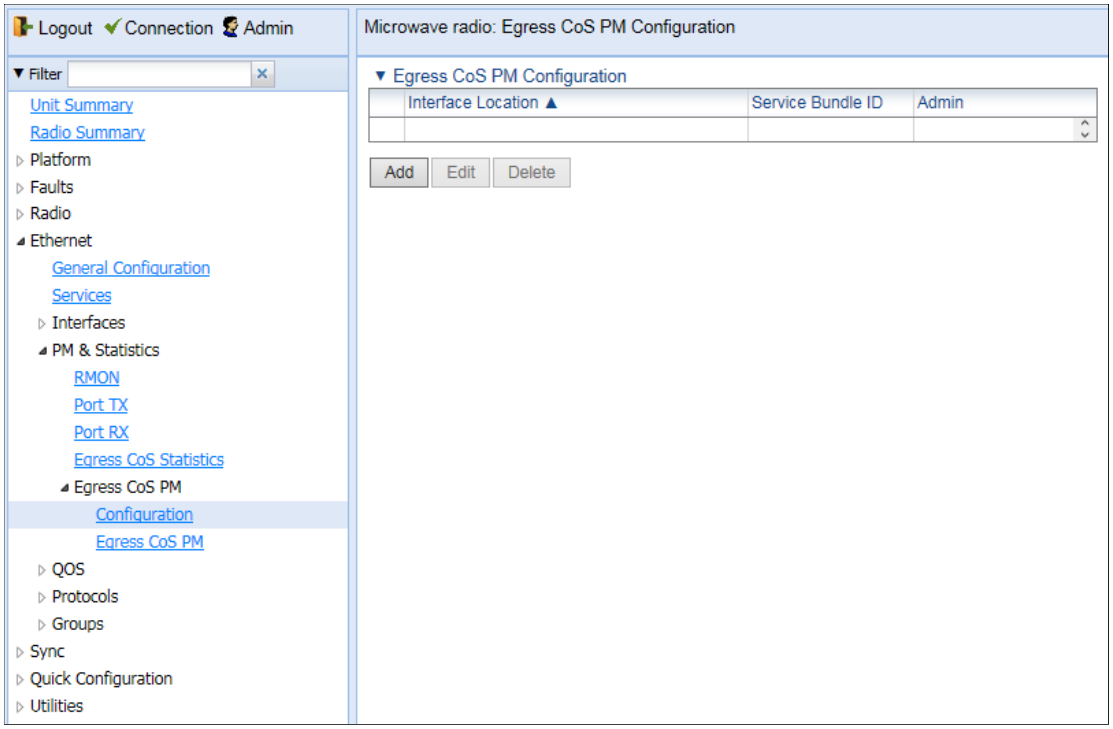
These PMs are available for any type of logical interface, including groups. To activate collection of these PMs, the user must add a PM collection rule on a logical interface and service bundle and set the relevant thresholds per CoS and Color. When the PM is configured on a group, queue traffic PMs are recorded for the group and not for the individual interfaces that belong to the group.

One collection rule is available per interface.

PMs for queue traffic are saved for 30 days, after which they are removed from the database. It is important to note that they are not persistent, which means they are not saved in the event of unit reset.

To configure queue-level PMs:

1 Select **Ethernet > PM & Statistics > Egress CoS PM > Configuration**. The Egress CoS PM Configuration page opens.



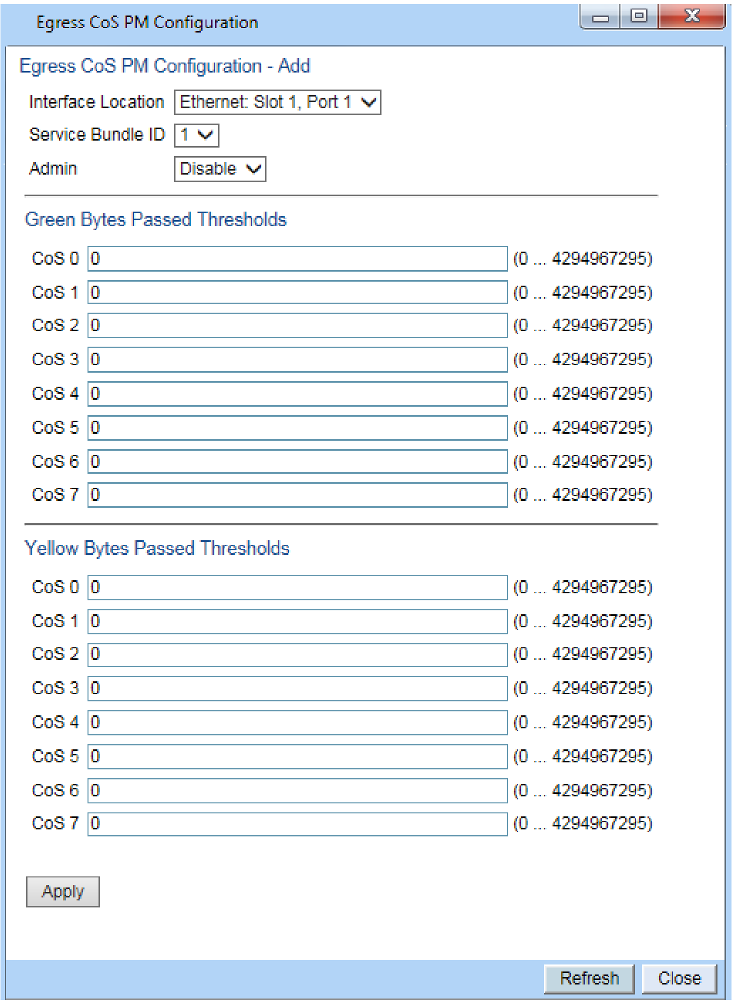
Microwave radio: Egress CoS PM Configuration

▼ Egress CoS PM Configuration

	Interface Location ▲	Service Bundle ID	Admin

Figure 223 Egress CoS PM Configuration Page

2 Click **Add**. The Egress CoS PM Configuration – Add page opens.



Egress CoS PM Configuration

Egress CoS PM Configuration - Add

Interface Location: Ethernet: Slot 1, Port 1

Service Bundle ID: 1

Admin: Disable

Green Bytes Passed Thresholds

CoS 0	0	(0 ... 4294967295)
CoS 1	0	(0 ... 4294967295)
CoS 2	0	(0 ... 4294967295)
CoS 3	0	(0 ... 4294967295)
CoS 4	0	(0 ... 4294967295)
CoS 5	0	(0 ... 4294967295)
CoS 6	0	(0 ... 4294967295)
CoS 7	0	(0 ... 4294967295)

Yellow Bytes Passed Thresholds

CoS 0	0	(0 ... 4294967295)
CoS 1	0	(0 ... 4294967295)
CoS 2	0	(0 ... 4294967295)
CoS 3	0	(0 ... 4294967295)
CoS 4	0	(0 ... 4294967295)
CoS 5	0	(0 ... 4294967295)
CoS 6	0	(0 ... 4294967295)
CoS 7	0	(0 ... 4294967295)

Figure 224 Egress CoS PM Configuration – Add Page

3 In the **Interface Location** field, select the interface for which you want to configure the collection rule.

4 In the **Service Bundle** field, select a service bundle (1-6).

5 In the **Admin** field, select **Enable** to enable the collection rule.

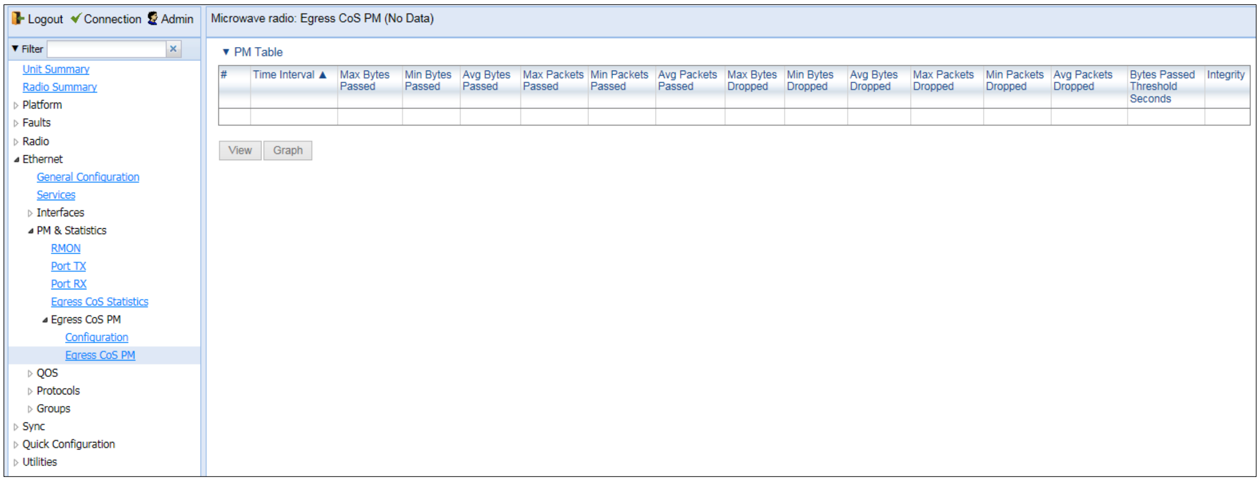
6 Enter the Green and Yellow thresholds for each CoS, in bytes (0-4294967295).

7 Click **Apply**.

8 Repeat these steps to configure collection rules for additional interfaces.

To display queue-level PMs:

1 Select **Ethernet > PM & Statistics > Egress CoS PM > Egress CoS PM**. The Egress CoS PM page opens.



Microwave radio: Egress CoS PM (No Data)

PM Table

#	Time Interval ▲	Max Bytes Passed	Min Bytes Passed	Avg Bytes Passed	Max Packets Passed	Min Packets Passed	Avg Packets Passed	Max Bytes Dropped	Min Bytes Dropped	Avg Bytes Dropped	Max Packets Dropped	Min Packets Dropped	Avg Packets Dropped	Bytes Passed Threshold Seconds	Integrity

Figure 225 Egress CoS PM Page

The **Integrity** column indicates whether the values received at the time and date of the measured interval are valid. An X in the column indicates that the values are invalid. This can occur for a number of reasons, including but not limited to a disconnected cable, a missing SFP module, muting of a radio interface, and an operational status of **Down**.

Chapter 11: Ethernet Protocols

This section includes:

- Configuring G.8032
- Configuring MSTP
- Configuring Ethernet Bandwidth Notification (ETH-BN)
- Configuring LLDP

Related Topics:

- Configuring Service OAM (SOAM) Fault Management (FM)

Configuring G.8032

This section includes:

- G.8032 Overview
- Configuring the Destination MAC Address
- Adding ERPIs
- Configuring the RPL Owner
- Configuring Timers
- Viewing the ERPI Configuration and Status Parameters
- Viewing ERPI State Information
- Initiating a Manual or Forced Switch and Clearing the Switch or Initiating Reversion
- Blocking or Unblocking R-APS Messages on a Service Point
- Viewing ERPI Statistics

G.8032 Overview

Note: P2P services are not affected by G.8032, and continue to traverse ports that are blocked by G.8032. G.8032 cannot be configured on management ports, including management ports used for traffic (PTP 850S).

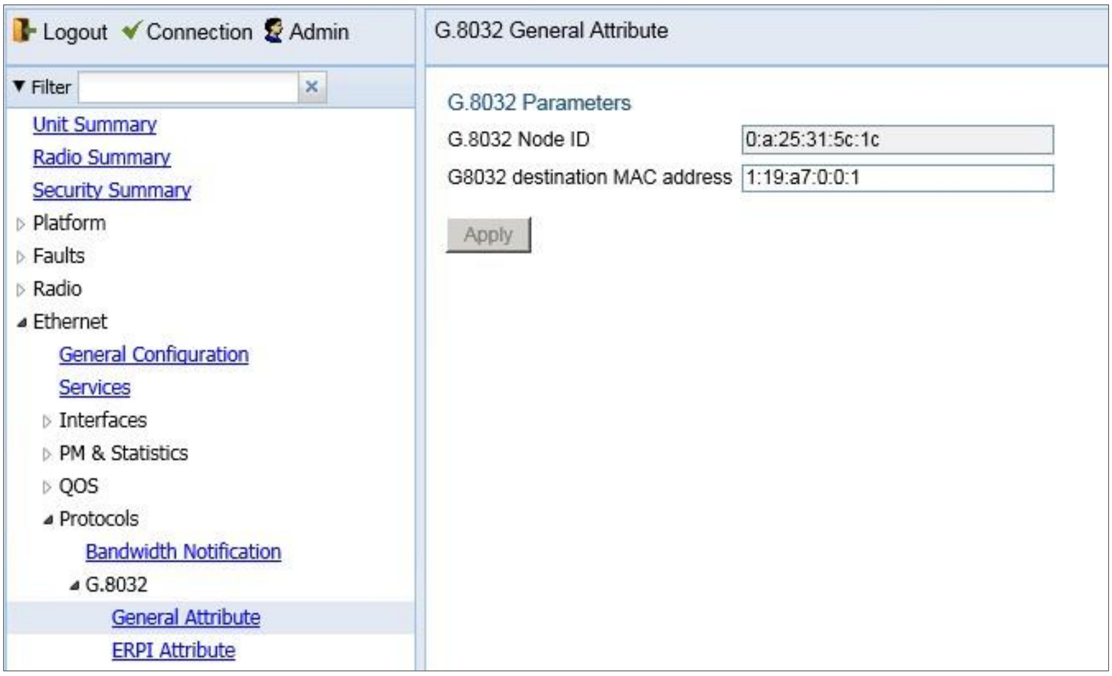
ERPS, as defined in the G.8032 ITU standard, is currently the most advanced ring protection protocol, providing convergence times of sub-50ms. ERPS prevents loops in an Ethernet ring by guaranteeing that at any time, traffic can flow on all except one link in the ring. This link is called the Ring Protection Link (RPL). Under normal conditions, the RPL is blocked, i.e., not used for traffic. One designated Ethernet Ring Node, the RPL Owner Node, is responsible for blocking traffic at one end of the RPL. When an Ethernet ring failure occurs, the RPL Owner unblocks its end of the RPL, allowing the RPL to be used for traffic. The other Ethernet Ring Node adjacent to the RPL, the RPL Neighbor Node, may also participate in blocking or unblocking its end of the RPL. A number of ERP instances (ERPIs) can be created on the same ring.

For a more detailed description of G.8032, refer to the Technical Description for the product you are using.

Configuring the Destination MAC Address

To configure the destination MAC address for G.8032:

1 Select **Ethernet > Protocols > G.8032 > General Attribute**. The G.8032 General Attribute page opens.



G.8032 General Attribute

G.8032 Parameters

G.8032 Node ID: 0:a:25:31:5c:1c

G8032 destination MAC address: 1:19:a7:0:0:1

Figure 305: G.8032 General Attribute Page

2 In the **G8032 destination MAC address field**, enter the destination MAC address for PDUs generated by the node.

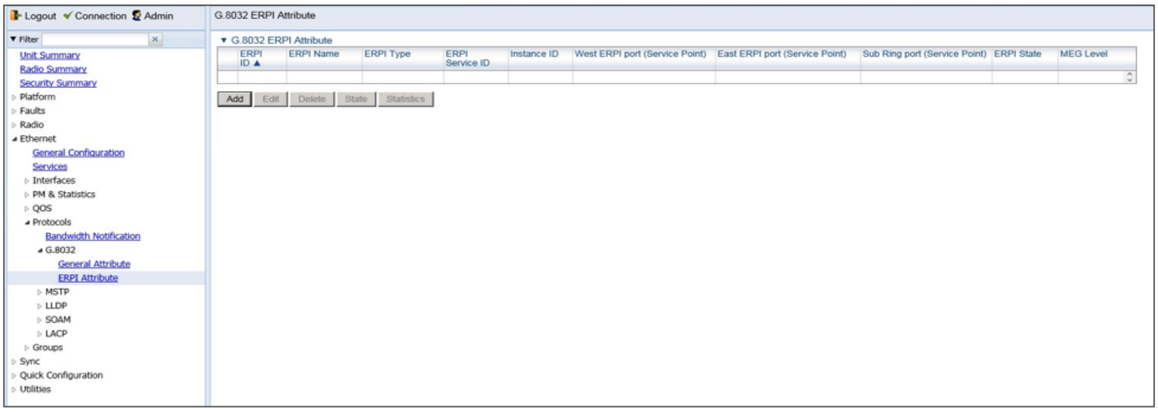
3 Click **Apply**.

Adding ERPIs

You can configure up to 16 Ethernet Ring Protection instances (ERPIs). Each ERPI is associated with an Ethernet service defined in the system.

To add an ERPI:

1 Select **Ethernet > Protocols > G.8032 > ERPI Attribute**. The G.8032 ERPI Attribute page opens.



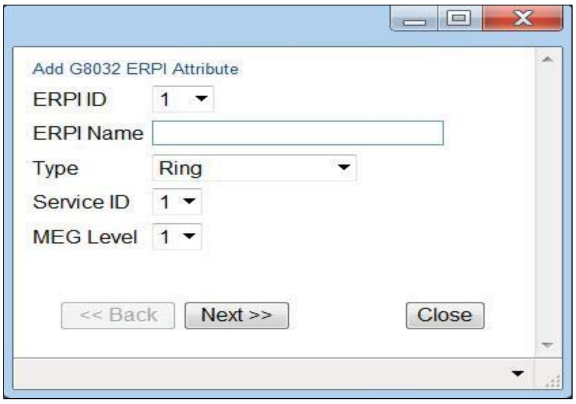
G.8032 ERPI Attribute

▼ G.8032 ERPI Attribute

ERPI ID ▲	ERPI Name	ERPI Type	ERPI Service ID	Instance ID	West ERPI port (Service Point)	East ERPI port (Service Point)	Sub Ring port (Service Point)	ERPI State	MEG Level

Figure 306: G.8032 ERPI Attribute Page

2 Click **Add**. The Add G8032 ERPI Attribute wizard opens.



Add G8032 ERPI Attribute

ERPI ID: 1

ERPI Name:

Type: Ring

Service ID: 1

MEG Level: 1

Figure 307: G.8032 ERPI Attribute Wizard – Page 1

3 In the **ERPI ID** field, select an available ID. The ERPI ID is a unique ID that identifies the ERPI.

4 Optionally, in the **ERPI Name** field, enter a descriptive name for the ERPI.

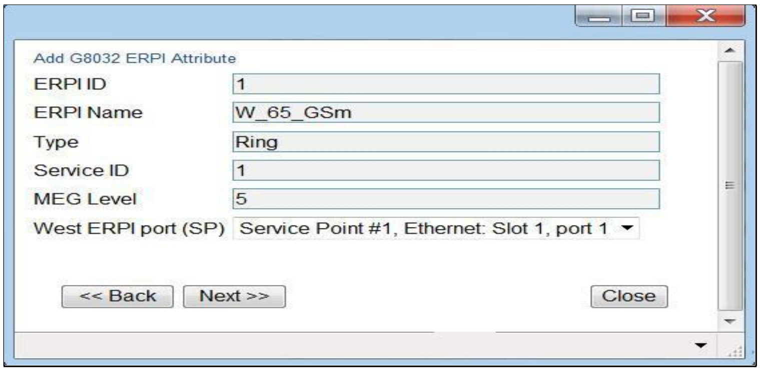
5 In the **Type** field, select the type of ERPI, based on the type of ring:

- Ring: A Ring is an Ethernet ring that is connected on two ports (East and West service points) to an interconnection node.
- Sub-ring: A Sub-Ring is an Ethernet ring which is connected to another ring or network through the use of interconnection nodes (East and West service points). On their own, the Sub-Ring links do not form a closed physical loop. A closed loop may be formed by the sub-ring links and the link between interconnection nodes that is controlled by other ring or network.
- Ring with sub-ring: The ERPI includes both a ring, with East and West service points, and a connection to a sub-ring using a Sub-Ring service point.

6 In the **Service ID** field, select the ID of the Ethernet service to which the ERPI belongs.

7 Optionally, in the **MEG Level** field, select the Maintenance Entity Group (MEG) level used for R-APS messages sent in the ERPI (0-7).

8 Click **Next**. The second page of the Add G.8032 ERPI Attribute wizard opens.



Add G8032 ERPI Attribute

ERPI ID: 1

ERPI Name: W_65_GSm

Type: Ring

Service ID: 1

MEG Level: 5

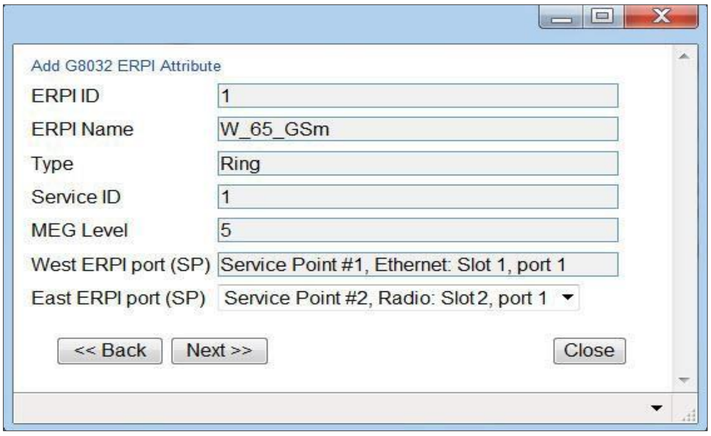
West ERPI port (SP): Service Point #1, Ethernet: Slot 1, port 1

Figure 308: G.8032 ERPI Attribute Wizard – Page 2

9 In the **West ERPI port (SP)** field, select the first endpoint for the ERPI. This can be any service point that has been configured for the service.

Note: Service points on the PTP 850 side of the link must have a single, determinate VLAN. This means the service point type must be dot1q, s-tag, or QinQ. On the customer side, any service point type can be used.

10 Click **Next**. The third page of the Add G.8032 ERPI Attribute wizard opens.



Add G8032 ERPI Attribute

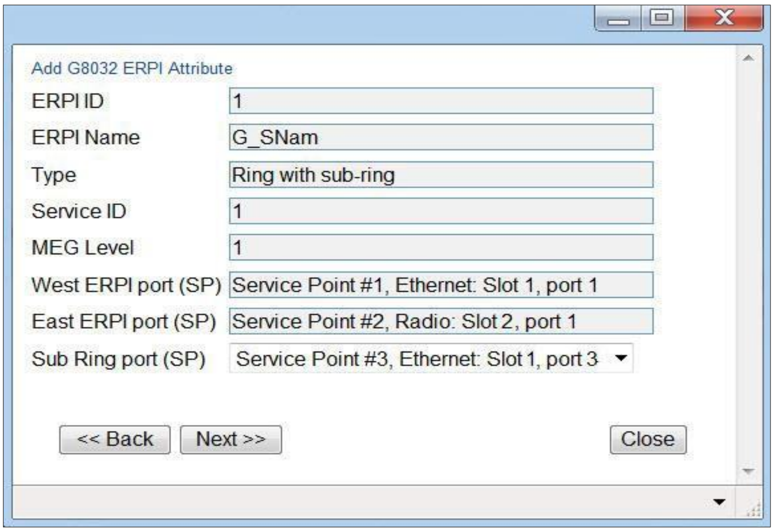
ERPI ID	1
ERPI Name	W_65_GSm
Type	Ring
Service ID	1
MEG Level	5
West ERPI port (SP)	Service Point #1, Ethernet: Slot 1, port 1
East ERPI port (SP)	Service Point #2, Radio: Slot 2, port 1

Figure 309: G.8032 ERPI Attribute Wizard – Page 3

11 In the **East ERPI port (SP)** field, select the second endpoint for the ERPI. This can be any service point that has been configured for the service.

12 Click **Next**:

- If the Type is Ring or Sub-ring, the Submit page opens. Go to Step 15.
- If the Type is Ring with sub-ring, the fourth page of the Add G.8032 ERPI Attribute wizard opens.



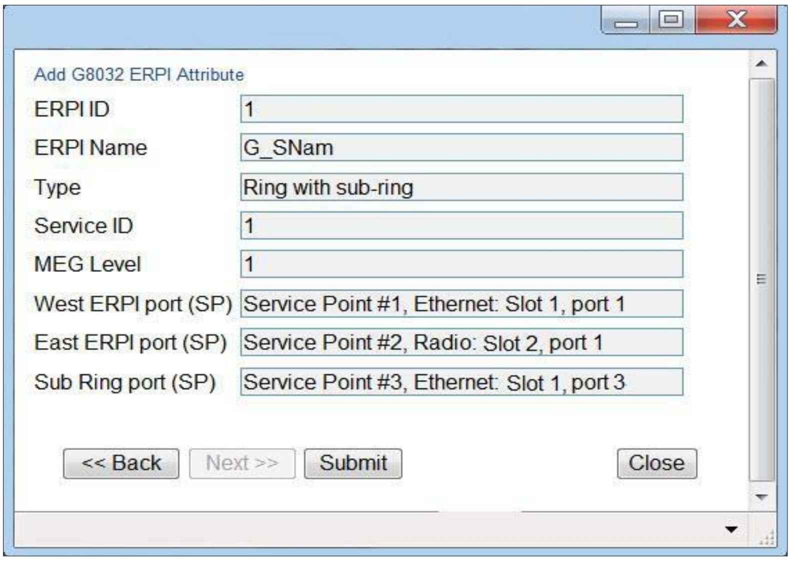
Add G8032 ERPI Attribute

ERPI ID	1
ERPI Name	G_SNam
Type	Ring with sub-ring
Service ID	1
MEG Level	1
West ERPI port (SP)	Service Point #1, Ethernet: Slot 1, port 1
East ERPI port (SP)	Service Point #2, Radio: Slot 2, port 1
Sub Ring port (SP)	Service Point #3, Ethernet: Slot 1, port 3

Figure 310: G.8032 ERPI Attribute Wizard – Page 4

13 In the **Sub Ring port (SP)** field, select the service point that connects the Ring with the Sub-Ring. This can be any service point that has been configured for the service.

14 Click **Next**. The Submit page opens.



Add G8032 ERPI Attribute

ERPI ID	1
ERPI Name	G_SNam
Type	Ring with sub-ring
Service ID	1
MEG Level	1
West ERPI port (SP)	Service Point #1, Ethernet: Slot 1, port 1
East ERPI port (SP)	Service Point #2, Radio: Slot 2, port 1
Sub Ring port (SP)	Service Point #3, Ethernet: Slot 1, port 3

Figure 311: G.8032 ERPI Attribute Wizard – Submit

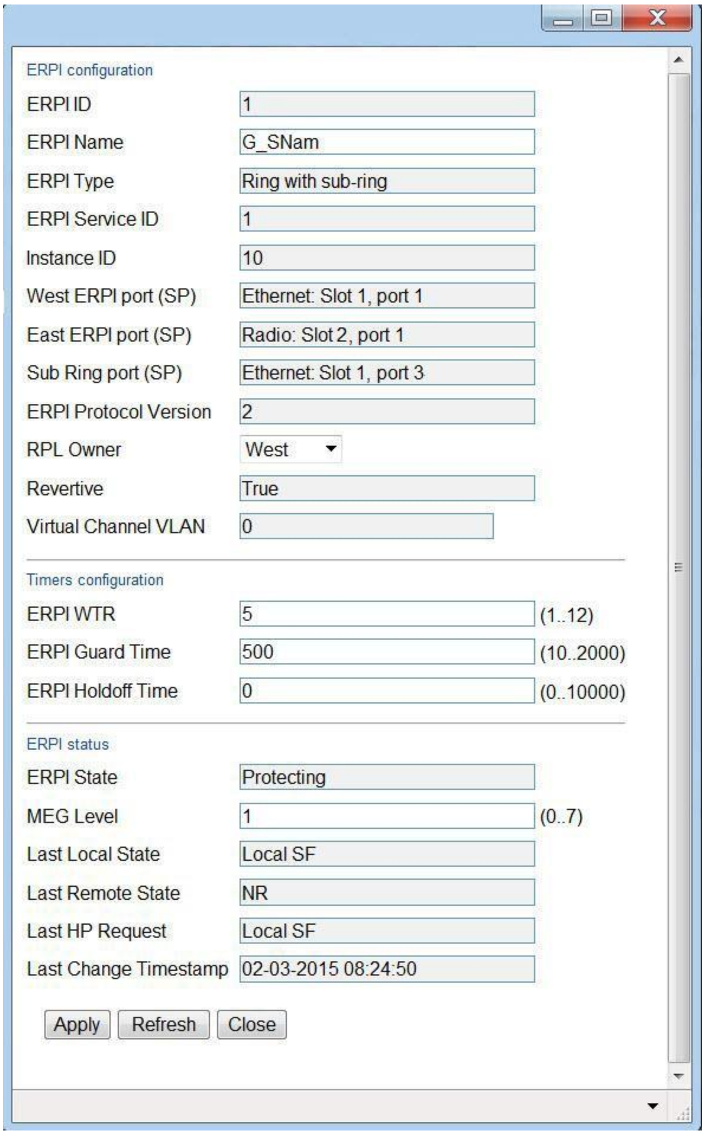
15 Verify that the parameters of the ERPI are correct and click **Submit**.

Configuring the RPL Owner

The RPL Owner Node is a node in the ERPI that is responsible for blocking traffic at one end of the ERPI. You can select one RPL per ERPI. To designate the RPL Owner Node:

1 Select **Ethernet > Protocols > G.8032 > ERPI Attribute**. The G.8032 ERPI Attribute page opens (*Figure 306*).

2 Select the ERPI and click **Edit**. The ERPI Attribute – Edit page opens.



ERPI configuration

ERPI ID	1	
ERPI Name	G_SNam	
ERPI Type	Ring with sub-ring	
ERPI Service ID	1	
Instance ID	10	
West ERPI port (SP)	Ethernet: Slot 1, port 1	
East ERPI port (SP)	Radio: Slot 2, port 1	
Sub Ring port (SP)	Ethernet: Slot 1, port 3	
ERPI Protocol Version	2	
RPL Owner	West	
Revertive	True	
Virtual Channel VLAN	0	

Timers configuration

ERPI WTR	5	(1..12)
ERPI Guard Time	500	(10..2000)
ERPI Holdoff Time	0	(0..10000)

ERPI status

ERPI State	Protecting	
MEG Level	1	(0..7)
Last Local State	Local SF	
Last Remote State	NR	
Last HP Request	Local SF	
Last Change Timestamp	02-03-2015 08:24:50	

Figure 312: G.8032 ERPI Attribute – Edit Page

3 In the **RPL Owner** field, select the service point you want to configure as RPL Owner.

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

Configuring Timers

You can configure timers per ERPI to control the ERPI's switching and convergence parameters. The following timers are available:

- **Wait to Restore (WTR) Timer** – Defines a minimum time the system waits after signal failure is recovered before reverting to idle state, when the RPL can again be blocked.
- **Guard Time** – The guard time is the minimum time the system waits after recovery from a signal failure before accepting new R-APS messages. The Guard Time should be greater than the maximum expected forwarding delay for which one R-APS message circles around the ring.
- **Hold-Off Time** – Determines the time period from failure detection to response. It is used to coordinate between recovery mechanisms (which mechanism takes place first).

To configure the ERPI timers:

1. Select **Ethernet > Protocols > G.8032 > ERPI Attribute**. The G.8032 ERPI Attribute page opens (*Figure 306*).
2. Select the ERPI and click **Edit**. The ERPI Attribute – Edit page opens (*Figure 312*).
3. In the **ERPI WTR** field, enter the Wait to Restore (WTR) timer (in minutes).
4. In the **ERPI Guard Time** field, enter the ERPI guard time (in msec). You must enter a multiple of 10.
5. In the **ERPI Holdoff Time** field, enter the ERPI hold-off time (in msec). You must enter a multiple of 100.
6. Click Apply, then Close.

8.1.2 Viewing the ERPI Configuration and Status Parameters

The G.8032 ERPI Attribute page (*Figure 306*) displays some of the configuration and status parameters for ERPIs configured in the system.

To display a full list of configuration and status parameters for an ERPI:

1. Select **Ethernet > Protocols > G.8032 > ERPI Attribute**. The G.8032 ERPI Attribute page opens .
2. Select the ERPI and click **Edit**. The ERPI Attribute – Edit page opens.
   - Table 63 lists and describes the parameters in the ERPI configuration section of the ERPI Attribute – Edit page.
   - Table 64 lists and describes the parameters in the ERPI status section of the ERPI Attribute – Edit page.

Table 63: ERPI Configuration Parameters

Parameter	Definition
ERPI ID	Read-only. A unique ID that identifies the ERPI.
ERPI Name	A descriptive name for the ERPI.
ERPI Type	Read-only. The ERPI type.
ERPI Service ID	Read-only. The ID of the Ethernet service to which the ERPI belongs.
Instance ID	Read-only. The MSTI to which the Ethernet service is mapped. See *Mapping Ethernet Services to MSTP Instances (MSTIs)*
West ERPI Port (SP)	Read-only. The interface to which the west ERPI service point belongs.
East ERPI Port (SP)	Read-only. The interface to which the east ERPI service point belongs.
Sub Ring Port (SP)	Read-only. The interface to which the service point that connects the Ring with the Sub-Ring belongs.
ERPI Protocol Version	Read-only. The ERPI (G.8032) protocol version currently being used in the unit.
RPL Owner	The RPL Owner Node is a node in the ERPI that is responsible for blocking traffic at one end of the ERPI. See *Configuring the RPL Owner*.
Revertive	Read-only. Indicates whether the ERPI is currently in revertive mode.
Virtual Channel VLAN	Read-only. The VLAN of the virtual channel. If the value is 0, there is no virtual channel.

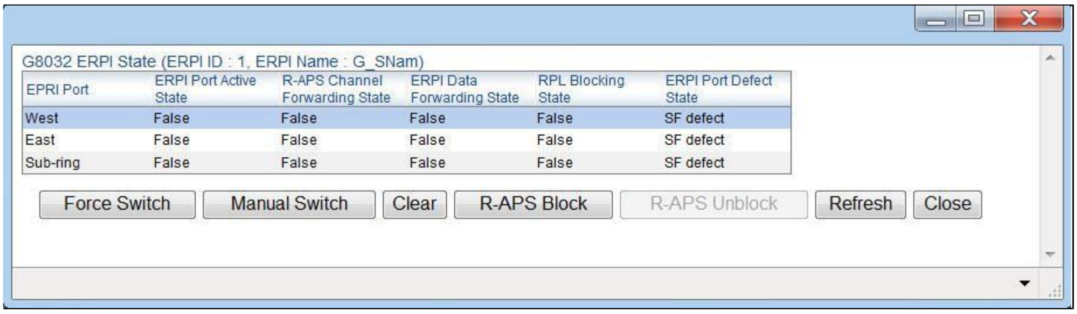
Table 64: ERPI Status Parameters

Parameter	Definition
ERPI State	Indicates the current ERPI state. Possible values are: • Initializing • Idle • Pending • Protecting • FS (Forced Switch) • MS (Manual Switch)
MEG Level	The Maintenance Entity Group (MEG) level used for R-APS messages sent in the ERPI.
Last Local State	Describes the current local state input to the ERPI state machine.
Last Remote State	Indicates the last event received from the other end of the link.
Last HP Request	Indicates the last high-priority event.
Last Change Timestamp	Indicates the time of the last ring state transition.

Viewing ERPI State Information

To view information about an ERPI's state:

1. Select **Ethernet > Protocols > G.8032 > ERPI Attribute**. The G.8032 ERPI Attribute page opens (*Figure 306*).
2. Select the ERPI and click **State**. The ERPI Attribute – State page opens.



G8032 ERPI State (ERPI ID : 1, ERPI Name : G_SNam)

EPRI Port	ERPI Port Active State	R-APS Channel Forwarding State	ERPI Data Forwarding State	RPL Blocking State	ERPI Port Defect State
West	False	False	False	False	SF defect
East	False	False	False	False	SF defect
Sub-ring	False	False	False	False	SF defect

Figure 313: G.8032 ERPI Attribute – State Page

Below table lists and describes the parameters in the ERPI Attribute – State page.

Table 65: ERPI State Parameters

Parameter	Definition
ERPI Port	Identifies whether the row is for the West endpoint, the East endpoint, or a Sub-Ring
ERPI Port Active State	Indicates whether or not the service point is active for traffic forwarding.
R-APS Channel Forwarding State	Indicates whether the service point is forwarding R-APS messages.
ERPI Data Forwarding State	Indicates whether the service point is in unblocked (forwarding) state.
RPL Blocking State	Only relevant if the ERPI to which the service point belongs is the RPL owner. Indicates whether the
ERPI Port Defect State	Indicates whether the service point is in Signal Fail (SF) or Signal Defect (SD) state. Note: Support for Signal Defect state is planned for future release.

Initiating a Manual or Forced Switch and Clearing the Switch or Initiating Reversion

You can initiate a manual or forced switch, clear the switch, and initiate reversion, from the G.8032 ERPI Attribute – State page:

1 Select **Ethernet > Protocols > G.8032 > ERPI Attribute**. The G.8032 ERPI Attribute page opens (*Figure 306*).

2 Select the ERPI and click **State**. The ERPI Attribute – State page opens (*Figure 313*).

3 Select the service point on which you want to perform the operation.

- To initiate a forced switch, click Force Switch.
- To initiate a manual switch, click Manual Switch.
- To clear a forced or manual switch, click Clear. You can also click Clear to trigger convergence prior to the expiration of the relevant timer.

Blocking or Unblocking R-APS Messages on a Service Point

To enable or disable transmission of R-APS messages on a service point:

1 Select **Ethernet > Protocols > G.8032 > ERPI Attribute**. The G.8032 ERPI Attribute page opens (*Figure 306*).

2 Select the ERPI and click **State**. The ERPI Attribute – State page opens (*Figure 313*).

3 Select the service point on which you want to perform the operation.

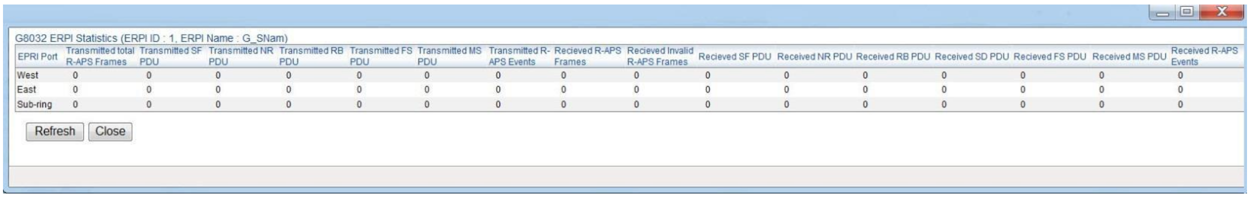
- To block R-APS message transmission on the service point, click R-APS Block.
- To enable R-APS message transmission on the service point, click R-APS Unblock.

Viewing ERPI Statistics

To view statistics about an ERPI:

1 Select **Ethernet > Protocols > G.8032 > ERPI Attribute**. The G.8032 ERPI Attribute page opens (*Figure 306*).

2 Select the ERPI and click **Statistics**. The ERPI Attribute – Statistics page opens.



G8032 ERPI Statistics (ERPI ID : 1, ERPI Name : G_SNam)

EPRI Port	Transmitted total R-APS Frames	Transmitted SF PDU	Transmitted NR PDU	Transmitted RB PDU	Transmitted FS PDU	Transmitted MS PDU	Transmitted R-APS Events	Recieved R-APS Frames	Recieved Invalid R-APS Frames	Recieved SF PDU	Received NR PDU	Received RB PDU	Received SD PDU	Recieved FS PDU	Received MS PDU	Received R-APS Events
West	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
East	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sub-ring	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 314: G.8032 ERPI Attribute – Statistics Page

Table 66 lists and describes the statistics shown in the ERPI Attribute – Statistics page.

Table 66: ERPI Statistics

Parameter	Definition
ERPI Port	Identifies whether the row is for the West endpoint, the East endpoint, or a Sub-Ring connection point.
Transmitted Total R-APS Frames	The number of R-APS frames that have been transmitted via the service point.
Transmitted SF PDU	The number of R-APS Signal Fail (SF) frames that have been transmitted via the service point.
Transmitted NR PDU	The number of R-APS No Request (NR) frames that have been transmitted via the service point.
Transmitted RB PDU	The number of R-APS RPL Blocked (RB) frames that have been transmitted via the service point.
Transmitted FS PDU	The number of R-APS Force Switched (FS) frames that have been transmitted via the service point.
Transmitted MS PDU	The number of R-APS Manual Switched (MS) frames that have been transmitted via the service point.
Transmitted R-APS	Reserved for future use.
Received R-APS Frames	The number of R-APS frames that have been received via the service point.
Received Invalid R-APS Frames	The number of R-APS frames with an invalid format that have been received via the service point.
Received SF PDU	The number of R-APS Signal Fail (SF) frames that have been received via the service point.
Received NR PDU	The number of R-APS No Request (NR) frames that have been received via the service point.
Received RB PDU	The number of R-APS RPL Blocked (RB) frames that have been received via the service point.
Received SD PDU	The number of R-APS Signal Degrade (SD) frames that have been received via the service point.
Received FS PDU	The number of R-APS Forced Switch (FS) frames that have been received via the service point.
Received MS PDU	The number of R-APS Manual Switch (MS) frames that have been received via the service point.
Received R-APS Events	Reserved for future use.

Configuring MSTP

This section includes:

- MSTP Overview
- Mapping Ethernet Services to MSTP instances (MSTIs)
- Configuring the MSTP Bridge Parameters
- Configuring the MSTP Port Parameters

MSTP Overview

Note: P2P services are not affected by MSTP, and continue to traverse ports

that are blocked by MSTP. MSTP cannot be configured on management ports, including

management ports used for traffic (PTP 850S).

MSTP, as defined in IEEE 802.1q, provides full connectivity for frames assigned to any given VLAN throughout a bridged LAN consisting of arbitrarily interconnected bridges.

With MSTP, an independent multiple spanning tree instance (MSTI) is configured for each group of services, and only one path is made available (unblocked) per spanning tree instance. This prevents network loops and provides load balancing capability. It also enables operators to differentiate among Ethernet services by mapping them to different, specific MSTIs. The maximum number of MSTIs is configurable, from 2 to 16.

MSTP is an extension of, and is backwards compatible with, Rapid Spanning Tree Protocol (RSTP).

PTP 820F, PTP 820G, and PTP 820GX support MSTP according to the following IEEE standards:

- 802.1q
- 802.1ad amendment (Q-in-Q)
- 802.1ah (TE instance)

For a more detailed description of MSTP support, refer to the *Technical Description* for the product you are using.

Mapping Ethernet Services to MSTP instances (MSTIs)

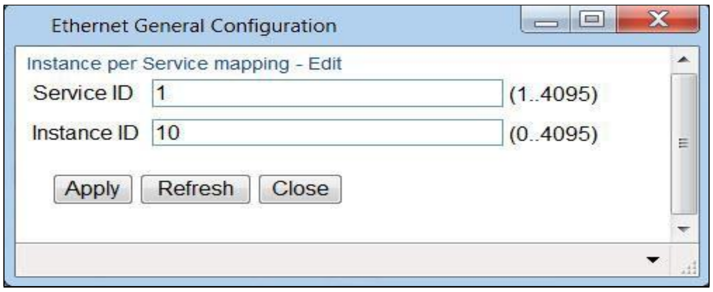
Ethernet services can be mapped to MSTP instances (MSTIs) in the Instances per Service Mapping section of the Ethernet General Configuration page. All mapping of Ethernet services to MSTP instances (MSTIs) should be performed before enabling MSTP.

To map Ethernet services to MSTP instances (MSTIs):

1 Select **Ethernet > General Configuration**. The Ethernet General Configuration page opens (*Figure 226*).

2 In the Instance per Service Mapping table, select the Service ID of the service you want to map.

3 Click **Edit**. The Instance per Service Mapping – Edit page opens.



Ethernet General Configuration

Instance per Service mapping - Edit

Service ID: 1 (1..4095)

Instance ID: 10 (0..4095)

Figure 315: Instance Per Service Mapping – Edit Page

4 In the **Instance ID** field, enter a number between 0 and 16, or 4095. A service mapped to MSTI 4095 is never blocked by any protocol.

5 Click **Apply**.

By default, all Ethernet services are mapped to MSTI 0, which represents the CIST (Common Instance Spanning Tree).

Configuring the MSTP Bridge Parameters

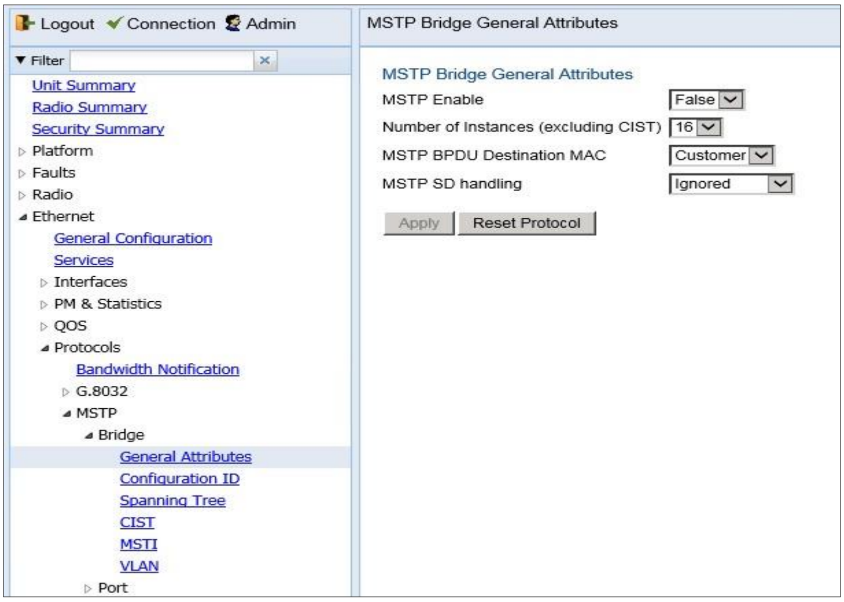
This section includes:

- Enabling MSTP and Configuring the MSTP Bridge General Attributes
- Viewing and Configuring the MSTP Bridge Configuration ID
- Viewing and Configuring the MSTP Bridge Spanning Tree
- Viewing and Configuring the MSTP Bridge CIST Parameters
- Viewing and Configuring the MSTP Bridge MSTI Parameters
- Viewing the MSTP VLAN Parameters

Enabling MSTP and Configuring the MSTP Bridge General Attributes

To configure the MSTP bridge general attributes:

1 Select **Ethernet > Protocols > MSTP > Bridge > General Attributes**. The MSTP Bridge General Attributes page opens.



MSTP Bridge General Attributes

MSTP Bridge General Attributes

MSTP Enable: False

Number of Instances (excluding CIST): 16

MSTP BPDU Destination MAC: Customer

MSTP SD handling: Ignored

Figure 316: MSTP Bridge General Attributes Page

2 In the **MSTP Enable** field, select **True** to enable MSTP on the unit. To disable MSTP, select **False**.

- ◦ Enabling MSTP starts the protocol and sets all ports in all MSTP instances to Blocking state. Convergence upon enabling the protocol generally takes less than two seconds.
- ◦ Disabling MSTP stops the MSTP protocol from running and sets all ports in all MSTP instances to Forwarding state.

3 In the **Number of Instances (excluding CIST)** field, select the number of Multiple Spanning Tree instances (MSTIs). Possible values are 1-16. This number does not include the Common and Internal Spanning Tree (CIST).

4 In the **MSTP BPDU Destination MAC** field, select the destination MAC address of BPDUs generated in the unit. Options are:

- ◦ Customer – The destination MAC address of BPDUs is 0x0180-C200-0000. Provider BPDUs are either tunneled or discarded.
- ◦ Provider – The destination MAC address of BPDUs is 0x0180-C200-0008. Customer BPDUs are either tunneled or discarded.

5 In the **MSTP SD Handling** field, select how MSTP handles Signal Degrade (SD) failures. Options are:

- ◦ Ignored – Signal Degrade (SD) failures are ignored in MSTP.
- ◦ Same as SF – SD failures trigger a topology change.

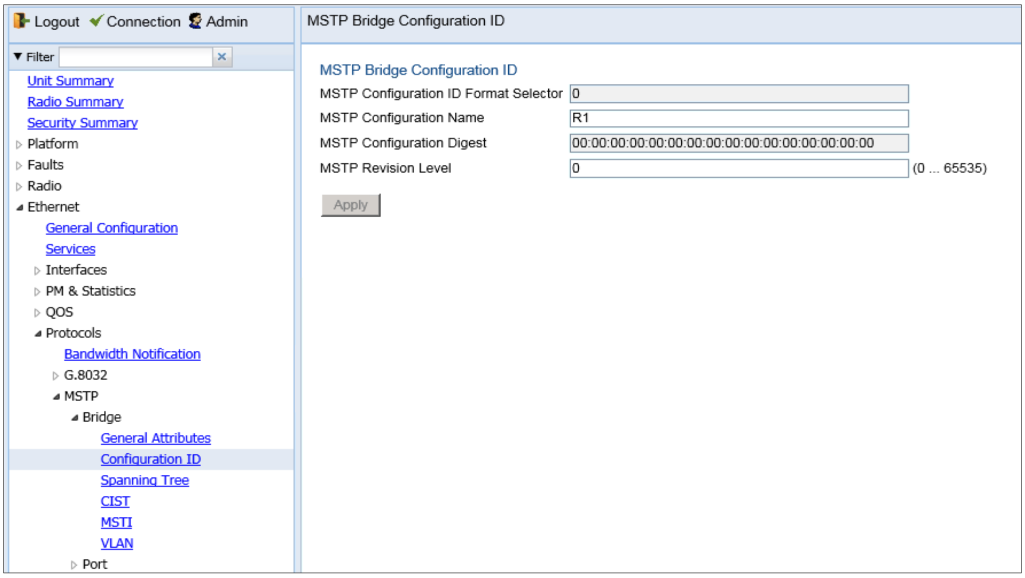
6 Click **Apply**.

To reset the MSTP stack, click **Reset Protocol**.

Viewing and Configuring the MSTP Bridge Configuration ID

To configure the Configuration Name and Revision Level:

1 Select **Ethernet > Protocols > MSTP > Bridge > Configuration ID**. The MSTP Bridge Configuration ID page opens.



MSTP Bridge Configuration ID

MSTP Bridge Configuration ID

MSTP Configuration ID Format Selector: 0

MSTP Configuration Name: R1

MSTP Configuration Digest: 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

MSTP Revision Level: 0 (0 ... 65535)

Figure 317: MSTP Bridge Configuration ID Page

2 Modify the configurable parameters.

3 Click **Apply**.

Table 67 lists and describes the parameters in the MSTP Bridge Configuration ID page.

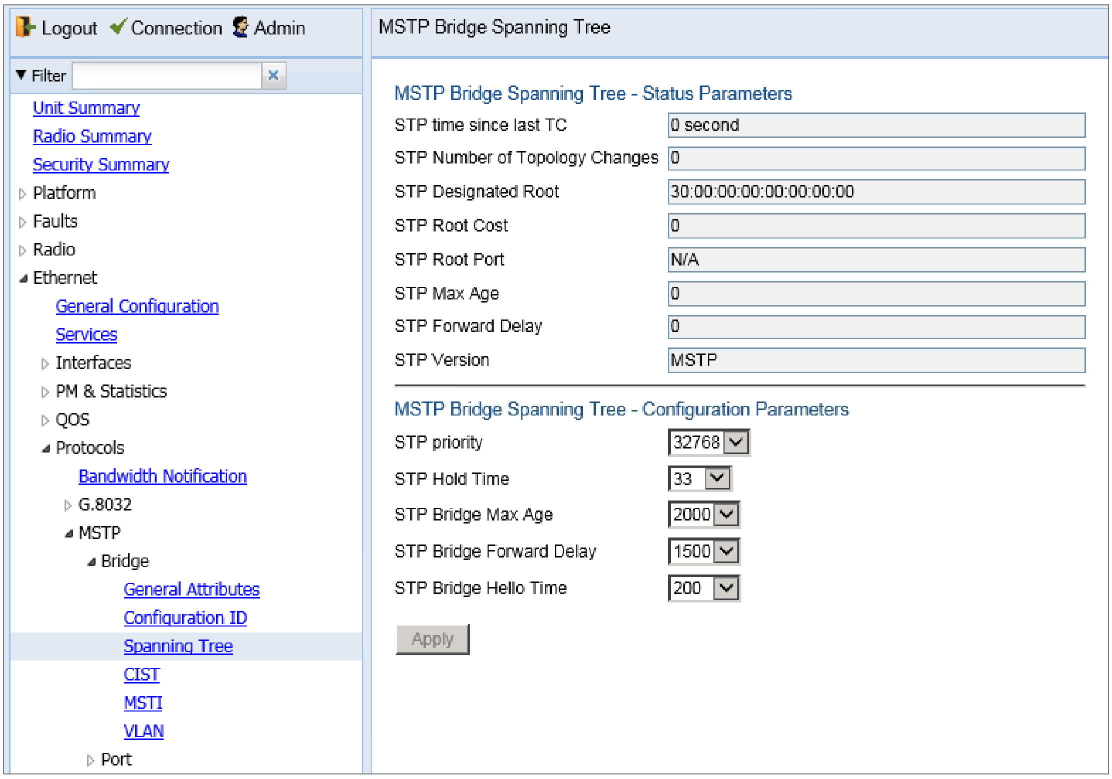
Table 67: MSTP Bridge Configuration ID Parameters

Parameter	Definition
MSTP Configuration ID	Read-only. Indicates the format specified in 802.1Q.
MSTP Configuration Name	Enter a valid configuration name. **Note:** Changing the Configuration Name when MSTP is enabled causes the MSTP stack to reset.
MSTP Configuration Digest	Read-only. Displays the MSTP Configuration Digest.
MSTP Revision Level	Enter a valid MSTP revision level. **Note:** Changing the Revision Level when MSTP is enabled causes the MSTP stack to reset.

Viewing and Configuring the MSTP Bridge Spanning Tree

To configure the bridge-level spanning tree parameters:

1 Select **Ethernet > Protocols > MSTP > Bridge > Spanning Tree**. The MSTP Bridge Spanning Tree page opens.



MSTP Bridge Spanning Tree

MSTP Bridge Spanning Tree - Status Parameters

STP time since last TC	0 second
STP Number of Topology Changes	0
STP Designated Root	30:00:00:00:00:00:00:00
STP Root Cost	0
STP Root Port	N/A
STP Max Age	0
STP Forward Delay	0
STP Version	MSTP

MSTP Bridge Spanning Tree - Configuration Parameters

STP priority	32768
STP Hold Time	33
STP Bridge Max Age	2000
STP Bridge Forward Delay	1500
STP Bridge Hello Time	200

Figure 318: MSTP Bridge Spanning Tree Page

2 Modify the configurable parameters, described in *Table 69*.

3 Click **Apply**.

Table 68 lists and describes the status parameters in the MSTP Bridge Spanning Tree page.

Table 68: MSTP Bridge Spanning Tree Status Parameters

Parameter	Definition
STP Time Since Last TC	The time that has elapsed (in cs) since the last time the bridge entity detected a topology change.
STP Number of Topology Changes	The total number of topology changes that have been detected by this bridge since the management entity was last reset or initialized. **Note:** Discontinuities in the value of this counter can occur upon reinitialization of the management system.
STP Designated Root	The Bridge ID of the spanning tree root, as determined by MSTP in this node. This value is used as the Root ID in all configuration BPDUs originated by this node.
STP Root Cost	The cost of the path to the root as seen from this bridge.
STP Root Port	The port number of the port that offers the lowest cost path from this bridge to the external root bridge
STP Max Age	The maximum age (in cs) of MSTP information learned from the network on any port before the information is discarded. **Note:** This field displays the value actually being used by the bridge, in contrast to the STP Bridge Max Age parameter described below, which is user-configurable and which represents the value that this and all other
STP Forward Delay	The speed at which ports change their spanning state when moving towards the Forwarding state. This value determines how long the port stays in Listening state and Learning state. This value is also used when a topology change has been detected and is underway for purposes of aging all dynamic entries in the filtering database. **Note:** This field displays the value actually being used by the bridge, in contrast to the STP Bridge Forward Delay parameter described below, which is user-configurable and which represents the value that this
STP Version	The STP version the bridge is currently running (MSTP).

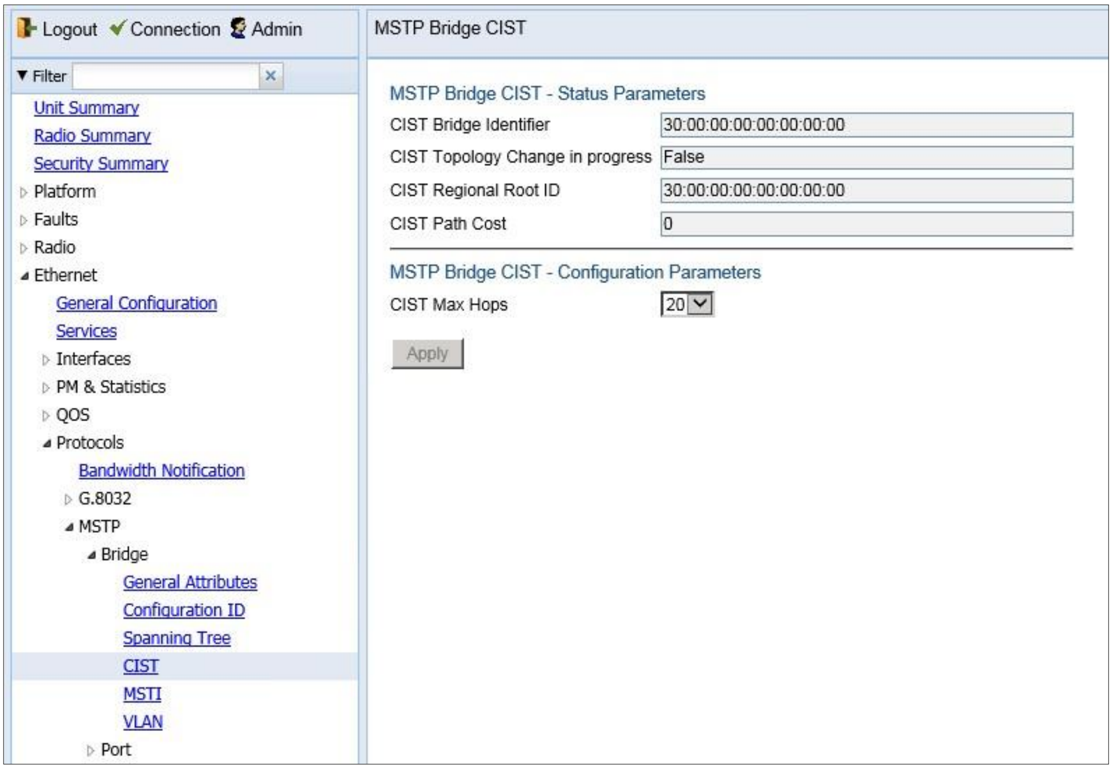
Table 69: MSTP Bridge Spanning Tree Configuration Parameters

Parameter	Definition
STP Priority	Select a value as the writeable portion of the Bridge ID. This value constitutes the first two octets of the Bridge ID. Possible values are 0-61440, in steps of 4096
STP Hold Time	Select a value (in cs) as the interval length during which no more than two configuration bridge PDUs will be transmitted by this node. Possible values are 10-100.
STP Bridge Max Age	Select a value (in cs) that all bridges will use, when this bridge is the root, as the maximum age of MSTP information learned from the network on any port before the information is discarded.
STP Bridge Forward Delay	Select a value (in cs) that all bridges will use, when this bridge is the root, as the speed at which ports change their spanning state when moving towards the Forwarding state. This value determines how long the port stays in Listening state and Learning state. This value is also used when a topology change has been detected and is underway for purposes of aging all dynamic entries in the filtering database. Options are 400-3000 cs.
STP Bridge Hello Time	Select the value (in cs) that all bridges will use, when this bridge is the root, as the Hello Time. The Hello Time determines how often the switch broadcasts its hello message to other switches, and is the same for all MSTIs. Options are 100-1000 cs.

Viewing and Configuring the MSTP Bridge CIST Parameters

To configure the maximum hops parameter for the Common and Internal Spanning Tree (CIST) and view CIST status information:

1 Select **Ethernet > Protocols > MSTP > Bridge > CIST**. The MSTP Bridge CIST page opens.



MSTP Bridge CIST

MSTP Bridge CIST - Status Parameters

CIST Bridge Identifier 30:00:00:00:00:00:00:00

CIST Topology Change in progress False

CIST Regional Root ID 30:00:00:00:00:00:00:00

CIST Path Cost 0

MSTP Bridge CIST - Configuration Parameters

CIST Max Hops 20

Figure 319: MSTP Bridge CIST Page

2 In the **CIST Max Hops** field, select the value that all bridges will use, when this bridge is the root, as the maximum number of hops allowed for a BPDU within a region before it is discarded. Options are 6-40.

3 Click **Apply**.

Table 70 lists and describes the status parameters in the MSTP Bridge CIST page.

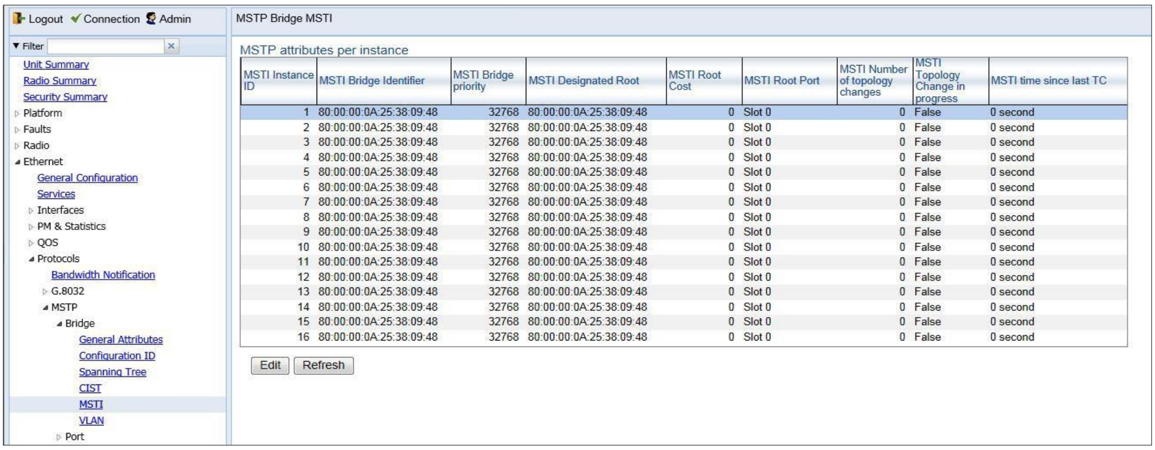
Table 70: MSTP Bridge CIST Status Parameters

Parameter	Definition
CIST Bridge Identifier	The Bridge ID of the CIST.
CIST Topology Change in Progress	Indicates whether a topology change is currently in progress for any port that is part of the CIST.
CIST Regional Root ID	The Bridge ID of the current CIST regional root.
CIST Path Cost	The CIST path cost from the transmitting bridge to the CIST regional root. If the transmitting bridge is the CIST regional root, the value of this parameter may be 0.

Viewing and Configuring the MSTP Bridge MSTI Parameters

To view the parameters of each MSTI in the system, and to configure the MSTI bridge priority for each MSTI:

1 Select **Ethernet > Protocols > MSTP > Bridge > MSTI**. The MSTP Bridge MSTI page opens.



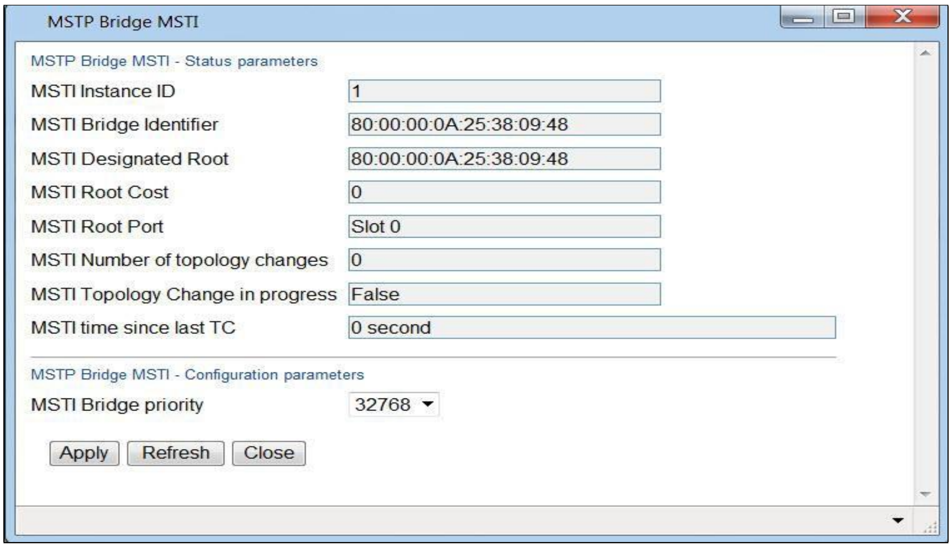
MSTP Bridge MSTI

MSTP attributes per instance

MSTI Instance ID	MSTI Bridge Identifier	MSTI Bridge priority	MSTI Designated Root	MSTI Root Cost	MSTI Root Port	MSTI Number of topology changes	MSTI Topology Change in progress	MSTI time since last TC
1	80:00:00:0A:25:38:09:48	32768	80:00:00:0A:25:38:09:48	0	Slot 0	0	False	0 second
2	80:00:00:0A:25:38:09:48	32768	80:00:00:0A:25:38:09:48	0	Slot 0	0	False	0 second
3	80:00:00:0A:25:38:09:48	32768	80:00:00:0A:25:38:09:48	0	Slot 0	0	False	0 second
4	80:00:00:0A:25:38:09:48	32768	80:00:00:0A:25:38:09:48	0	Slot 0	0	False	0 second
5	80:00:00:0A:25:38:09:48	32768	80:00:00:0A:25:38:09:48	0	Slot 0	0	False	0 second
6	80:00:00:0A:25:38:09:48	32768	80:00:00:0A:25:38:09:48	0	Slot 0	0	False	0 second
7	80:00:00:0A:25:38:09:48	32768	80:00:00:0A:25:38:09:48	0	Slot 0	0	False	0 second
8	80:00:00:0A:25:38:09:48	32768	80:00:00:0A:25:38:09:48	0	Slot 0	0	False	0 second
9	80:00:00:0A:25:38:09:48	32768	80:00:00:0A:25:38:09:48	0	Slot 0	0	False	0 second
10	80:00:00:0A:25:38:09:48	32768	80:00:00:0A:25:38:09:48	0	Slot 0	0	False	0 second
11	80:00:00:0A:25:38:09:48	32768	80:00:00:0A:25:38:09:48	0	Slot 0	0	False	0 second
12	80:00:00:0A:25:38:09:48	32768	80:00:00:0A:25:38:09:48	0	Slot 0	0	False	0 second
13	80:00:00:0A:25:38:09:48	32768	80:00:00:0A:25:38:09:48	0	Slot 0	0	False	0 second
14	80:00:00:0A:25:38:09:48	32768	80:00:00:0A:25:38:09:48	0	Slot 0	0	False	0 second
15	80:00:00:0A:25:38:09:48	32768	80:00:00:0A:25:38:09:48	0	Slot 0	0	False	0 second
16	80:00:00:0A:25:38:09:48	32768	80:00:00:0A:25:38:09:48	0	Slot 0	0	False	0 second

Figure 320: MSTP Bridge MSTI Page

2 To view all the bridge parameters of an MSTI and/or configure its bridge priority, select the MSTI and click **Edit.**



MSTP Bridge MSTI

MSTP Bridge MSTI - Status parameters

MSTI Instance ID	1
MSTI Bridge Identifier	80:00:00:0A:25:38:09:48
MSTI Designated Root	80:00:00:0A:25:38:09:48
MSTI Root Cost	0
MSTI Root Port	Slot 0
MSTI Number of topology changes	0
MSTI Topology Change in progress	False
MSTI time since last TC	0 second

MSTP Bridge MSTI - Configuration parameters

MSTI Bridge priority	32768

Figure 321: MSTP Bridge MSTI – Edit Page

3 To view all the bridge parameters of an MSTI and/or configure its bridge priority, select the MSTI and click **Edit.**

4 In the **MSTI Bridge Priority** field, enter the MSTI writeable portion of the Bridge ID. Possible values are 0-61440, in steps of 4096.

5 Click **Apply**, then **Close**.

Table 71 lists and describes the status parameters in the MSTP Bridge MSTI page.

Table 71: MSTP Bridge MSTI Status Parameters

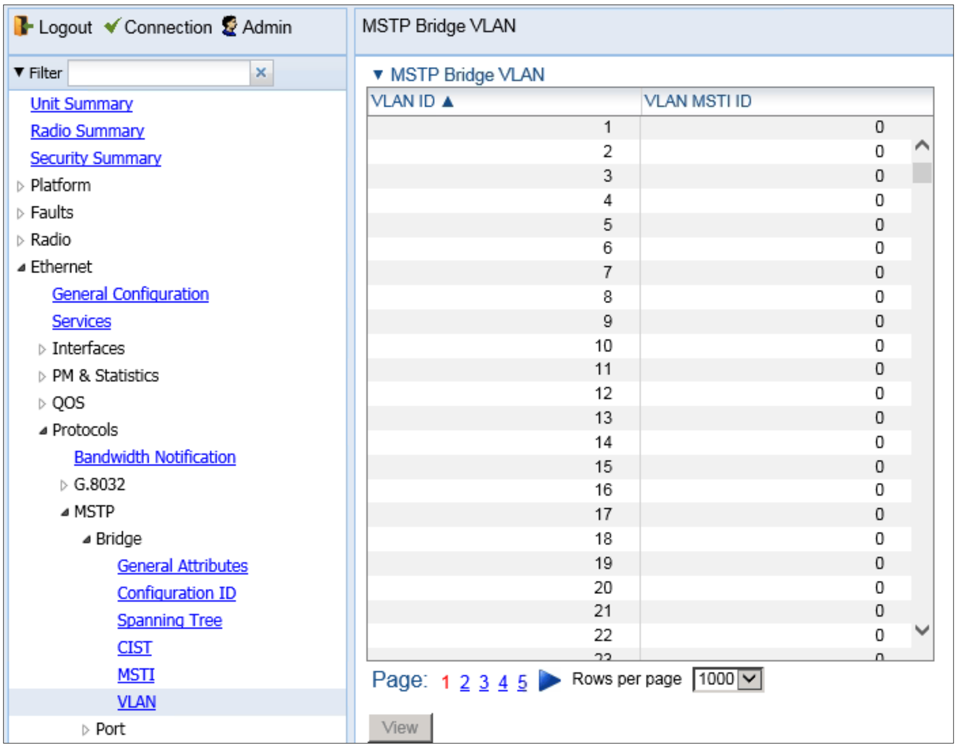
Parameter	Definition
MSTI Instance ID	The MSTI ID.
MSTI Bridge Identifier	The Bridge ID for the MSTI.
MSTI Designated Root	The Bridge ID of the root bridge for the MSTI.
MSTI Root Cost	The path cost from the transmitting bridge to the root bridge for the MSTI.
MSTI Root Port	The root port for the MSTI.
MSTI Number of Topology Changes	The number of topology changes that the bridge has detected in the MSTI since the last time the management entity was reset or initialized.
MSTI Topology Change in Progress	Indicates whether a topology change is currently in progress on any port in the MSTI.
MSTI Time Since Last TC	The number of centi-seconds that have elapsed since the last time the bridge identified a topology change for a

Viewing the MSTP VLAN Parameters

Each Ethernet service is mapped to an MSTI. By default, all services (VLAN ID) are assigned to MSTI 0 (CIST). See *Mapping Ethernet Services to MSTP instances (MSTIs)*.

To view the VLAN ID to MSTI mapping table:

1 Select **Ethernet > Protocols > MSTP > Bridge > VLAN**. The MSTP Bridge VLAN page opens.



MSTP Bridge VLAN

MSTP Bridge VLAN

VLAN ID ▲	VLAN MSTI ID
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0
22	0
23	0

Rows per page 1000

Figure 322: MSTP Bridge VLAN Page

Configuring the MSTP Port Parameters

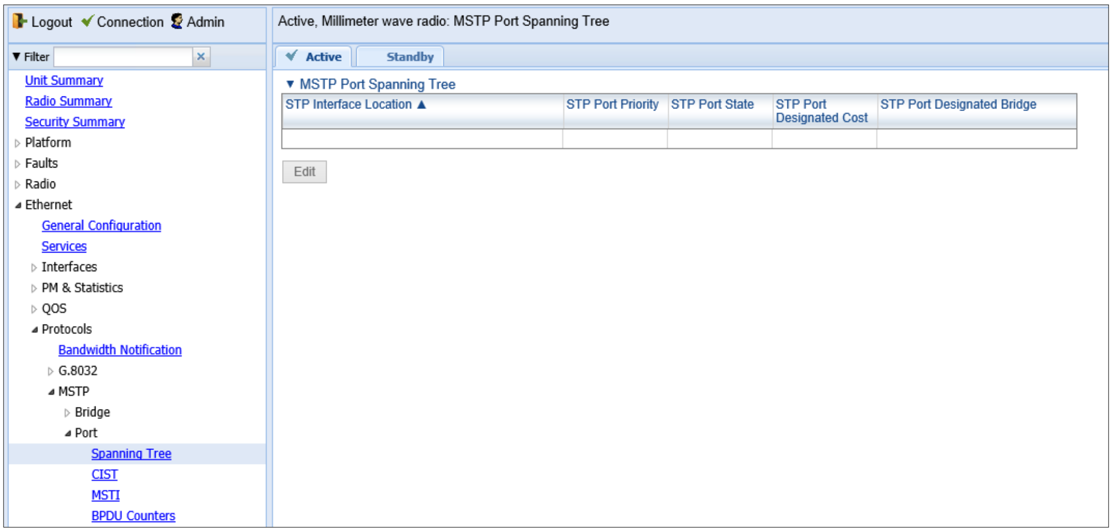
This section includes:

- Viewing and Configuring the MSTP Port Spanning Tree
- Viewing and Configuring the MSTP Port CIST Parameters
- Viewing and Configuring the MSTP Port MSTI Parameters
- Viewing and Resetting the BPDU Counters

Viewing and Configuring the MSTP Port Spanning Tree

To view the port-level spanning tree parameters and configure the STP port priority:

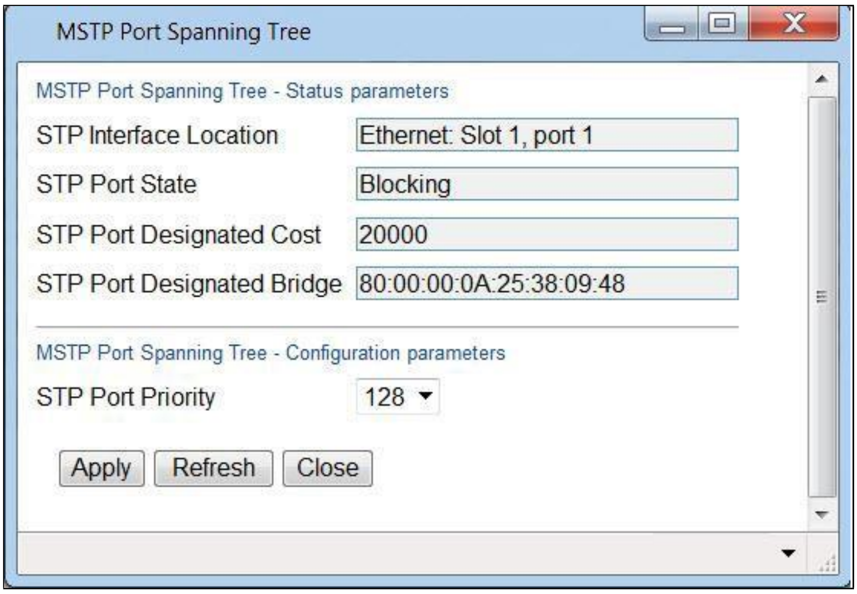
1 Select **Ethernet > Protocols > MSTP > Port > Spanning Tree**. The MSTP Port Spanning Tree page opens.



STP Interface Location ▲	STP Port Priority	STP Port State	STP Port Designated Cost	STP Port Designated Bridge

Figure 323: MSTP Port Spanning Tree Page

2 Select an interface and click **Edit**. The MSTP Port Spanning Tree – Edit page opens.



MSTP Port Spanning Tree
MSTP Port Spanning Tree - Status parameters
MSTP Port Spanning Tree - Configuration parameters
Apply
Refresh
Close

STP Interface Location: Ethernet: Slot 1, port 1

STP Port State: Blocking

STP Port Designated Cost: 20000

STP Port Designated Bridge: 80:00:00:0A:25:38:09:48

STP Port Priority: 128

Figure 324: MSTP Port Spanning Tree – Edit Page

3 In the **STP Port Priority** field, select the CIST port priority of the interface. You can select values from 0-240, in multiples of 16.

4 Click Apply, then Close.

Table 72 lists and describes the status parameters in the MSTP Port Spanning Tree page.

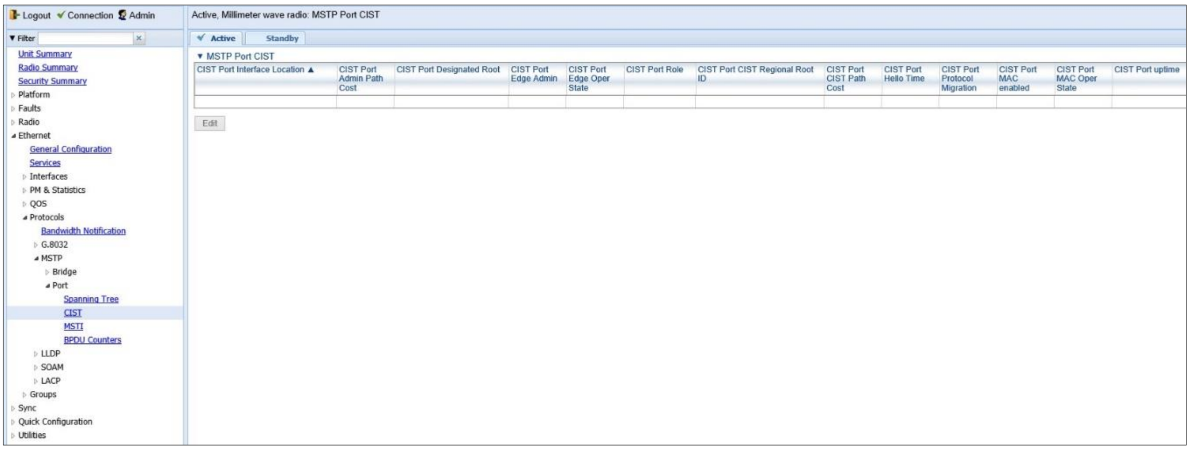
Table 72: MSTP Port Spanning Tree Status Parameters

Parameter	Definition
STP Interface	The slot number and port number of the port.
STP Port State	The port's current state, as defined by application of STP. The port's state controls the action the port takes upon receipt of a frame. Possible values are: • **Forwarding** – The port sends and receives traffic normally. • **Blocking** – The port does not send or receive traffic, but does receive BPDUs. • **Learning** – The port receives traffic but does not forward the traffic. The port learns the source MAC addresses of incoming frames. • **Listening** – The port monitors BPDUs, but does not forward traffic and does not learn the source MAC addresses of incoming frames.
STP Port Designated Cost	The CIST Path Cost of the segment connected to this port. This value is compared to the root path cost in received
STP Port Designated	The CIST Bridge ID of the bridge that this port considers to be the designated bridge for this port's segment.

Viewing and Configuring the MSTP Port CIST Parameters

To view and configure CIST port parameters:

1 Select **Ethernet > Protocols > MSTP > Port > CIST**. The MSTP Port CIST page opens.



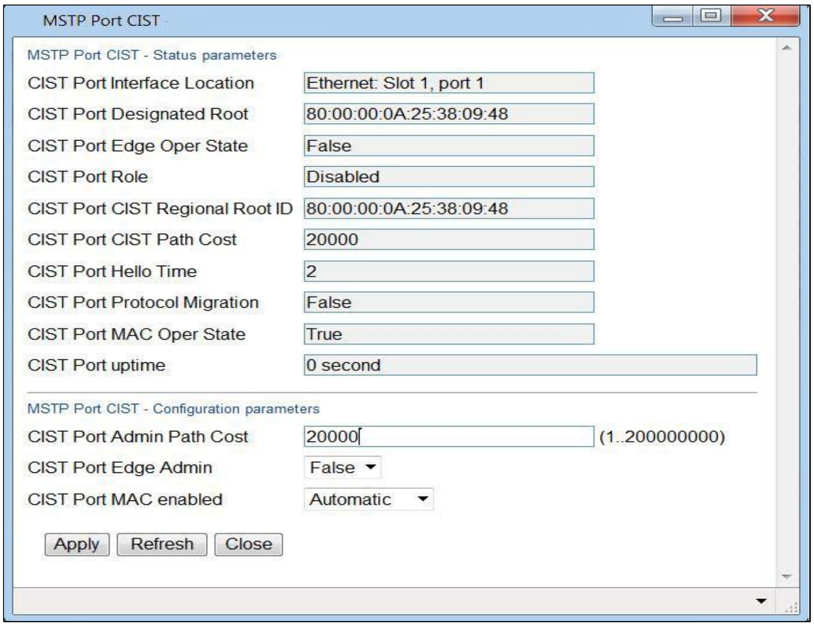
Active, Millimeter wave radio: MSTP Port CIST

MSTP Port CIST

CIST Port Interface Location ▲	CIST Port Admin Path Cost	CIST Port Designated Root	CIST Port Edge Admin	CIST Port Edge Oper State	CIST Port Role	CIST Port CIST Regional Root ID	CIST Port CIST Path Cost	CIST Port Hello Time	CIST Port Protocol Migration	CIST Port MAC enabled	CIST Port MAC Oper State	CIST Port uptime

Figure 325: MSTP Port CIST Page

2 Select an interface and click **Edit**. The MSTP Port CIST – Edit page opens.



MSTP Port CIST

MSTP Port CIST - Status parameters

CIST Port Interface Location: Ethernet: Slot 1, port 1

CIST Port Designated Root: 80:00:00:0A:25:38:09:48

CIST Port Edge Oper State: False

CIST Port Role: Disabled

CIST Port CIST Regional Root ID: 80:00:00:0A:25:38:09:48

CIST Port CIST Path Cost: 20000

CIST Port Hello Time: 2

CIST Port Protocol Migration: False

CIST Port MAC Oper State: True

CIST Port uptime: 0 second

MSTP Port CIST - Configuration parameters

CIST Port Admin Path Cost: 20000 (1..200000000)

CIST Port Edge Admin: False

CIST Port MAC enabled: Automatic

Figure 326: MSTP Port CIST – Edit Page

3 In the **CIST Port Admin Path Cost** field, enter an assigned value for the contribution of this port to the path cost of paths towards the spanning tree root.

4 In the **CIST Port Edge Admin** field, select the port's administrative edge port parameter, for the CIST.

5 In the **CIST MAC enabled** field, select the port's MAC Enabled parameter. A value of **True** indicates that administratively, the MAC is set as if it were connected to a point-to-point LAN. Options are:

- Force True – The MAC is treated as if it is connected to a point-to-point LAN, regardless of any indications to the contrary that are generated by the MAC entity.
- Force False –The MAC is treated as if it is connected to a non-point-to-point LAN, regardless of any indications to the contrary that are generated by the MAC entity.
- Automatic – The MAC Enabled parameter is set to True if the MAC is connected to a point-to-point or full-duplex LAN. The MAC Enabled parameter is set to False if the MAC is connected to a non-point-to-point and half-duplex LAN.

6 Click **Apply**, then **Close**.

Table 73 lists and describes the status parameters in the MSTP Port Spanning Tree page.

Table 73: MSTP Port CIST Status Parameters

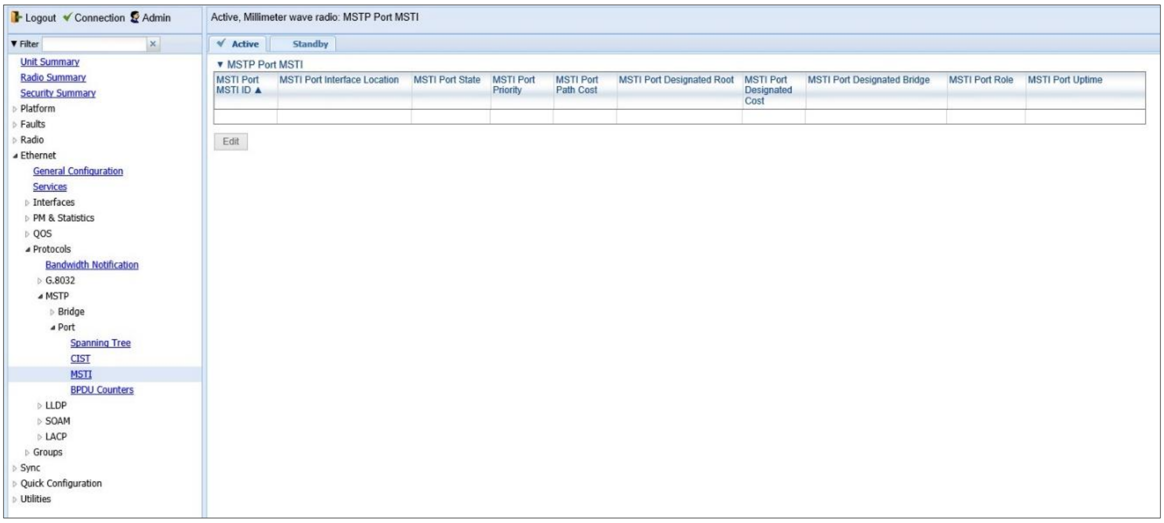
Parameter	Definition
CIST Port Interface	The slot number and port number of the port.
CIST Port Designated Root	The CIST Regional Root ID component of the port's Port Priority vector for the CIST
CIST Port Edge Oper State	Indicates whether or not the port is operating as an Edge port. Possible values are: • **True** – The port is operating as an Edge port, which means it does not process the BPDUs that it receives. • **False** – The port is operating as a non-Edge port, which means it processes the BPDUs that it receives. If CIST Port Edge Admin is set to **True**, the system
CIST Port Role	The port's current role in the CIST. Transient port roles may be: • **Blocking** – The port does not send or receive traffic, but does receive BPDUs. • **Learning** – The port receives traffic but does not forward the traffic. The port learns the source MAC addresses of incoming frames. • **Listening** – The port monitors BPDUs, but does not forward traffic and does not learn the source MAC addresses of incoming frames. Final port roles may be: • **Disabled** – The port is in Operational - Down state and is not included in the MSTP calculation. • **Designated** – The port is in Operational - Up state and has been designated to forward traffic. • **Root** – The port is forwarding traffic towards the root bridge
CIST Port CIST Regional Route ID	The Bridge ID of the current CIST Regional Root.
CIST Port CIST Path Cost	The CIST path cost from the transmitting bridge to the CIST regional root. If the transmitting bridge is the CIST regional root, the value of this parameter will be 0.
CIST Port Hello Time	The port's Hello Time timer parameter value, for the CIST (in
CIST Port Protocol Migration	The current value of the mcheck variable for the port.

CIST Port MAC Oper State	The current state of the port's MAC operational parameter. True indicates the MAC is operational.
CIST Port Uptime	The number of seconds that have elapsed since the port was last reset or initialized.

Viewing and Configuring the MSTP Port MSTI Parameters

To view and configure MSTI port parameters:

1 Select **Ethernet > Protocols > MSTP > Port > MSTI**. The MSTP Port MSTI page opens.



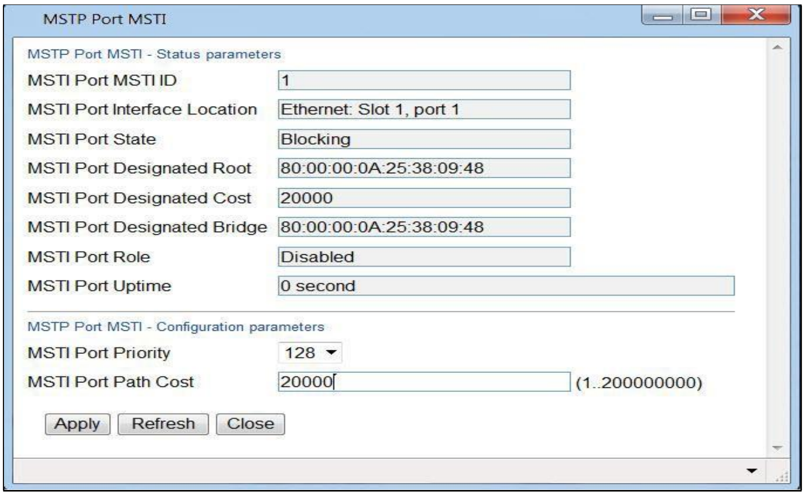
Active, Millimeter wave radio: MSTP Port MSTI

▼ MSTP Port MSTI

MSTI Port MSTI ID ▲	MSTI Port Interface Location	MSTI Port State	MSTI Port Priority	MSTI Port Path Cost	MSTI Port Designated Root	MSTI Port Designated Cost	MSTI Port Designated Bridge	MSTI Port Role	MSTI Port Uptime

Figure 327: MSTP Port MSTI Page

2 To view the parameters for a specific MSTI-port combination in a separate window and modify several of the parameters, select the row with the MSTI- port combination you want to view and/or modify and click **Edit**. The MSTP Port MSTI – Edit page opens.



MSTP Port MSTI - Status parameters

MSTI Port MSTI ID	1
MSTI Port Interface Location	Ethernet: Slot 1, port 1
MSTI Port State	Blocking
MSTI Port Designated Root	80:00:00:0A:25:38:09:48
MSTI Port Designated Cost	20000
MSTI Port Designated Bridge	80:00:00:0A:25:38:09:48
MSTI Port Role	Disabled
MSTI Port Uptime	0 second

MSTP Port MSTI - Configuration parameters

MSTI Port Priority	128
MSTI Port Path Cost	20000 (1..200000000)

Figure 328: MSTP Port MSTI – Edit Page

3 In the **MSTI Port Priority** field, select the port's Priority parameter value for the MSTI, i.e., the priority field for the Port ID for the MSTI. You can select values from 0-240, in multiples of 16.

4 In the **MSTI Port Path Cost** field, select the port's Path Cost parameter value for the MSTI.

5 Click **Apply**, then **Close**.

Table 74 lists and describes the status parameters in the MSTP MSTI Tree page.

Table 74: MSTP Port MSTI Status Parameters

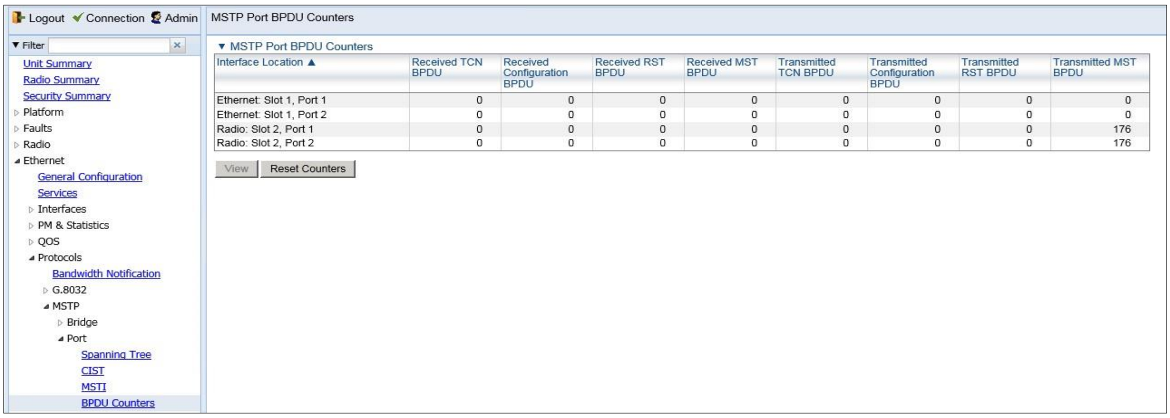
Parameter	Definition
MSTI Port MSTI ID	The MSTI ID.
MSTI Port Interface Location	The slot number and port number of the port.
MSTI Port State	The port's current state for the MSTI. Possible values are: ● **Forwarding** – The port sends and receives traffic normally. ● **Blocking** – The port does not send or receive traffic, but does receive BPDUs. ● **Learning** – The port receives traffic but does not forward the traffic. The port learns the source MAC addresses of incoming frames. ● **Listening** – The port monitors BPDUs, but does not forward traffic and does not learn the source MAC addresses of incoming frames. ● **Disabled** – The port is disabled (not by MSTP).
MSTI Port Designated Root	The Regional Root ID component of the port's Port Priority vector for the MSTI.
MSTI Port Designated Cost	The Internal Root Path Cost component of the port's MSTI port priority vector, for the MSTI.
MSTI Port Designated Bridge	The Designated Bridge ID component of the port's MSTI port priority vector.
MSTI Port Role	The port's current role in the MSTI. Transient port roles may be: ● **Blocking** – The port does not send or receive traffic, but does receive BPDUs. ● **Learning** – The port receives traffic but does not forward the traffic. The port learns the source MAC addresses of incoming frames. ● **Listening** – The port monitors BPDUs, but does not forward traffic and does not learn the source MAC addresses of incoming frames. Final port roles may be: ● **Disabled** – The port is in Operational - Down state and is not included in the MSTP calculation. ● **Designated** – The port is in Operational - Up state and has been designated to forward traffic. ● **Root** – The port is forwarding traffic towards the root bridge. ● **Alternate** – The port is not forwarding traffic (blocked) but can become a Designated port after MSTP calculation.

MSTI Port Uptime	The port's uptime parameter value for the MSTI. This is the number of seconds that have elapsed since the port was last reset or initialized.

Viewing and Resetting the BPDU Counters

To view and reset the BPDU counters:

1 Select **Ethernet > Protocols > MSTP > Port > BPDU Counters**. The MSTP Port BPDU Counters page opens.



MSTP Port BPDU Counters

▼ MSTP Port BPDU Counters

Interface Location ▲	Received TCN BPDU	Received Configuration BPDU	Received RST BPDU	Received MST BPDU	Transmitted TCN BPDU	Transmitted Configuration BPDU	Transmitted RST BPDU	Transmitted MST BPDU
Ethernet: Slot 1, Port 1	0	0	0	0	0	0	0	0
Ethernet: Slot 1, Port 2	0	0	0	0	0	0	0	0
Radio: Slot 2, Port 1	0	0	0	0	0	0	0	176
Radio: Slot 2, Port 2	0	0	0	0	0	0	0	176

Figure 329: MSTP Port BDPU Counters Page

- To reset the counters, click Reset Counters.
- To display the counters for a specific interface in a separate page, select the interface and click View.

Table 75 describes the available MSTP BPDU counters.

Table 75: MSTP BPDU Counters

Parameter	Definition
Interface Location	The location of the port.
Received TCN	The number of Topology Change Notifications (TCNs) received since the last counter reset.
Received Configuration BPDU	The number of configuration BPDUs received since the last counter reset.
Received RST BPDU	The number of Rapid Spanning Tree (RST) BPDUs received
Received MST BPDU	The number of Multiple Spanning Tree (MST) BPDUs received since the last counter reset.
Transmitted TCN BPDU	The number of Topology Change Notifications (TCNs) transmitted since the last counter reset.
Transmitted Configuration BPDU	The number of configuration BPDUs transmitted since the last counter reset.
Transmitted RST BPDU	The number of Rapid Spanning Tree (RST) BPDUs transmitted since the last counter reset.
Transmitted MST BPDU	The number of Multiple Spanning Tree (MST) BPDUs transmitted since the last counter reset.

Configuring Ethernet Bandwidth Notification (ETH-BN)

This section includes:

- ETH-BN Overview
- Adding an ETH-BN entity
- Editing an ETH-BN Entity
- Deleting an ETH-BN Entity
- Viewing the Statistics for an ETH-BN Entity

ETH-BN Overview

Ethernet Bandwidth Notification (ETH-BN) is defined by the Y.1731 OAM standard. The purpose of ETH-BN is to inform the L2 or L3 customer switch of the capacity of the radio link in transmit direction. This enables the switch to respond to fluctuations in the radio link by, for example, reconfiguring the shaper on the egress port facing the radio link or rerouting traffic to other egress ports.

Once ETH-BN is enabled, the radio unit reports bandwidth information to upstream third-party switches. The ETH-BN entity creates a logical relationship between a radio interface, called the Monitored Interface, and an Ethernet interface, called the Control Interface. When bandwidth degrades from the nominal value in the Monitored Interface, messages relaying the actual bandwidth values (BNM frames) are periodically sent over the Control Interface. Once the bandwidth returns to its nominal level, BNM messages are no longer sent. Optionally, the device can be configured to send BNM frames even when bandwidth is at its nominal level.

Note

Only single interfaces, not groups, can be used as the Monitored Interface and the Control Interface.

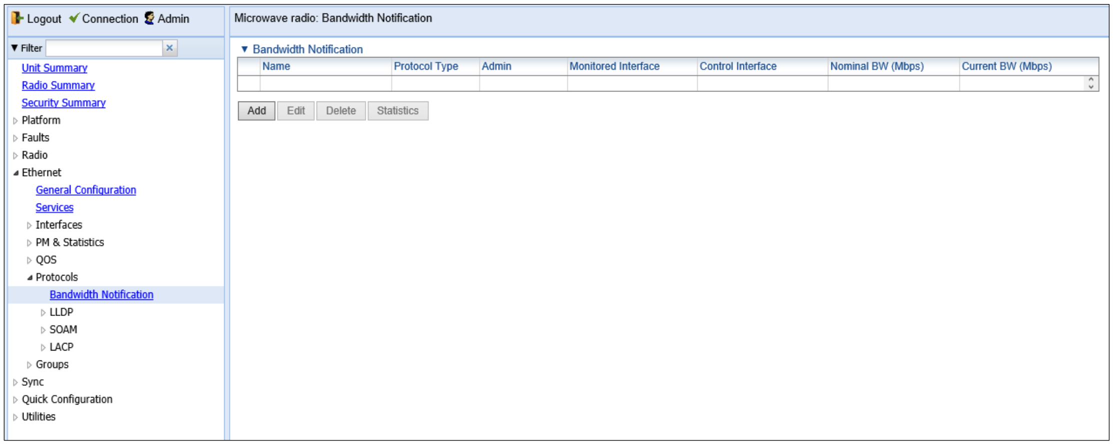
The same radio interface can be configured as a Monitored Interface for multiple EBN instances. However, an Ethernet interface can only be configured as a Control Interface for a single EBN instance.

Adding an ETH-BN entity

To add an ETH-BN entity:

1. Select **Ethernet > Protocols > Bandwidth Notification**. The Bandwidth Notification page opens.

Figure 226 Bandwidth Notification Page



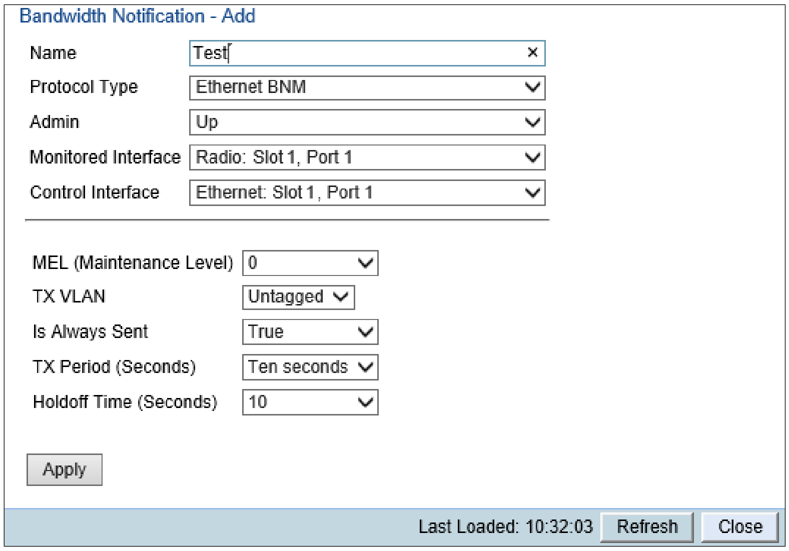
Microwave radio: Bandwidth Notification

Bandwidth Notification

Name	Protocol Type	Admin	Monitored Interface	Control Interface	Nominal BW (Mbps)	Current BW (Mbps)

2. Click **Add**. The Bandwidth Notification - Add page opens.

Figure 227 Bandwidth Notification – Add Page



Bandwidth Notification - Add

Name	Test
Protocol Type	Ethernet BNM
Admin	Up
Monitored Interface	Radio: Slot 1, Port 1
Control Interface	Ethernet: Slot 1, Port 1
MEL (Maintenance Level)	0
TX VLAN	Untagged
Is Always Sent	True
TX Period (Seconds)	Ten seconds
Holdoff Time (Seconds)	10

Last Loaded: 10:32:03

3. In the Name field, enter a name for the ETH-BN entity.
4. In the Protocol Type field, select Ethernet BNM.
5. In the Admin field, select Up to enable ETH-BN monitoring or Down to disable ETH-BN monitoring.
6. In the Monitored Interface field, select the Monitored Interface. This is the interface which is constantly monitored for its bandwidth value.
7. In the Control Interface field, select the Control Interface. This is the interface to which messages are transmitted when bandwidth in the monitored interface degrades below the nominal value.
8. In the **MEL** field, select the CFM Maintenance Level in the messages (0-7).

> Note
>
> If CFM MEPs are being used, the MEL must be set to a value greater than the MEG level of the MEP. Otherwise, the BNM frames will be dropped.
> If CFM MEPs are not being used, the MEL for ETH-BN must be set to a value greater than 0. Otherwise, the BNM frames will be dropped.

9. In the **Tx VLAN** field, specify the VLAN on which messages are transmitted. Options are:
   - Untagged.
   - 1 – 4090.

> Note
>
> The CoS of the VLAN is automatically set to 7.

10. In the **Is Always Sent** field, specify whether periodic BNM frames should be sent even when there is no bandwidth degradation in the monitored interface:
    - **True** – BNM frames are always sent, even when the bandwidth is at its nominal value.
    - **False** – BNM frames are only sent when the current bandwidth is lower than the nominal bandwidth (default value).
11. In the **Tx Period** field, specify how often messages are transmitted when **Is Always Sent** is set to **True** or, if not, when bandwidth is below the nominal value. Options are:
    - One second
    - Ten seconds (default)
    - Sixty seconds
12. In the **Holdoff Time** field, specify the amount of time (in seconds) the system waits when bandwidth degradation occurs, before transmitting a message. If the bandwidth is below

the nominal value when the holdoff period ends, the system starts transmitting messages. Options are 0-10. The default value is 10.

Note

If the bandwidth fluctuates before the Holdoff Time expires, and is lower than the nominal bandwidth when the Holdoff Time expires, the first BNM frame sent when the timer expires gives the lowest bandwidth that was recorded while the timer was running. Subsequent BNM frames are sent with the actual current bandwidth.

13. Click **Apply**, then **Close**.

Table 62 ETH-BN Status Parameters

Parameter	Definition
Nominal BW	The maximum radio TX bitrate achievable with the current radio configuration.
Current BW	The current radio TX bitrate.

Editing an ETH-BN Entity

To edit an ETH-BN entity:

1. Select **Ethernet > Protocols > Bandwidth Notification**. The Bandwidth Notification page opens (***Error! Reference source not found.***).
2. Select the ETH-BN entity in the Bandwidth Notification page.
3. Click Edit. The Bandwidth Notification - Edit page opens.
   The Edit page is similar to the Bandwidth Notification – Add page (***Error! Reference source n ot found.***). However, the **Control interface** and **Monitored interface** parameters are read-only, and additional read-only parameters display the **Nominal BW**, and the **Current BW**.
4. Edit the ETH-BN attributes, as described in *Adding an ETH-BN entity*.
5. Click Apply, then **Close**.

Deleting an ETH-BN Entity

To delete an ETH-BN entity:

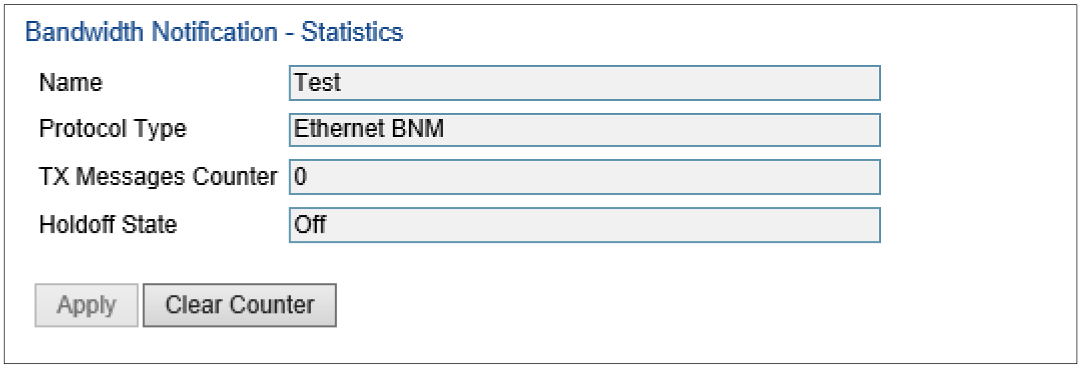
1. Select **Ethernet > Protocols > Bandwidth Notification**. The Bandwidth Notification page opens (***Error! Reference source not found.***).
2. Select the ETH-BN entity in the Bandwidth Notification page.
3. Click **Delete**. The ETH-BN entity is removed.

Viewing the Statistics for an ETH-BN Entity

To view the statistics for an ETH-BN entity:

1. Select **Ethernet > Protocols > Bandwidth Notification**. The Bandwidth Notification page opens.
2. Select the ETH-BN entity in the Bandwidth Notification page.
3. Click Statistics. The Bandwidth Notification - Statistics page opens.

Figure 228 Bandwidth Notification - Statistics Page (ETH-BN)



Bandwidth Notification - Statistics

Name	Test
Protocol Type	Ethernet BNM
TX Messages Counter	0
Holdoff State	Off

Table 63 ETH-BN Entity Statistics Parameters

Parameter	Definition
Name	The name of the ETH-BN entity.
Protocol Type	Ethernet BNM.
Tx Messages Counter	The number of bandwidth messages transmitted since the counter was last reset.
Holdoff State	The Holdoff state of the monitored link. Options are: • **Off** – Holdoff time measurement has not been started. • **Counting** – Holdoff time measurement has started but the timeout has not elapsed yet. • **On** – Holdoff measurement time has ended and the current bandwidth is still below the nominal value.

Configuring LLDP

This section includes:

- LLDP Overview
- Displaying Peer Status
- Configuring the General LLDP Parameters
- Configuring the LLDP Port Parameters
- Displaying the Unit’s Management Parameters

- Displaying Peer Unit’s Management Parameters
- Displaying the Local Unit’s Parameters
- Displaying LLDP Statistics

LLDP Overview

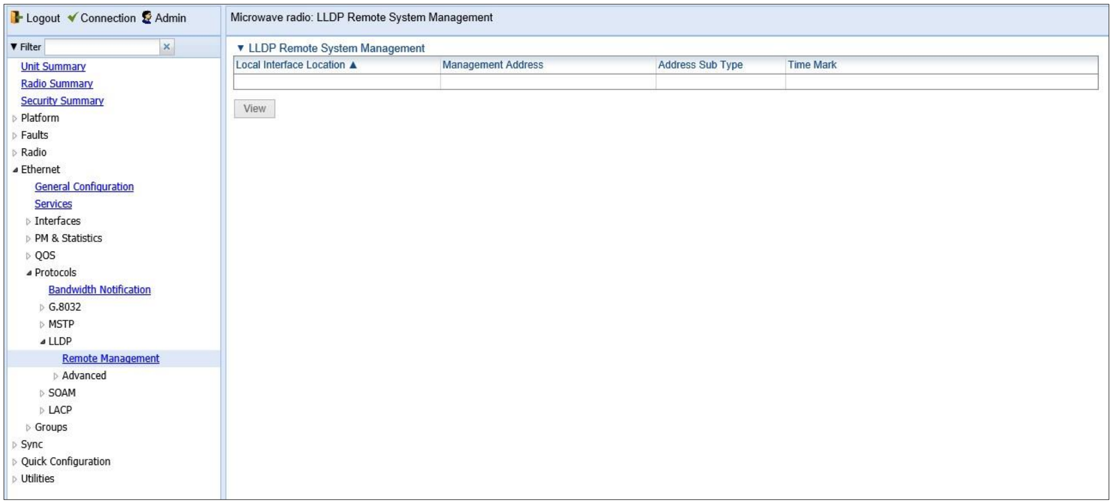
Link Layer Discovery Protocol (LLDP) is a vendor-neutral layer 2 protocol that can be used by a network element attached to a specific LAN segment to advertise its identity and capabilities and to receive identity and capacity information from physically adjacent layer 2 peers. LLDP is a part of the IEEE 802.1AB – 2005 standard that enables automatic network connectivity discovery by means of a port identity information exchange between each port and its peer. Each port periodically sends and also expects to receive frames called Link Layer Discovery Protocol Data Units (LLDPDU). LLDPDUs contain information in TLV format about port identity, such as MAC address and IP address.

LLDP is used to send notifications to the NMS, based on data of the local unit and data gathered from peer systems. These notifications enable the NMS to build an accurate network topology.

Displaying Peer Status

To display a summary of the important LLDP management information regarding the unit's nearest neighbor (peer):

1 Select **Ethernet > Protocols > LLDP > Remote Management**. The LLDP Remote Management page opens.



Microwave radio: LLDP Remote System Management

▼ LLDP Remote System Management

Local Interface Location ▲	Management Address	Address Sub Type	Time Mark

Figure 229 LLDP Remote System Management Page

Below tatble describes the LLDP remote system management parameters. These parameters are read-only.

Table 64 LLDP Remote System Management Parameters

Parameter	Definition
Local Interface Location	The location of the local interface.
Management Address	The octet string used to identify the management address component associated with the remote
Address Sub Type	The type of management address identifier encoding used in the associated LLDP Agent Remote
Time Mark	The time the entry was created.

Configuring the General LLDP Parameters

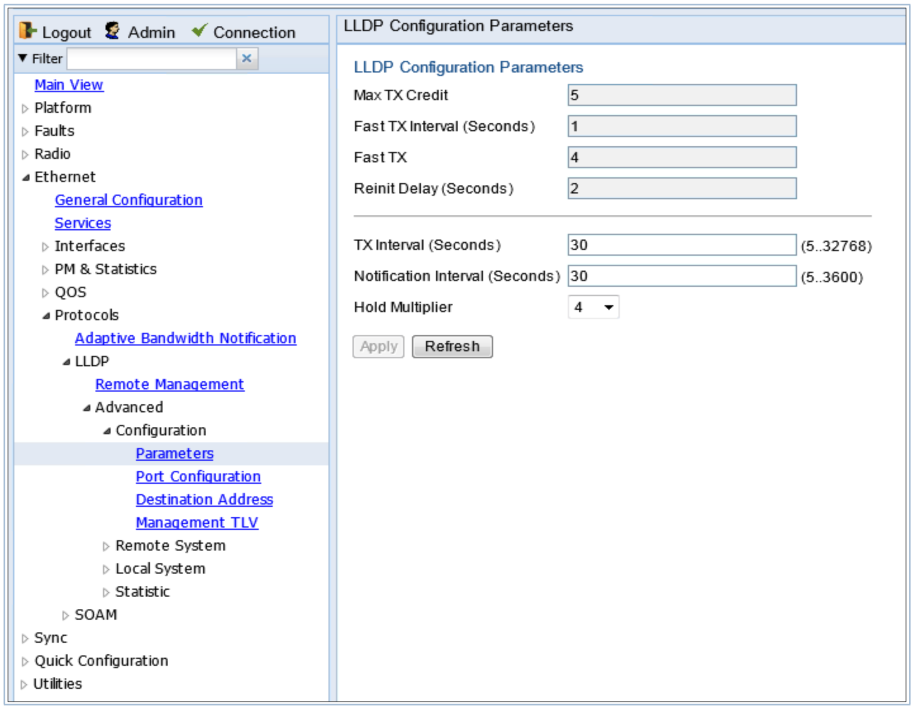
This section explains how to define the general LLDP parameters for the unit. For instructions on defining port-specific parameters, see Configuring the LLDP Port Parameters.

Note

The management IP address advertised by the local element depends on the IP protocol (IPv4 or IPv6) configured for the unit. See Defining the IP Protocol Version for Initiating Communications.

To display and configure the general LLDP parameters for the unit:

1 Select **Ethernet > Protocols > LLDP > Advanced > Configuration > Parameters**. The LLDP Configuration Parameters page opens.



LLDP Configuration Parameters

Max TX Credit: 5

Fast TX Interval (Seconds): 1

Fast TX: 4

Reinit Delay (Seconds): 2

TX Interval (Seconds): 30 (5..32768)

Notification Interval (Seconds): 30 (5..3600)

Hold Multiplier: 4

Figure 230 LLDP Configuration Parameters Page

2 Modify the configurable parameters, described in *Table 64*.

3 Click **Apply**.

Below table lists and describes the status parameters in the LLDP Configuration Parameters page.

Table 65 LLDP Read-Only Configuration Parameters

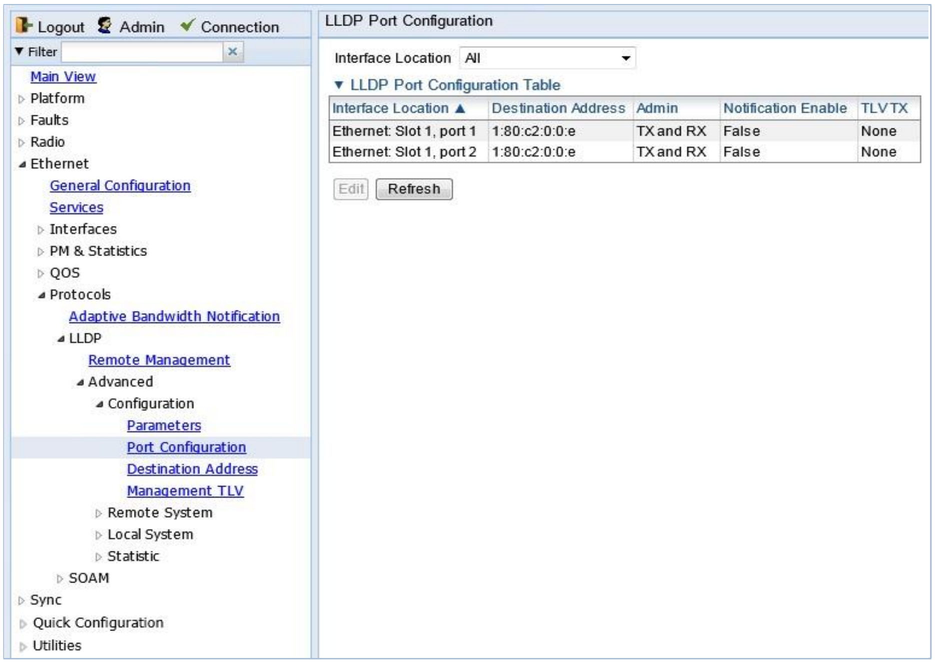
Parameter	Definition
Max TX Credit	Displays the maximum number of consecutive LLDPDUs that can be transmitted at any one time. In this release, the Max TX Credit is set
Fast TX Interval (Seconds)	Displays, in seconds, the interval at which LLDP frames are transmitted during fast transmission periods, such as when the unit detects a new peer. In this release, the Fast TX Interval is set
Fast TX	The initial value used to initialize the variable which determines the number of transmissions that are made during fast transmission periods. In this release, the Fast TX No. is set at 4.
Reinit Delay (Seconds)	Defines the minimum time, in seconds, the system waits after the LLDP Admin status becomes Disabled until it will process a request to reinitialize LLDP. For instructions on disabling or enabling LLDP on a port, see *Configuring the LLDP Port Parameters*. In this release, the Reinit Delay is set at 2.
TX Interval (Seconds)	Defines the interval, in seconds, at which LLDP frames are transmitted. You can select a value from 5 to 32768. The default value

Notification Interval (Seconds)	Defines the interval, in seconds, between transmission of LLDP notifications during normal transmission periods. You can select a value from 5 to 3600. The default value is 10.
Hold Multiplier	Defines the time-to-live (TTL) multiplier. The TTL determines the length of time LLDP frames are retained by the receiving device. The TTL is determined by multiplying the TX Interval by the Hold Multiplier. You can select a value from 2 to 10. The default value is 4.

Configuring the LLDP Port Parameters

To enable LLDP per port and determine how LLDP operates and which TLVs are sent for each port:

1 Select **Ethernet > Protocols > LLDP > Advanced > Configuration > Port Configuration.** The LLDP Port Configuration page opens.



LLDP Port Configuration

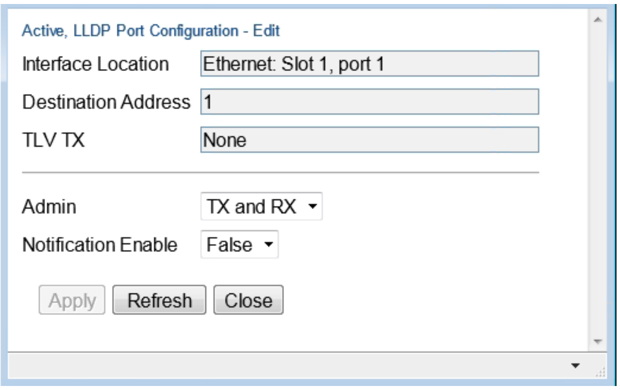
Interface Location: All

▼ LLDP Port Configuration Table

Interface Location ▲	Destination Address	Admin	Notification Enable	TLV TX
Ethernet: Slot 1, port 1	1:80:c2:0:0:e	TX and RX	False	None
Ethernet: Slot 1, port 2	1:80:c2:0:0:e	TX and RX	False	None

Figure 231 LLDP Port Configuration Page

2 Select an interface and click **Edit.** The LLDP Port Configuration - Edit page opens.



Active, LLDP Port Configuration - Edit

Interface Location: Ethernet: Slot 1, port 1

Destination Address: 1

TLV TX: None

Admin: TX and RX

Notification Enable: False

Figure 232 LLDP Port Configuration - Edit Page

3 In the **Admin** field, select from the following options to define how the LLDP protocol operates for this port:

- **TX Only** – LLDP agent transmits LLDP frames on this port but does not update information about its peer.
- **RX Only** – LLDP agent receives but does not transmit LLDP frames on this port.
- **TX and RX** – LLDP agent transmits and receives LLDP frames on this port (default value).
- **Disabled** – LLDP agent does not transmit or receive LLDP frames on this port.

4 In the **Notification Enable** field, select from the following options to define, on a per agent basis, whether or not notifications from the agent to the NMS are enabled:

- **True** – The agent sends a Topology Change trap to the NMS whenever the system information received from the peer changes.
- **False** – Notifications to the NMS are disabled (default value).

5 Click **Apply**, then **Close**.

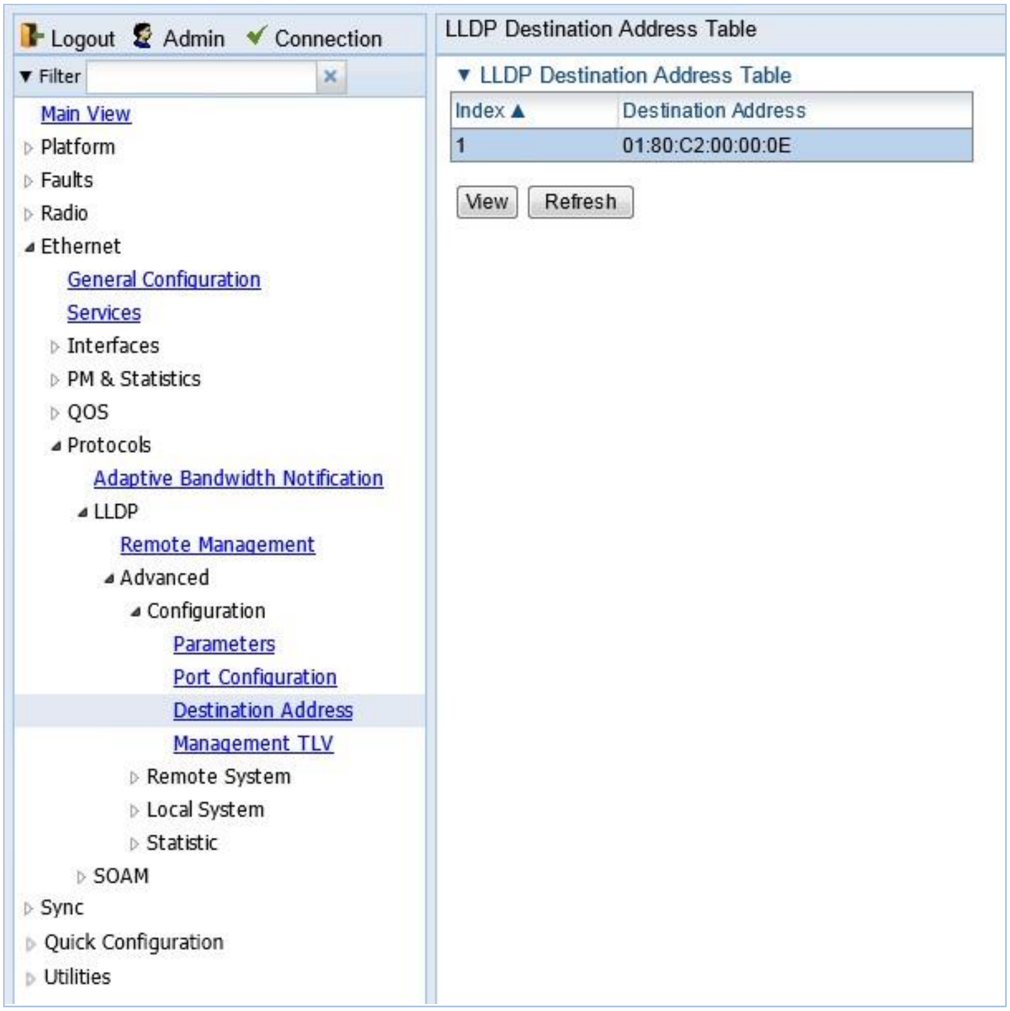
Table 66 LLDP Port Configuration Status Parameters

Parameter	Definition
Interface Location	Identifies the port.
Destination Address	The destination address of the LLDP agent associated with this port.
TLV TX	Indicates which of the unit's capabilities is transmitted by the LLDP agent for the port: • **PortDesc** – The LLDP agent transmits Port Description TLVs. • **SysName** – The LLDP agent transmits System Name TLVs. • **SysDesc** – The LLDP agent transmits System Description TLVs. • **SysCap** – The LLDP agent transmits System Capabilities TLVs.

Displaying the Unit's Management Parameters

To display the unit's destination LLDP MAC address:

1 Select **Ethernet > Protocols > LLDP > Advanced > Configuration > Destination Address**. The LLDP Destination Address Table page opens.



LLDP Destination Address Table

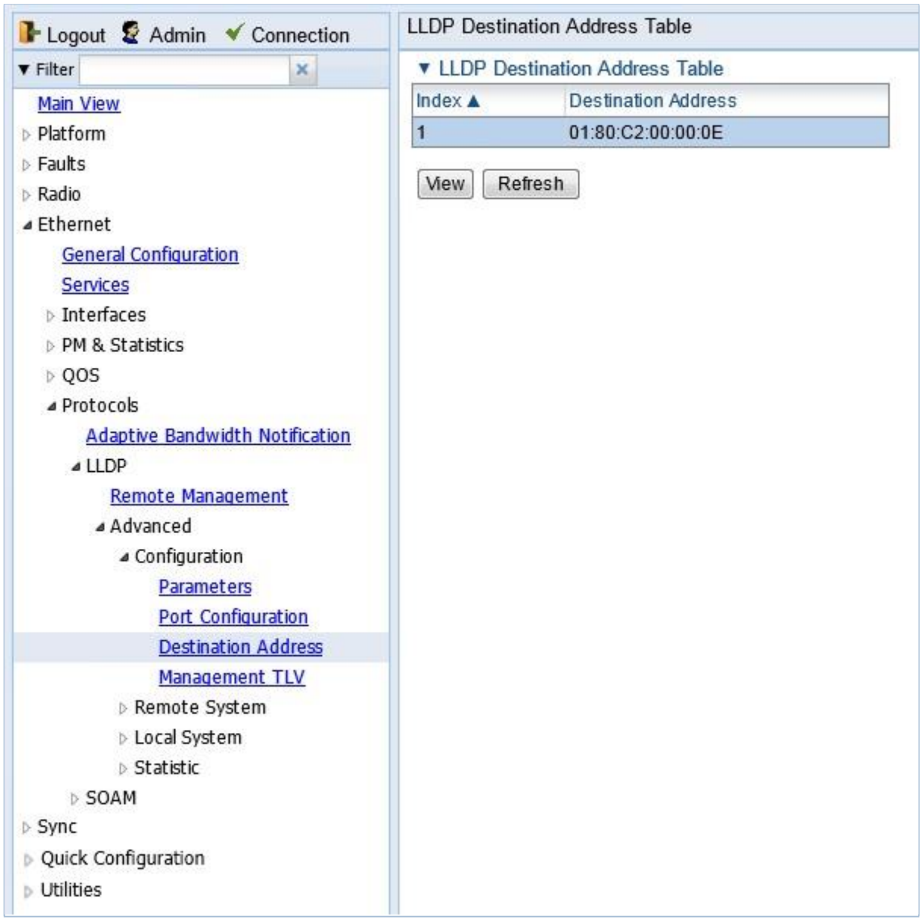
▼ LLDP Destination Address Table

Index ▲	Destination Address
1	01:80:C2:00:00:0E

Figure 233 LLDP Destination Address Table Page

To displays the MAC address associated with the unit for purposes of LLDP transmissions:

1 Select **Ethernet > Protocols > LLDP > Advanced > Configuration > Management TLV**. The LLDP Management TLV Configuration page opens.



LLDP Destination Address Table

▼ LLDP Destination Address Table

Index ▲	Destination Address
1	01:80:C2:00:00:0E

Figure 234 LLDP Management TLV Configuration Page

Below table lists and describes the status parameters in the LLDP Management TLV Configuration page.

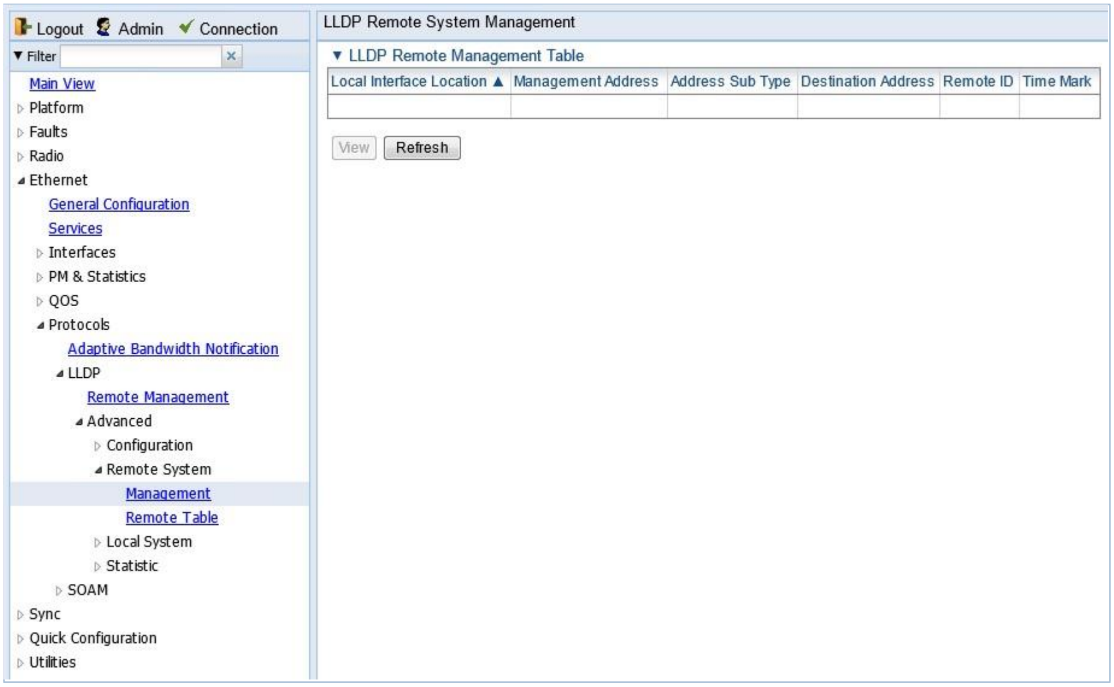
Table 67 LLDP Management TLV Parameters

Parameter	Definition
Interface Location	Identifies the port.
Destination Address	Defines the MAC address associated with the port for purposes of LLDP transmissions.
Management Address	The unit's IP address.
Address Subtype	Defines the type of the management address identifier encoding used for the Management Address.
Tx Enable	Indicates whether the unit's Management Address is transmitted with LLDPDUs. In this release, the Management Address is always

Displaying Peer Unit's Management Parameters

To display LLDP management information about the unit's nearest neighbor (peer):

1 Select **Ethernet > Protocols > LLDP > Advanced > Remote System > Management**. The LLDP Remote System Management page opens.



Local Interface Location ▲	Management Address	Address Sub Type	Destination Address	Remote ID	Time Mark

Figure 235 LLDP Remote System Management Page

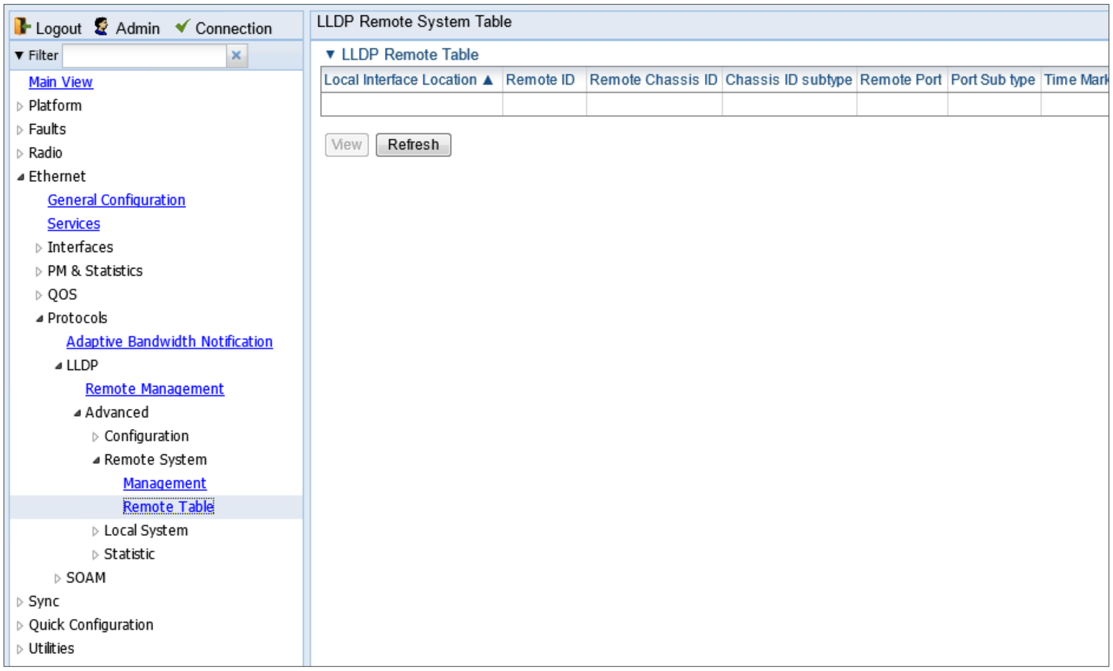
Below table describes the LLDP remote system management parameters. These parameters are read-only.

Table 68 LLDP Remote System Management Parameters

Parameter	Definition
Local Interface Location	The location of the local interface.
Management Address	The octet string used to identify the management address component associated with the remote system.
Address Sub Type	The type of management address identifier encoding used in the associated LLDP Agent Remote Management Address.
Destination Address	The peer LLDP agent's destination MAC Address.
Remote ID	An arbitrary local integer value used by this agent to identify a particular connection instance, unique only for the indicated remote system.
Time Mark	The time the entry was created.

To display unit parameter information received via LLDP from the unit's nearest neighbor (peer):

1 Select **Ethernet > Protocols > LLDP > Advanced > Remote System > Remote Table**. The LLDP Remote System Table page opens.



Local Interface Location ▲	Remote ID	Remote Chassis ID	Chassis ID subtype	Remote Port	Port Sub type	Time Mark

Figure 236 LLDP Local System Parameters Page

Below table describes the parameters in the LLDP Local System Parameters page. These parameters are read-only.

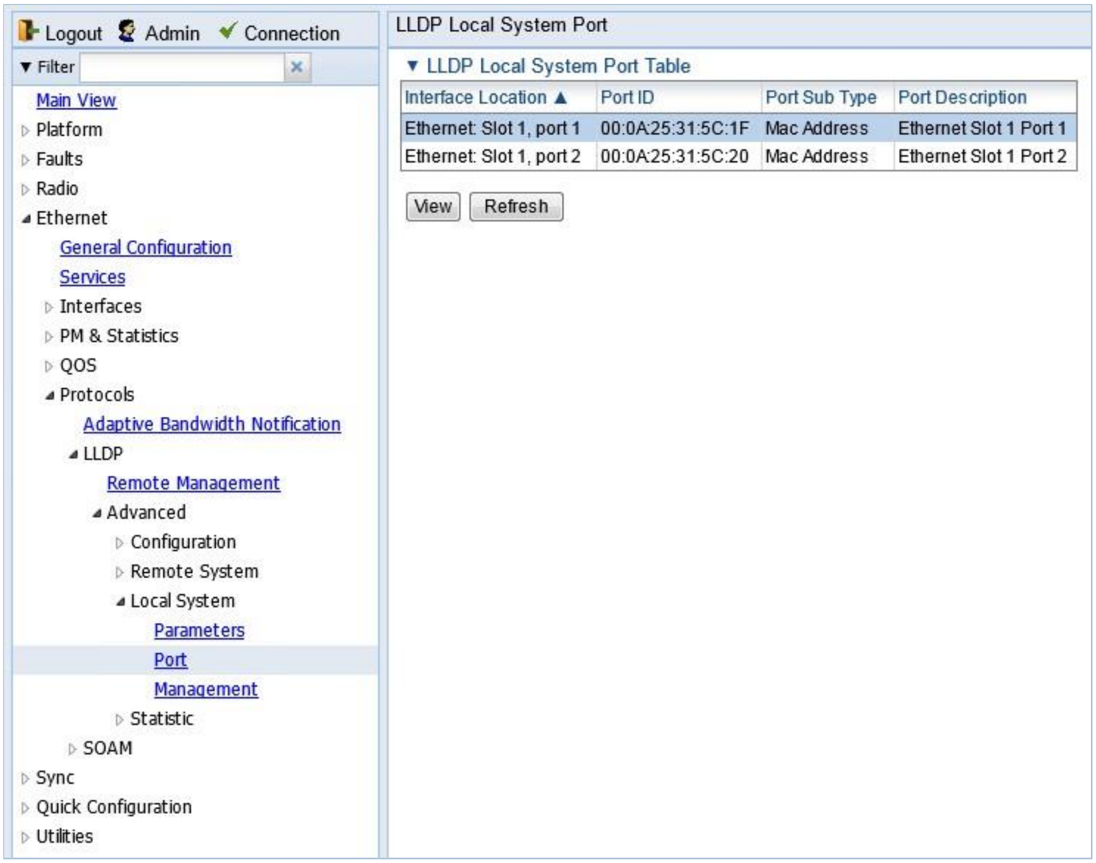
Table 69 LLDP Local System Parameters

Parameter	Definition
System Name	The system name included in TLVs transmitted by the LLDP agent, as defined in the **Name** field of the Unit Parameters page. See *Configuring Unit Parameters*.
System Description	The system description included in TLVs transmitted by the LLDP agent, as defined in the **Description** field of the Unit Parameters page. See *Configuring Unit Parameters*.
Chassis ID	The MAC Address of the local unit.
Chassis ID SubType	The type of encoding used to identify the local unit. In this release, this parameter is always set to MAC Address.

Capabilities Supported	A bitmap value used to identify which system capabilities are supported on the local system, as included in TLVs transmitted by the LLDP agent. The bitmap is defined by the following parameters: 0 – other 1 – repeater 2 – bridge 3 – wlanAccessPoint 4 – router 5 – telephone 6 – docsisCableDevice 7 – stationOnly 8 – cVLANComponent 9 – sVLANComponent 10– twoPortMACRelay
Capabilities Enabled	A bitmap value used to identify which system capabilities are enabled on the local system, as included in TLVs transmitted by the LLDP agent. The bitmap is defined by the following parameters: 0 – other 1 – repeater 2 – bridge 3 – wlanAccessPoint 4 – router 5 – telephone 6 – docsisCableDevice 7 – stationOnly 8 – cVLANComponent 9 – sVLANComponent 10 – twoPortMACRelay

To display the unit's port parameters, as transmitted by the LLDP agents:

1 Select **Ethernet > Protocols > LLDP > Advanced > Local System > Port**. The LLDP Local System Port page opens.



Interface Location ▲	Port ID	Port Sub Type	Port Description
Ethernet: Slot 1, port 1	00:0A:25:31:5C:1F	Mac Address	Ethernet Slot 1 Port 1
Ethernet: Slot 1, port 2	00:0A:25:31:5C:20	Mac Address	Ethernet Slot 1 Port 2

Figure 237 LLDP Local System Port Page

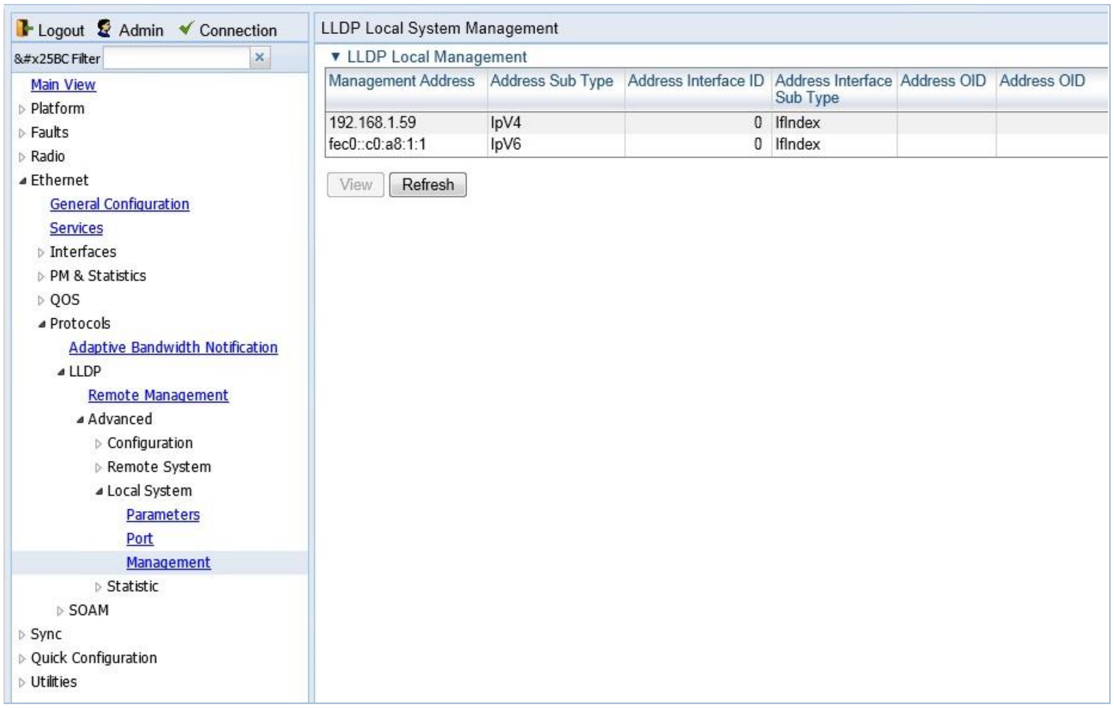
Below table describes the parameters in the LLDP Local System Port page. These parameters are read-only.

Table 70 LLDP Local System Port Parameters

Parameter	Definition
Interface Location	Identifies the port.
Port ID	The port's MAC address.
Port Sub Type	The type of encoding used to identify the port in LLDP transmissions. In this release, this parameter is always set to MAC Address.
Port Description	A description of the port.

To display the unit's management parameters, as transmitted by the LLDP agents:

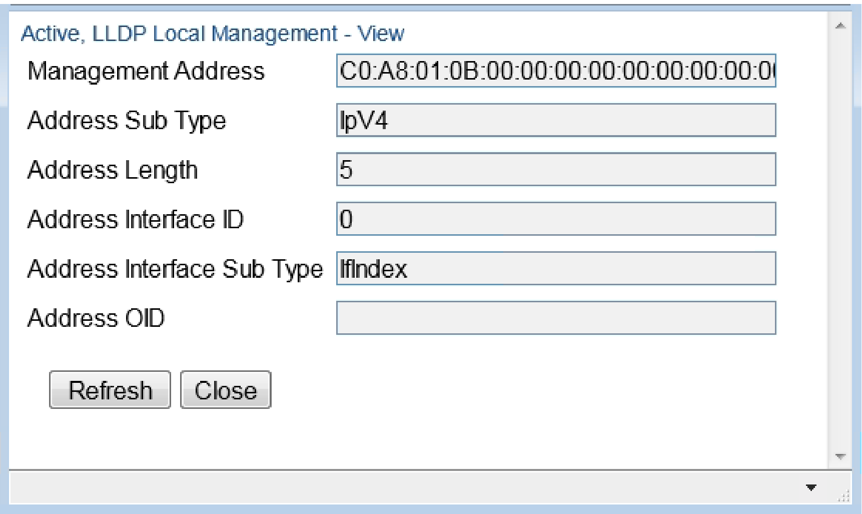
1 Select **Ethernet > Protocols > LLDP > Advanced > Local System > Management**. The LLDP Local System Management page opens.



Management Address	Address Sub Type	Address Interface ID	Address Interface Sub Type	Address OID	Address OID
192.168.1.59	IpV4	0	IfIndex		
fec0::c0:a8:1:1	IpV6	0	IfIndex		

Figure 238 LLDP Local System Management Page

2 To display all the parameters, select a row and click View.



Management Address	C0:A8:01:0B:00:00:00:00:00:00:00:00:0
Address Sub Type	IpV4
Address Length	5
Address Interface ID	0
Address Interface Sub Type	IfIndex
Address OID	

Figure 239 LLDP Local System Management – View Page

Below table describes the parameters in the LLDP Local System Management page. These parameters are read-only.

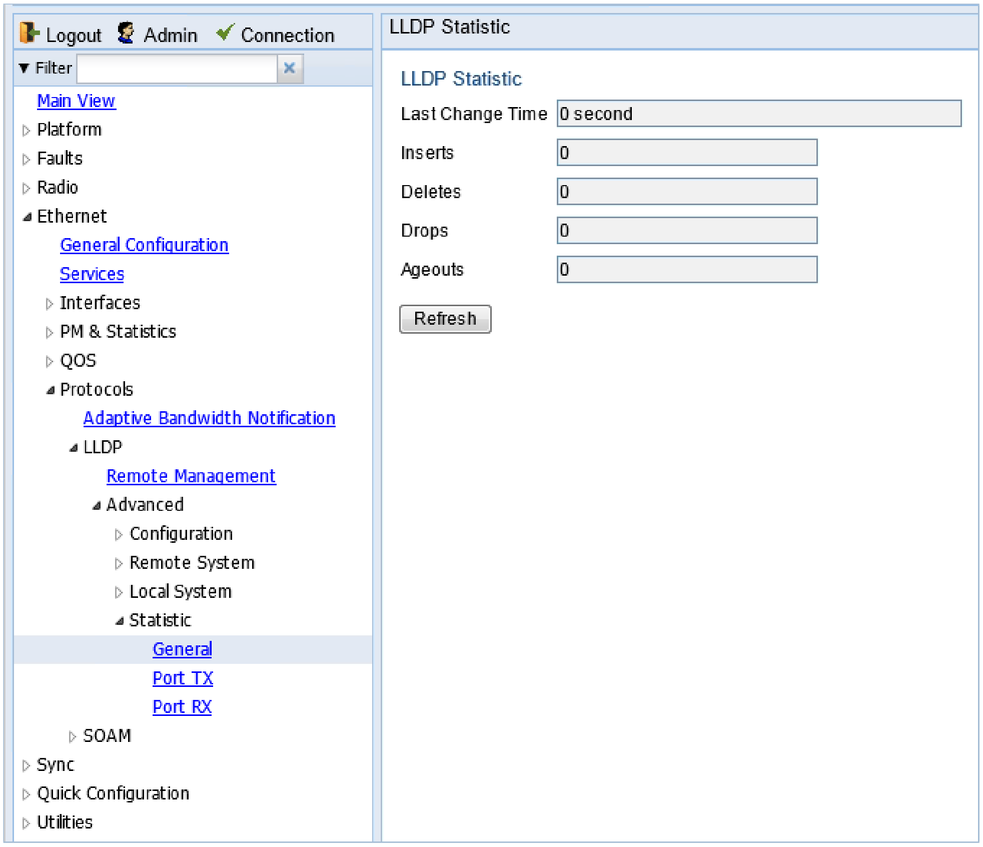
Table 71 LLDP Local System Management Parameters

Parameter	Definition
Management Address	The local unit's IP address.
Address Sub Type	The format of the local unit's IP Address.
Address Length	Reserved for future use.
Address Interface ID	Reserved for future use.
Address Interface Sub Type	Reserved for future use.
Address OID	Reserved for future use.

Displaying LLDP Statistics

To display statistics about changes reported via LLDP by the remote unit:

1 Select **Ethernet > Protocols > LLDP > Advanced > Statistic > General**. The LLDP Statistic page opens.



LLDP Statistic

Last Change Time: 0 second

Inserts: 0

Deletes: 0

Drops: 0

Ageouts: 0

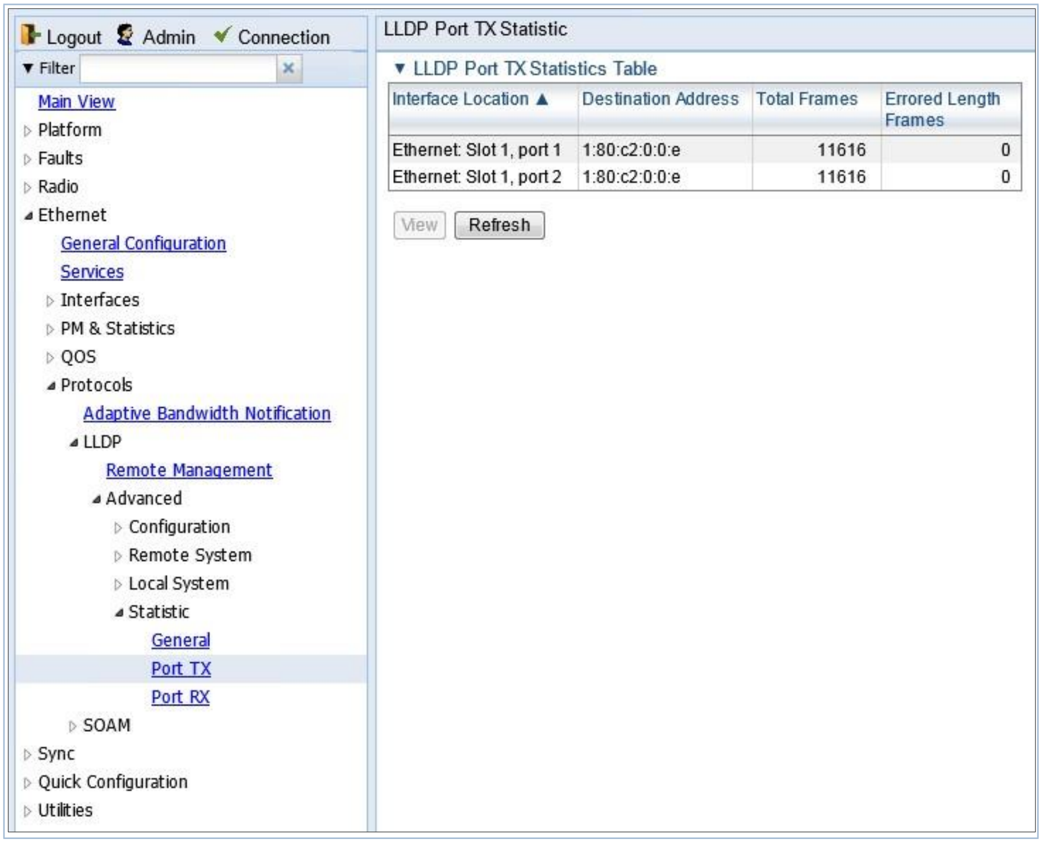
Figure 240 LLDP Statistic Page

Table 72 LLDP Statistics

Parameter	Definition
Last Change Time	The time of the most recent change in the remote unit, as reported via LLDP.
Inserts	The number of times the information from the remote system has changed.
Deletes	The number of times the information from the remote system has been deleted.
Drops	Reserved for future use.
Ageouts	The number of times the information from the remote system has been deleted from the local unit's database because the information's TTL has expired. The **RX Ageouts** counter in the Port RX page is similar to this counter, but is for specific ports rather than the entire unit.

To display statistics about LLDP transmissions and transmission errors:

1 Select **Ethernet > Protocols > LLDP > Advanced > Statistic > Port TX**. The LLDP Port TX Statistic page opens.



LLDP Port TX Statistic

▼ LLDP Port TX Statistics Table

Interface Location ▲	Destination Address	Total Frames	Errored Length Frames
Ethernet: Slot 1, port 1	1:80:c2:0:0:e	11616	0
Ethernet: Slot 1, port 2	1:80:c2:0:0:e	11616	0

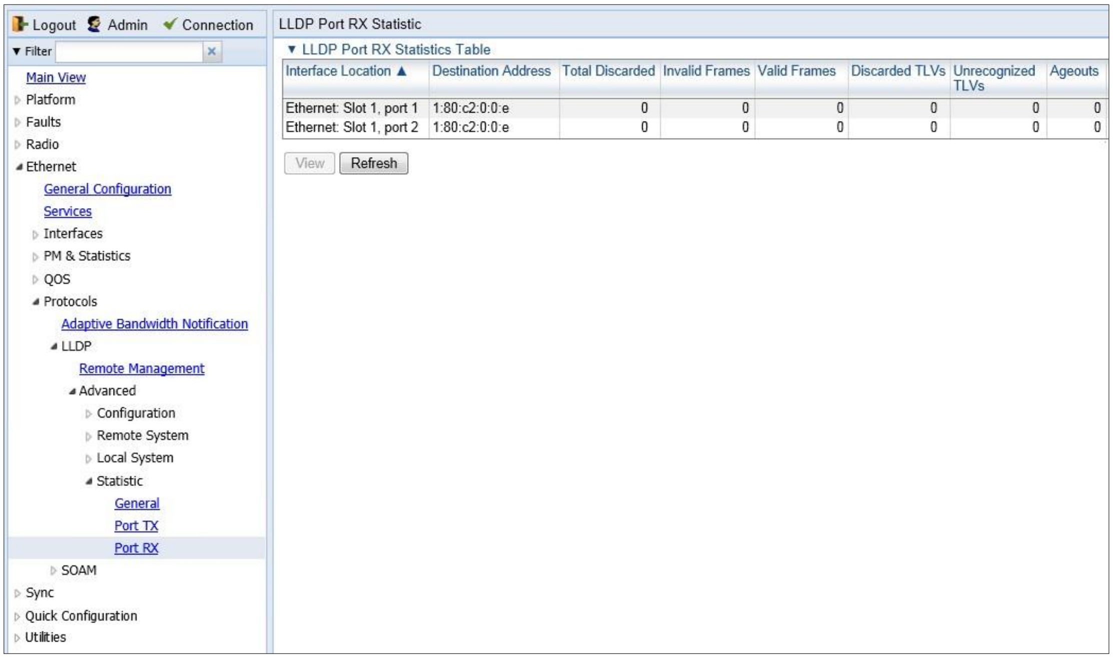
Figure 241 LLDP Port TX Statistics Page

Table 73 LLDP Port TX Statistics

Parameter	Definition
Interface Location	The index value used to identify the port in LLDP transmissions.
Destination Address	The LLDP MAC address associated with this entry.
Total Frames	The number of LLDP frames transmitted by the LLDP agent on this port to the destination MAC address.
Errored Length Frames	The number of LLDPDU Length Errors recorded for this port and destination MAC address. If the set of TLVs that is selected in the LLDP local system MIB by network management would result in an LLDPDU that violates LLDPDU length restrictions, then the No. of Length Error statistic is incremented by 1, and an LLDPDU is sent containing the mandatory TLVs plus as many of the optional TLVs in the set as will fit in the remaining LLDPDU length.

To display statistics about LLDP frames received by the unit:

1 Select **Ethernet > Protocols > LLDP > Advanced > Statistic > Port RX**. The LLDP Port TX Statistic page opens.



LLDP Port RX Statistic

▼ LLDP Port RX Statistics Table

Interface Location ▲	Destination Address	Total Discarded	Invalid Frames	Valid Frames	Discarded TLVs	Unrecognized TLVs	Ageouts
Ethernet: Slot 1, port 1	1:80:c2:0:0:e	0	0	0	0	0	0
Ethernet: Slot 1, port 2	1:80:c2:0:0:e	0	0	0	0	0	0

Figure 242 LLDP Port RX Statistics Page

Table 74 LLDP Port RX Statistics

Parameter	Definition
Interface Location	The index value used to identify the port in LLDP transmissions.
Destination Address	The LLDP MAC address associated with this entry.
Total Discarded	The number of LLDP frames received by the LLDP agent on this port, and then discarded for any reason. This counter can provide an indication that LLDP header formatting problems may exist with the local LLDP agent in the sending system or that LLDPDU validation problems may exist with the local LLDP agent in the receiving system.
Invalid Frames	The number of invalid LLDP frames received by the LLDP agent on this port while the agent is enabled.
Valid Frames	The number of valid LLDP frames received by the LLDP agent on this port.
Discarded TLVs	The number of LLDP TLVs discarded for any reason by the LLDP agent on this port.
Unrecognized TLVs	The number of LLDP TLVs received on the given port that are not recognized by LLDP
Ageouts	The number of age-outs that occurred on the port. An age-out is the number of times the complete set of information advertised by the remote system has been deleted from the unit's database because the information timeliness interval has expired. This counter is similar to the LLDP No. of Ageouts counter in the LLDP Statistic page, except that it is per port rather than for the entire unit. This counter is set to zero during agent initialization. This counter is incremented only once when the complete set of information is invalidated (aged out) from all related tables on a particular port. Partial ageing is not allowed.

Chapter 12: Synchronization

This section includes:

- Configuring the Sync Source
- Configuring the Outgoing Clock and SSM Messages
- Configuring 1588 Transparent Clock
- Configuring 1588 Boundary Clock

Configuring the Sync Source

Note

To configure a sync source on which the sync source Quality parameter must be set according to ANSI specifications and you must change the ETSI/ANSI mode to ANSI before configuring the sync source. See Changing the ETSI/ANSI Mode (CLI).

Frequency signals can be taken by the system from Ethernet and radio interfaces.

The reference frequency may also be conveyed to external equipment through different interfaces. For instructions how to configure the outgoing clock, see Configuring the Outgoing Clock and SSM Messages.

Frequency is distributed by configuring the following parameters in each node:

System Synchronization Sources – These are the interfaces from which the frequency is taken and distributed to other interfaces. Up to 16 sources can be configured in each node. A revertive timer can be configured. For each interface, you must configure:

- **Priority (1-16)** – No two synchronization sources can have the same priority.
- **Quality** – The quality level applied to the selected synchronization source. This enables the system to select the source with the highest quality as the current synchronization source.

Each unit determines the current active clock reference source interface:

- The interface with the highest available quality is selected.
- From among interfaces with identical quality, the interface with the highest priority is selected.

Note

You can configure a revertive timer for the PTP 850 unit. When the

revertive timer is configured, the unit will not switch to another synchronization source unless that source has been stable for at least the number of seconds defined in the revertive timer. This helps to prevent a situation in which numerous switchovers occur when a synchronization source reports a higher quality for a brief time interval, followed by a degradation of the source's quality. By default, the revertive timer is set to 0, which means that it is disabled.

Configuration of the revertive timer must be performed via CLI. See

Configuring the Revertive Timer (CLI).

When configuring the Sync source, the Sync mode must be set to its default setting of automatic. To display the current Sync mode, enter the following CLI command in root view:

```
Root > platform sync mode show
```

If the Sync mode is set to pipe, you must set it to automatic by entering the following CLI command in root view:

```
Root > platform sync mode set automatic
```

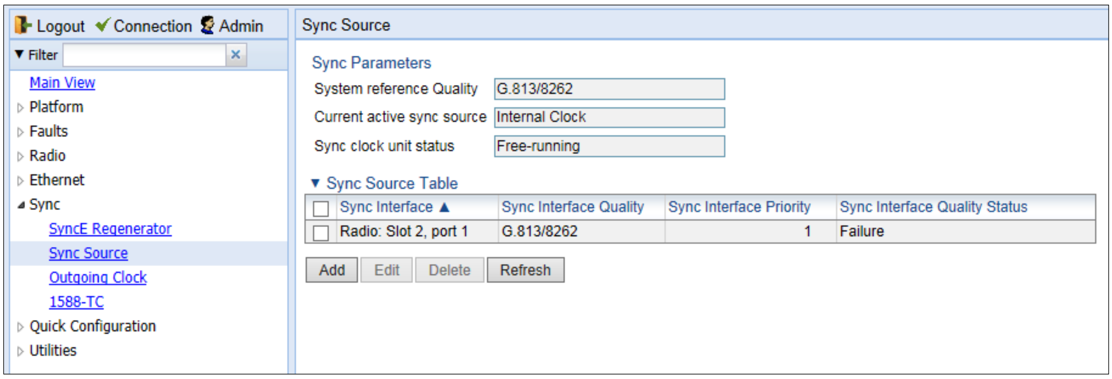
When configuring an Ethernet interface as a Sync source, the Media Type of the interface must be RJ45 or SFP, not Auto-Type.

Viewing the Sync Source Status

To view the current sync source and its quality:

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

Figure 243 Sync Source Page



Sync Parameters

System reference Quality: G.813/8262

Current active sync source: Internal Clock

Sync clock unit status: Free-running

Sync Source Table

	Sync Interface ▲	Sync Interface Quality	Sync Interface Priority	Sync Interface Quality Status
□	Radio: Slot 2, port 1	G.813/8262	1	Failure

Table 75 Sync Source Parameters

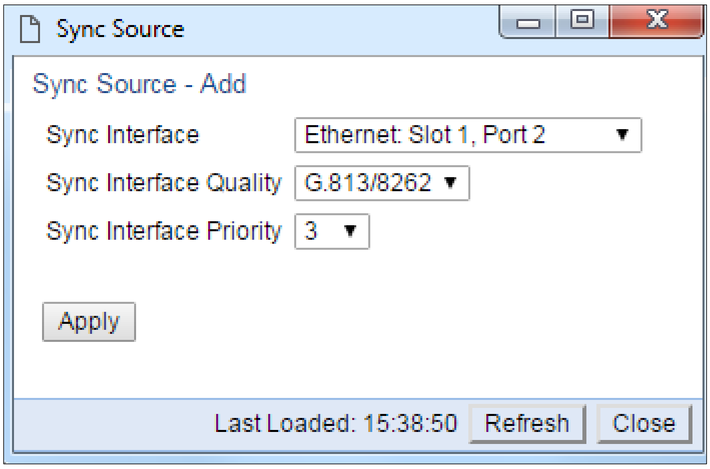
Parameter	Definition
System Reference Quality	The quality of the current synchronization source interface. A value of **DNU** indicates that no synchronization source interfaces are currently defined.
Current Active Sync Source	The currently active system synchronization source interface.
Sync Clock Unit Status	The status of the unit's Sync E mechanism.
Sync Interface	Displays the interface that is configured as a synchronization source.
Sync Interface Quality	Displays the quality level assigned to this synchronization source. This enables the system to select the source with the highest quality as the current synchronization source. If the **Sync Interface Quality** is set to **Automatic**, the quality is determined by the received SSMs. If no valid SSM messages are received or in case of interface failure (such as LOS, LOC, LOF), the quality becomes "Failure." SSM must be enabled on the remote interface in order for the interface to receive SSM messages. For instructions how to enable SSM, see Configuring the Outgoing Clock and SSM Messages.
Sync Interface Priority	Displays the priority assigned to this synchronization source.
Sync Interface Quality Status	Displays the current actual synchronization quality of the interface.

Adding a Sync Source

To add a synchronization source:

1 In the Sync Source page (Figure 243), click **Add**. The Sync Source – Add page opens.

Figure 244 Sync Source – Add Page



Sync Source

Sync Source - Add

Sync Interface: Ethernet: Slot 1, Port 2

Sync Interface Quality: G.813/8262

Sync Interface Priority: 3

2 In the **Sync Interface** field, select the interface you want to define as a synchronization source. You can select from the following interface types:

- Ethernet interfaces
- Radio interface

Note

In order to select an Ethernet interface, you must first specify the media type for this interface. See Configuring Ethernet Interfaces.

3 In the **Sync Interface Quality** field, select the quality level applied to the selected synchronization source. This enables the system to select the source with the highest quality as the current synchronization source.

- If the **Sync Interface Quality** is set to **Automatic**, the quality is determined by the received SSMs. If no valid SSM messages are received or in case of interface failure (such as LOS, LOC, LOF), the quality becomes **Failure**. SSM must be enabled on the remote interface in order for the interface to receive SSM messages. For instructions how to enable SSM, see Configuring the Outgoing Clock and SSM Messages.
- If the **Sync Interface Quality** is set to a fixed value, then the quality status becomes **Failure** upon interface failure (such as LOS, LOC, LOF).

4 In the **Sync Interface Priority** field, select the priority of this synchronization source relative to other synchronization sources configured in the unit (1-16). You cannot assign the same priority to more than one synchronization source. Once a priority value has been assigned, it no longer appears in the **Sync Interface Priority** dropdown list.

5 Click **Apply**, then **Close**.

Editing a Sync Source

To edit a synchronization source:

1 In the Sync Source page (Figure 243), click **Edit**. The Sync Source – Edit page opens.

2 Edit the parameters, as defined above. You can edit all the parameters except **Sync Interface**, which is read-only.

3 Click **Apply**, then **Close**.

Deleting a Sync Source

To delete a synchronization source:

1 Select the synchronization source in the Sync Source page (Figure 243).

2 Click **Delete**. The synchronization source is deleted.

Configuring the Outgoing Clock and SSM Messages

Note

Under certain circumstances in which an adequate clock signal is unavailable, an interface may go from locked state to holdover state. Normally, when an interface is in holdover state, it uses stored data to determine its outgoing clock. However, you can set the unit to apply a default quality of DNU (Do Not Use) to any interface in holdover state via the CLI. For instructions, see Changing the Default Quality (CLI).

In the Outgoing Clock page, you can view and configure the following synchronization settings per interface:

The interface's clock source (outgoing clock).

For radio interfaces, the synchronization radio channel (used for interoperability).

SSM message administration.

In order to provide topological resiliency for synchronization transfer, PTP 850E implements the passing of SSM messages over the radio interfaces. SSM timing in PTP 850E complies with ITU-T G.781.

In addition, the SSM mechanism provides reference source resiliency, since a network may have more than one source clock. The following are the principles of operation:

At all times, each source interface has a “quality status” which is determined as follows:

- If quality is configured as fixed, then the quality status becomes “failure” upon interface failure (such as LOS, LOC, LOF).
- If quality is automatic, then the quality is determined by the received SSMs. If no valid SSM messages are received or in case of interface failure (such as LOS, LOC, LOF), the quality becomes "failure.

Each unit holds a parameter which indicates the quality of its reference clock. This is the quality of the current synchronization source interface.

The reference source quality is transmitted through SSM messages to all relevant radio interfaces.

In order to prevent loops, an SSM with quality “Do Not Use” is sent from the active source interface (both radio and Ethernet)

In order for an interface to transmit SSM messages, SSM must be enabled on the interface. By default, SSM is disabled on all interfaces.

When configuring the outgoing clock and SSM administration, the Sync mode must be set to its default setting of automatic. To display the current Sync mode, enter the following CLI command in root view:

```
root> platform sync mode show
```

If the Sync mode is set to pipe, you must set it to automatic by entering the following CLI command in root view:

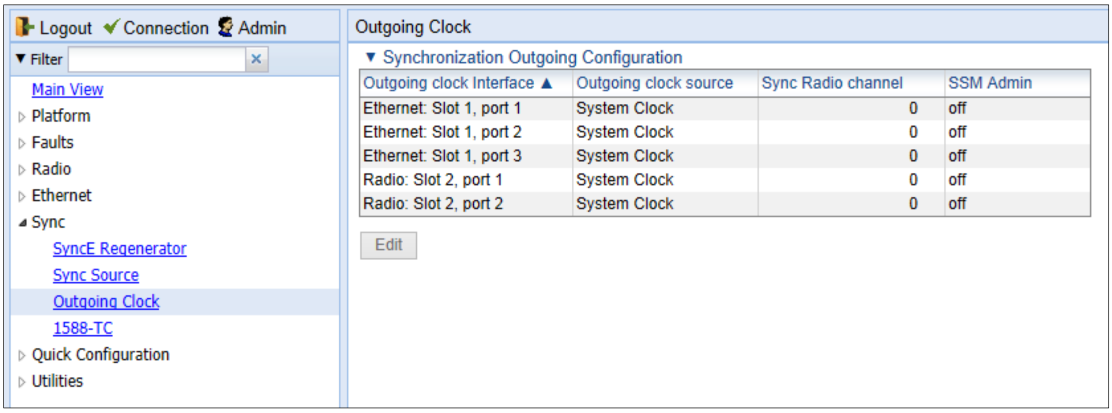
```
root> platform sync mode set automatic
```

To configure the outgoing clock on an Ethernet interface, the Media Type of the interface must be RJ45 or SFP, not Auto-Type. To view and configure the Media Type of an Ethernet interface, see Configuring Ethernet Interfaces.

To view and configure the synchronization parameters of the unit’s interfaces:

1 Select **Sync > Outgoing Clock**. The Outgoing Clock page opens.

Figure 245 Outgoing Clock Page

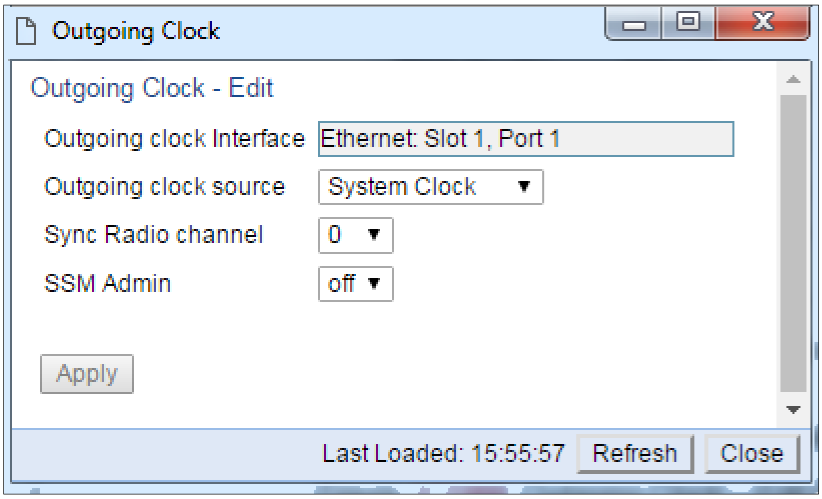


Synchronization Outgoing Configuration

Outgoing clock Interface ▲	Outgoing clock source	Sync Radio channel	SSM Admin
Ethernet: Slot 1, port 1	System Clock	0	off
Ethernet: Slot 1, port 2	System Clock	0	off
Ethernet: Slot 1, port 3	System Clock	0	off
Radio: Slot 2, port 1	System Clock	0	off
Radio: Slot 2, port 2	System Clock	0	off

2 Select the interface you want to configure and click **Edit**. The Outgoing Clock – Edit page opens.

Figure 246 Outgoing Clock – Edit Page



Outgoing Clock - Edit

Outgoing clock Interface: Ethernet: Slot 1, Port 1

Outgoing clock source: System Clock ▼

Sync Radio channel: 0 ▼

SSM Admin: off ▼

Last Loaded: 15:55:57

3 In the **Outgoing clock source** field, select the interface's synchronization source. Options are:

- **Local Clock** – The interface uses its internal clock as its synchronization source.
- **System Clock** – Default value. The interface uses the system clock as its synchronization source.
- **Source Interface** – Reserved for future use.
- **Time Loop** – Reserved for future use.

4 In **Sync Radio Channel** field, use the default value of 0.

5 In the **SSM Admin** field, select **On** or **Off** to enable or disable SSM for the interface. By default, SSM is disabled on all interfaces.

Configuring 1588 Transparent Clock

PTP 850E uses 1588v2-compliant Transparent Clock to counter the effects of delay variation. Transparent Clock measures and adjusts for delay variation, enabling the PTP 850E to guarantee ultra-low PDV.

A Transparent Clock node resides between a master and a slave node, and updates the timestamps of PTP packets passing from the master to the slave to compensate for delay, enabling the terminating clock in the slave node to remove the delay accrued in the Transparent Clock node. The Transparent Clock node is itself neither a master nor a slave node, but rather, serves as a bridge between master and slave nodes.

Note that in release 11.1:

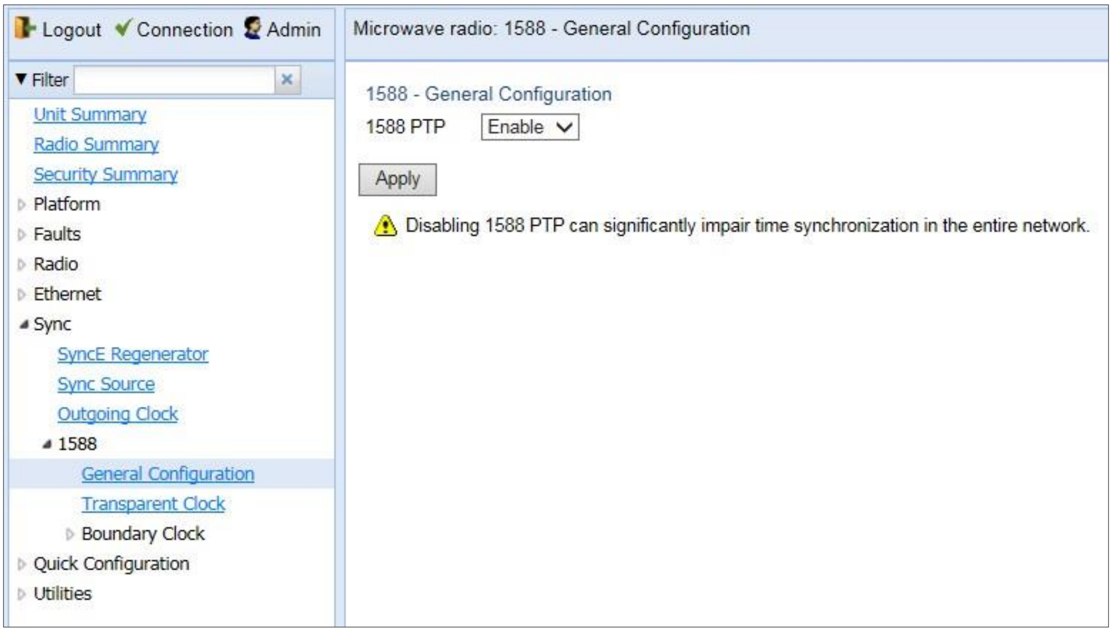
- 1588 TC is not supported when Master-Slave communication is using the IPv6 transport layer.
- 1588 TC cannot be used in Multiband configurations.

> Note
>
> Make sure to enable Transparent Clock on the remote side of the link before enabling it on the local side.

To configure Transparent Clock:

1. Add the port receiving synchronization from the customer side as a Sync source, with Sync Interface Priority 1. See *Adding a Sync Source*.
2. Add a radio interface as a Sync source, with lower priority than the port receiving synchronization from the customer side. See *Adding a Sync Source*.
3. On the remote side of the radio link, add the radio interface facing the local device as a Sync source, with Sync Interface Priority 1. See *Adding a Sync Source*.
4. On the remote side of the radio link, if there is an Ethernet port conveying synchronization, add this port as a Sync source, with lower priority than the radio interface. See *Adding a Sync Source*.
5. Verify that the Sync Interface Quality Status of the first Sync source is not Failure. See Viewing the Sync Source Status.

6 Select **Sync > 1588 > General Configuration**. The 1588 – General Configuration page opens.



Microwave radio: 1588 - General Configuration

1588 - General Configuration

1588 PTP Enable

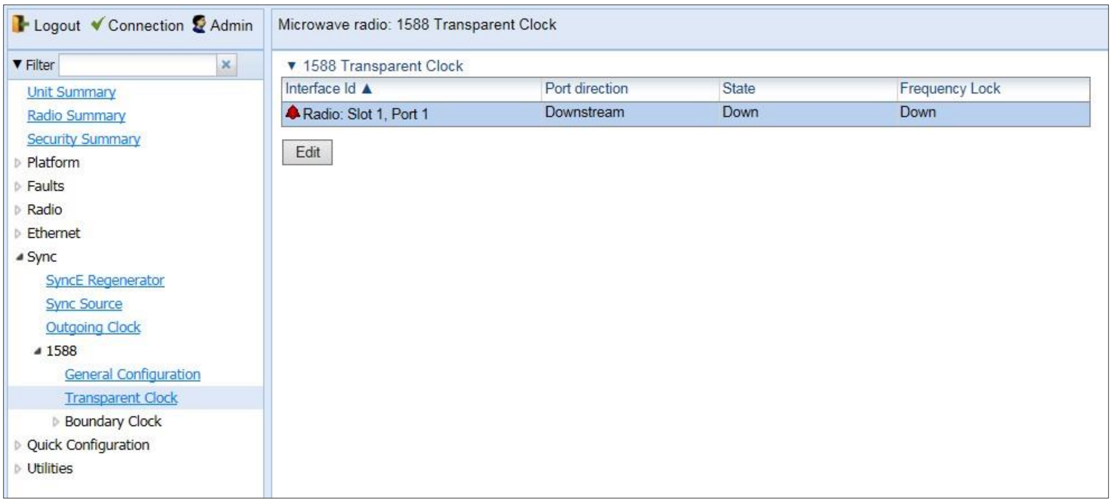
Disabling 1588 PTP can significantly impair time synchronization in the entire network.

Figure 168: 1588 General Configuration Page

7 In the **1588 PTP** field, select **Enable**.

8 Click **Apply**.

9 Select **Sync > 1588 > Transparent Clock**. The 1588 Transparent Clock page opens.



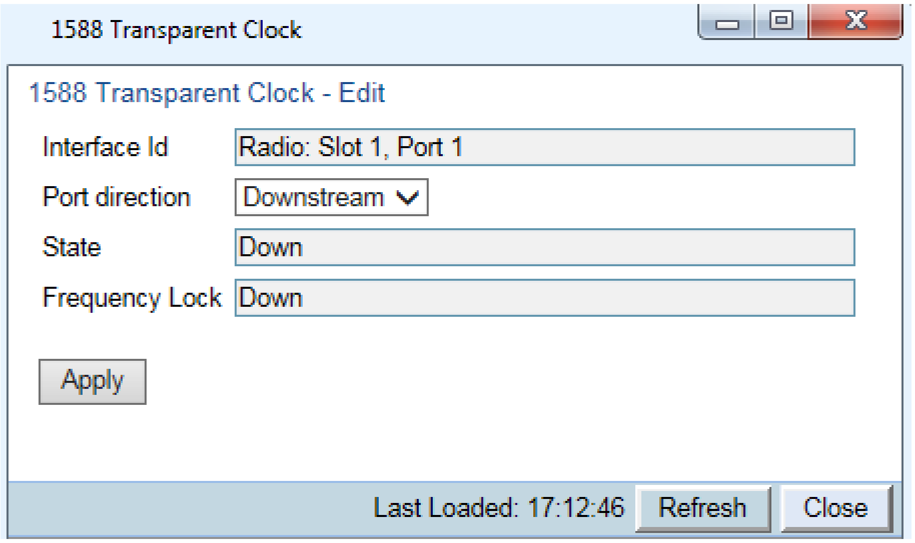
Microwave radio: 1588 Transparent Clock

▼ 1588 Transparent Clock

Interface Id ▲	Port direction	State	Frequency Lock
Radio: Slot 1, Port 1	Downstream	Down	Down

Figure 169: 1588 Transparent Clock Page

10 Select the radio interface and click **Edit**. The 1588 Transparent Clock – Edit page opens.



1588 Transparent Clock - Edit

Interface Id: Radio: Slot 1, Port 1
Port direction: Downstream
State: Down
Frequency Lock: Down

Last Loaded: 17:12:46

Figure 247 1588 Transparent Clock – Edit Page

11 In the **Port direction** field, select **Upstream** or **Downstream**. This field must be set to different values on the two sides of the link, so that if you set the local side to **Upstream**, you must set the remote side to **Downstream**, and vice versa. Otherwise than that, it does not matter how you set this field.

12 Click **Apply**, then **Close**.

13 1588 packets should be mapped to CoS 7. By default, 1588 packets are *not* mapped to any CoS. To map 1588 packets to CoS 7, you must *disable* CoS preservation for 1588 packets. This must be performed via CLI, using the following command:

```
root> ethernet generalcfg ptp-tc cos-preserve set admin disable
```

14 To map 1588 packets to CoS 7, enter the following command:

```
root> ethernet generalcfg ptp-tc cos-preserve cos value 7
```

After you enter these commands, 1588 packets will automatically be mapped to CoS 7.

> Note
>
> If necessary, you can use the ethernet generalcfg ptp-tc cos- preserve cos value command to map a different CoS value (0-7) to 1588 packets, but it is recommended to map 1588 packets to CoS 7.

To disable Transparent Clock synchronization:

1 Select **Sync > 1588 > General Configuration.** The 1588 – General Configuration page opens (*Figure 168*).

2 In the **1588 PTP** field, select **Disable**.

3 Click **Apply**.

Note

Disabling 1588 PTP can drastically affect time synchronization performance in the entire network.

Configuring 1588 Boundary Clock

Boundary Clock complies with ITU-T Telecom Profile G.8275.1. This enables PTP 850E, with Boundary Clock, to meet the rigorous synchronization requirements of 5G networks.

The Boundary Clock in PTP 850E supports up to 16 1588 slave clock devices.

The Boundary Clock terminates the PTP flow it receives on the slave port, recovers the time and phase, and regenerates the PTP flow on the master ports.

The Boundary Clock node selects the best synchronization source available in the domain and regenerates PTP towards the slave clocks. This reduces the processing load from grandmaster clocks and increases the scalability of the synchronization network, while rigorously maintaining timing accuracy.

The PTP 850E Boundary Clock mechanism requires the use of untagged Ethernet multicast PTP packets as specified in G.8275.1.

Note

Boundary Clock and Transparent Clock can be used together in the same PTP 850E node.

Note that in release 11.1:

- 1588 BC can only be used in a chain or star topology. It cannot be used in a ring topology.
- 1588 BC is not supported when Master-Slave communication is using the IPv6 transport layer.

Enabling Boundary Clock

Note

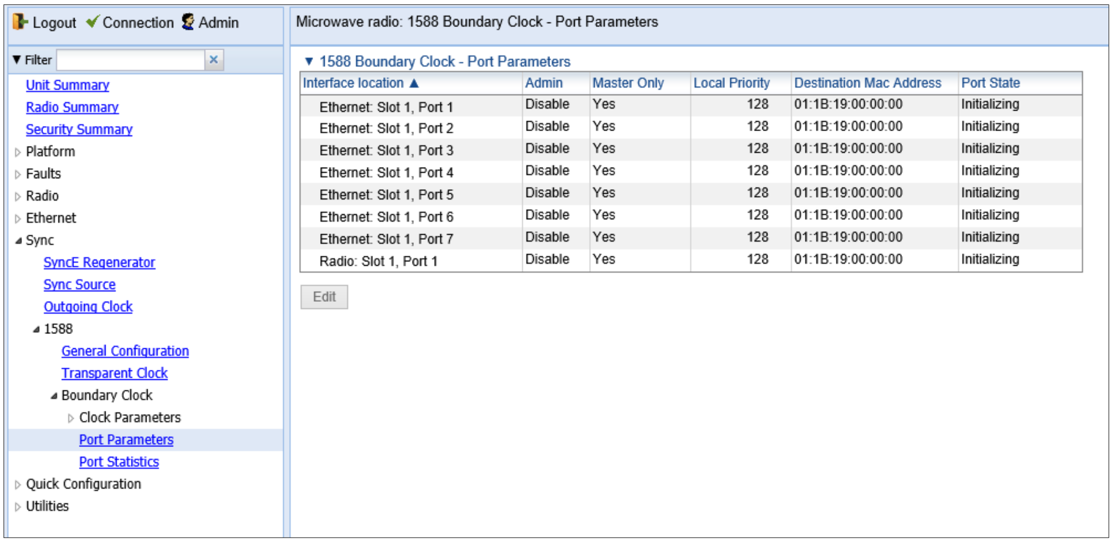
Before configuring Boundary Clock, you must configure Transparent Clock. See Configuring 1588 Transparent Clock.

To enable Boundary Clock:

1. Select Sync > 1588 > General Configuration. The 1588 – General Configuration page opens (Figure 191).
2. In the **1588 PTP** field, select **Enable**.
3. Click Apply.

4. Select **Sync > 1588 > Boundary Clock > Port Parameters**. The 1588 Boundary Clock – Port Parameters page opens. You can configure up to 16 interfaces per unit to be part of the Boundary Clock node. These interfaces can be radio and Ethernet interfaces, but not TDM interfaces or groups (e.g., LAG or Multi-Carrier ABC groups).

Figure 248 1588 Boundary Clock – Port Parameters Page



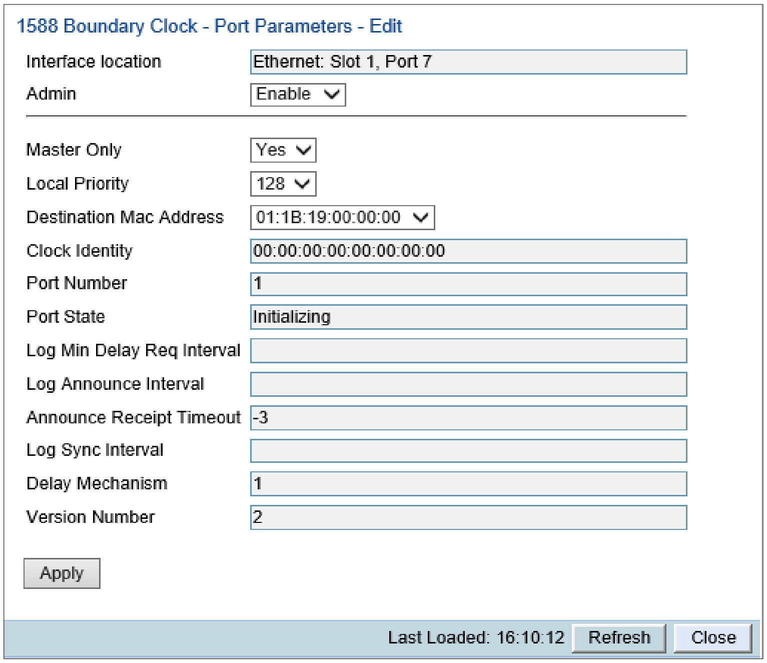
Microwave radio: 1588 Boundary Clock - Port Parameters

▼ 1588 Boundary Clock - Port Parameters

Interface location ▲	Admin	Master Only	Local Priority	Destination Mac Address	Port State
Ethernet: Slot 1, Port 1	Disable	Yes	128	01:1B:19:00:00:00	Initializing
Ethernet: Slot 1, Port 2	Disable	Yes	128	01:1B:19:00:00:00	Initializing
Ethernet: Slot 1, Port 3	Disable	Yes	128	01:1B:19:00:00:00	Initializing
Ethernet: Slot 1, Port 4	Disable	Yes	128	01:1B:19:00:00:00	Initializing
Ethernet: Slot 1, Port 5	Disable	Yes	128	01:1B:19:00:00:00	Initializing
Ethernet: Slot 1, Port 6	Disable	Yes	128	01:1B:19:00:00:00	Initializing
Ethernet: Slot 1, Port 7	Disable	Yes	128	01:1B:19:00:00:00	Initializing
Radio: Slot 1, Port 1	Disable	Yes	128	01:1B:19:00:00:00	Initializing

5. Select an interface and click **Edit**. The 1588 Boundary Clock – Port Parameters – Edit page opens.

Figure 249 1588 Boundary Clock – Port Parameters – Edit Page



1588 Boundary Clock - Port Parameters - Edit

Interface location	Ethernet: Slot 1, Port 7
Admin	Enable
Master Only	Yes
Local Priority	128
Destination Mac Address	01:1B:19:00:00:00
Clock Identity	00:00:00:00:00:00:00:00
Port Number	1
Port State	Initializing
Log Min Delay Req Interval	
Log Announce Interval	
Announce Receipt Timeout	-3
Log Sync Interval	
Delay Mechanism	1
Version Number	2

Last Loaded: 16:10:12

6. In the **Admin** field, select **Enable**.

7. In the **Master Only** field, select from the following options:

- Yes – The port can only be used as the master port, which means the port acts as a PTP synchronization source for other nodes.
- No – The port can be used as either a master port or the slave port. The slave port receives PTP synchronization input from an external grandmaster clock. The Best Master Clock Algorithm (BMCA) determines the port's role, based on its determination of which is the best available grandmaster clock. Only one slave port can exist in a single PTP 850E node at any one time.

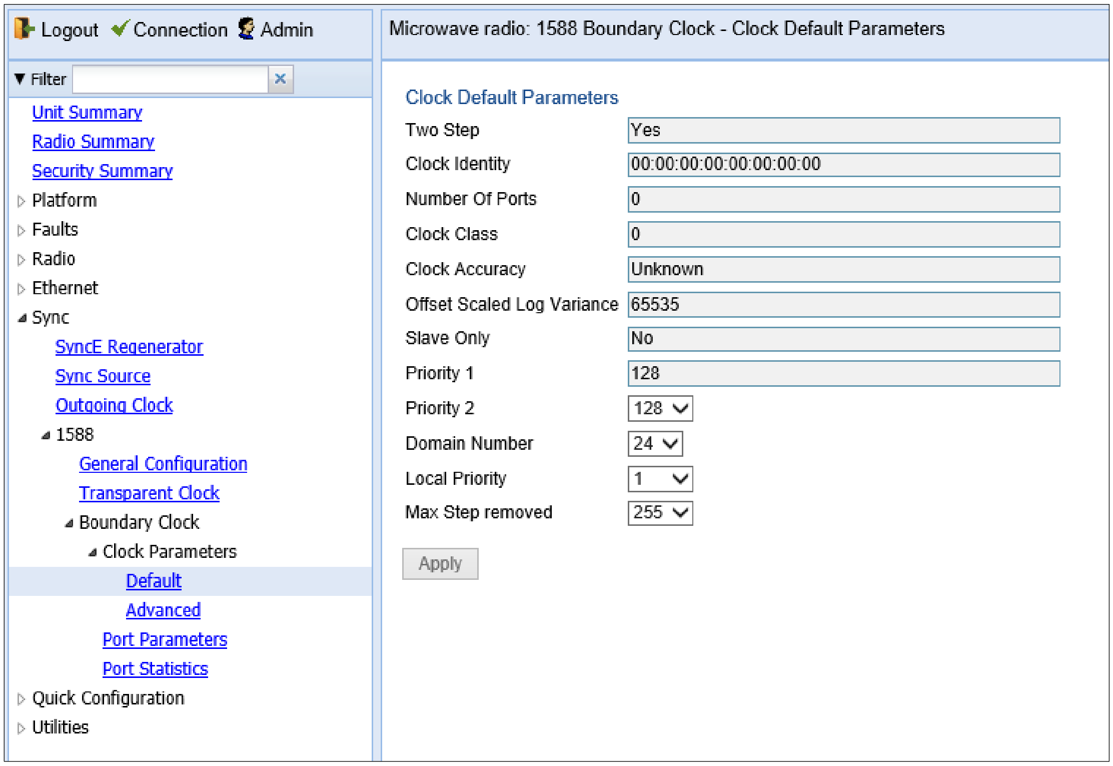
8. Optionally, in the **Local Priority** field, select a value between 1-255. The default value is 128. The Local Priority value is taken into account when two identical announce messages are received by at least two different ports. In such a case, the Boundary Clock mechanism selects the slave port based on the best (lowest) Local Priority.
9. In the **Destination Mac Address** field, select a MAC address for multicast re-transmission of PTP packets. Options are:
   - 01-1B-19-00-00-00 – General group address. An 802.1Q VLAN Bridge would forward the frame unchanged.
   - 01-80-C2-00-00-0E – Individual LAN Scope group address. An 802.1Q VLAN Bridge would drop the frame.
10. Click **Apply**.
11. Repeat these steps to add up to 16 interfaces to the unit's Boundary Clock node.
12. To map PTP packets into the Boundary Clock node, a service point must be created on each interface in the Boundary Clock node. This service point must be defined to gather untagged packets. See *Adding a Service Point*.
13. Add a port receiving synchronization from the customer side as a Sync source, with Sync Interface Priority 1. See ***Error! Reference source not f ound.***.
14. Add a radio interface as a Sync source, with lower priority than the port receiving synchronization from the customer side. See ***Error! Reference s ource not found.***.
15. On the remote side of the radio link, add the radio interface facing the local device as a Sync source, with Sync Interface Priority 1. See ***Error! Reference s ource not found.***.
16. On the remote side of the radio link, if there is an Ethernet port conveying synchronization, add this port as a Sync source, with lower priority than the radio interface. See ***Error! Reference source not found.***.
17. Verify that the Sync Interface Quality Status of the first Sync source is not Failure. See ***Error! Reference source not found.***.

Displaying and Setting the Boundary Clock Default Parameters

To display and set the Boundary Clock default parameters:

1. Select **Sync > 1588 > Boundary Clock > Clock Parameters > Default**. The 1588 Boundary Clock – Clock Default Parameters page opens.

Figure 250 1588 Boundary Clock – Clock Default Parameters Page



Microwave radio: 1588 Boundary Clock - Clock Default Parameters

Clock Default Parameters

Two Step	Yes
Clock Identity	00:00:00:00:00:00:00:00
Number Of Ports	0
Clock Class	0
Clock Accuracy	Unknown
Offset Scaled Log Variance	65535
Slave Only	No
Priority 1	128
Priority 2	128
Domain Number	24
Local Priority	1
Max Step removed	255

2. In the **Priority 2** field, you can select a value between 0 and 255. The default value is 128. The Priority 2 value is one of the factors used by the BMCA to determine the grandmaster. The PTP 850E's Boundary Clock node advertises this value when it is not locked on an external grandmaster.
3. In the Domain **Number** field, you can select a value between 24 and 43. The default value is 24.
4. In the **Local Priority** field, you can select a value between 1 and 255. The default value is 128. The Local Priority value is taken into account when two identical announce messages are received by at least two different ports. In such a case, the Boundary Clock mechanism selects the slave port based on the best (lowest) Local Priority.
5. In the **Max Step removed** field, you can select the maximum number of PTP clocks traversed from the grandmaster to the slave clock in the local PTP 850E Boundary Clock node. The value range is 1-255. The default value is 255. If the defined number is exceeded, packets from this grandmaster candidate are discarded and the grandmaster will not be eligible for use by the Boundary Clock node.
6. To implement your changes, click **Apply**.

Figure 251 Boundary Clock Default Parameters

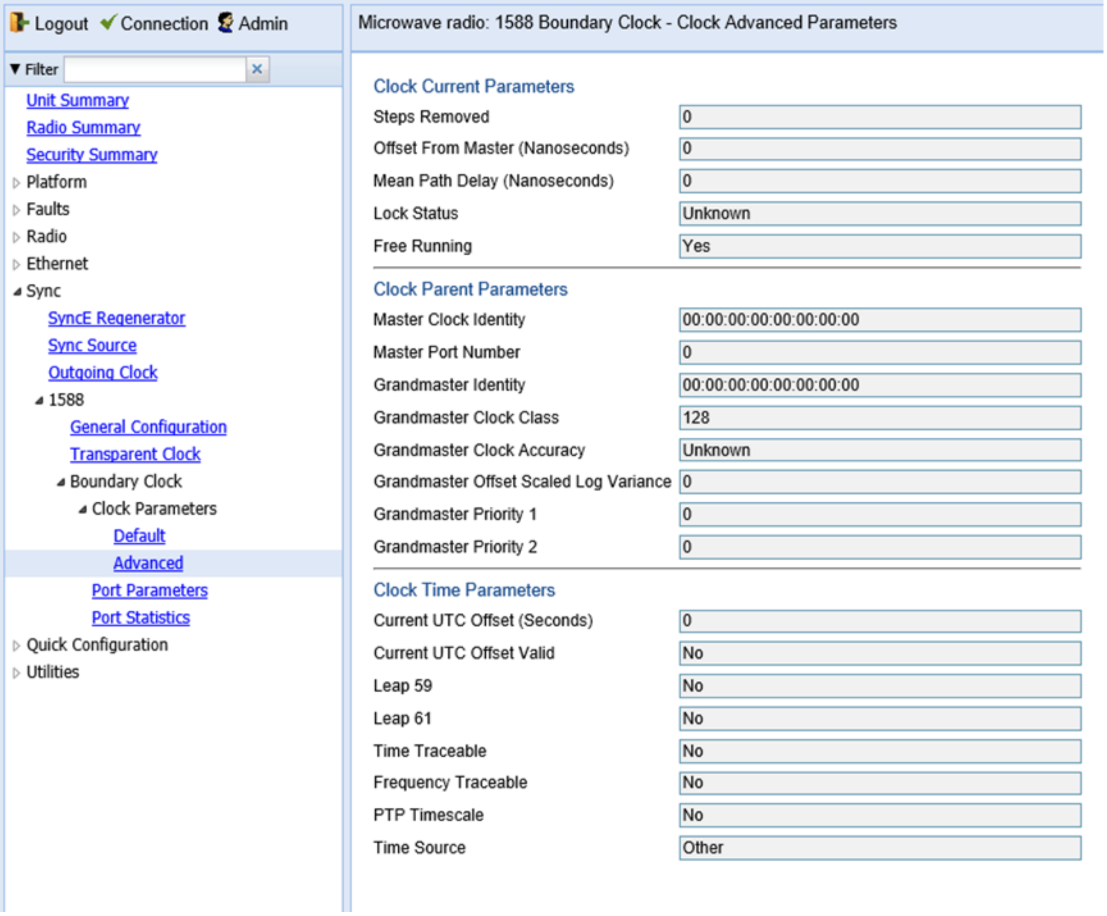
Parameter	Definition
Two Step	Indicates whether the Boundary Clock node is operating in two-step mode. In PTP 850E, this is always set to Yes.
Clock Identity	Identifies the system clock.
Number of Ports	Displays the number of ports on the unit on which Boundary Clock is enabled. The maximum is 16 per PTP 850E unit.
Clock Class	One of the elements of the clock quality, as defined in IEEE-1588.
Clock Accuracy	One of the elements of the clock quality, as defined in IEEE-1588.
Offset Scaled Log Variance	One of the elements of the clock quality, as defined in IEEE-1588.
Slave Only	Indicates whether the Boundary Clock node is operating in slave mode only. In PTP 850E, this is always set to No.
Priority 1	Always displays 128.

Displaying the Boundary Clock Advanced Parameters

To display and set the Boundary Clock advanced parameters:

1. Select **Sync > 1588 > Boundary Clock > Clock Parameters > Advanced**. The 1588 Boundary Clock – Clock Advanced Parameters page opens.

Figure 252 1588 Boundary Clock – Clock Advanced Parameters Page



Microwave radio: 1588 Boundary Clock - Clock Advanced Parameters

Clock Current Parameters

Steps Removed	0
Offset From Master (Nanoseconds)	0
Mean Path Delay (Nanoseconds)	0
Lock Status	Unknown
Free Running	Yes

Clock Parent Parameters

Master Clock Identity	00:00:00:00:00:00:00:00
Master Port Number	0
Grandmaster Identity	00:00:00:00:00:00:00:00
Grandmaster Clock Class	128
Grandmaster Clock Accuracy	Unknown
Grandmaster Offset Scaled Log Variance	0
Grandmaster Priority 1	0
Grandmaster Priority 2	0

Clock Time Parameters

Current UTC Offset (Seconds)	0
Current UTC Offset Valid	No
Leap 59	No
Leap 61	No
Time Traceable	No
Frequency Traceable	No
PTP Timescale	No
Time Source	Other

All of the advanced Boundary Clock parameters are read-only. Beow table lists and describes the Boundary Clock advanced parameters.

Table 76 Boundary Clock Advanced Parameters

Parameter	Definition
Steps Removed	The number of PTP clocks traversed from the grandmaster to the slave clock in the local PTP 850E Boundary Clock node. You can define a maximum number of steps in the Clock Default Parameters page. See Displaying and Setting the Boundary Clock Default Parameters.
Offset from Master (Nanoseconds)	The time difference between the master clock and the local slave clock (in ns).
Mean Path Delay (Nanoseconds)	The mean propagation time for the link between the master and the local slave (in ns).
Lock Status	Provides 1588 Boundary Clock stack lock status information.
Free Running	APR stack manual freerun state.
Master Clock Identity	The clock identity of the current master clock.
Master Port Number	The clock identity of the current master port.

Parameter	Definition
Grandmaster Identity	The clock identity of the current grandmaster.
Grandmaster Clock Class	The clock class of the current grandmaster. The clock class is one of the elements of the clock quality, as defined in IEEE-1588.
Grandmaster Clock Accuracy	The clock accuracy of the current grandmaster. The clock accuracy is one of the elements of the clock quality, as defined in IEEE-1588.
Grandmaster Offset Scaled Log Variance	The offset scaled log variance of the current grandmaster. The offset scaled log variance is one of the elements of the clock quality, as defined in IEEE-1588.
Grandmaster Priority 1	The Priority 1 value of the current grandmaster.
Grandmaster Priority 2	The Priority 2 value of the current grandmaster.
Current UTC Offset (Seconds)	The current UTC offset value (in seconds).
Current UTC Offset Valid	Indicates whether the current UTC offset value is valid.
Leap 59	Indicates that the last minute of the current UTC day contains 59 seconds.
Leap 61	Indicates that the last minute of the current UTC day contains 61 seconds.
Time Traceable	Traceability to the primary time reference.
Frequency Traceable	Traceability to the primary frequency reference.
PTP Timescale	Indicates whether the clock time scale of the grandmaster clock is PTP.
Time Source	The source of the time used by the grandmaster clock.

Displaying the Boundary Clock Port Parameters

To display the Boundary Clock port parameters:

1. Select Sync > 1588 > Boundary Clock > Port Parameters. The 1588 Boundary Clock – Port Parameters page opens (Figure 194).
2. Select the port you want to configure and click Edit. The 1588 Boundary Clock – Port Parameters – Edit page opens (*Figure 195*).

For an explanation of the configurable fields, see Enabling Boundary Clock. Below lists and describes the read-only Boundary Clock port parameters.

Table 77 Boundary Clock Port Parameters

Parameter	Definition
Clock Identity	The PTP 850E unit's clock identity. The same value is used for every port that belongs to the Boundary Clock node.
Port Number	Displays the number of the port according to the activation sequence of every port.

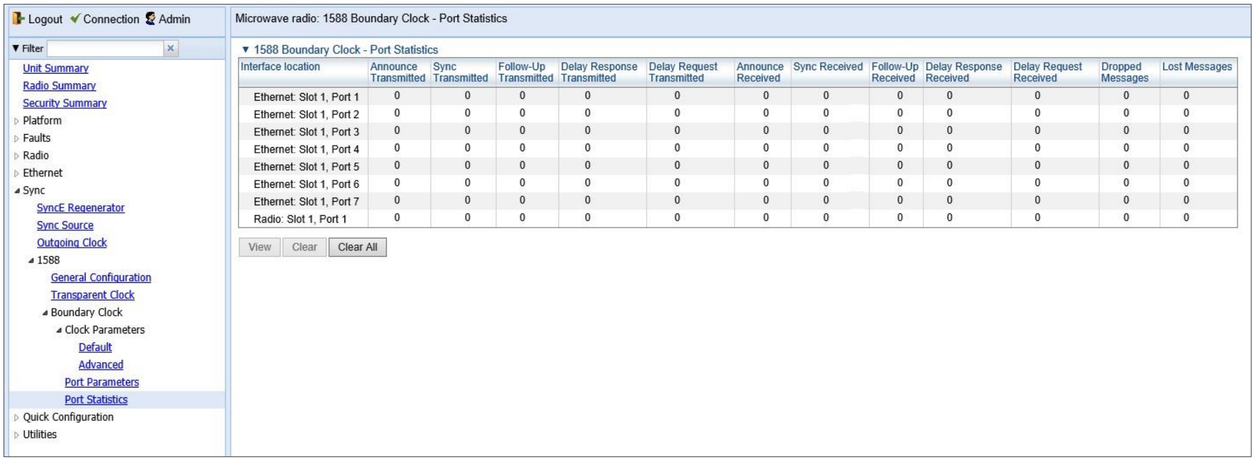
Parameter	Definition
Port State	Indicates whether the port is currently acting as Master (distributing PTP to other nodes) or Slave (receiving PTP from a grandmaster).
Log Min Delay Req Interval	The minimum allowed interval between Delay Request messages.
Log Announce Interval	The interval between Announce messages.
Announce Receipt Timeout	The maximum allowed number of intervals without receiving any Announce messages.
Log Sync Interval	Interval between sync messages.
Delay Mechanism	Always displays 1.
Version Number	Always displays 2.

Displaying the Boundary Clock Port Statistics

To display the Boundary Clock port statistics:

1. Select **Sync > 1588 > Boundary Clock > Port Statistics**. The 1588 Boundary Clock – Port Statistics page opens.

Figure 253 1588 Boundary Clock – Port Statistics Page



Microwave radio: 1588 Boundary Clock - Port Statistics

▼ 1588 Boundary Clock - Port Statistics

Interface location	Announce Transmitted	Sync Transmitted	Follow-Up Transmitted	Delay Response Transmitted	Delay Request Transmitted	Announce Received	Sync Received	Follow-Up Received	Delay Response Received	Delay Request Received	Dropped Messages	Lost Messages
Ethernet: Slot 1, Port 1	0	0	0	0	0	0	0	0	0	0	0	0
Ethernet: Slot 1, Port 2	0	0	0	0	0	0	0	0	0	0	0	0
Ethernet: Slot 1, Port 3	0	0	0	0	0	0	0	0	0	0	0	0
Ethernet: Slot 1, Port 4	0	0	0	0	0	0	0	0	0	0	0	0
Ethernet: Slot 1, Port 5	0	0	0	0	0	0	0	0	0	0	0	0
Ethernet: Slot 1, Port 6	0	0	0	0	0	0	0	0	0	0	0	0
Ethernet: Slot 1, Port 7	0	0	0	0	0	0	0	0	0	0	0	0
Radio: Slot 1, Port 1	0	0	0	0	0	0	0	0	0	0	0	0

- To display the statistics for a specific port in a separate page, click **View**.
- To clear the statistics for a specific port, select the port's row and click **Clear**.
- To clear the statistics for all Boundary Clock ports, click **Clear All**.

Table 78 Boundary Clock Port Statistics

Parameter	Definition
Announce Transmitted	The number of Announce messages that have been transmitted from the port.
Sync Transmitted	The number of Sync messages that have been transmitted from the port.
Follow-Up Transmitted	The number of Follow-Up messages that have been transmitted from the port.
Delay Response Transmitted	The number of Delay Response messages that have been transmitted from the port.
Delay Request Transmitted	The number of Delay Request messages that have been transmitted from the port.
Announce Received	The number of Announce messages that have been received by the port.
Sync Received	The number of Sync messages that have been received by the port.
Follow-Up Received	The number of Follow-Up messages that have been received by the port.
Delay Response Received	The number of Delay Response messages that have been received by the port.
Delay Request Received	The number of Delay Request messages that have been received by the port.
Dropped Messages	The number of dropped messages.
Lost Messages	The number of lost messages.

Disabling 1588 PTP

To disable 1588 PTP synchronization:

1. Select **Sync > 1588 > Boundary Clock > Port Parameters**. The 1588 Boundary Clock – Port Parameters page opens (*Figure 194*).
2. Select an interface and click **Edit.** The 1588 Boundary Clock – Port Parameters
3. In the **Admin** field, select **Disable**.

> Note
>
> It is important to disable Boundary Clock on the interfaces before disabling 1588 PTP.

4. Select **Sync > 1588 > General Configuration**. The 1588 – General Configuration page.
5. In the **1588 PTP** field, select **Disable**.
6. Click **Apply**.

> Note
>
> Disabling 1588 PTP disables both Transparent Clock and Boundary Clock, and can drastically affect time synchronization performance in the entire network.

Chapter 13: Access Management and Security

This section includes:

- Quick Security Configuration
- Configuring the General Access Control Parameters
- Configuring the Password Security Parameters
- Configuring the Session Timeout
- Configuring Users
- Configuring RADIUS
- Viewing Remote Access User Connectivity and Permissions
- Configuring X.509 CSR Certificates
- Enabling HTTPS
- Downloading and Installing an RSA Key
- Blocking Telnet Access
- Uploading the Security Log
- Uploading the Configuration Log

Note

Another security feature, HTTPS cipher hardening, can be configured via CLI. For instructions, see Configuring HTTPS Cipher Hardening (CLI).
PTP 850E devices support SDN, with NETCONF/YANG capabilities. This enables PTP 850E devices to be managed via SDN using Cambium's SDN controller, SDN Master. NETCONF must be enabled via CLI. See Enabling NETCONF (CLI).
You can terminate all active sessions via a CLI command.

Related topics:

- Changing Your Password
- Configuring AES-256 Payload Encryption

Quick Security Configuration

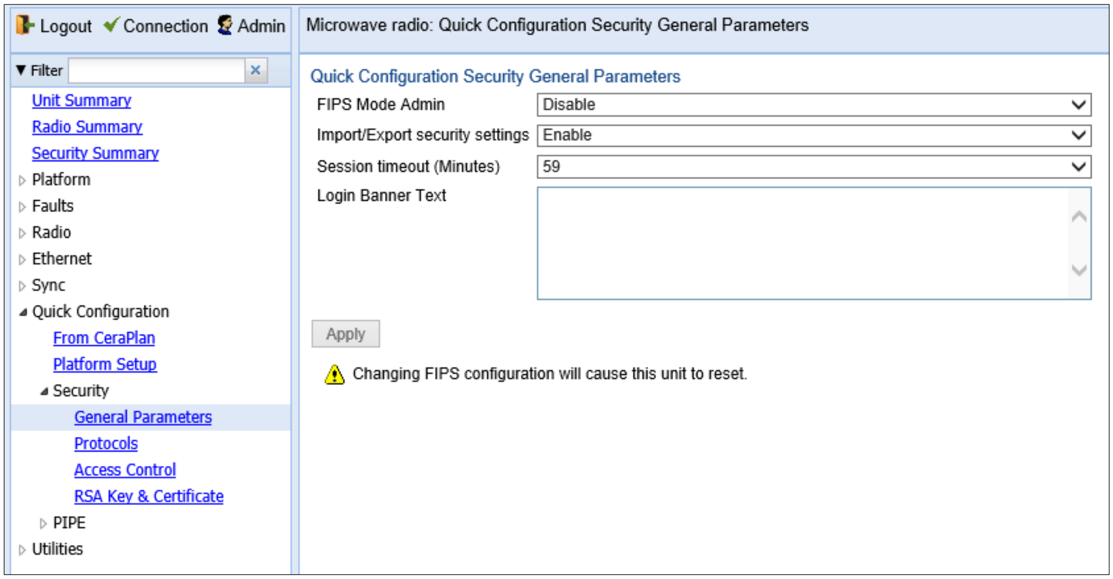
The Web EMS provides a set of Quick Configuration pages that enable you to quickly configure the unit's access and security parameters. This section describes these pages, with cross references to the sections in which each parameter is described in depth.

Quick Security Configuration – General Parameters Page

To configure the FIPS Admin, import and export security settings, session timeout, a login banner, and AES-256 payload encryption:

1 Select **Quick Configuration > Security > General Parameters**. The Quick Configuration Security General Parameters page opens.

Figure 254 Quick Configuration Security General Parameters Page



Microwave radio: Quick Configuration Security General Parameters

Quick Configuration Security General Parameters

FIPS Mode Admin	Disable
Import/Export security settings	Enable
Session timeout (Minutes)	59
Login Banner Text	

⚠ Changing FIPS configuration will cause this unit to reset.

Note

The FIPS Mode Admin field is not relevant for PTP 850E.

2 The **Import/Export security settings** field determines whether security configurations are included in configuration backup files. If you select **Enable**, security configurations will *not* be included in backup files.

3 In the **Session timeout** field, you can configure a session timeout, in minutes, from 1 to 60 minutes. The default session timeout is 10 minutes. For details,

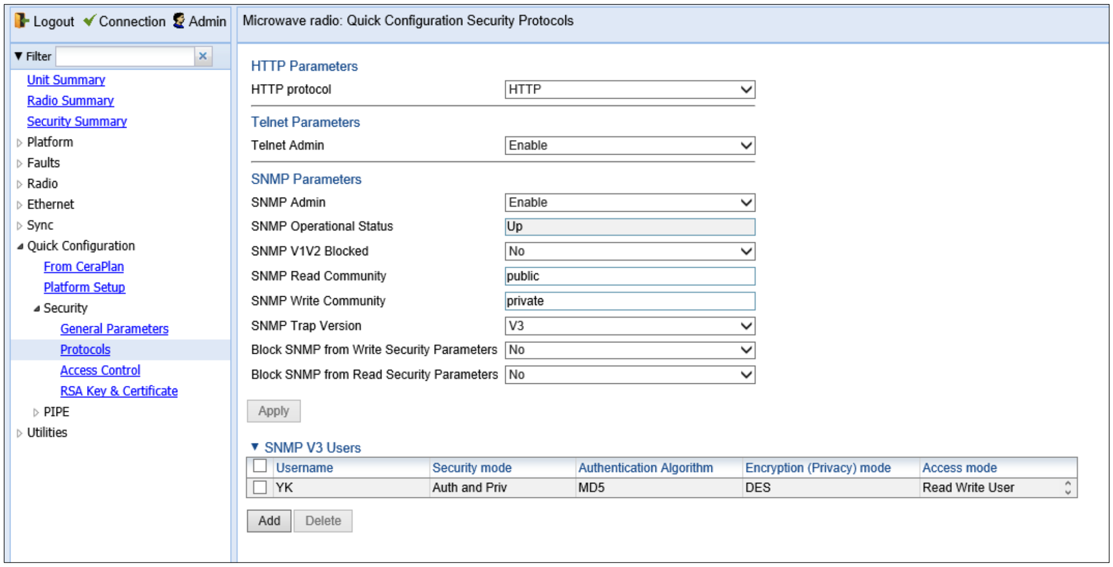
4 In the **Login Banner Text** field, you can define a login banner of up to 2,000 bytes. This banner will appear every time a user establishes a connection with the Web EMS. The banner appears before the login prompt, so that users will always see the login banner and must manually close the banner before logging in to the Web EMS. For details, see *Defining a Login Banner*.

Quick Security Configuration – Protocols Page

To configure the HTTP type, Telnet blocking, and SNMP parameters:

1. Select **Quick Configuration > Security > Protocols**. The Quick Configuration Security Protocols page opens.

Figure 255 Quick Configuration Security Protocols Page



Microwave radio: Quick Configuration Security Protocols

HTTP Parameters

HTTP protocol	HTTP

Telnet Parameters

Telnet Admin	Enable

SNMP Parameters

SNMP Admin	Enable
SNMP Operational Status	Up
SNMP V1V2 Blocked	No
SNMP Read Community	public
SNMP Write Community	private
SNMP Trap Version	V3
Block SNMP from Write Security Parameters	No
Block SNMP from Read Security Parameters	No

▼ SNMP V3 Users

□	Username	Security mode	Authentication Algorithm	Encryption (Privacy) mode	Access mode
□	YK	Auth and Priv	MD5	DES	Read Write User

2. In the **HTTP protocol** field, you can determine the web interface protocol for accessing the unit (HTTP or HTTPS). By default, the web interface protocol is HTTP. For details, see *Enabling HTTPS*.

> Note
>
> After changing the HTTP protocol, management is lost. To restore management, simply refresh the page.

3. In the **Telnet Admin** field, you can block or enable telnet access to the unit. By default, telnet access is enabled. For details, see *Blocking Telnet Access*.
4. In the **SNMP Parameters** area, you can configure the unit's SNMP parameters. For details, see ***Error! Reference source not found.***.
   n addition, you can configure the following parameters only in the Quick Configuration Security Protocols page:
   I. In the **Block SNMP from Write Security Parameters** field, select **Yes** if you want to block SNMP from writing security parameters.
   II. In the **Block SNMP from Read Security Parameters** field, select **Yes** if you want to block SNMP from reading security parameters.

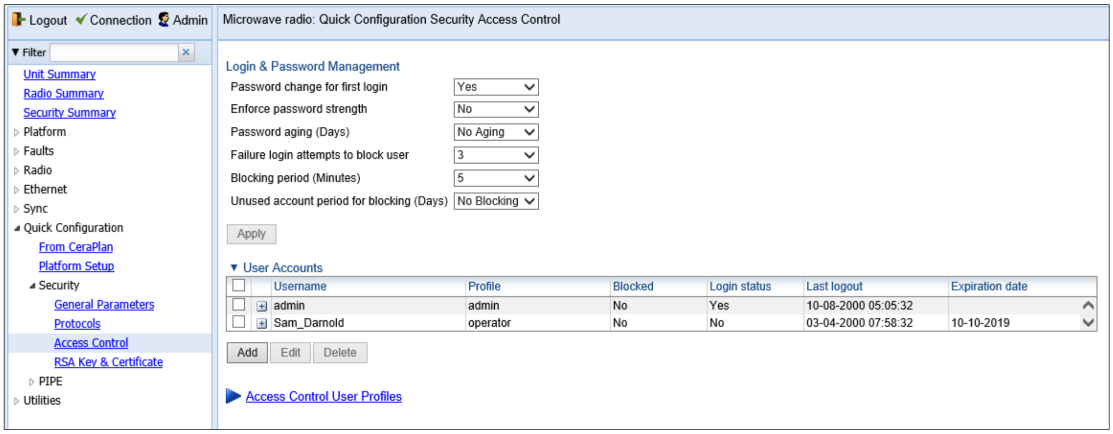
5. When you are finished editing the parameters described above, click **Apply**.
6. In the **SNMP V3 Users** are, you can click **Add** to add SNMP V3 users. For details, see ***Error! Reference source not found.***.

Quick Security Configuration – Access Control Page

To configure parameters relating to users and login parameters:

1. Select **Quick Configuration > Security > Access Control**. The Quick Configuration Security Protocols page opens.

Figure 256 Quick Configuration Security Access Control Page



Microwave radio: Quick Configuration Security Access Control

Login & Password Management

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

Apply

▼ User Accounts

□	Username	Profile	Blocked	Login status	Last logout	Expiration date
□	⊞ admin	admin	No	Yes	10-08-2000 05:05:32	
□	⊞ Sam_Darnold	operator	No	No	03-04-2000 07:58:32	10-10-2019

Add Edit Delete

Access Control User Profiles

2. In the **Login & Password Management** area, you can configure enhanced security requirements for user passwords and for logging into the unit. For details, see ***Error! Reference source not found.*** and ***Error! Reference source not found.***.
3. When you are finished editing the login and password parameters, click **Apply**.
4. In the **User Accounts** area, you can configure individual users:
   I. To add a user, click **Add**.
   II. To edit an existing user, select the user in the User Accounts table and click **Edit**.

For details, see ***Error! Reference source not found.***.

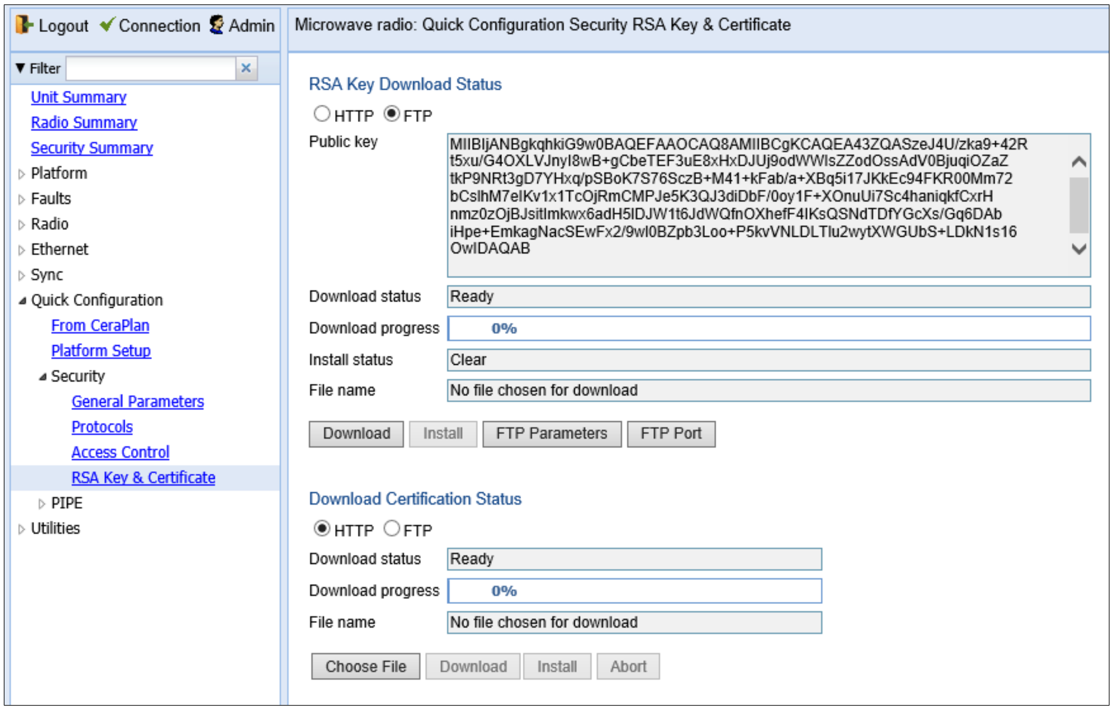
5. To configure user profiles, click **Access Control User Profiles**. For details, see *Configuring User Profiles*.

Quick Security Configuration – RSA Key & Certificate Page

To download and install an RSA key and/or a Certificate Signing Request (CSR) file:

1. Select **Quick Configuration > Security > RSA Key & Certificate**. The Quick Configuration Security RSA Key & Certificate page opens.

Figure 257 Quick Configuration Security RSA Key & Certificate Page



Microwave radio: Quick Configuration Security RSA Key & Certificate

RSA Key Download Status

○ HTTP ● FTP

Public key

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA43ZQASzeJ4U/zka9+42R
t5xu/G4OXLVJnyI8wB+gCbeTEF3uE8xHxDJUj9odWWIsZZodOssAdV0BjuqiOZaZ
tkP9NRt3gD7YHxq/pSBoK7S76SczB+M41+kFab/a+XBq5i17JKkEc94FKR00Mm72
bCslhM7elKv1x1TcOjRmCMPJe5K3QJ3diDbF/0oy1F+XOnuUi7Sc4haniqkfCxrH
nmz0zOjBJsitlmkwx6adH5lDJW1t6JdWQfnOXhefF4IKsQSNdTDfYGcXs/Gq6DAb
iHpe+EmkagNacSEwFx2/9wl0BZpb3Loo+P5kvVNLDLTlu2wytXWGUbS+LDkN1s16
OwIDAQAB
```

Download status	Ready
Download progress	0%
Install status	Clear
File name	No file chosen for download

Download Certification Status

● HTTP ○ FTP

Download status	Ready
Download progress	0%
File name	No file chosen for download

2. In the **RSA Key Download Status** area, you can download and install an RSA key. For details, see *Downloading and Installing an RSA Key*.
3. In the **Download Certification Status** area, you can download and install a CSR file. For details, see *Configuring X.509 CSR Certificates*.

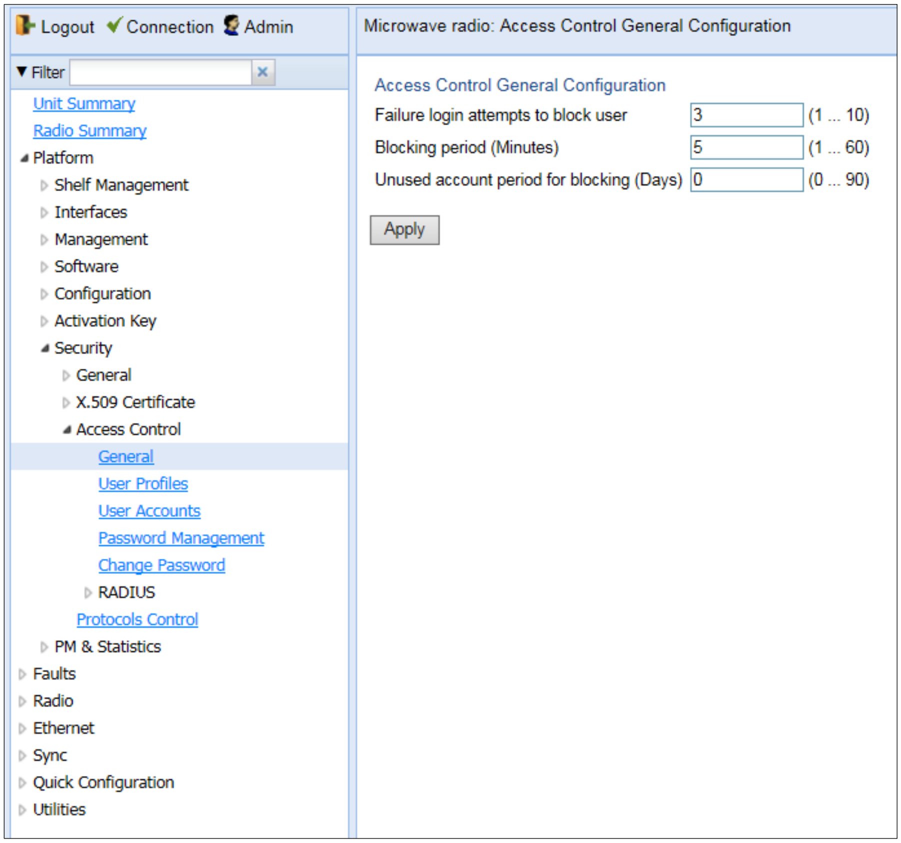
Configuring the General Access Control Parameters

To avoid unauthorized login to the system, PTP 850 automatically blocks users upon a configurable number of failed login attempts. You can also configure PTP 850 to block users that have not logged into the unit for a defined number of days.

To configure the blocking criteria:

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

Figure 258 Access Control General Configuration Page



Microwave radio: Access Control General Configuration

Access Control General Configuration

Failure login attempts to block user	3	(1 ... 10)
Blocking period (Minutes)	5	(1 ... 60)
Unused account period for blocking (Days)	0	(0 ... 90)

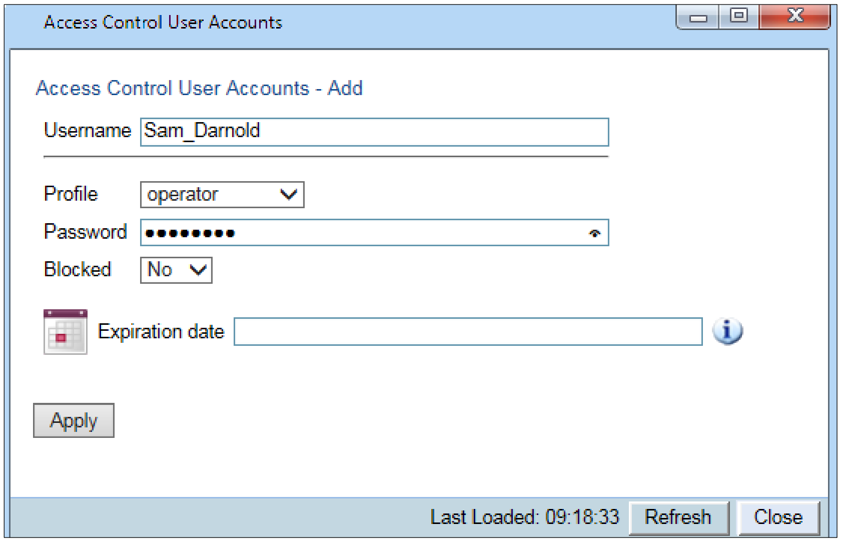
2. In the **Failure login attempts to block user** field, select the number of failed login attempts that will trigger blocking. If a user attempts to login to the system with incorrect credentials this number of times consecutively, the user will temporarily be prevented from logging into the system for the time period defined in the **Blocking period** field. Valid values are 1-10. The default value is 3.
3. In the **Blocking period (Minutes)** field, enter the length of time, in minutes, that a user is prevented from logging into the system after the defined number of failed login attempts. Valid values are 1-60. The default value is 5.

4. In the **Unused account period for blocking (Days)** field, you can configure a number of days after which a user is prevented from logging into the system if the user has not logged in for the configured number of days. Valid values are 0, or 30-90. If you enter 0, this feature is disabled. The default value is 0.
5. Click **Apply**.

Once a user is blocked, you can unblock the user from the User Accounts page. To unblock a user:

1. Select **Platform > Security > Access Control > User Accounts**. The Access Control User Accounts page opens (Figure 264).
2. Select the user and click **Edit**. The Access Control User Accounts - Edit page opens.

Figure 259 Access Control User Accounts - Edit Page


Access Control User Accounts
Access Control User Accounts - Add
Apply
Last Loaded: 09:18:33
Refresh
Close

Username Sam_Darnold

Profile operator

Password ••••••••

Blocked No

Expiration date

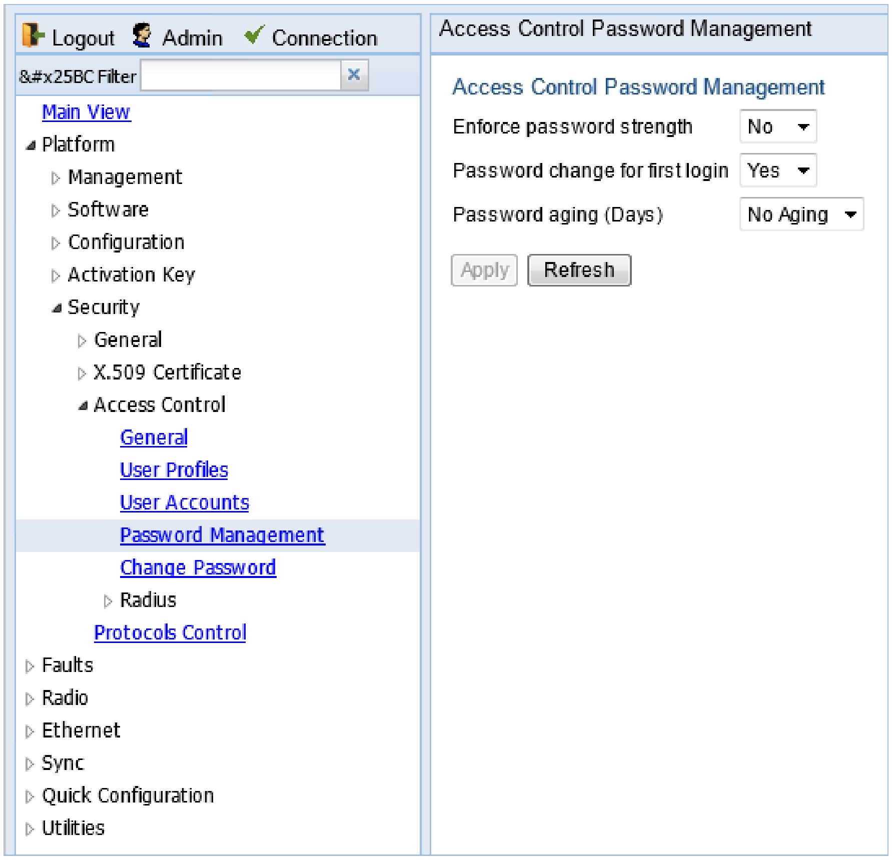
3. In the **Blocked** field, select **No**.
4. Click **Apply**, then **Close**.

Configuring the Password Security Parameters

To configure enhanced security requirements for user passwords:

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

Figure 260 Access Control Password Management Page



Access Control Password Management

Access Control Password Management

Enforce password strength: No

Password change for first login: Yes

Password aging (Days): No Aging

2. In the **Enforce password strength** field, select **Yes** or **No**. When **Yes** is selected:
   - Password length must be at least eight characters.
   - Password must include characters of at least three of the following character types: lower case letters, upper case letters, digits, and special characters. For purposes of meeting this requirement, upper case letters at the beginning of the password and digits at the end of the password are not counted.
   - The last five passwords you used cannot be reused.
3. In the **Password change for first login** field, select **Yes** or **No**. When **Yes** is selected, the system requires the user to change his or her password the first time the user logs in.
4. In the **Password aging (Days)** field, select the number of days that user passwords will remain valid from the first time the user logs into the system. You can enter 20-90, or **No Aging**. If you select **No Aging**, password aging is disabled and passwords remain valid indefinitely.

5. Click **Apply**.

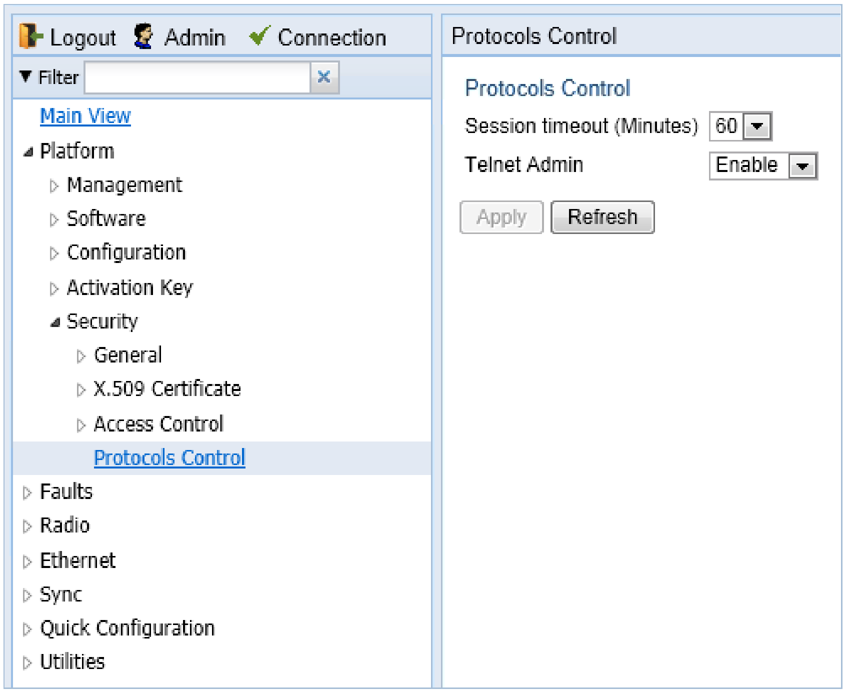
Configuring the Session Timeout

By default, there is a 10 minute session timeout. If you do not perform any activity on the system for the period of time defined as the session timeout, the user session times out and you will have to log in to the system again.

To modify the session timeout:

1. Select **Platform > Security > Protocols Control**. The Protocols Control page opens.

Figure 261 Protocols Control Page



Protocols Control

Protocols Control

Session timeout (Minutes) 60

Telnet Admin Enable

2. In the **Session timeout (Minutes)** field, select a session timeout, in minutes, from 1 to 60.

Note

For information about the **Telnet Admin** field, see *Blocking Telnet Access*.

3. Click **Apply**.

Configuring Users

This section includes:

- User Configuration Overview
- Configuring User Profiles
- Configuring Users

Related topics:

- Changing Your Password

User Configuration Overview

User configuration is based on the Role-Based Access Control (RBAC) model. According to the RBAC model, permissions to perform certain operations are assigned to specific roles. Users are assigned to particular roles, and through those role assignments acquire the permissions to perform particular system functions.

In the PTP 850 GUI, these roles are called user profiles. Up to 50 user profiles can be configured. Each profile contains a set of privilege levels per functionality group, and defines the management protocols (access channels) that can be used to access the system by users to whom the user profile is assigned.

The system parameters are divided into the following functional groups:

- Security
- Management
- Radio
- TDM
- Ethernet
- Synchronization

A user profile defines the permitted access level per functionality group. For each functionality group, the access level is defined separately for read and write operations. The following access levels can be assigned:

- **None** – No access to this functional group.
- **Normal** – The user has access to parameters that require basic knowledge about the functional group.
- **Advanced** – The user has access to parameters that require advanced knowledge about the functional group, as well as parameters that have a significant impact on the system as a whole, such as restoring the configuration to factory default settings.

Configuring User Profiles

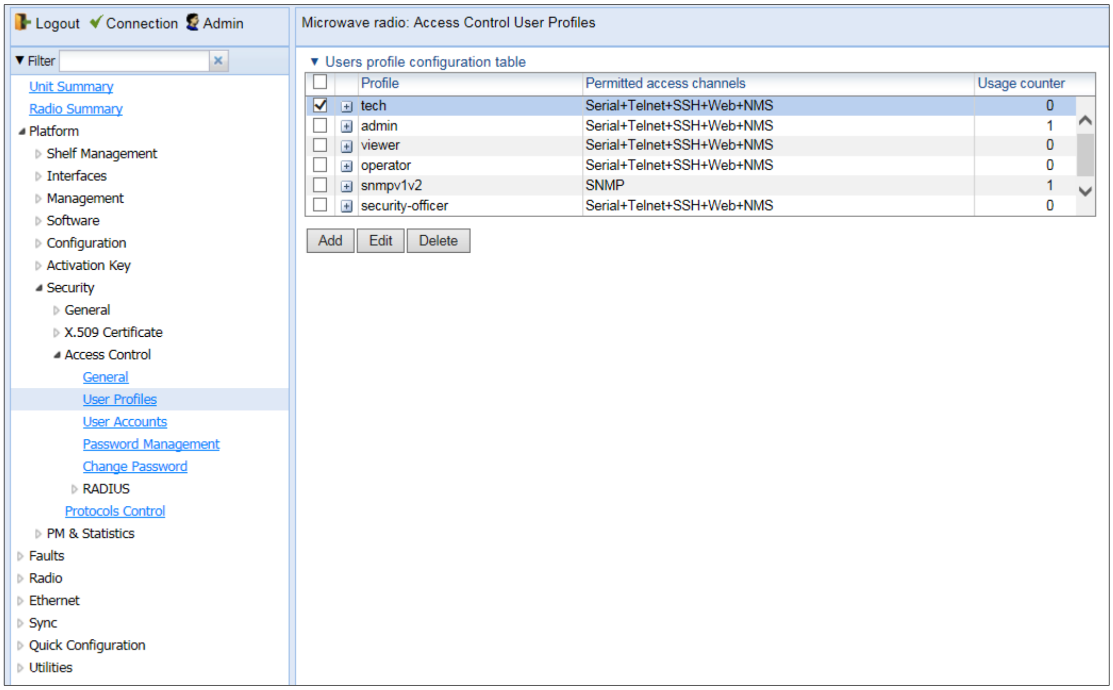
User profiles enable you to define system access levels. Each user must be assigned a user profile. Each user profile contains a detailed set of read and write permission levels per functionality group.

The system includes a number of pre-defined user profiles. You can edit these profiles, and add user profiles. Together, the system supports up to 50 user profiles.

To add a user profile:

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

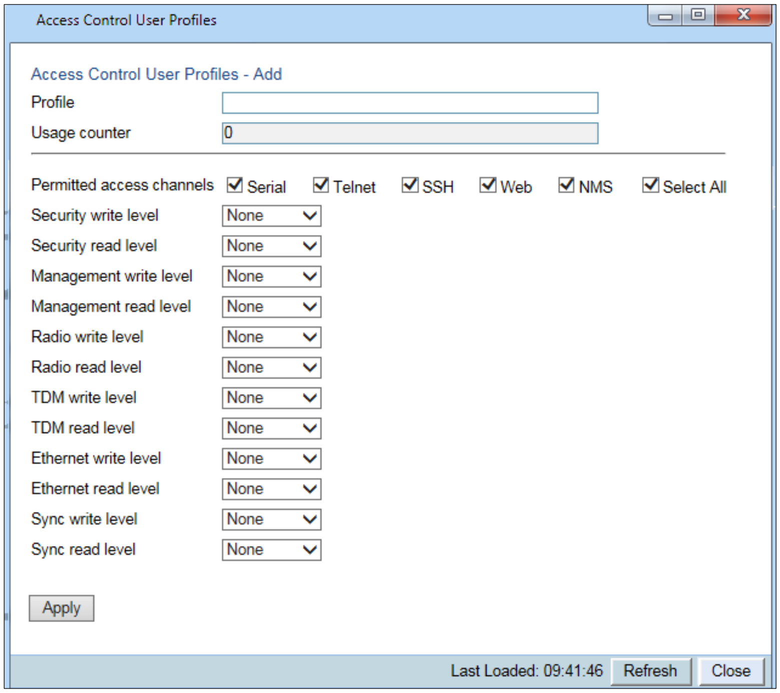
Figure 262 Access Control User Profiles Page



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

2. Click **Add**. The Access Control User Profiles - Add page opens.

Figure 263 Access Control User Profiles - Add Page



Access Control User Profiles - Add

Profile	
Usage counter	0
Permitted access channels	☑ Serial ☑ Telnet ☑ SSH ☑ Web ☑ NMS ☑ Select All
Security write level	None
Security read level	None
Management write level	None
Management read level	None
Radio write level	None
Radio read level	None
TDM write level	None
TDM read level	None
Ethernet write level	None
Ethernet read level	None
Sync write level	None
Sync read level	None

Last Loaded: 09:41:46

3. In the **Profile** field, enter a name for the profile. The profile name can include up to 49 characters. Once you have created the user profile, you cannot change its name.

> **Note**
>
> The **Usage counter** field displays the number of users to whom the user profile is assigned.

4. In the **Permitted access channels** row, select the access channels the user will be permitted to use to access the system.
5. For each functionality group, select one of these options for write level and read level. All users with this profile will be assigned these access levels:
   - **None**
   - **Normal**
   - **Advanced**
6. Click **Apply**, then **Close**.

To view a user profile, click + next to the profile you want to view.

To edit a user profile, select the profile and click **Edit**. You can edit all of the profile parameters except the profile name.

To delete a user profile, select the profile and click **Delete**.

> **Note**
>
> You cannot delete a user profile if the profile is assigned to any users.

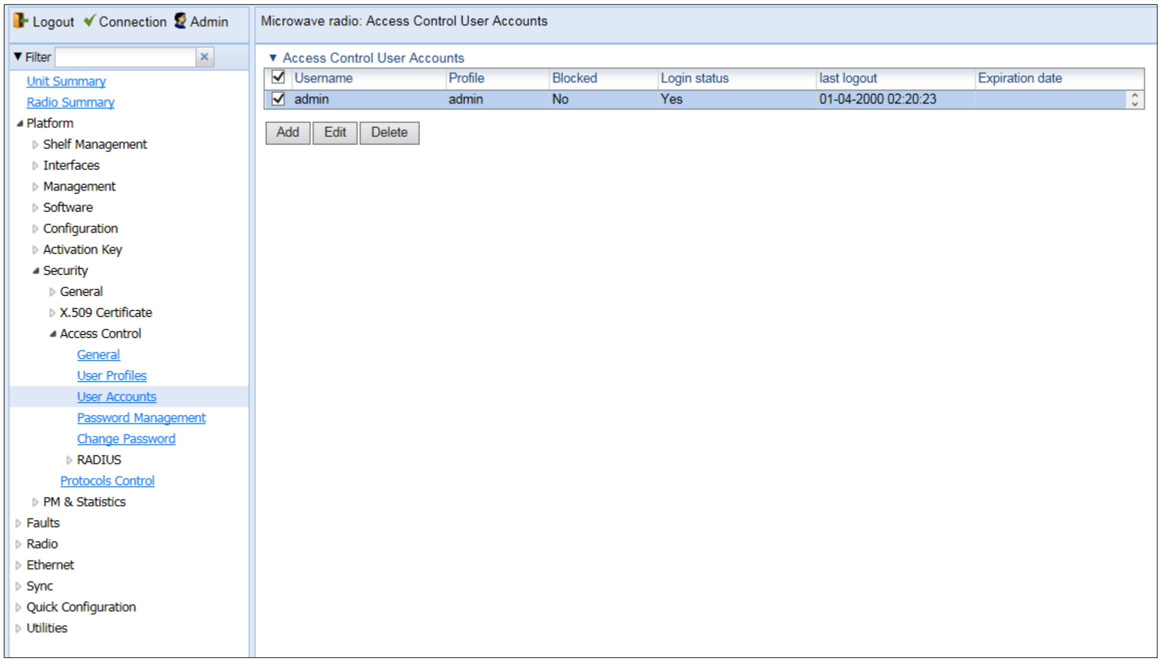
Configuring Users

You can configure up to 2,000 users. Each user has a user name, password, and user profile. The user profile defines a set of read and write permission levels per functionality group. See Configuring User Profiles.

To add a new user:

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

Figure 264 Access Control User Accounts Page



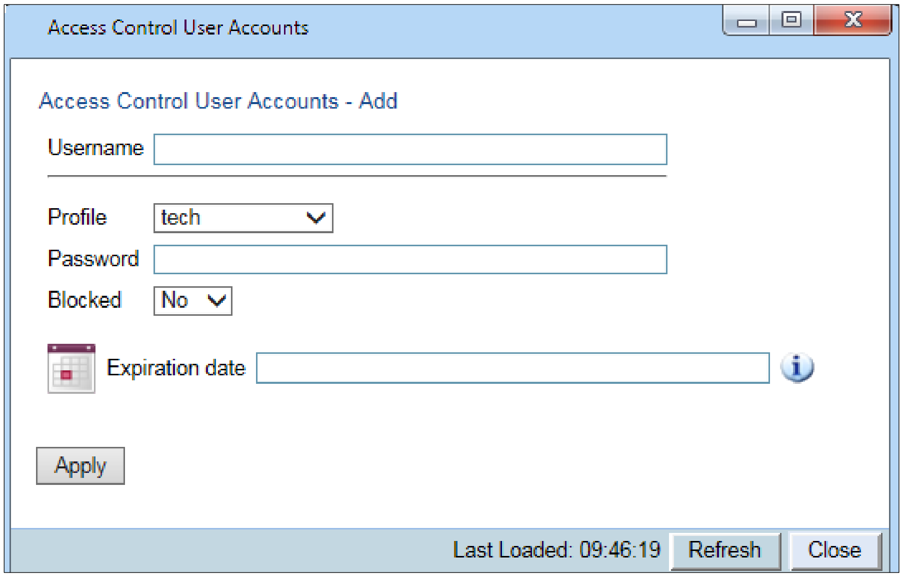
Microwave radio: Access Control User Accounts

Access Control User Accounts

☑	Username	Profile	Blocked	Login status	last logout	Expiration date
☑	admin	admin	No	Yes	01-04-2000 02:20:23	

2. Click **Add**. The Access Control User Profiles - Add page opens.

Figure 265 Access Control User Accounts - Add Page



Access Control User Accounts

Access Control User Accounts - Add

Username

Profile tech

Password

Blocked No

Expiration date

3. In the **User name** field, enter a user name for the user. The user name can be up to 32 characters.
4. In the **Profile** field, select a User Profile. The User Profile defines the user's access levels for functionality groups in the system. See Configuring User Profiles.
5. In the **Password** field, enter a password for the user. If **Enforce Password Strength** is activated (see Configuring the Password Security Parameters), the password must meet the following criteria:
   - Password length must be at least eight characters.
   - Password must include characters of at least three of the following character types: lower case letters, upper case letters, digits, and special characters. For purposes of meeting this requirement, upper case letters at the beginning of the password and digits at the end of the password are not counted.
   - The last five passwords you used cannot be reused.
6. In the **Blocked** field, you can block or unblock the user. Selecting **Yes** blocks the user. You can use this option to block a user temporarily, without deleting the user from the system. If you set this option to **Yes** while the user is logged into the system, the user will be automatically logged out of the system within 30 seconds.

Note

Users can also be blocked by the system automatically. You can unblock the user by selecting **No** in the **Blocked** field. See Configuring the General Access Control Parameters.

7. Optionally, in the **Expiration date** field, you can configure the user to remain active only until a defined date. After that date, the user automatically becomes inactive. To set an expiration date, click the calendar icon and select a date, or enter a date in the format dd-mm-yyyy.

In addition to the configurable parameters described above, the Access Control User Accounts page displays the following information for each user:

- **Login Status** – Indicates whether the user is currently logged into the system.
- **Last Logout** – The date and time the user most recently logged out of the system.

To edit a user's account details, select the user and click **Edit**. You can edit all of the user account parameters except the **User name** and **password**.

To add a user, click **Add**.

To delete a user, select the user and click **Delete**.

Configuring RADIUS

This section includes:

- RADIUS Overview
- Activating RADIUS Authentication
- Configuring the RADIUS Server Attributes
- Configuring a RADIUS Server

RADIUS Overview

The RADIUS protocol provides centralized user management services. PTP 850E supports RADIUS server and provides a RADIUS client for authentication and authorization. When RADIUS is enabled, a user attempting to log into the system from any access channel (CLI, WEB, NMS) is not authenticated locally. Instead, the user's credentials are sent to a centralized standard RADIUS server which indicates to the PTP 850E whether the user is known, and which privilege is to be given to the user.

The following RADIUS servers are supported:

- FreeRADIUS
- RADIUS on Windows Server (IAS)
  - Windows Server 2008

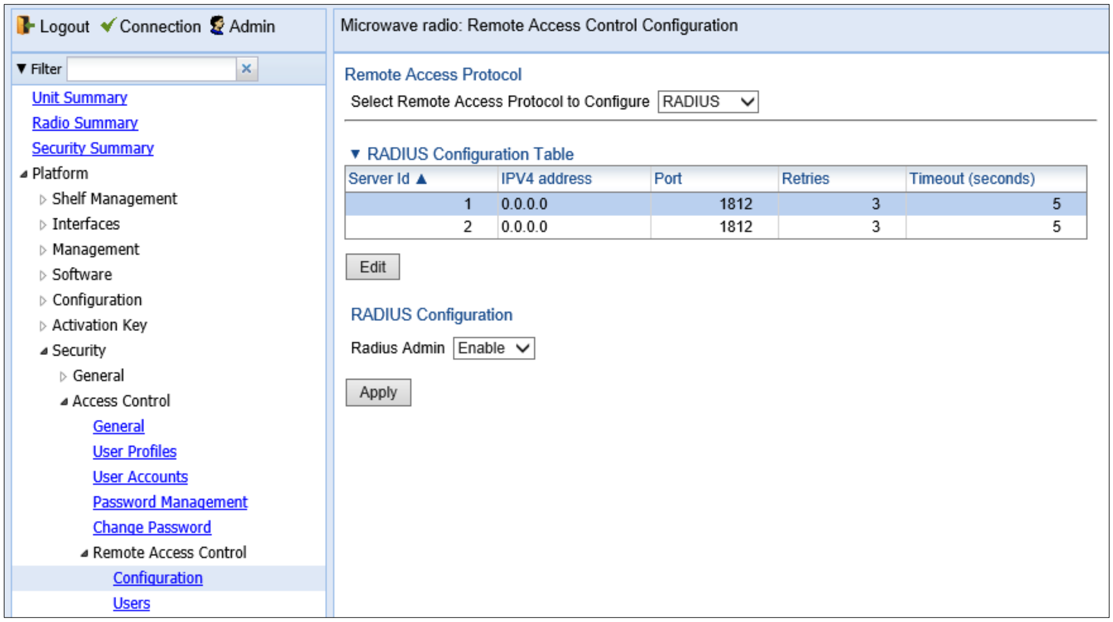
You can define up to two Radius servers. If you define two, one serves as the primary server and the other as the secondary server.

Activating RADIUS Authentication

To activate RADIUS authentication:

1. Select **Platform** > **Security** > **Access Control** > **Remote Access Control** > **Configuration**. The Remote Access Control Configuration page opens.

Figure 266 Remote Access Control Configuration Page (RADIUS)



Microwave radio: Remote Access Control Configuration

Remote Access Protocol

Select Remote Access Protocol to Configure RADIUS

RADIUS Configuration Table

Server Id ▲	IPV4 address	Port	Retries	Timeout (seconds)
1	0.0.0.0	1812	3	5
2	0.0.0.0	1812	3	5

Edit

RADIUS Configuration

Radius Admin Enable

Apply

2. In the **Select Remote Access Protocol to Configure** field, select **RADIUS**.
3. Configure the RADIUS server attributes. See *Configuring the RADIUS Server Attributes*.
4. In the **RADIUS Admin** field, select **Enable**.
5. Click **Apply**.

Note

When the Protocol is changed, all active sessions are terminated when you click Apply.

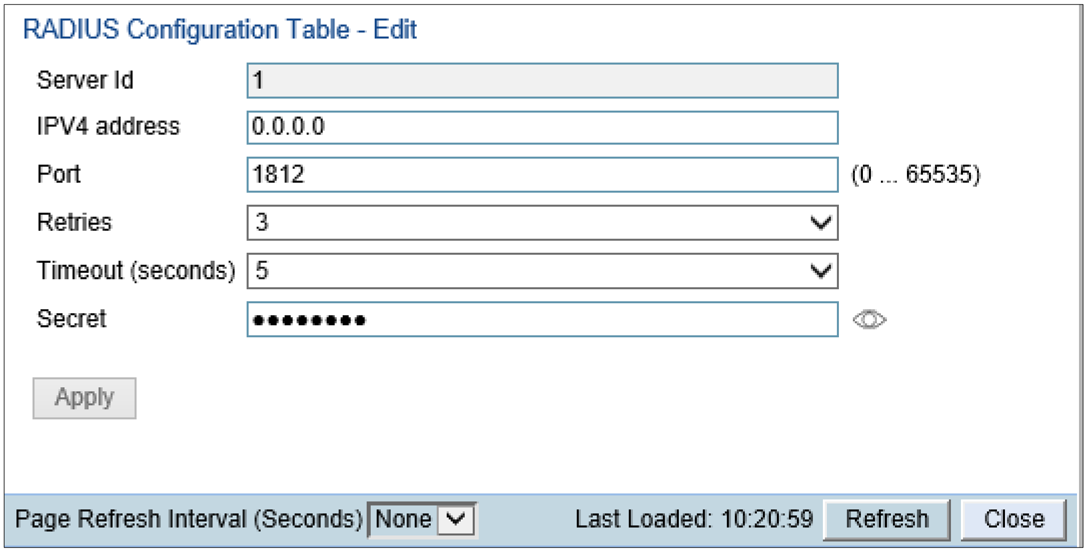
Configuring the RADIUS Server Attributes

To configure the RADIUS server attributes:

1. Select **Platform** > **Security** > **Access Control** > **Remote Access Control** > **Configuration**. The Remote Access Control Configuration page opens (***Error! Reference source not found.***). Verify t hat **RADIUS** is selected in the **Protocol** field.
2. In the Radius Configuration table, select the line that corresponds to the RADIUS server you want to configure:
   - Select **Server ID 1** to configure the Primary Radius server.
   - Select **Server ID 2** to configure the Secondary Radius server.

3. Click **Edit**. The Radius Configuration – Edit page opens.

Figure 267 Radius Configuration – Edit Page



RADIUS Configuration Table - Edit

Server Id	1
IPV4 address	0.0.0.0
Port	1812 (0 ... 65535)
Retries	3
Timeout (seconds)	5
Secret	●●●●●●●●●

Page Refresh Interval (Seconds) None

Last Loaded: 10:20:59

4. In the **IPV4 address** field, enter the IP address of the RADIUS server.
5. In the **Port** field, enter the port of the RADIUS server.
6. In the **Retries** field, enter the number of times the unit will try to communicate with the RADIUS server before declaring the server to be unreachable.
7. In the **Timeout** field, enter the timeout (in seconds) that the agent will wait in each communication with the selected RADIUS server before retrying if no response is received.
8. In the **Secret** field, enter the shared secret of the RADIUS server. The string must be between 22-128 characters long.

1 Click **Apply**, then **Close**.

In addition to the configurable parameters described above, the Remote Access Control Configuration page displays the following information for each RADIUS server:

- Server **Id** – The server ID of the Radius server:
  - 1 – The primary Radius server.
  - 2 – The secondary Radius server.

Configuring a RADIUS Server

If you want to use the PTP 850 RADIUS feature, you must first install a RADIUS server and configure it to work with the PTP 850 device.

The following subsections describe how to configure a Win2008 RADIUS server and a Linux FreeRADIUS server to work with an PTP 850. For the sake of simplicity, the subsections describe how to create three users: an Advanced user with Advanced read/write permissions, a Normal user with regular read/write permissions, and a Viewer user with no read/write permissions.

Note

These RADIUS servers are third-party software. The instructions provided in this section are illustrative only and are provided for the convenience of PTP 850E users. For exact and up-to-date instructions, we urge you to rely on the documentation provided with the RADIUS server you are using. Cambium is not responsible for syntax changes or variations in different GNU distributions.

Configuring a Win 2008 RADIUS Server

The following sub-sections describe how to configure a Win 2008 RADIUS Server to work with an PTP 850 device.

Step 1 – Creating Groups and Users

To create groups and users:

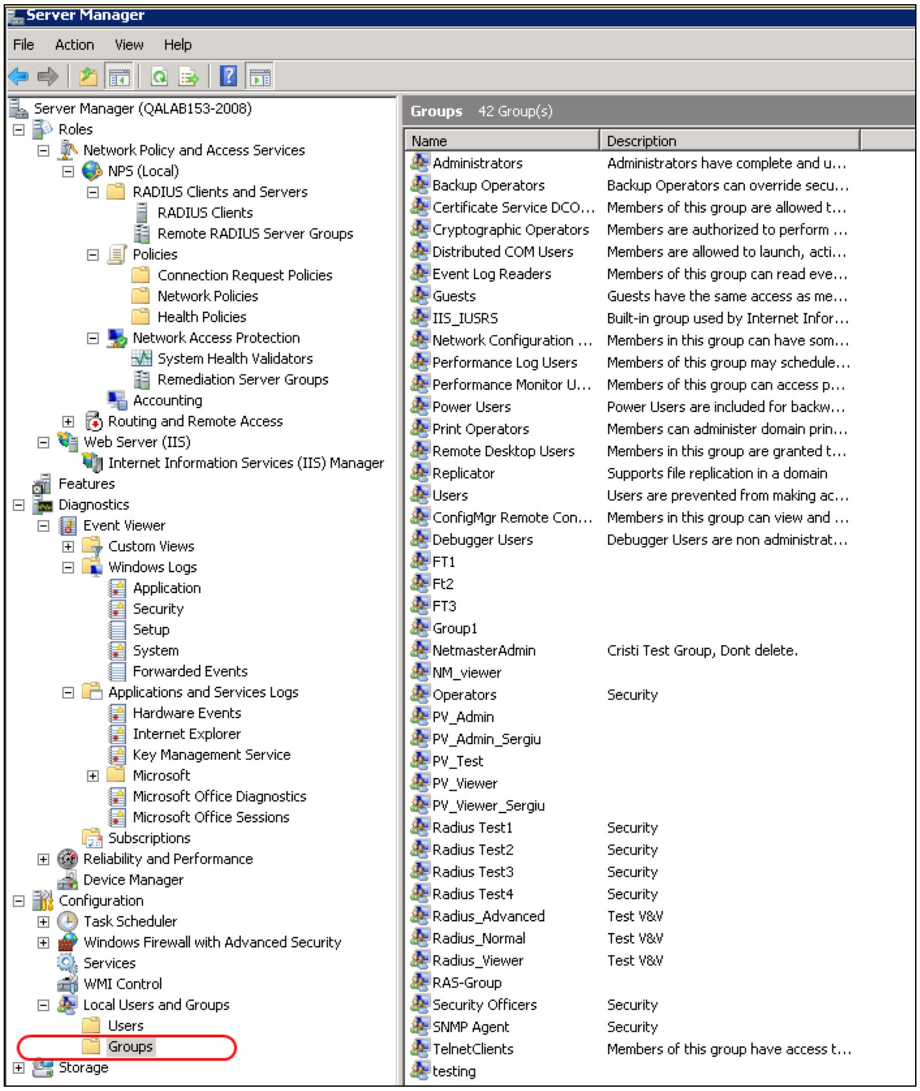
1. Create three user groups, as follows:

   I. In the Server Manager, navigate to **Configuration** > **Local Users and Groups**.

   II. Right click **Groups** and create the following three user groups:

   - Radius_Advanced
   - Radius_Normal
   - Radius_Viewer

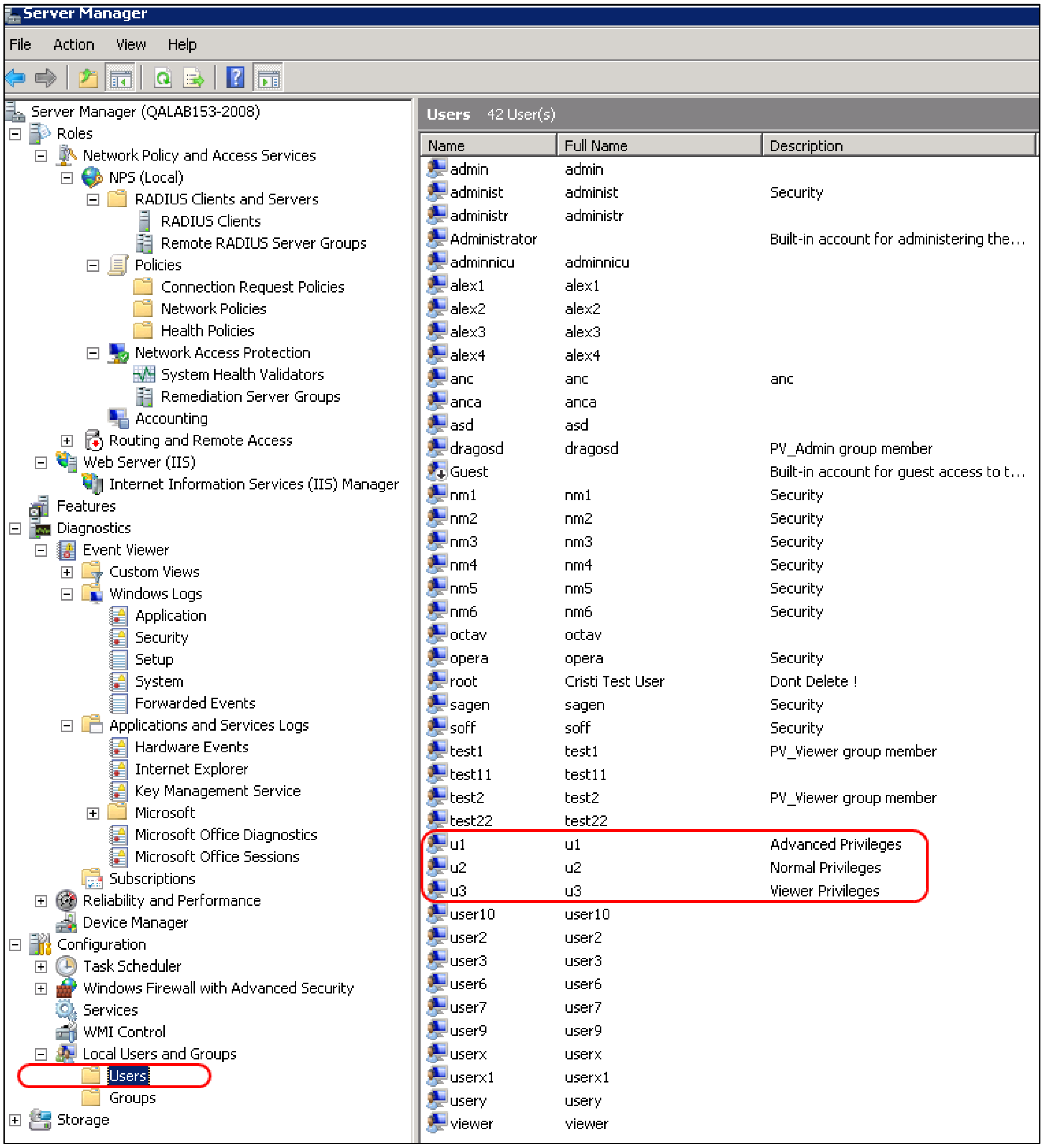
Figure 268 Server Manager – Creating User Groups



Name	Description
Administrators	Administrators have complete and u…
Backup Operators	Backup Operators can override secu…
Certificate Service DCO…	Members of this group are allowed t…
Cryptographic Operators	Members are authorized to perform …
Distributed COM Users	Members are allowed to launch, acti…
Event Log Readers	Members of this group can read eve…
Guests	Guests have the same access as me…
IIS_IUSRS	Built-in group used by Internet Infor…
Network Configuration …	Members in this group can have som…
Performance Log Users	Members of this group may schedule…
Performance Monitor U…	Members of this group can access p…
Power Users	Power Users are included for backw…
Print Operators	Members can administer domain prin…
Remote Desktop Users	Members in this group are granted t…
Replicator	Supports file replication in a domain
Users	Users are prevented from making ac…
ConfigMgr Remote Con…	Members in this group can view and …
Debugger Users	Debugger Users are non administrat…
FT1	
Ft2	
FT3	
Group1	
NetmasterAdmin	Cristi Test Group, Dont delete.
NM_viewer	
Operators	Security
PV_Admin	
PV_Admin_Sergiu	
PV_Test	
PV_Viewer	
PV_Viewer_Sergiu	
Radius Test1	Security
Radius Test2	Security
Radius Test3	Security
Radius Test4	Security
Radius_Advanced	Test V&V
Radius_Normal	Test V&V
Radius_Viewer	Test V&V
RAS-Group	
Security Officers	Security
SNMP Agent	Security
TelnetClients	Members of this group have access t…
testing	

2. Create three users:
    - u1
    - u2
    - u3

Figure 269 Server Manager – Creating Users

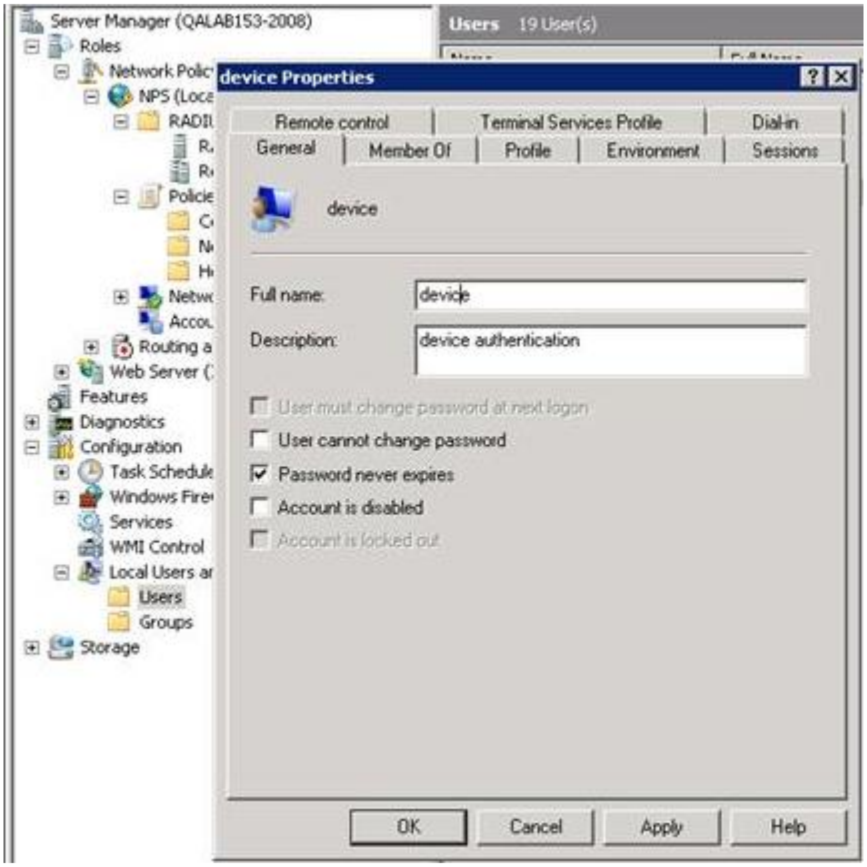


Users   42 User(s)

Name	Full Name	Description
admin	admin	
administ	administ	Security
administr	administr	
Administrator		Built-in account for administering the...
adminnicu	adminnicu	
alex1	alex1	
alex2	alex2	
alex3	alex3	
alex4	alex4	
anc	anc	anc
anca	anca	
asd	asd	
dragosd	dragosd	PV_Admin group member
Guest		Built-in account for guest access to t...
nm1	nm1	Security
nm2	nm2	Security
nm3	nm3	Security
nm4	nm4	Security
nm5	nm5	Security
nm6	nm6	Security
octav	octav	
opera	opera	Security
root	Cristi Test User	Dont Delete !
sagen	sagen	Security
soff	soff	Security
test1	test1	PV_Viewer group member
test11	test11	
test2	test2	PV_Viewer group member
test22	test22	
u1	u1	Advanced Privileges
u2	u2	Normal Privileges
u3	u3	Viewer Privileges
user10	user10	
user2	user2	
user3	user3	
user6	user6	
user7	user7	
user9	user9	
userx	userx	
userx1	userx1	
usery	usery	
viewer	viewer	

3. In the Device Properties – General tab, make sure to select **Password never expires.** If you leave the default setting (**User must change password at next logon**), authentication may fail.

Figure 270 Server Manager – User Password Settings



Full name: device

Description: device authentication

☐ User must change password at next logon
☐ User cannot change password
☑ Password never expires
☐ Account is disabled
☐ Account is locked out

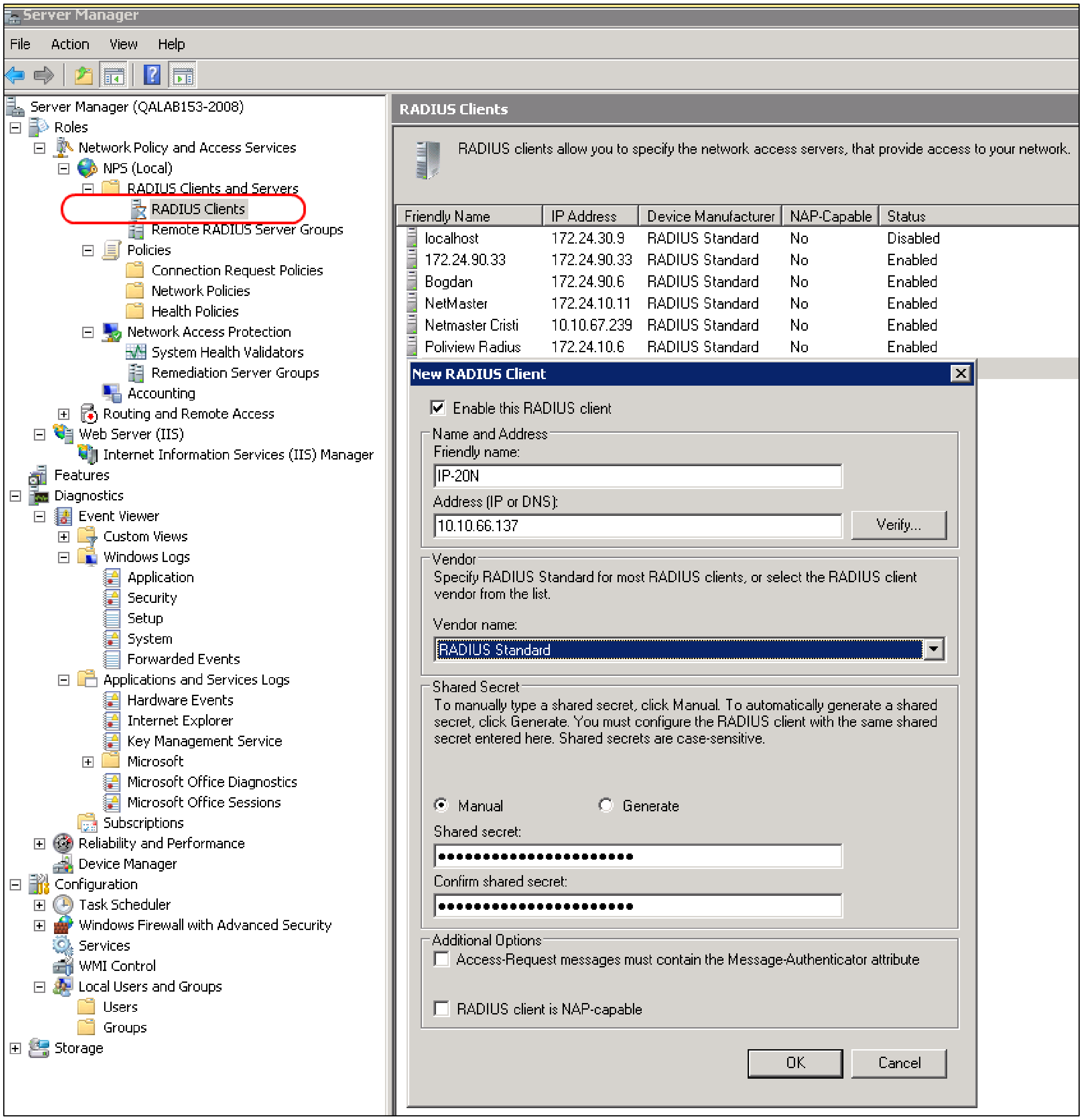
4. Attach each user to a group, as follows:
   - Attach u1 to Radius_Advanced
   - Attach u2 to Radius_Normal
   - Attach u3 to Radius_Viewer

Step 2 – Creating a RADIUS Client

Define the PTP 850 device as a RADIUS client, as follows:

1. In the Server Manager, navigate to Roles > Network Policy and Access Services > NPS (Local) > RADIUS Clients and Servers > RADIUS Clients.
2. Right-click **RADIUS Clients**, and select **New RADIUS Client**. The New RADIUS Client window appears.

Figure 271 Server Manager – Creating a RADIUS Client



RADIUS clients allow you to specify the network access servers, that provide access to your network.

Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
localhost	172.24.30.9	RADIUS Standard	No	Disabled
172.24.90.33	172.24.90.33	RADIUS Standard	No	Enabled
Bogdan	172.24.90.6	RADIUS Standard	No	Enabled
NetMaster	172.24.10.11	RADIUS Standard	No	Enabled
Netmaster Cristi	10.10.67.239	RADIUS Standard	No	Enabled
Poliview Radius	172.24.10.6	RADIUS Standard	No	Enabled

New RADIUS Client

☑ Enable this RADIUS client

Name and Address

Friendly name: IP-20N

Address (IP or DNS): 10.10.66.137

Vendor

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name: RADIUS Standard

Shared Secret

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••••••••••••••••••••

Confirm shared secret: ••••••••••••••••••••••

Additional Options

□ Access-Request messages must contain the Message-Authenticator attribute

□ RADIUS client is NAP-capable

3. In the New RADIUS Client window:

    I. Select the **Enable this RADIUS client** check box.

    II. Enter a descriptive **Friendly name** for the device, such as PTP 850.

    III. Enter the device IP **Address**.

    IV. Select **RADIUS Standard** as the **Vendor name**.

    V. In the **Shared Secret** section, select **Manual**, and enter a **Shared secret**, then enter it again in **Confirm shared secret**. Note down the secret because you will need to enter the same value in the **Secret** field of the Radius Configuration – Edit page.

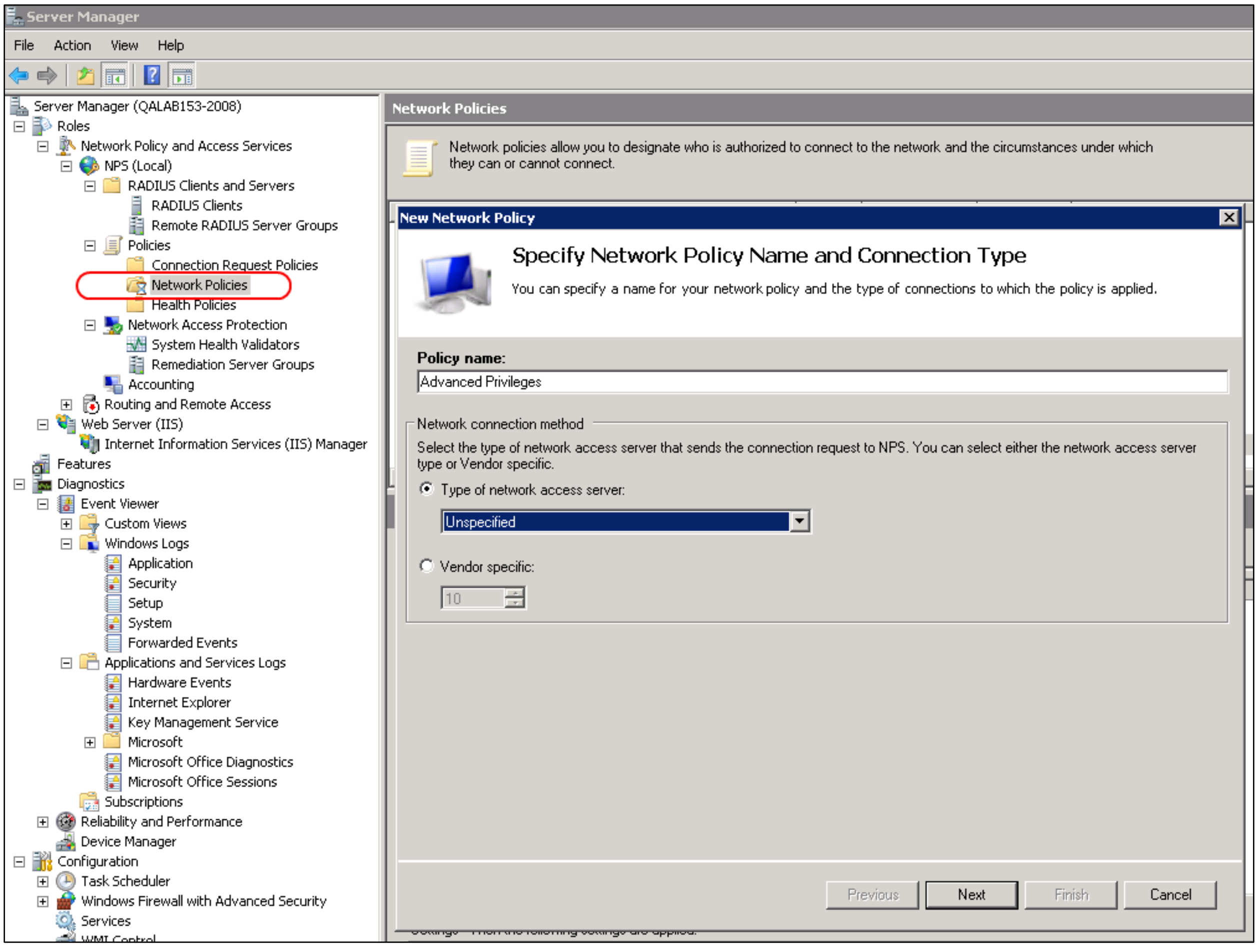
Step 3 – Creating a Network Policy

Create a network policy for each of the three groups you created: Radius_Advanced, Radius_Normal, Radius_Viewer. That is, follow the instructions in this section, for each of the three groups.

To create a network policy:

1. In the Server Manager, navigate to Roles > Network Policy and Access Service > NPS (Local) > Policies > Network Policies.
2. Right-click **Network Policies**, and select **New**. The New Network Policy wizard appears.
3. In the specify Network Policy Name and Connection Type, give the policy a descriptive name, indicating whether it is a policy for the Advanced, the Normal or the Viewer group.

Figure 272 Create Network Policy – Specify Name and Connection Type



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name: Advanced Privileges

Network connection method

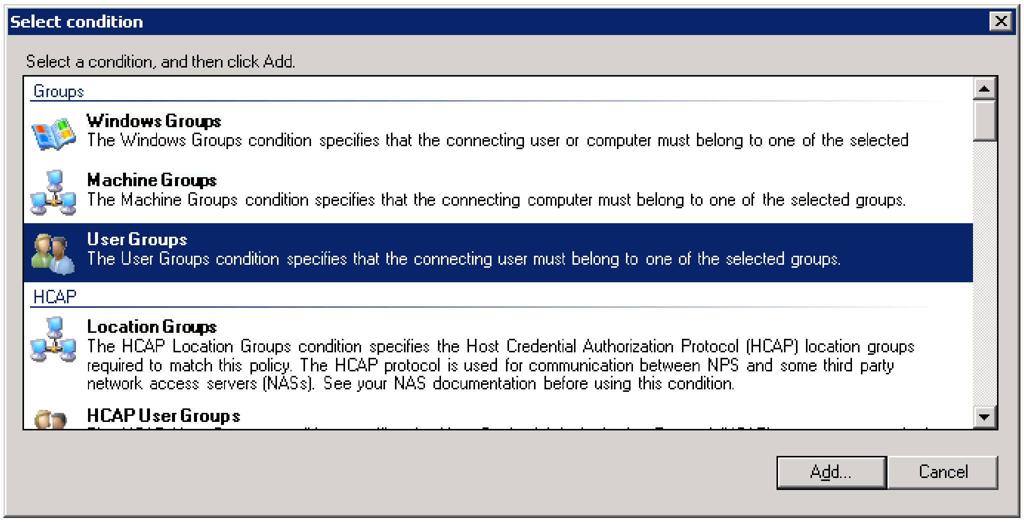
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.

● Type of network access server: Unspecified

○ Vendor specific: 10

4. Click **Next.**
5. In the Specify Conditions window, click **Add.**
6. In the Select Condition window that appears, select the **User Groups** condition and click **Add.**

Figure 273 Create Network Policy – Select Condition



Select condition

Select a condition, and then click Add.

Groups

Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected

Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.

User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

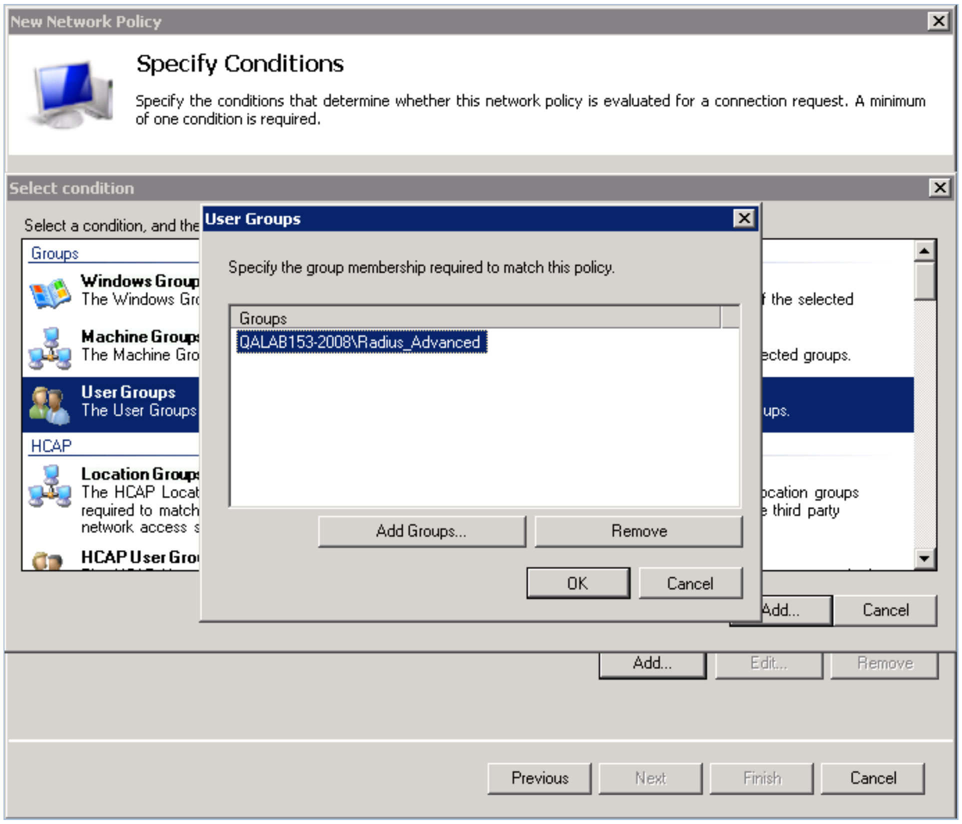
HCAP

Location Groups
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.

HCAP User Groups

7. In the User Groups window that appears, click **Add Groups**.
8. In the Select Group window that appears, click **Advanced**.
9. In the Select Group window that appears, click **Find Now** to list all groups, and then select the appropriate group from the list: Radius_Advanced, Radius_Normal, or Radius_Viewer.
10. Click **OK**.

Figure 274 Create Network Policy – User Group added to Policy’s Conditions



New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Select condition

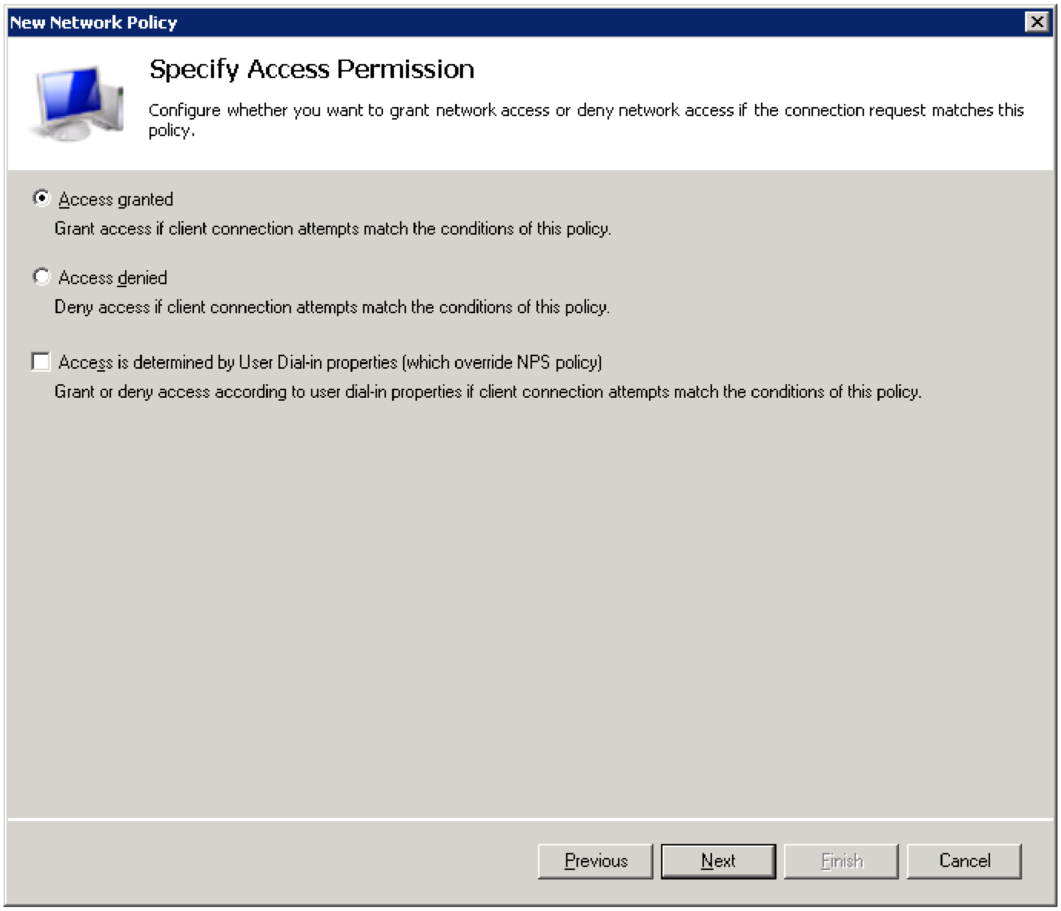
User Groups

Specify the group membership required to match this policy.

Groups: QALAB153-2008\Radius_Advanced

11. Click **OK** to save settings.
12. Click **Next.**
13. In the Specify Access Permission window that appears, select the **Access Granted** option.

Figure 275 Create Network Policy – Specifying Access Permission



New Network Policy

Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

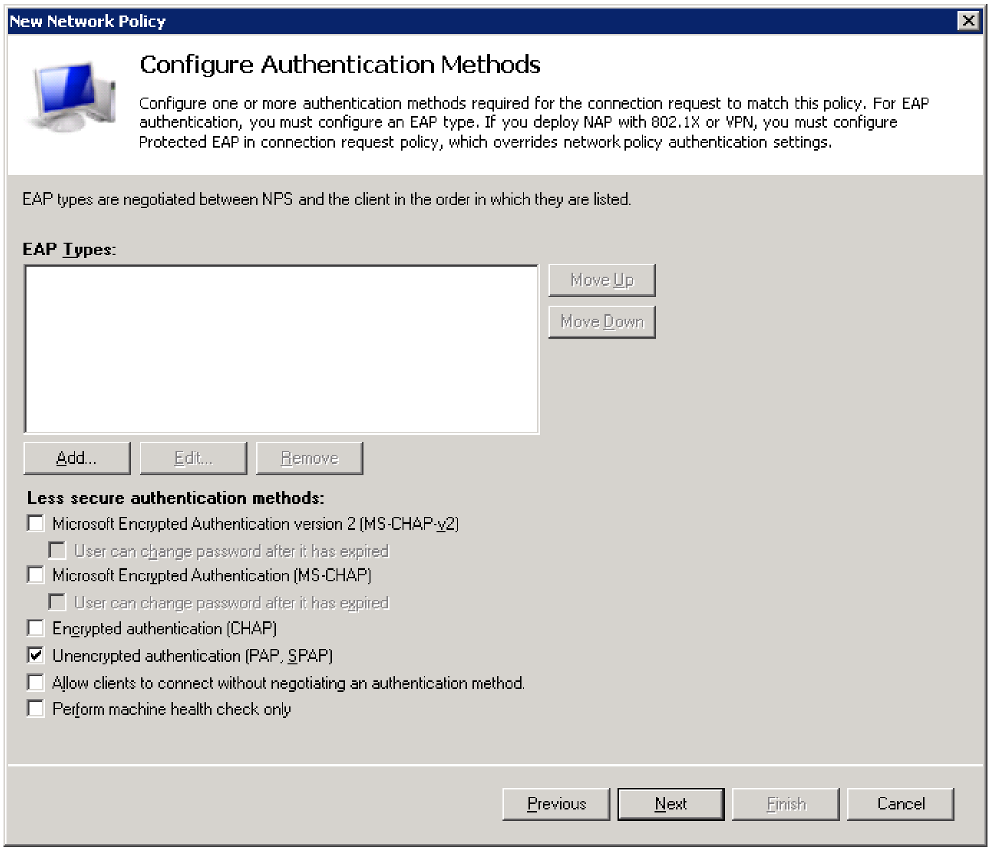
● Access granted
Grant access if client connection attempts match the conditions of this policy.

○ Access denied
Deny access if client connection attempts match the conditions of this policy.

□ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

14. Click **Next.**
15. In the Configure Authentication Methods window that appears, make sure only the **Unencrypted Authentication (PAP, SPAP)** option is selected.

Figure 276 Create Network Policy – Configuring Authentication Methods



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Less secure authentication methods:

☐ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

☐ User can change password after it has expired

☐ Microsoft Encrypted Authentication (MS-CHAP)

☐ User can change password after it has expired

☐ Encrypted authentication (CHAP)

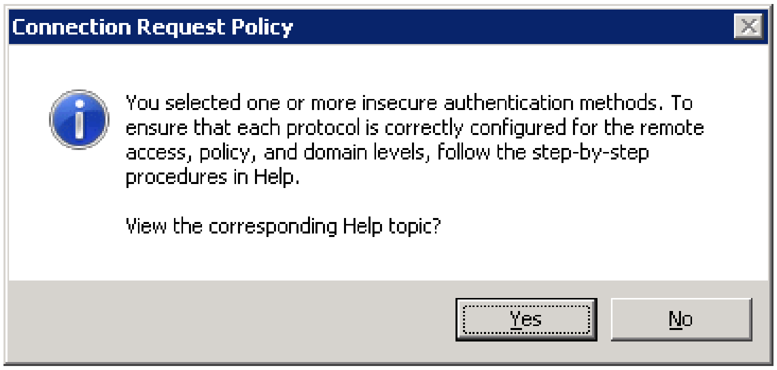
☑ Unencrypted authentication (PAP, SPAP)

☐ Allow clients to connect without negotiating an authentication method.

☐ Perform machine health check only

16. In the query window that appears, click **No**.

Figure 277 Create Network Policy – Insecure Authentication Method Query



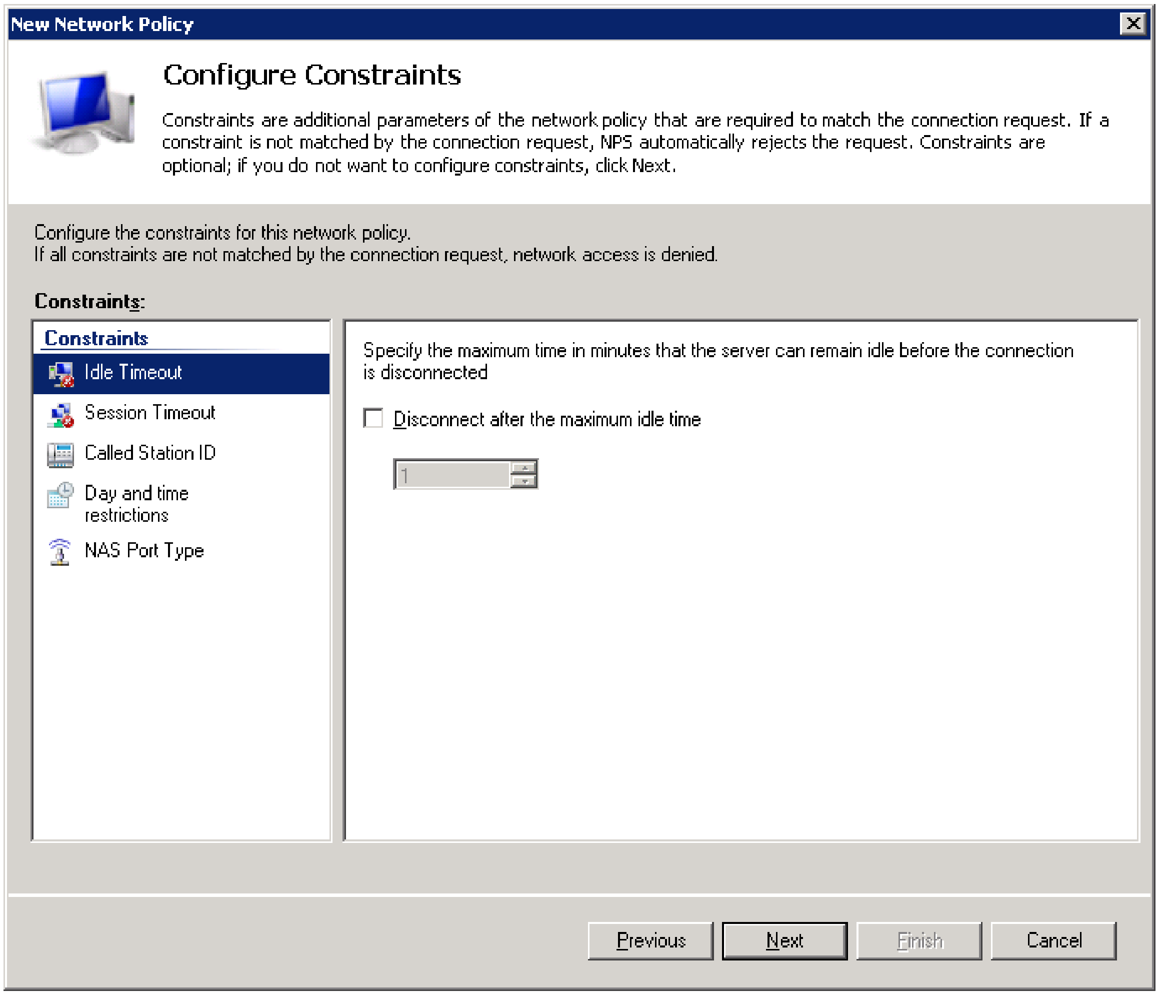
Connection Request Policy

You selected one or more insecure authentication methods. To ensure that each protocol is correctly configured for the remote access, policy, and domain levels, follow the step-by-step procedures in Help.

View the corresponding Help topic?

17. In the Configure Constraints window that appears, click **Next**

Figure 278 Create Network Policy – Configuring Constraints



Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

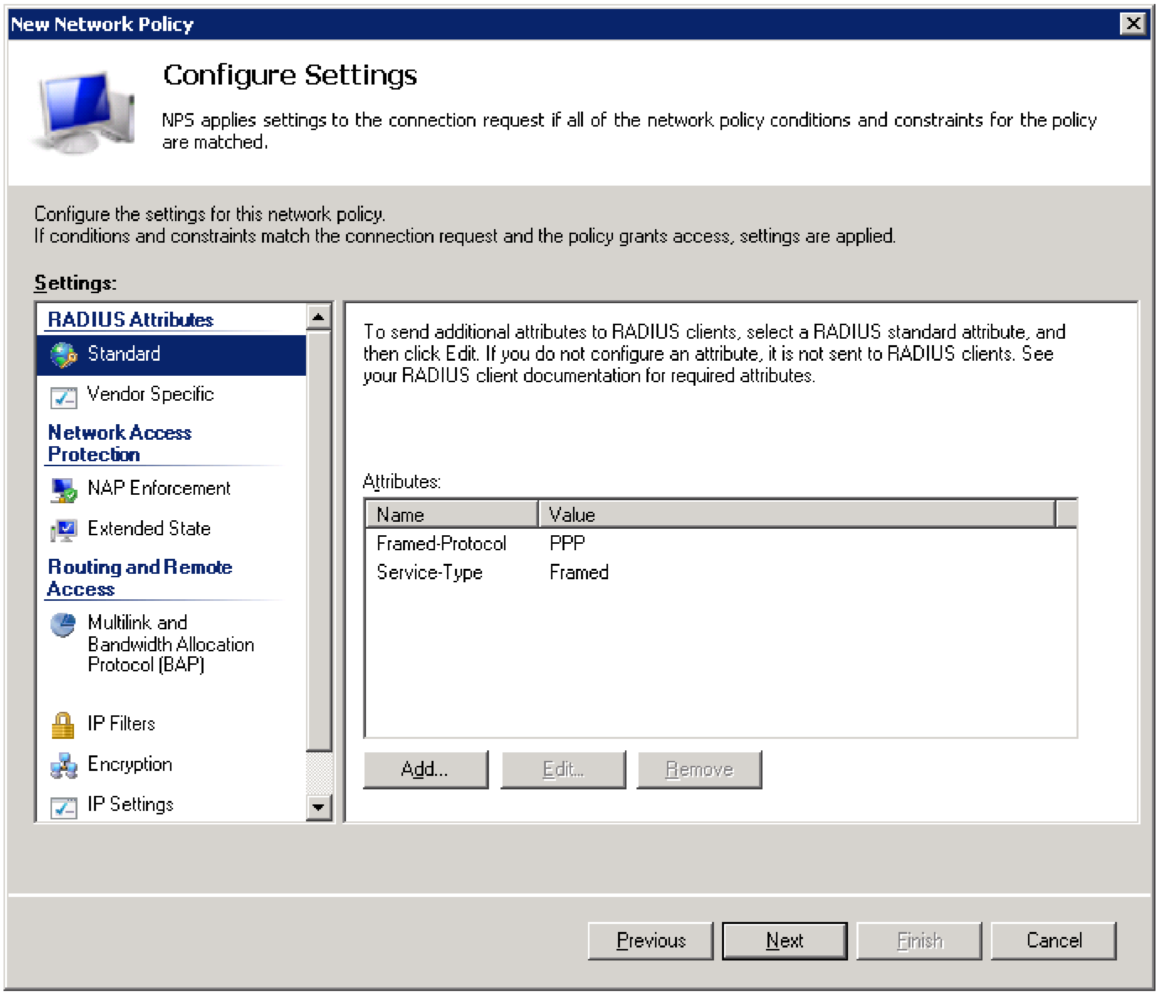
Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

□ Disconnect after the maximum idle time

1

18. In the Configure Settings window that appears:
    I. Remove all **Standard** RADIUS attributes. Make sure the Attributes table is empty.

Figure 279 Create Network Policy – Configuring Settings



New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

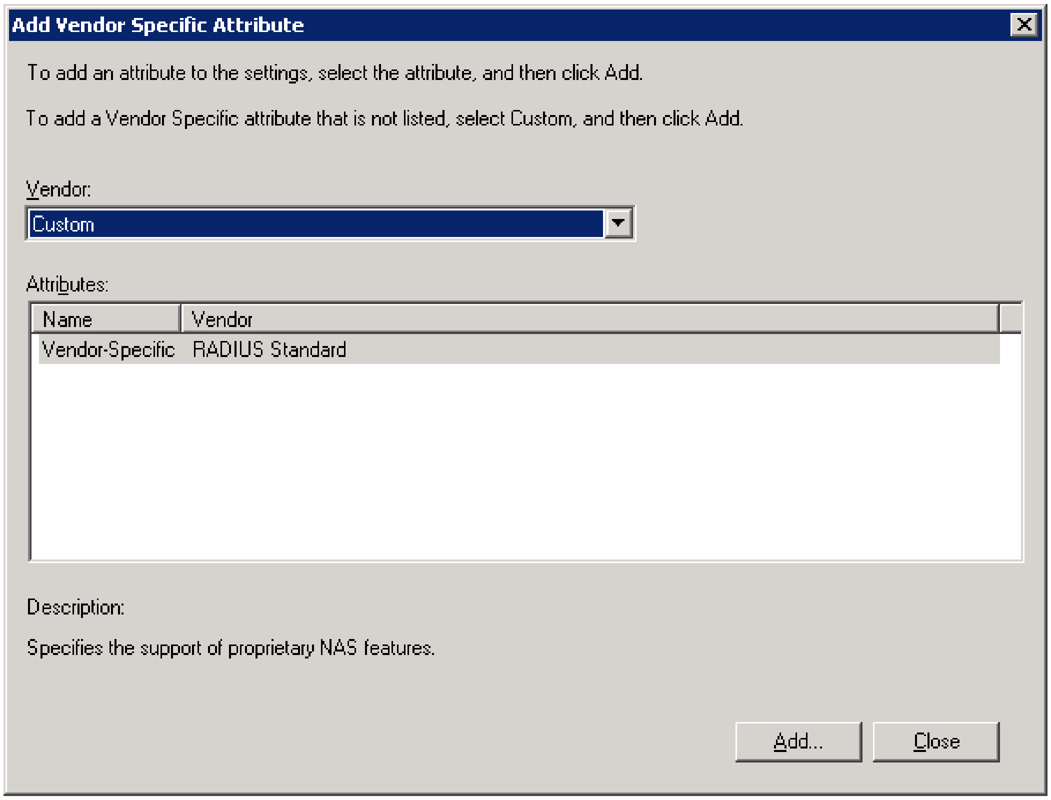
II. Select the **Vendor Specific** checkbox and click **Add** under the Attributes table.

19. In the Add Vendor Specific Attribute window that appears:

I. Select **Custom** in the **Vendor** drop down field.

II. Click Add.

Figure 280 Create Network Policy – Adding Vendor Specific Attributes



Add Vendor Specific Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.

Vendor: Custom

Attributes:

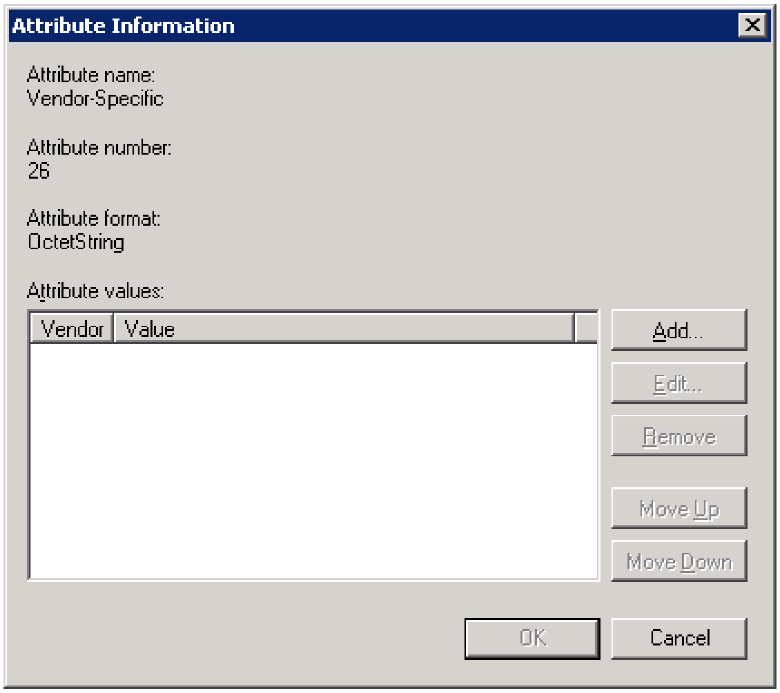
Name	Vendor
Vendor-Specific	RADIUS Standard

Description:

Specifies the support of proprietary NAS features.

20. In the Attribute Information window that appears, click **Add**.

Figure 281 Create Network Policy – Selecting to Add Attribute Information



Attribute Information

Attribute name:
Vendor-Specific

Attribute number:
26

Attribute format:
OctetString

Attribute values:

Vendor	Value

21. In the Vendor-Specific Attribute Information window that appears:

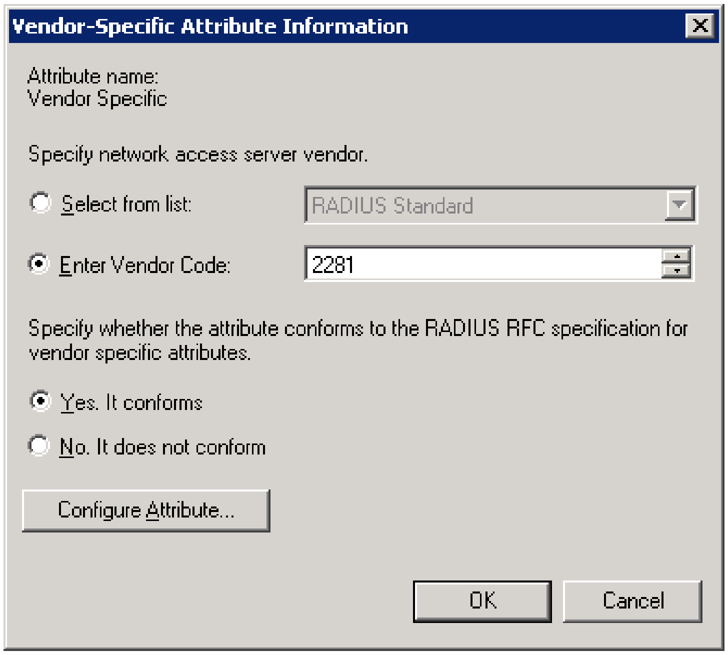
i Select **Enter Vendor Code**.

ii Enter **2281** in the **Enter Vendor Code** field.

iii Select the option **Yes. It conforms**.

iv Click **Configure Attribute**.

Figure 282 Create Network Policy – Specifying the Vendor



Vendor-Specific Attribute Information

Attribute name:
Vendor Specific

Specify network access server vendor.

○ Select from list: RADIUS Standard

● Enter Vendor Code: 2281

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

● Yes. It conforms

○ No. It does not conform

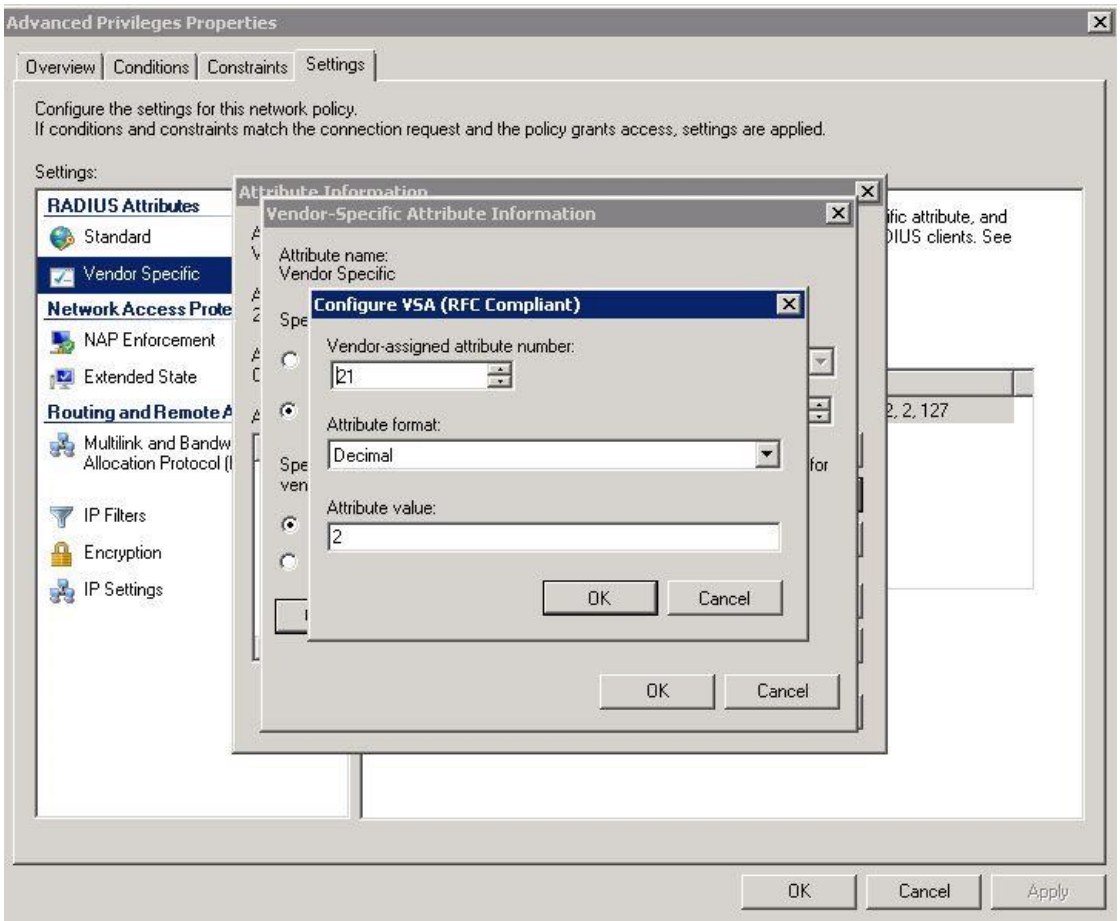
22. In the Configure VSA (RFC Compliant) window that appears, configure 13 attributes as follows:

i For **Vendor-assigned attribute number** from 21 till 32, select **Decimal** in the **Attribute format** field. These twelve attributes define the Read access level (None, Regular, or Advanced), and the Write access level (None, Regular, or Advanced) for each of the six functional groups (Ethernet, Management, Radio, Security, Sync, TDM). Therefore, in the **Attribute value** field enter the value corresponding to the access level you wish to permit to members of the group whose policy you are configuring, where:

- **2** = Advanced
- **1** = Regular
- **0** = None

Thus for example, enter 2 for all twelve attributes if you are configuring a policy for the Radius_Advanced group. This gives Advanced read permissions and Advanced write permissions, for all six functional groups, to the members of the Radius_Advanced group.

Figure 283 Create Network Policy – Configuring Vendor-Specific Attribute Information



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

Attribute name:
Vendor Specific

Vendor-assigned attribute number: 21

Attribute format: Decimal

Attribute value: 2

ii For **Vendor-assigned attribute number** 50, select **Decimal** in the **Attribute format** field. The **Attribute value** of this attribute defines the access channel(s) permitted to members of the group whose policy you are configuring. The **Attribute value** is the sum of the values corresponding to the access channels you wish to permit, where the value for each access channel is:

- none=0
- serial=1
- telnet=2
- ssh=4
- web=8
- nms=16
- snmp=32
- snmpV3=64

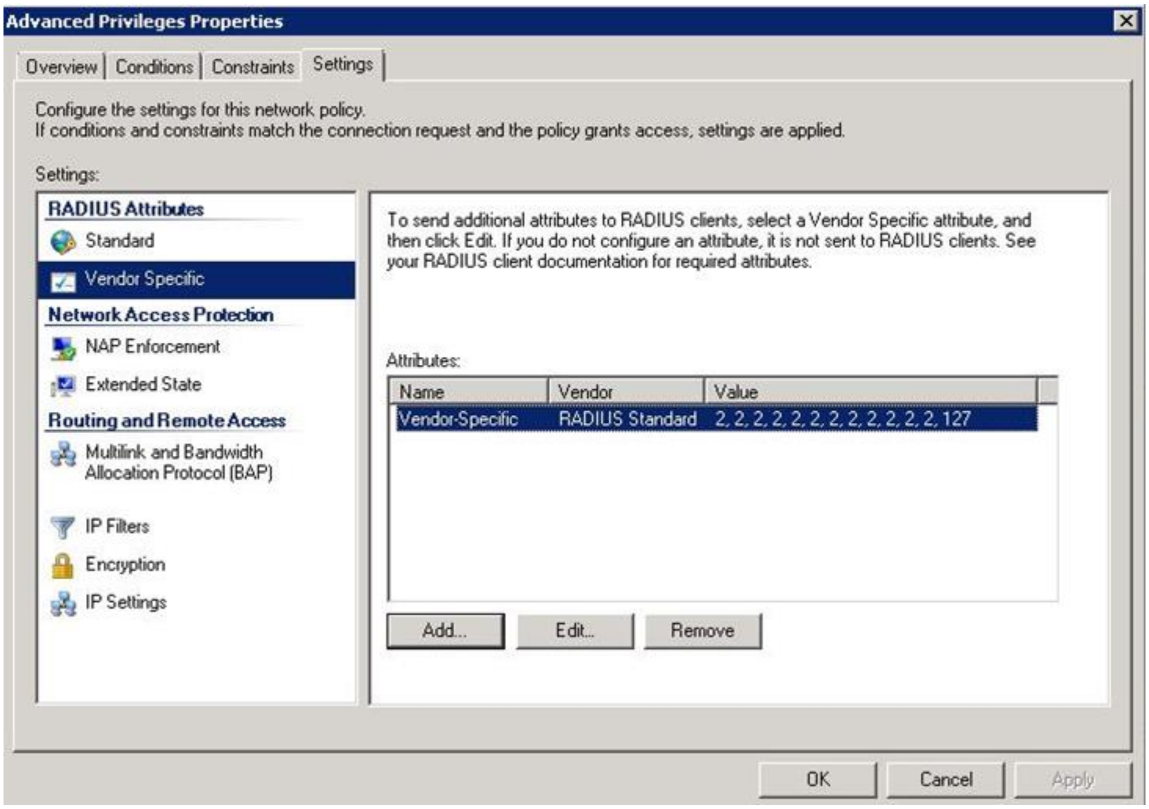
Thus for example, enter **127** to allow access from all channels: Serial + Telnet + SSH + Web + NMS + SNMP +SNMPv3;
Or enter **24** to allow access only from NMS + SNMP channels.

iii Click **OK**.

23. Click **OK**.

The following figure shows the Attributes table for the Radius_Advanced group, where access to the device is allowed from all channels.

Figure 284 Create Network Policy – Stopping/Starting NPS Services



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Name	Vendor	Value
Vendor-Specific	RADIUS Standard	2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 127

Configuring a Linux FreeRADIUS Server

The following sub-sections describe how to configure a Linux FreeRADIUS server to work with an PTP 850E device.

To so do, you will need to modify the following files:

- `/etc/raddb/users`
- `/etc/raddb/clients.conf`
- `/usr/share/freeradius/dictionary.Cambium`
- `/etc/raddb/dictionary`

Step 1 – Creating Users

This step describes how to create the following three users:

- `u1 – with advanced read/write privileges, password 1111`
- `u2 – with normal read/write privileges, password 2222`
- `u3 – with no read/write privileges, password 3333`

To create these RADIUS users:

1. Add the users in the `/etc/raddb/users` file, using any editor you like, according to the following example:

```
# user1 - advanced privileges
u1   auth-type := local, Cleartext-Password := "1111"
    security-ro = advanced,
    security-wo = advanced,
    mng-ro = advanced,
    mng-wo = advanced,
    radio-ro = advanced,
    radio-wo = advanced,
    tdm-ro = advanced,
    tdm-wo = advanced,
    eth-ro = advanced,
    eth-wo = advanced,
    sync-ro = advanced,
    sync-wo = advanced,
    access_channel = u1accesschannel,
    fall-through = yes
# user2 - regular privileges
u2   auth-type := local, Cleartext-Password := "2222"
    security-ro = regular,
    security-wo = regular,
    mng-ro = regular,
    mng-wo = regular,
    radio-ro = regular,
    radio-wo = regular,
    tdm-ro = regular,
    tdm-wo = regular,
    eth-ro = regular,
    eth-wo = regular,
    sync-ro = regular,
    sync-wo = regular,
    access_channel = u2accesschannel,
    fall-through = yes
# user3 - no privilege (viewer)
u3   auth-type := local, Cleartext-Password := "3333"
    security-ro = none,
    security-wo = none,
    mng-ro = none,
    mng-wo = none,
    radio-ro = none,
    radio-wo = none,
    tdm-ro = none,
    tdm-wo = none,
    eth-ro = none,
    eth-wo = none,
    sync-ro = none,
    sync-wo = none,
    access_channel = u3accesschannel,
    fall-through = yes
```

1 Save the changes in the /etc/raddb/users file.

Step 2 – Defining the Permitted Access Channels

The access_channel of each user we configured in the /etc/raddb/users file, defines the channels through which that user is allowed to access the unit.

This is done by summing the values corresponding to the allowed channels, where the values are:

```
###   none          0
###   serial         1
###   telnet         2
###   ssh           4
###   web           8
###   nms           16
###   snmp          32
###   snmpV3         64
```

For example:

- The value 127 denotes permission to access the device from all channels:
  Serial + Telnet + SSH + Web + NMS + SNMP +SNMPv3
- The value 24 indicates permission to access the device only from the Web + NMS channels.

To define each user's access channels:

1 In the usr/share/freeradius/dictionary.Cambium file, configure the values of the access channels according to the following example:

```
###  access channel for u1 user:serial+telnet+ssh+web+nms+snmp+snmpV4
VALUE   ACCESS_CHANNEL     u1accesschannel     127
```

2 Save the changes to the usr/share/freeradius/dictionary.Cambium file.

Step 3 – Specifying the RADIUS client

This step describes how to define a device as a RADIUS client. The RADIUS server accepts attempts to connect to a device only if that is device is defined as a RADIUS client.

To define a device as a RADIUS client:

1. In the `/etc/raddb/clients.conf` file, add the device according to the following example.
    - The example shows how to add an PTP 850E device with IP address 192.168.1.118:

      ```
      # IP50-E
      client 192.168.1.118 {
          secret     = default_not_applicable
          shortname    = Cambium-PTP 850E
      }
      ```

    - Keep in mind:
        - The `secret` must be between 22 and 128 characters long. Note down the secret because you will need to enter the same value in the Secret field of the Radius Configuration – Edit page.
        - The `shortname` is not mandatory, but should be added, and should be different for each RADIUS client.
2. Save the changes to the `/etc/raddb/clients.conf` file.

Step 4 – Adding a call to the Cambium Dictionary File

To add a call to the Cambium dictionary file:

1. Add the following at the end of the `/etc/raddb/dictionary` file, using any editor you like:

   ```
   #include the dictionary.Cambium file
   $INCLUDE dictionary.Cambium
   ```

2. Save the changes in the `/etc/raddb/dictionary` file.

Note

Make sure to use absolute path mode if the target file is located in a different directory. For example:
$INCLUDE ../share/freeradius/dictionary.Cambium)

Step 5 – Restarting the RADIUS server

After configuring all of the above, restart the RADIUS process.

To restart the RADIUS process:

1 Stop the process by entering:

```
killall -9 radiusd
```

2 Start the process running in the background by entering:

```
radius -X &
```

Note

To check the logs each time a user connects to the server, enter:
radius –X &

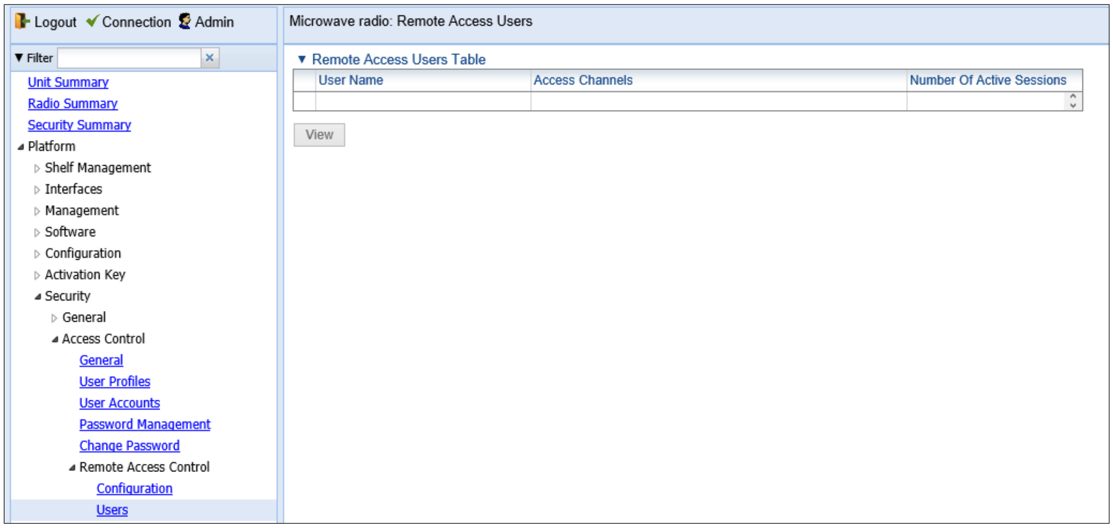
Viewing Remote Access User Connectivity and Permissions

You can view remote access user connectivity and permissions information for all RADIUS users currently connected.

To view remote access users:

1. Select **Platform > Security > Access Control > Remote Access Control > Users**. The Remote Access Users page opens.

Figure 285 Remote Access Users Page



Microwave radio: Remote Access Users

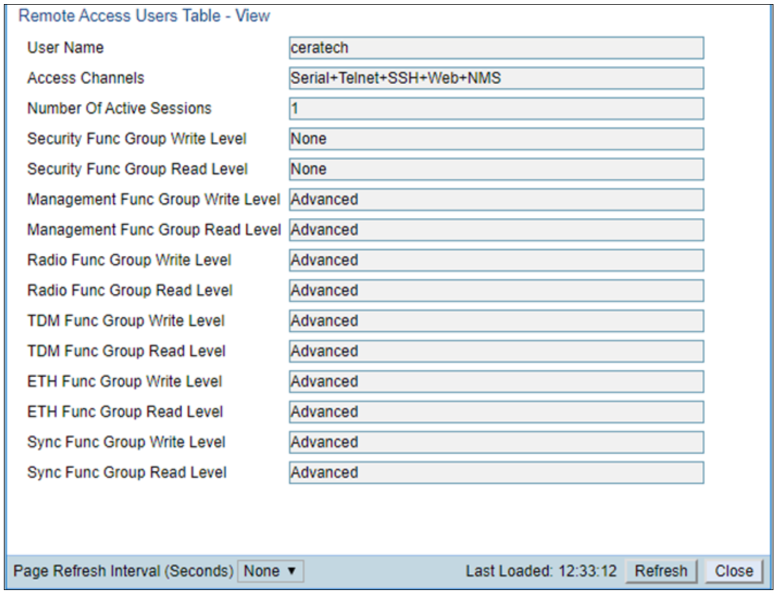
Remote Access Users Table

User Name	Access Channels	Number Of Active Sessions

- The **User ID** column displays the user's name.
- The **Access Channels** column displays the access channels the user is allowed to use to access the unit.
- The **User Instances** column displays the number of open sessions the user currently has.

To view the user's authorized access levels, select the user and click **View.** The Remote Access Users Table – View page opens.

Figure 286 Remote Access Users Table - View



Remote Access Users Table - View

User Name	ceratech
Access Channels	Serial+Telnet+SSH+Web+NMS
Number Of Active Sessions	1
Security Func Group Write Level	None
Security Func Group Read Level	None
Management Func Group Write Level	Advanced
Management Func Group Read Level	Advanced
Radio Func Group Write Level	Advanced
Radio Func Group Read Level	Advanced
TDM Func Group Write Level	Advanced
TDM Func Group Read Level	Advanced
ETH Func Group Write Level	Advanced
ETH Func Group Read Level	Advanced
Sync Func Group Write Level	Advanced
Sync Func Group Read Level	Advanced

Page Refresh Interval (Seconds) None

Last Loaded: 12:33:12

For each of the six functional groups (**Security**, **Management**, **Radio**, **TDM**, **Eth**, **Sync**), the page displays the Read access level (**None**, **Regular**, or **Advanced**), and the Write access level (**None**, **Regular**, or **Advanced**).

Configuring X.509 CSR Certificates

The web interface protocol for accessing PTP 850 can be configured to HTTP (default) or HTTPS. It cannot be set to both at the same time.

Before setting the protocol to HTTPS, you must:

1. Create and upload a CSR file. See Generating a Certificate Signing Request (CSR) File.
2. Download the certificate to the PTP 850 and install the certificate. See Downloading a Certificate.
3. Enable HTTPS. This must be performed via CLI. See Enabling HTTPS (CLI).

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

Note

For these operations, SFTP must be used.

Generating a Certificate Signing Request (CSR) File

Note

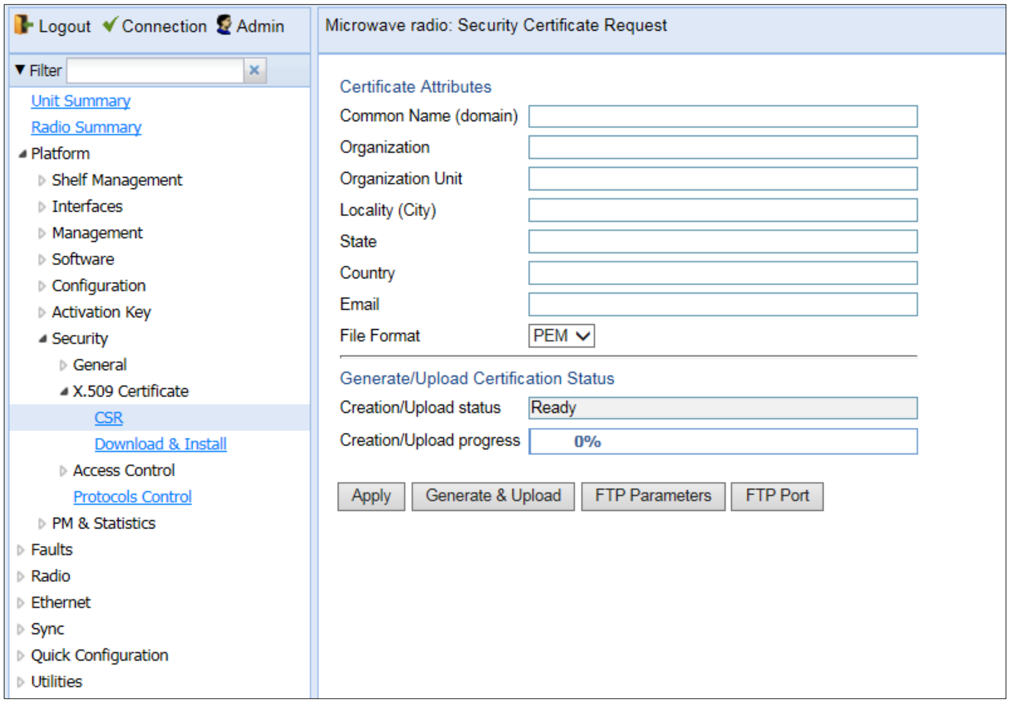
If you need a customized public RSA key, you must download and

install the RSA key first, before generating a CSR file. Otherwise, the CSR file will include the current public RSA key. See Downloading and Installing an RSA Key.

To generate a Certificate Signing Request (CSR) file:

1. Select **Platform > Security > X.509 Certificate > CSR**. The Security Certificate Request page opens.

Figure 287 Security Certificate Request Page



Microwave radio: Security Certificate Request

Certificate Attributes

Common Name (domain)

Organization

Organization Unit

Locality (City)

State

Country

Email

File Format: PEM

Generate/Upload Certification Status

Creation/Upload status: Ready

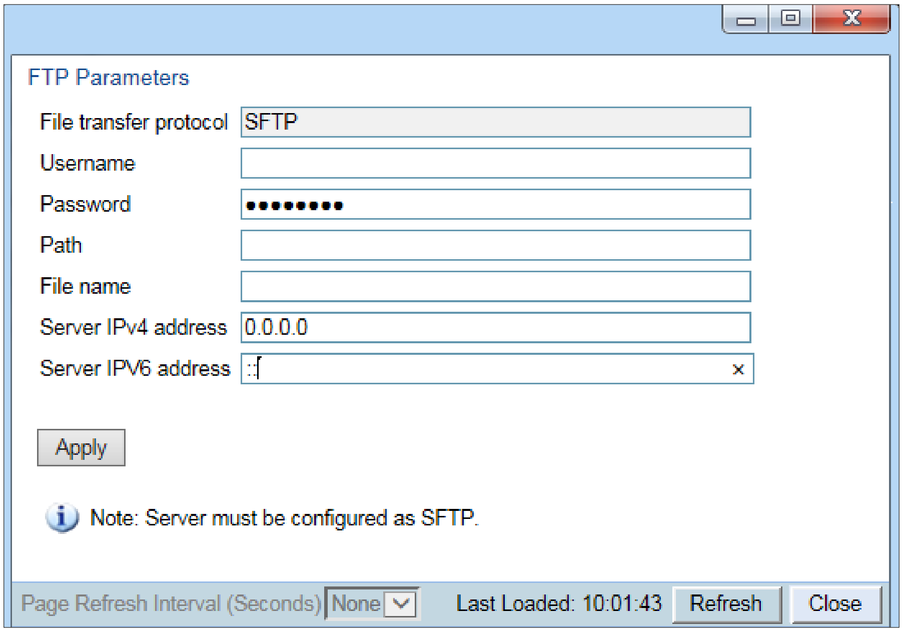
Creation/Upload progress: 0%

2. In the **Common Name** field, enter the fully–qualified domain name for your web server. You must enter the exact domain name.
3. In the **Organization** field, enter the exact legal name of your organization. Do not abbreviate.
4. In the **Organization Unit** field, enter the division of the organization that handles the certificate.
5. In the **Locality** field, enter the city in which the organization is legally located.
6. In the **State** field, enter the state, province, or region in which the organization is located. Do not abbreviate.
7. In the **Country** field, enter the two-letter ISO abbreviation for your country (e.g., US).
8. In the **Email** field, enter an e-mail address that can be used to contact your organization.
9. In the **File Format** field, select the **PEM** file format. Note that the **DER** file format is planned for future release.

> **Note**
>
> In this version, only PEM is supported.

10. Click **Apply** to save your settings.
11. Click **FTP Parameters** to display the FTP Parameters page.

Figure 288 FTP Parameters Page (Security Certificate Request)



FTP Parameters

File transfer protocol	SFTP
Username	
Password	●●●●●●●●
Path	
File name	
Server IPv4 address	0.0.0.0
Server IPV6 address	::

Note: Server must be configured as SFTP.

12. In the **Username** field, enter the user name you configured in the SFTP server.
13. In the **Password** field, enter the password you configured in the SFTP server. If you did not configure a password for your SFTP user, simply leave this field blank.
14. In the **Path** field, enter the directory path to which you are uploading the CSR. Enter the path relative to the SFTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
15. In the **File name** field, enter the name you want to give to the exported CSR.
16. If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the SFTP server in the **Server IPV4 address** field. See Defining the IP Protocol Version for Initiating Communications.
17. If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the SFTP server in the **Server IPv6 address** field. See Defining the IP Protocol Version for Initiating Communications.
18. Click **Apply**, then Close, to save the FTP parameters and return to the Security Log Upload page.
19. Click **Generate & Upload.** The file is generated and uploaded.

The **CSR Status** field displays the status of any pending CSR generation and upload. Possible values are:

- **Ready** – The default value, which appears when CSR generation and upload is in progress.
- **File-in-transfer** – The upload operation is in progress.
- **Success** – The file has been successfully uploaded.
- **Failure** – The file was not successfully uploaded.

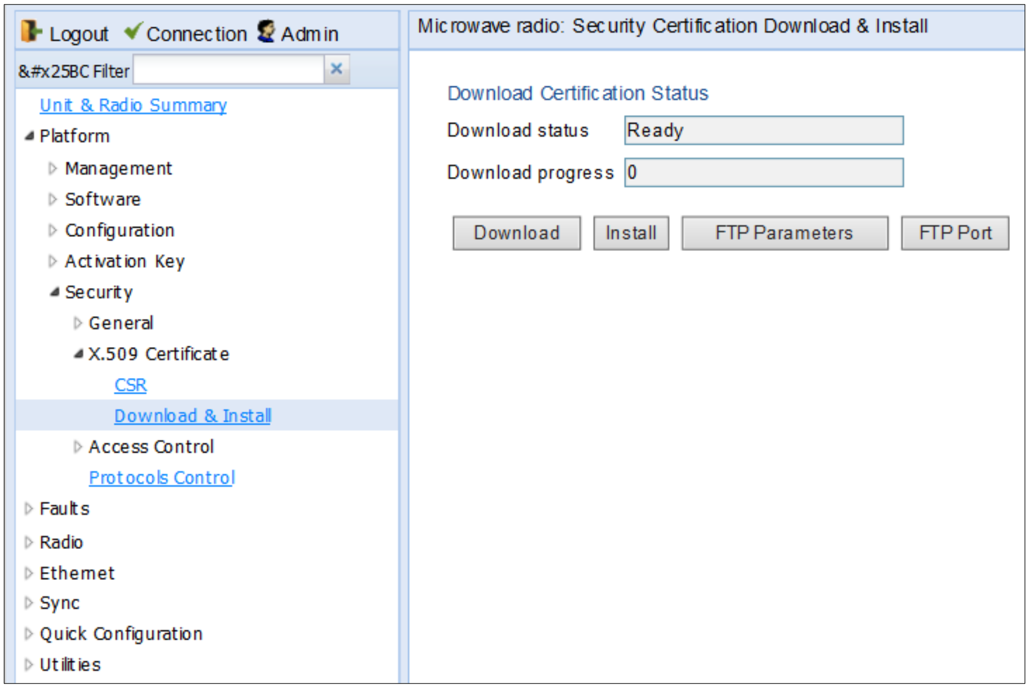
The **CSR Percentage** field displays the progress of any current CSR upload operation.

Downloading a Certificate

To download a certificate:

1. Select **Platform > Security > X.509 Certificate > Download & Install**. The Security Certification Download and Install page opens.

Figure 289 Security Certification Download and Install Page



Microwave radio: Security Certification Download & Install

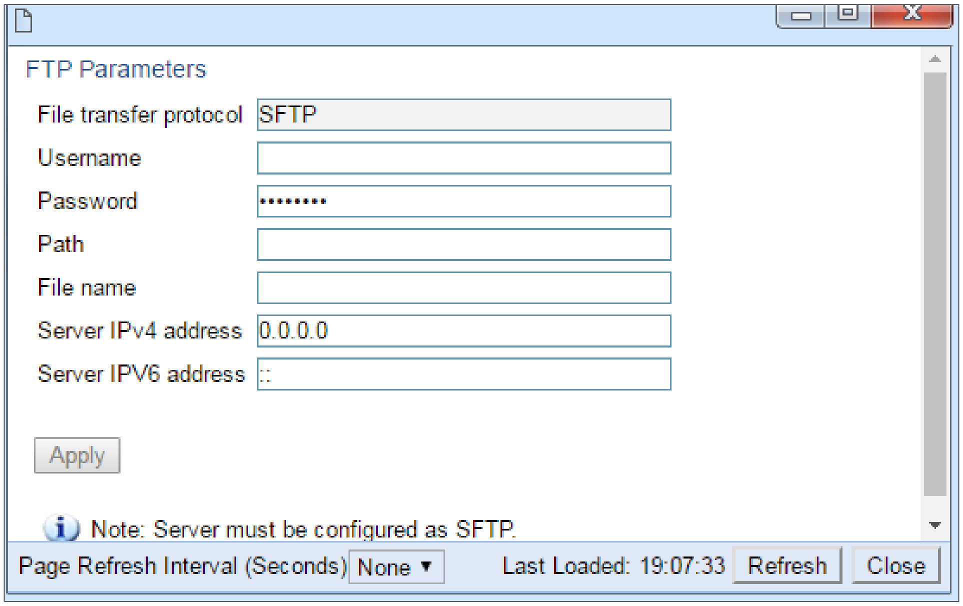
Download Certification Status

Download status: Ready

Download progress: 0

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

Figure 290 FTP Parameters Page (Security Certification Download & Install)



FTP Parameters

File transfer protocol: SFTP

Username:

Password: ••••••••

Path:

File name:

Server IPv4 address: 0.0.0.0

Server IPV6 address: ::

Note: Server must be configured as SFTP.

Page Refresh Interval (Seconds) None ▾ Last Loaded: 19:07:33

3. In the **User name for logging** field, enter the user name you configured in the SFTP server.

4. In the **User password to server** field, enter the password you configured in the SFTP server. If you did not configure a password for your SFTP user, simply leave this field blank.
5. In the **Path** field, enter the directory path from which you are uploading the certificate. Enter the path relative to the SFTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
6. In the **File Name** field, enter the certificate's file name in the SFTP server.
7. If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the SFTP server in the **Server IPV4 address** field. See Defining the IP Protocol Version for Initiating Communications.
8. If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the SFTP server in the **Server IPv6 address** field. See Defining the IP Protocol Version for Initiating Communications.
9. Click **Apply** to save your settings.
10. Click **Download**. The certificate is downloaded.
11. Click **Install**. The certificate is installed on the PTP 850.

Enabling HTTPS

By default, HTTP is used by PTP 850E as its web interface protocol.

To enable HTTPS instead of HTTP:

1 Select **Platform > Security > Protocols Control**. The Protocols Control page opens (***Error! Reference source not found.***).

2 In the **HTTP protocol** field, select **HTTPS**.

3 Click **Apply**.

Note

Make sure you have installed a valid certificate in the PTP 850E before changing the web interface protocol to HTTPS. Failure to do this may prevent users from accessing the Web EMS.

Downloading and Installing an RSA Key

PTP 850 devices support RSA keys for communication using HTTPS and SSH protocol. The PTP 850 device comes with randomly generated default private and public RSA keys. However, you can replace the private key with a customer-defined private key. The corresponding RSA public key will be generated based on this private key. The file must be in PEM format. Supported RSA private key sizes are 2048, 4096, and 8192.

The following is an example of a valid RSA private key file:

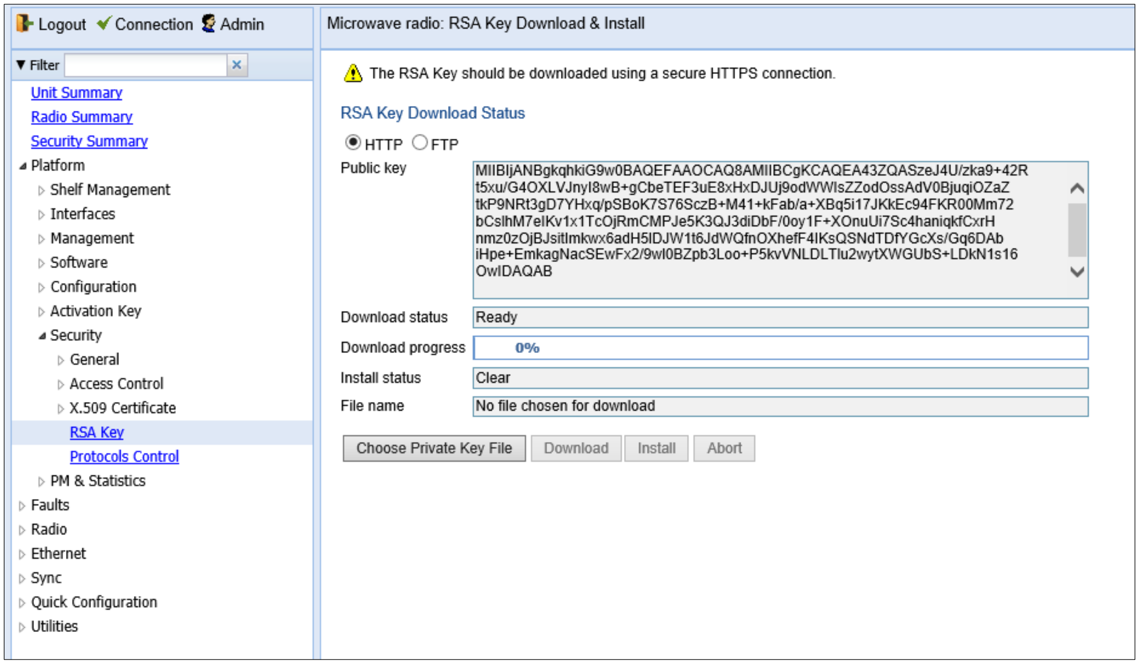
```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC+7jRmt27yF4xDh5Pc8w4ikvXU
```

```
u32BI0eOyELmeUBnEeIHbCOXD3upi8+ZnH51Q+8hzgoSqXgEYFgZMoF/sXCrO2yf62UJ5ohj3zadhx/
7585zoGwHtYz1S62hsa4+cdAI/i1Vbc6CoUBh5642XYje+Q+q1XJtObed884eaQcXUFLIBipYKvVx2kue
IymansE91WJU+UjFIc3aiQG8qsSgW5Ar6wet0pXkP2Vdemo//QAXXjcTqqMBuizrIhIcvi+OKYFI9kSh2
1ZqSgjvK3cfAssCJBIY5d6t6bVkX9p2gjo/IPnErjAv7W6IZoemotb5KAeSHeR1sYTw17/xIpM7AgMBA
AECggEAAwIiLKQMOq4kh/UXD/OPAIPDXyp1jjaTw8dBm811OG5wttzXGrxJ+OIFX5Rn79DbHnbayC
iJL8tMe2dx5yhY+hA247roX3ua0w57cuPxnp21izc+S0fC7H/TTM1jpRCbATparuTRMIitinZshJGA73Ls
od3v36GEXxm/6dHnz/drCs2F4NdHWpjMAAG/1CiBwut8jNkJUwa78Ivk3JF+XRoZ0txN2mIybQxxzju
NXqZbNO6H3Ua2u1iYyD+McfgOWCCUfSnstGRhFg0OsQuqj6d74qKVQWaukEH91SVZHEoqX6Dgp
Ky4INZBxORZmITNmadwNhw5O7rvFxZ205u4gQKBgQDT5bXvc0Ok+Ypm2xnIbu2GFjxNYwYhR3T
vHPy14NIO5Q9I/uDqwrSL1igzaIr6EbZyLu8cDXa4aybrzCyBfPeG89Qq+a6J3JR/RwJndLyjV4h5CT8Zy
4O/wjgTrP3Rhq7LAbWgLjSarafLgruHTcnOifhkK7MK7Fr+xi2IJfOKQQKBgQDmq1eYNzIMPIATESIsf
bkcL49jSsu70kYg0g5IoI6+bVPo9K7mopICtWC/fwdNIUAfO+vr/231YUfSo7YNEDNNRoT/NwvqqtAYx
ZaIUdIQxhMywF9jjYBBuq6+f/7+dwDfNBtMb2q7hceTdk6yZ8/MehCkvSwOBmP+Iq0FwTmmewKBg
QCIxmj31G1ve+rTXUZmkKIy7OJwiLAbCRRqnXr3r9Om43151i2QfJNTc1AwKVzTI1ftLNrUT5Q541qn
zyxigaoFYmzy0jPCI1d128/9sE6EW87hImLDg3ynYQMOIaDRc1T8bXHyxzNQb9t+U+DykeD4POifNbD
1MsRd3h1xDn/iAQKBgHmKpukJkCNgYgjp7g3AYR084izLaHZa4aDBjc0v4QQtzxzccJwN5SmQMJ42
bL6wecz7YeBEAshcrd+La42Oj7mUAtgHRTwtLOEgm6TQmANGmy8OtjRahs4bc5/ICZNDWS5C4m9
v9aIBYFuO5wCSOqffWY20L9Zj/6RR+HEj0yCpAoGAHwrbRqPVZtZptFuNsCq130dtmqI7HFQAIqrc5D
wP7YSsznE6biHfLUw891xu0vmevALrCaoeOMaidugohgiorSJO4qk7I3XN3pUJhPYqbhtdCVnBI2Fm
9pr3V/SHGvrI1NW92cXObeQ2UEBiKPOyQKfOBIbac707u0HqaTu+/ts=
-----END PRIVATE KEY-----
```

To download and install a private RSA key:

1. Select **Platform > Security > RSA Key**. The RSA Key Download & Install page opens.

Figure 291 RSA Key Download & Install Page (HTTP Selected)



Microwave radio: RSA Key Download & Install

The RSA Key should be downloaded using a secure HTTPS connection.

RSA Key Download Status

● HTTP ○ FTP

Public key

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA43ZQASzeJ4U/zka9+42R
t5xu/G4OXLVJnyI8wB+gCbeTEF3uE8xHxDJUj9odWWIsZZodOssAdV0BjuqiOZaZ
tkP9NRt3gD7YHxq/pSBoK7S76SczB+M41+kFab/a+XBq5i17JKkEc94FKR00Mm72
bCslhM7eIKv1x1TcOjRmCMPJe5K3QJ3diDbF/0oy1F+XOnuUi7Sc4haniqkfCxrH
nmz0zOjBJsitImkwx6adH5IDJW1t6JdWQfnOXhefF4IKsQSNdTDfYGcXs/Gq6DAb
iHpe+EmkagNacSEwFx2/9wI0BZpb3Loo+P5kvVNLDLTIu2wytXWGUbS+LDkN1s16
OwIDAQAB
```

Download status: Ready

Download progress: 0%

Install status: Clear

File name: No file chosen for download

2. Select **HTTP** to download the file via HTTP/HTTPS or **FTP** to download the file via SFTP.

Note

It is strongly recommended not to use HTTP to download RSA key files

Downloading an RSA Key via HTTP or HTTPS

To download and install a private RSA key file using HTTP or HTTPS:

1 Select **HTTP**.

2 Click **Choose Private Key File.**

3 Browse to and select the file.

4 Click **Download.** The download begins. You can view the status of the download in the **Download Status** field. See **Error! Reference source not found.**.

5 Once the download has been completed, click **Install** to install the RSA key file. You can view the status of the installation in the **Install Status** field. See **Error! Reference source not found.**.

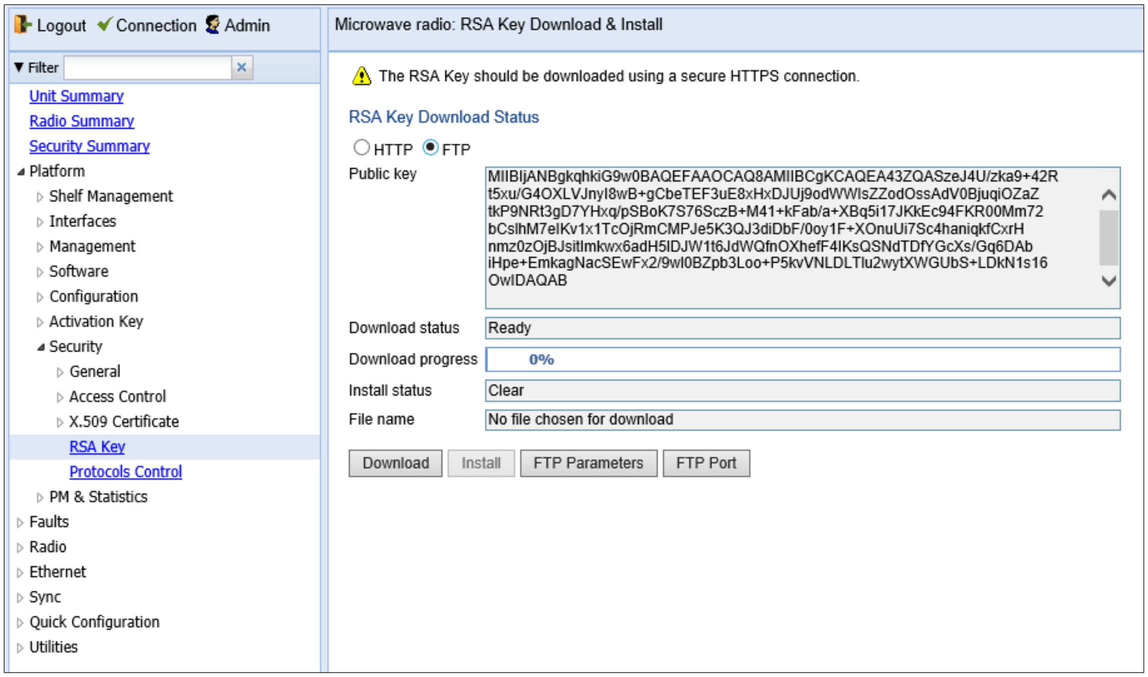
> Note
>
> To discontinue the download process, click Abort.

Downloading an RSA Key via SFTP

To download and install a private RSA key file using SFTP:

1. Install and configure SFTP server software on the PC or laptop you are using to perform the software upgrade. See *Installing and Configuring an FTP or SFTP Server*.
2. In the RSA Key Download & Install page, select **FTP**.

Figure 292 RSA Key Download & Install Page (FTP Selected)



Microwave radio: RSA Key Download & Install

The RSA Key should be downloaded using a secure HTTPS connection.

RSA Key Download Status

○ HTTP ● FTP

Public key

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA43ZQASzeJ4U/zka9+42R
t5xu/G4OXLVJnyI8wB+gCbeTEF3uE8xHxDJUj9odWWIsZZodOssAdV0BjuqiOZaZ
tkP9NRt3gD7YHxq/pSBoK7S76SczB+M41+kFab/a+XBq5i17JKkEc94FKR00Mm72
bCslhM7eIKv1x1TcOjRmCMPJe5K3QJ3diDbF/0oy1F+XOnuUi7Sc4haniqkfCxrH
nmz0zOjBJsitlmkwx6adH5lDJW1t6JdWQfnOXhefF4IKsQSNdTDfYGcXs/Gq6DAb
iHpe+EmkagNacSEwFx2/9wl0BZpb3Loo+P5kvVNLDLTlu2wytXWGUbS+LDkN1s16
OwIDAQAB
```

Download status: Ready

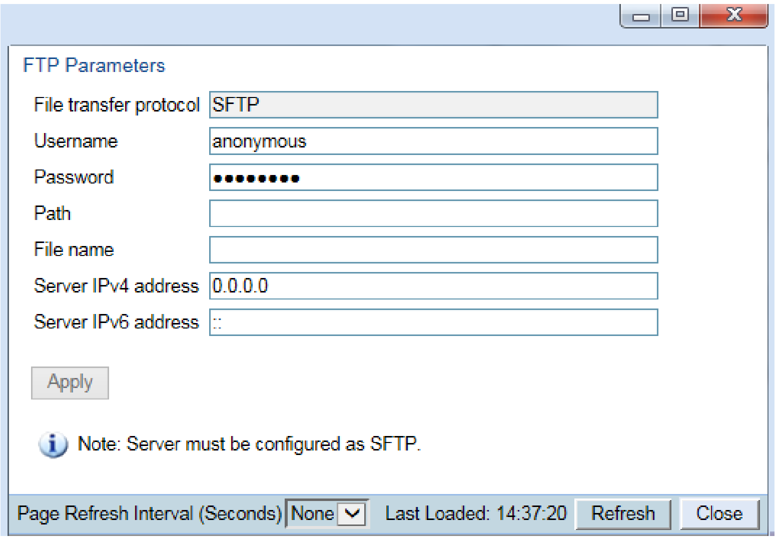
Download progress: 0%

Install status: Clear

File name: No file chosen for download

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

Figure 293 FTP Parameters Page



FTP Parameters

File transfer protocol	SFTP
Username	anonymous
Password	••••••••
Path	
File name	
Server IPv4 address	0.0.0.0
Server IPv6 address	::

Note: Server must be configured as SFTP.

Page Refresh Interval (Seconds) None Last Loaded: 14:37:20

4. The **File Transfer Protocol** field is read-only and displays **SFTP**. RSA key files cannot be downloaded to an PTP 850 device using FTP.
5. In the **Username** field, enter the user name you configured in the SFTP server.
6. In the **Password** field, enter the password you configured in the SFTP server. If you did not configure a password for your SFTP user, simply leave this field blank.
7. In the **Path** field, enter the directory path from which you are downloading the file. Enter the path relative to the SFTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//"..
8. If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the SFTP server in the **Server IPv4 address** field. See ***Error! Reference source not found.***.
9. If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the SFTP server in the **Server IPv6 address** field. See ***Error! Reference source not found.***.
10. Click **Apply** to save your settings.
11. In the RSA Key Download & Install page, click **Download**. The download begins. You can view the status of the download in the **Download Status** field. See **Error! Reference source not found.**.
12. Once the download has been completed, click **Install** to install the RSA key file. You can view the status of the installation in the **Install Status** field.

Note

To discontinue the download process, click Abort.

Table 79 RSA File Download & Install Status Parameters

Parameter	Definition
Download Status	The status of any pending RSA file download. Possible values are: • Ready – The default value, which appears when no download is in progress. • In Progress – The download is in progress. • Aborted – The download was aborted by user command. If an error occurs during the download, an appropriate error message is displayed in this field. When the download is complete, one of the following status indications appears: • Success – File downloaded and verified successfully. • Failed – File download failed or verification failed. When the system is reset, the Download Status returns to Ready.
Download Progress	Displays the progress of the current download.
Install Status	The status of any pending installation. Possible values are: • **Success** • **Failed**

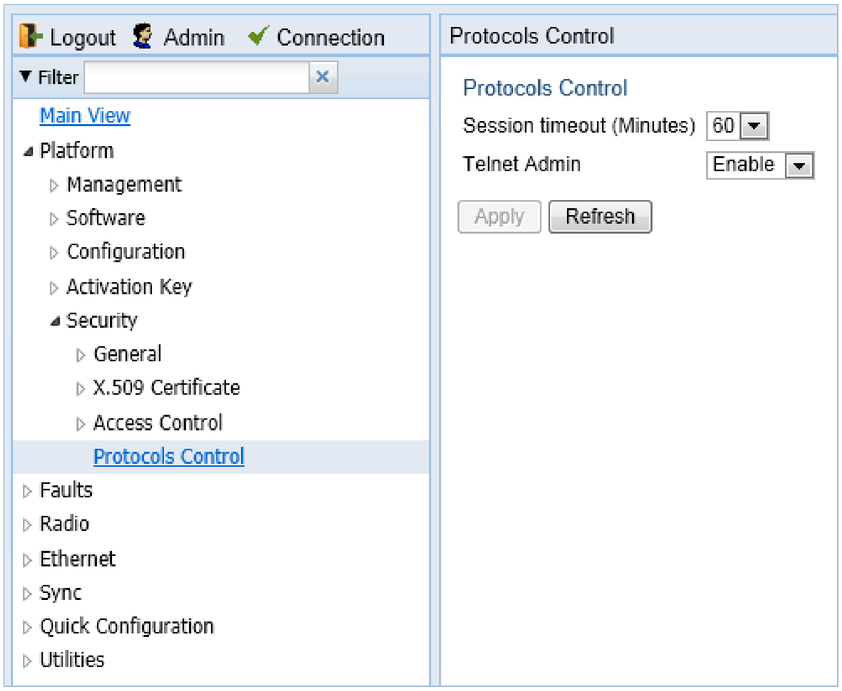
Blocking Telnet Access

You can block telnet access to the unit. By default, telnet access is not blocked.

To block telnet access:

1 Select **Platform > Security > Protocols Control**. The Protocols Control page opens.

Figure 294 Protocols Control Page



Protocols Control

Session timeout (Minutes) 60

Telnet Admin Enable

2 In the **Telnet Admin** field, select **Disable** to block telnet access. By default, telnet access is enabled (**Enable**).

3 Click **Apply**.

Uploading the Security Log

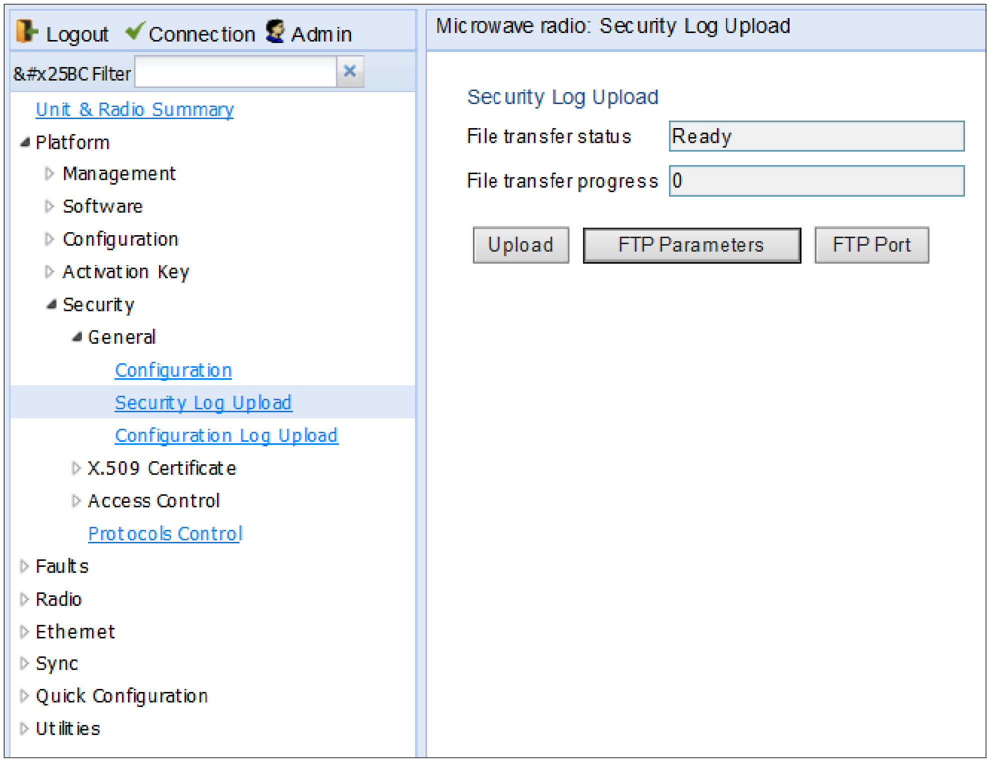
The security log is an internal system file which records all changes performed to any security feature, as well as all security related events.

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

To upload the security log:

1. Install and configure an FTP server on the PC or laptop you are using to perform the upload. See Installing and Configuring an FTP or SFTP Server.
2. Select **Platform > Security > General > Security Log Upload**. The Security Log Upload page opens.

Figure 295 Security Log Upload Page

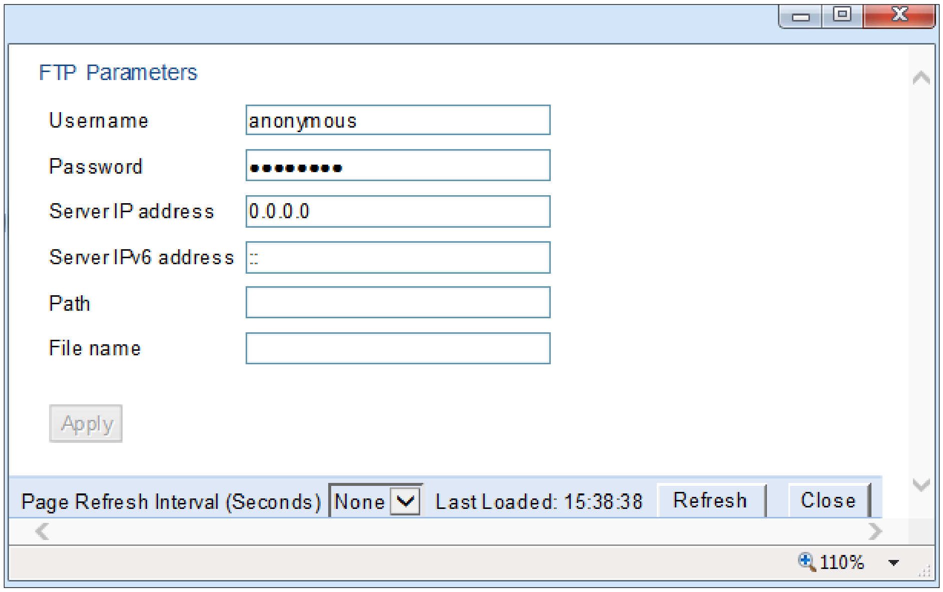


File transfer status: Ready

File transfer progress: 0

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

Figure 296 FTP Parameters Page (Security Log Upload)



FTP Parameters

Username	anonymous
Password	••••••••
Server IP address	0.0.0.0
Server IPv6 address	::
Path	
File name	

4. In the **File transfer protocol** field, select the file transfer protocol you want to use (**FTP** or **SFTP**).
5. In the **Username** field, enter the user name you configured in the FTP server.
6. In the **Password** field, enter the password you configured in the FTP server. If you did not configure a password for your FTP user, simply leave this field blank.
7. If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the FTP server in the **Server IPV4 address** field. See Defining the IP Protocol Version for Initiating Communications.
8. If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the FTP server in the **Server IPv6 address** field. See Defining the IP Protocol Version for Initiating Communications.
9. In the **Path** field, enter the directory path to which you are uploading the files. Enter the path relative to the FTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
10. In the **File name** field, enter the name you want to give to the exported security log.
11. Click **Apply**, then **Close** to save the FTP parameters and return to the Security Log Upload page.
12. Click **Upload**. The upload begins.

The **File transfer operation status** field displays the status of any pending security log upload. Possible values are:

- **Ready** – The default value, which appears when no file transfer is in progress.
- **File-in-transfer** – The upload operation is in progress.
- **Success** – The file has been successfully uploaded.
- **Failure** – The file was not successfully uploaded.

- The **File transfer progress** field displays the progress of any current security log upload operation.

Uploading the Configuration Log

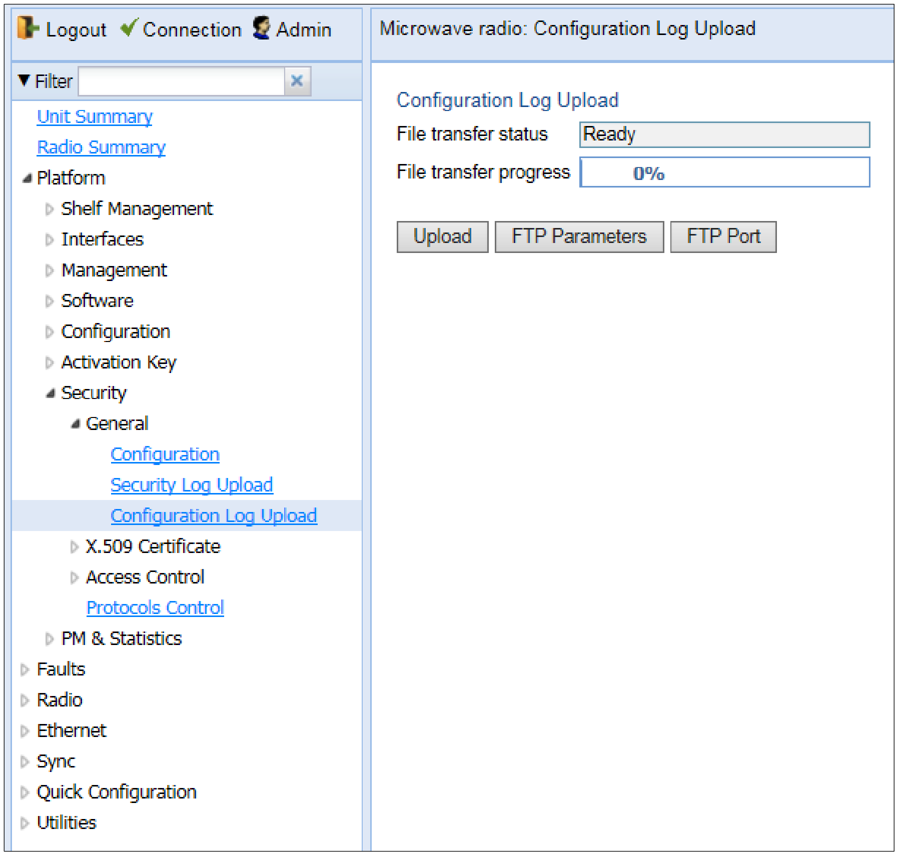
The configuration log lists actions performed by users to configure the system. This file is mostly used for security, to identify suspicious user actions. It can also be used for troubleshooting.

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

To upload the configuration log:

1. Install and configure an FTP server on the PC or laptop you are using to perform the upload. See Installing and Configuring an FTP or SFTP Server.
2. Select **Platform > Security > General > Configuration Log Upload**. The Configuration Log Upload page opens.

Figure 297 Configuration Log Upload Page



Microwave radio: Configuration Log Upload

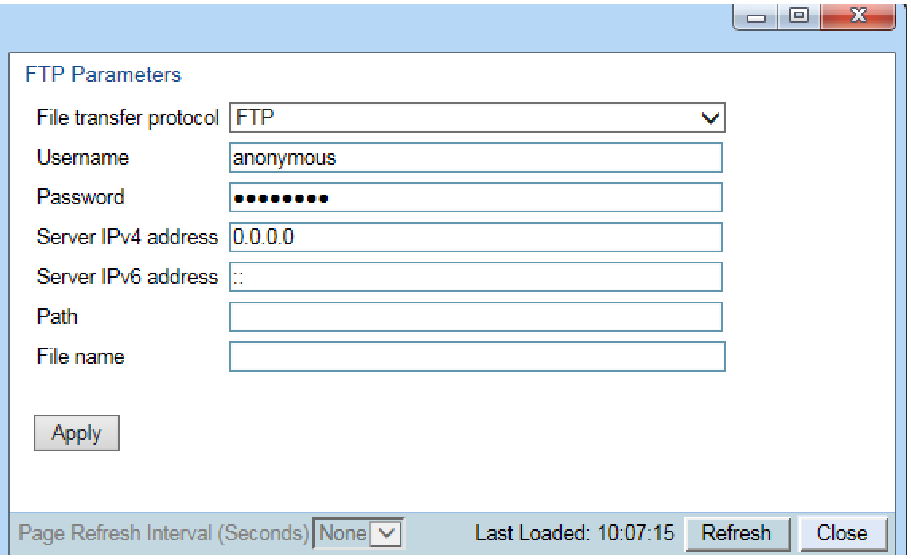
Configuration Log Upload

File transfer status: Ready

File transfer progress: 0%

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

Figure 298 Configuration Log Upload Page



FTP Parameters

File transfer protocol	FTP
Username	anonymous
Password	••••••••
Server IPv4 address	0.0.0.0
Server IPv6 address	::
Path	
File name	

4. In the **File transfer protocol** field, select the file transfer protocol you want to use (**FTP** or **SFTP**).
5. In the **Username** field, enter the user name you configured in the FTP server.
6. In the **Password** field, enter the password you configured in the FTP server. If you did not configure a password for your FTP user, simply leave this field blank.
7. If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the FTP server in the **Server IPV4 address** field. See Defining the IP Protocol Version for Initiating Communications.
8. If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the FTP server in the **Server IPv6 address** field. See Defining the IP Protocol Version for Initiating Communications.
9. In the **Path** field, enter the directory path to which you are uploading the files. Enter the path relative to the FTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
10. In the **File Name** field, enter the name you want to give to the exported configuration log.

Note

The directory path and fie name, together, cannot be more than:

If the IP address family is configured to be IPv4: 236 characters

If the IP address family is configured to be IPv6: 220 characters

11. Click **Apply**, and **Close** to save the FTP parameters and return to the Configuration Log Upload page.
12. Click **Upload**. The upload begins.

The **File transfer operation status** field displays the status of any pending configuration log upload. Possible values are:

- **Ready** – The default value, which appears when no file transfer is in progress.

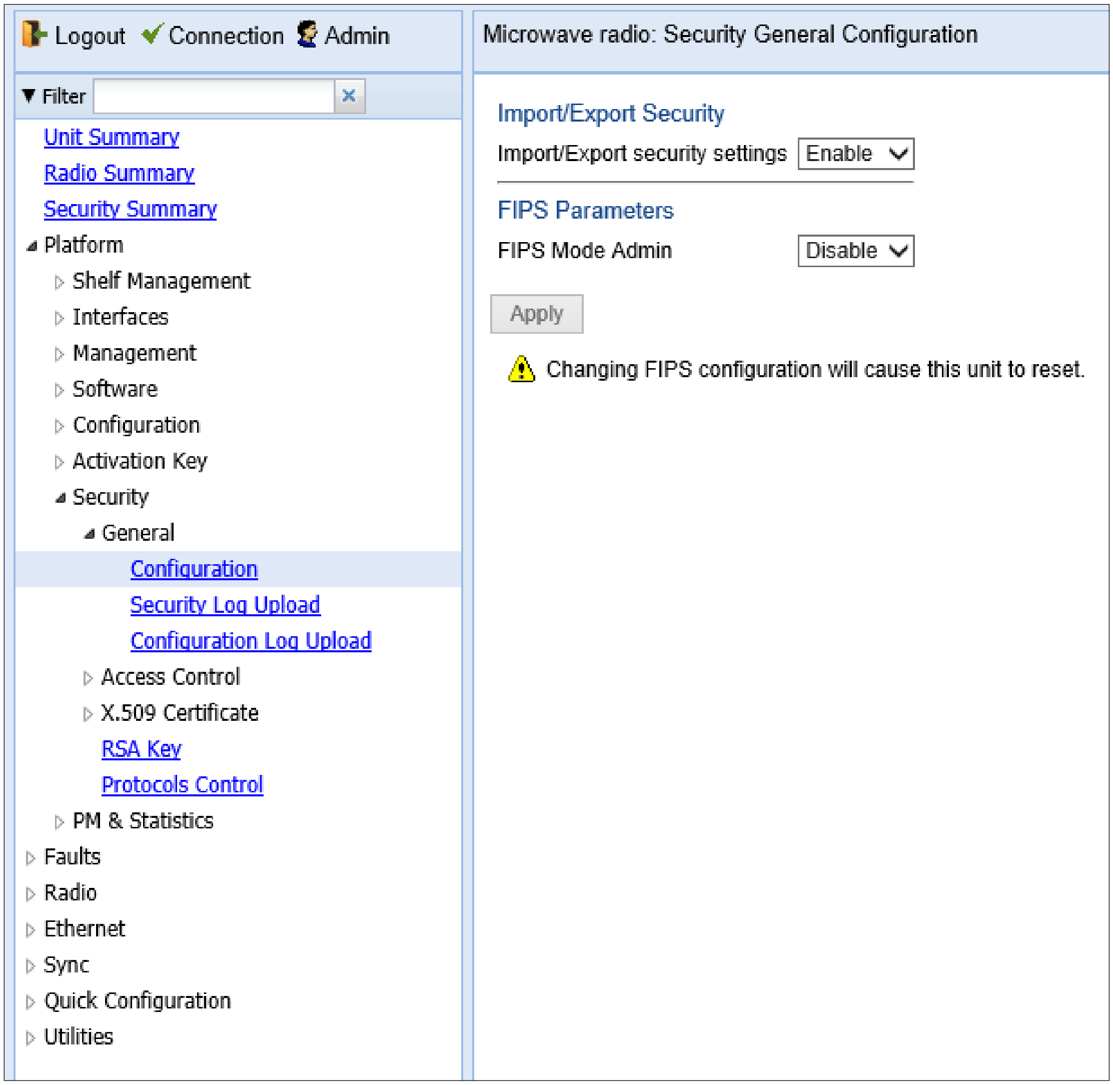
- **File-in-transfer** – The upload operation is in progress.
- **Success** – The file has been successfully uploaded.
- **Failure** – The file was not successfully uploaded.
- The **File transfer progress** field displays the progress of any current configuration log upload operation.

Configuring the Import/Export Security Settings

You can configure the unit to exclude security configurations from configuration backup files:

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

Figure 299 Security General Configuration Page



Microwave radio: Security General Configuration

Import/Export Security

Import/Export security settings Enable

FIPS Parameters

FIPS Mode Admin Disable

Changing FIPS configuration will cause this unit to reset.

2 The **Import/Export security settings** field determines whether security configurations are included in configuration backup files. To enhance unit security, it is recommended to select **Enable** in this field, so that security configurations will *not* be included in backup files.

3 Click **Apply**.

Chapter 14: Alarm Management and Troubleshooting

This section includes:

- Viewing Current Alarms
- Viewing Alarm Statistics
- Viewing and Savin the Event Log
- Editing Alarm Text and Severity and Disabling Alarms and Events
- Configuring Voltage Alarm Thresholds and Displaying Voltage PMs
- Uploading Unit Info
- Performing Diagnostics

Note

CW mode, used to transmit a single or dual frequency tones for debugging purposes, can be configured using the CLI. See Working in CW Mode (Single or Dual Tone) (CLI).

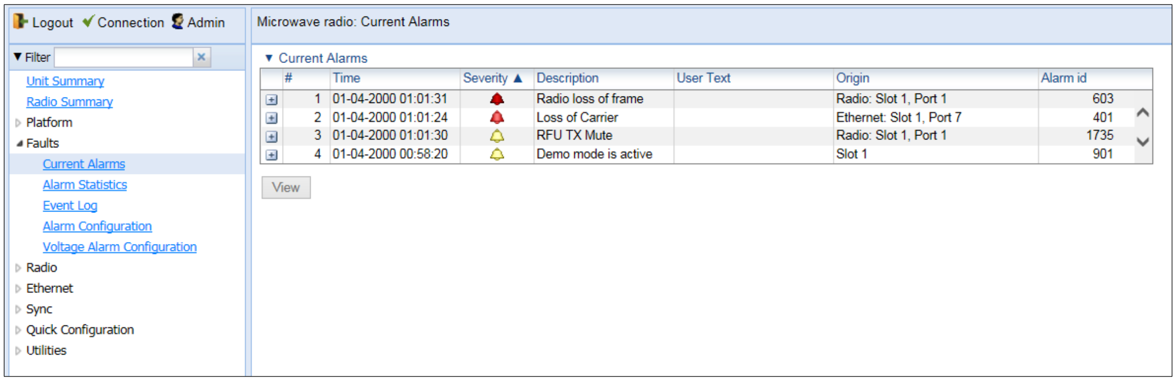
You can configure a wait time of up to 120 seconds after an alarm is cleared in the system before the alarm is actually reported as being cleared. This prevents traps flooding the NMS in the event that some external condition causes the alarm to be raised and cleared continuously. By default, the timeout for trap generation is disabled. It can be enabled and disabled via CLI. See Configuring a Timeout for Trap Generation (CLI).

Viewing Current Alarms

To display a list of current alarms in the unit:

1. Select **Faults > Current Alarms.** The Current Alarms page opens. The Current Alarms page displays current alarms in the unit. Each row in the Current Alarms table describes an alarm and provides basic information about the alarm. For a description of the information provided in the Current Alarms page, see Table 80.

Figure 300 Current Alarms Page



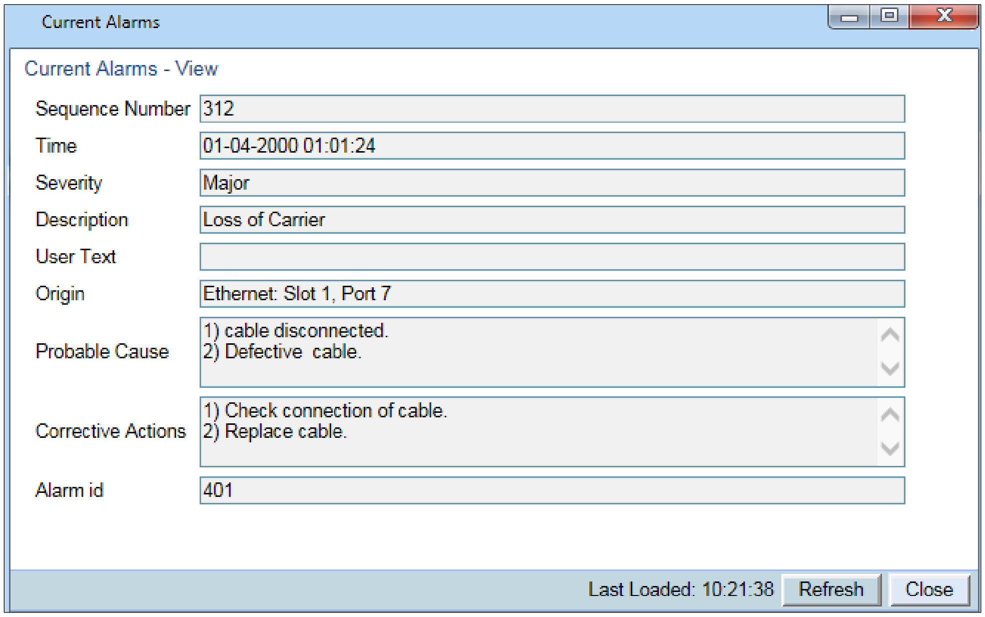
Microwave radio: Current Alarms

Current Alarms

	#	Time	Severity ▲	Description	User Text	Origin	Alarm id
⊞	1	01-04-2000 01:01:31	●	Radio loss of frame		Radio: Slot 1, Port 1	603
⊞	2	01-04-2000 01:01:24	●	Loss of Carrier		Ethernet: Slot 1, Port 7	401
⊞	3	01-04-2000 01:01:30	○	RFU TX Mute		Radio: Slot 1, Port 1	1735
⊞	4	01-04-2000 00:58:20	○	Demo mode is active		Slot 1	901

2. To view more detailed information about an alarm, click + at the beginning of the row or select the alarm and click **View**.

Figure 301 Current Alarms - View Page



Current Alarms - View

Sequence Number	312
Time	01-04-2000 01:01:24
Severity	Major
Description	Loss of Carrier
User Text	
Origin	Ethernet: Slot 1, Port 7
Probable Cause	1) cable disconnected. 2) Defective cable.
Corrective Actions	1) Check connection of cable. 2) Replace cable.
Alarm id	401

Last Loaded: 10:21:38

Table 80 Alarm Information

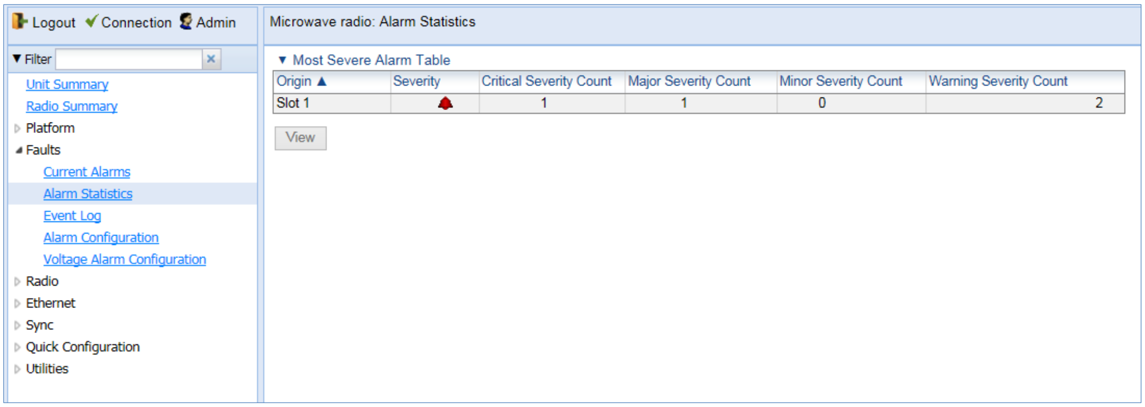
Parameter	Definition
Sequence Number (#)	A unique sequence number assigned to the alarm by the system.
Time	The date and time the alarm was triggered.
Severity	The severity of the alarm. In the Current Alarms table, the severity is indicated by a symbol. You can display a textual description of the severity by holding the cursor over the symbol. **Note:** You can edit the severity of alarm types in the Alarm Configuration page. See Editing Alarm Text and Severity.
Description	A system-defined description of the alarm.
User Text	Additional text that has been added to the system-defined description of the alarm by users. **Note:** You can add user text to alarms in the Alarm Configuration page. See Editing Alarm Text and Severity.
Origin	The module that generated the alarm.
Probable Cause	This field only appears in the Current Alarms - View page. One or more possible causes of the alarm, to be used for troubleshooting.
Corrective Actions	This field only appears in the Current Alarms - View page. One or more possible corrective actions to be taken in troubleshooting the alarm.
Alarm ID	A unique ID that identifies the alarm type.

Viewing Alarm Statistics

To display a summary of alarms per module and per interface:

1. Select **Faults > Alarm Statistics**. The Alarm Statistics page opens.

Figure 302 Alarm Statistics Page



Microwave radio: Alarm Statistics

▼ Most Severe Alarm Table

Origin ▲	Severity	Critical Severity Count	Major Severity Count	Minor Severity Count	Warning Severity Count
Slot 1	🔔	1	1	0	2

The Alarm Statistics page displays the number of current alarms per severity level for each module, interface, and virtual interface (such as Multi-Carrier ABC groups) in the unit. Only modules and interfaces for which one or more alarms are currently raised are listed in the Alarm Statistics page.

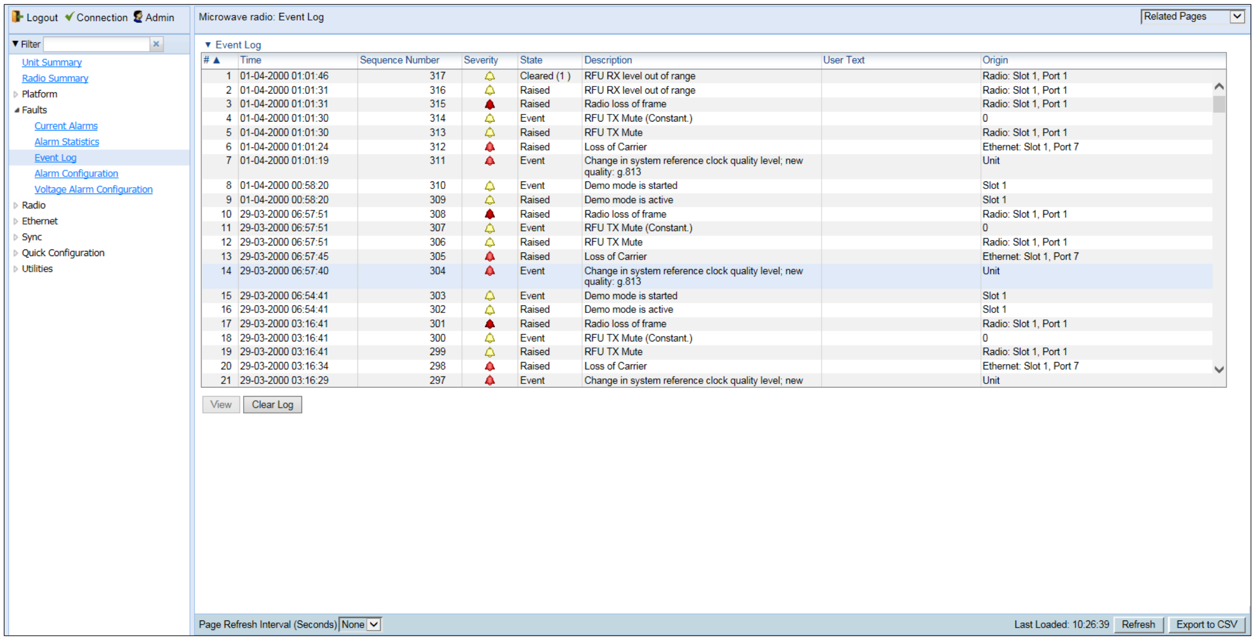
Viewing and Saving the Event Log

The Event Log displays a list of current and historical events and information about each event.

To display the Event Log:

1. Select **Faults > Event Log**. The Event Log opens. For a description of the information provided in the Event Log, see Table 81 Event Log Information.
2. To export the Event Log to a CSV file, click **Export to CSV** in the lower right corner of the Event Log page.

Figure 303 Event Log



Microwave radio: Event Log

Event Log

# ▲	Time	Sequence Number	Severity	State	Description	User Text	Origin
1	01-04-2000 01:01:46	317	△	Cleared (1)	RFU RX level out of range		Radio: Slot 1, Port 1
2	01-04-2000 01:01:31	316	△	Raised	RFU RX level out of range		Radio: Slot 1, Port 1
3	01-04-2000 01:01:31	315	▲	Raised	Radio loss of frame		Radio: Slot 1, Port 1
4	01-04-2000 01:01:30	314	△	Event	RFU TX Mute (Constant.)		0
5	01-04-2000 01:01:30	313	△	Raised	RFU TX Mute		Radio: Slot 1, Port 1
6	01-04-2000 01:01:24	312	▲	Raised	Loss of Carrier		Ethernet: Slot 1, Port 7
7	01-04-2000 01:01:19	311	▲	Event	Change in system reference clock quality level; new quality: g.813		Unit
8	01-04-2000 00:58:20	310	△	Event	Demo mode is started		Slot 1
9	01-04-2000 00:58:20	309	△	Raised	Demo mode is active		Slot 1
10	29-03-2000 06:57:51	308	▲	Raised	Radio loss of frame		Radio: Slot 1, Port 1
11	29-03-2000 06:57:51	307	△	Event	RFU TX Mute (Constant.)		0
12	29-03-2000 06:57:51	306	△	Raised	RFU TX Mute		Radio: Slot 1, Port 1
13	29-03-2000 06:57:45	305	▲	Raised	Loss of Carrier		Ethernet: Slot 1, Port 7
14	29-03-2000 06:57:40	304	▲	Event	Change in system reference clock quality level; new quality: g.813		Unit
15	29-03-2000 06:54:41	303	△	Event	Demo mode is started		Slot 1
16	29-03-2000 06:54:41	302	△	Raised	Demo mode is active		Slot 1
17	29-03-2000 03:16:41	301	▲	Raised	Radio loss of frame		Radio: Slot 1, Port 1
18	29-03-2000 03:16:41	300	△	Event	RFU TX Mute (Constant.)		0
19	29-03-2000 03:16:41	299	△	Raised	RFU TX Mute		Radio: Slot 1, Port 1
20	29-03-2000 03:16:34	298	▲	Raised	Loss of Carrier		Ethernet: Slot 1, Port 7
21	29-03-2000 03:16:29	297	▲	Event	Change in system reference clock quality level; new		Unit

Page Refresh Interval (Seconds) None

Last Loaded: 10:26:39

Table 81 Event Log Information

Parameter	Definition
Time	The date and time the event was triggered.
Sequence Number (#)	A unique sequence number assigned to the event by the system.
Severity	The severity of the event. In the Event Log table, the severity is indicated by a symbol. You can display a textual description of the severity by holding the cursor over the symbol. **Note:** You can edit the severity of event types in the Alarm Configuration page. See Editing Alarm Text and Severity.
State	Indicates whether the event is currently raised or has been cleared.
Description	A system-defined description of the event.

Parameter	Definition
User Text	Additional text that has been added to the system-defined description of the event by users. **Note:** You can add user text to events in the Alarm Configuration page. See Editing Alarm Text and Severity.
Origin	The module that generated the event.

Editing Alarm Text and Severity | Disabling Alarms and Event

You can view a list of alarm types, edit the severity level assigned to individual alarm types, and add additional descriptive text to individual alarm types.

This section includes:

Displaying Alarm Information

Viewing the Probable Cause and Corrective Actions for an Alarm Type

Editing an Alarm Type and Disabling Alarms and Events

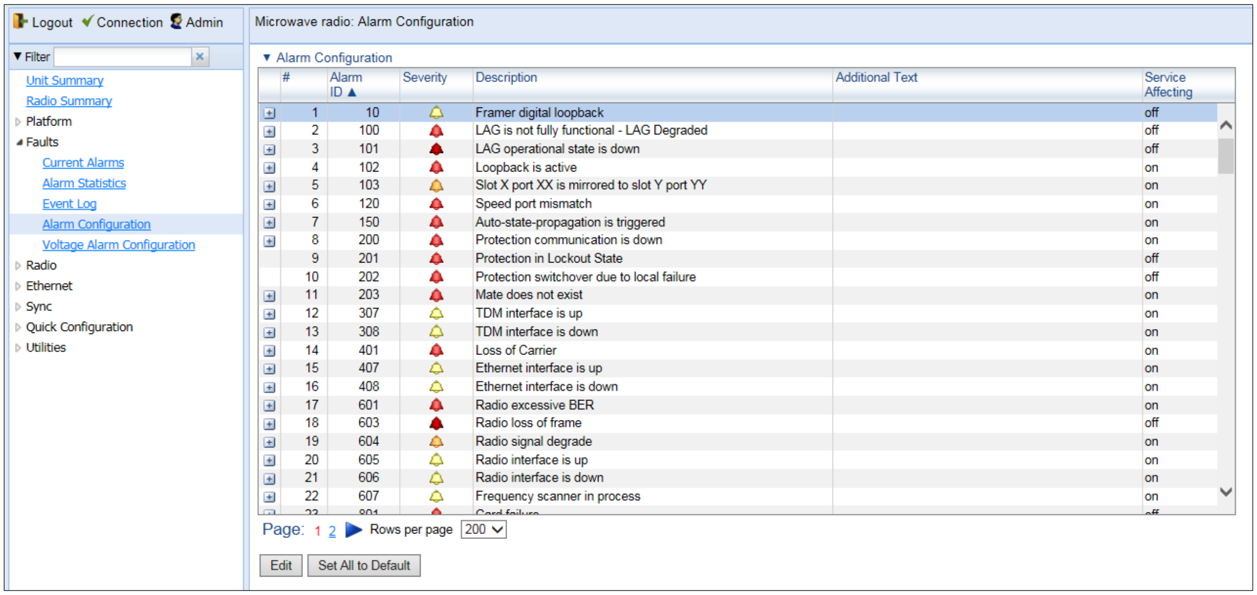
Setting Alarms to their Default Values

Displaying Alarm Information

To view the list of alarms defined in the system:

1. Select **Faults > Alarm Configuration**. The Alarm Configuration page opens. For a description of the information provided in the Alarm Configuration page, see Table 82 Alarm Configuration Page Parameters.

Figure 304 Alarm Configuration Page



Microwave radio: Alarm Configuration

▼ Alarm Configuration

#	Alarm ID ▲	Severity	Description	Additional Text	Service Affecting
1	10	🔔	Framer digital loopback		off
2	100	🔔	LAG is not fully functional - LAG Degraded		off
3	101	🔔	LAG operational state is down		off
4	102	🔔	Loopback is active		on
5	103	🔔	Slot X port XX is mirrored to slot Y port YY		on
6	120	🔔	Speed port mismatch		on
7	150	🔔	Auto-state-propagation is triggered		on
8	200	🔔	Protection communication is down		on
9	201	🔔	Protection in Lockout State		off
10	202	🔔	Protection switchover due to local failure		off
11	203	🔔	Mate does not exist		on
12	307	🔔	TDM interface is up		on
13	308	🔔	TDM interface is down		on
14	401	🔔	Loss of Carrier		on
15	407	🔔	Ethernet interface is up		on
16	408	🔔	Ethernet interface is down		on
17	601	🔔	Radio excessive BER		on
18	603	🔔	Radio loss of frame		off
19	604	🔔	Radio signal degrade		on
20	605	🔔	Radio interface is up		on
21	606	🔔	Radio interface is down		on
22	607	🔔	Frequency scanner in process		on
23	801	🔔	Card failure		off

Page: 1 2 ▶ Rows per page 200

Edit | Set All to Default

Table 82 Alarm Configuration Page Parameters

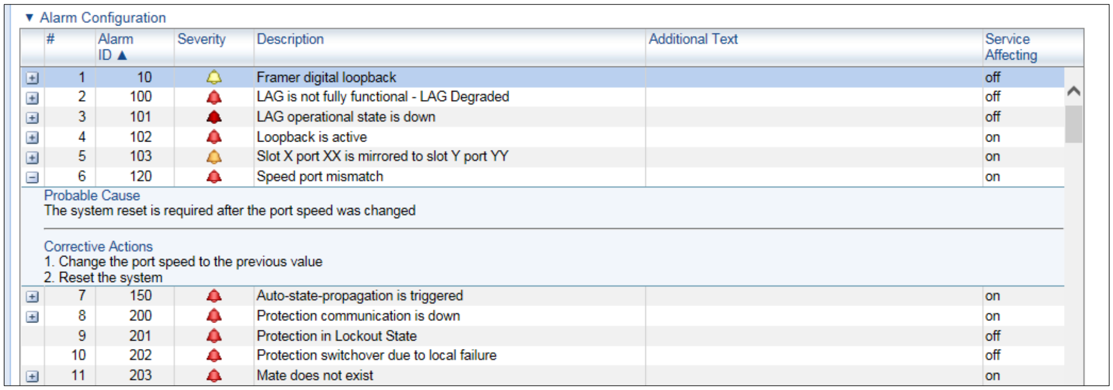
Parameter	Definition
Sequence Number (#)	A unique sequence number assigned to the row by the system.

Parameter	Definition
Alarm ID	A unique ID that identifies the alarm type.
Severity	The severity assigned to the alarm type. You can edit the severity in the Alarm Configuration – Edit page. See Editing an Alarm Type.
Description	A system-defined description of the alarm.
Additional Text	Additional text that has been added to the system-defined description of the alarm by users. You can edit the text in the Alarm Configuration – Edit page. See Editing an Alarm Type.
Service Affecting	Indicates whether the alarm is considered by the system to be service-affecting (**on**) or not (**off**).

Viewing the Probable Cause and Corrective Actions for an Alarm Type

Most alarm types include a system-defined probable cause and suggested corrective actions. To view an alarm type's probable cause and corrective actions, click + on the left side of the alarm type's row in the Alarm Configuration page. The Probable Cause and Corrective Actions appear underneath the alarm type's row, as shown below. If there is no +, that means no Probable Cause and Corrective Actions are defined for the alarm type.

Figure 305 Alarm Configuration Page – Expanded



▼ Alarm Configuration

	#	Alarm ID ▲	Severity	Description	Additional Text	Service Affecting
⊞	1	10	🔔	Framer digital loopback		off
⊞	2	100	🔔	LAG is not fully functional - LAG Degraded		off
⊞	3	101	🔔	LAG operational state is down		off
⊞	4	102	🔔	Loopback is active		on
⊞	5	103	🔔	Slot X port XX is mirrored to slot Y port YY		on
⊟	6	120	🔔	Speed port mismatch		on

Probable Cause
The system reset is required after the port speed was changed

Corrective Actions
1. Change the port speed to the previous value
2. Reset the system

	#	Alarm ID ▲	Severity	Description	Additional Text	Service Affecting
⊞	7	150	🔔	Auto-state-propagation is triggered		on
⊞	8	200	🔔	Protection communication is down		on
	9	201	🔔	Protection in Lockout State		off
	10	202	🔔	Protection switchover due to local failure		off
⊞	11	203	🔔	Mate does not exist		on

Editing an Alarm Type and Disabling Alarms and Events

You can change the severity of an alarm type, and add additional text to the alarm type's description.

You can also choose to disable selected alarms and events. Any alarm or event can be disabled, so that no indication of the alarm is displayed, and no traps are sent for the alarm.

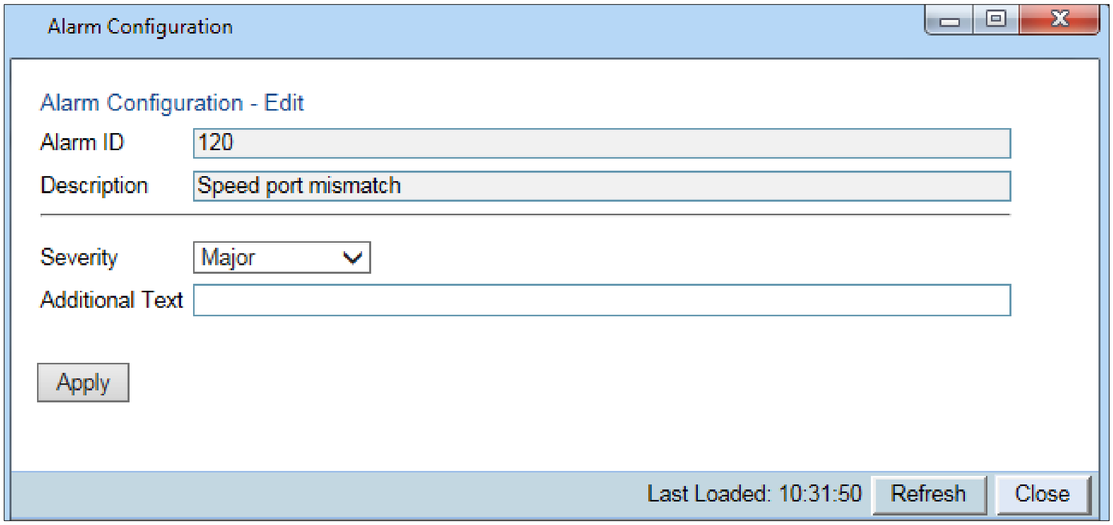
If you disable an alarm that is currently raised, the alarm is treated as if it has been cleared. If an alarm that has been disabled is enabled while it is in a raised state, the alarm is treated as if it has just been raised when it is enabled.

If a timeout for trap generation is configured, and a disabled alarm is enabled while the alarm is raised, the timeout count begins to run when the alarm is enabled. If an alarm is disabled while raised, the timeout count begins to run upon disabling the alarm, and an alarm cleared trap is sent when the timeout expires.

To change the severity of an alarm type and add additional text to the alarm type's description:

1. Select the alarm type in the Alarm Configuration page (Figure 304).
2. Click **Edit**. The Alarm Configuration - Edit page opens.

Figure 306 Alarm Configuration - Edit Page



Alarm ID: 120

Description: Speed port mismatch

Severity: Major

Additional Text:

3. Modify the **Severity** and/or **Additional Text** fields.
4. Click **Apply**, then **Close**.

Setting Alarms to their Default Values

To set all alarms to their default severity levels and text descriptions, click **Set All to Default** in the Alarm Configuration page (Figure 304).

Configuring Voltage Alarm Thresholds and Displaying Voltage PMs

You can configure undervoltage and overvoltage alarm thresholds and display voltage PMs.

The default thresholds for PTP 850E are:

- Undervoltage Raise Threshold: 36V
- Undervoltage Clear Threshold: 38V
- Overvoltage Raise Threshold: 60V
- Overvoltage Clear Threshold: 58V

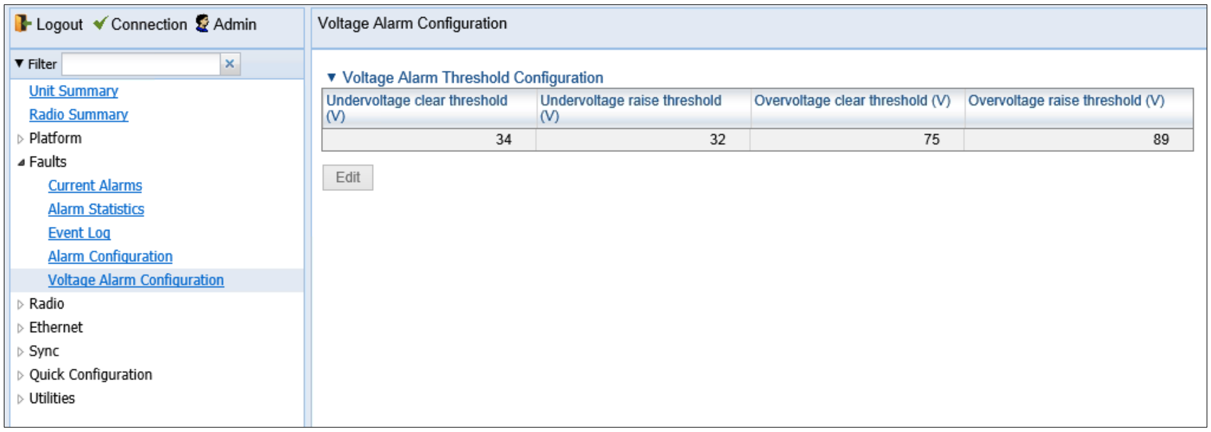
These thresholds determine when the following alarms are raised and cleared:

- Alarm #32000: Under voltage
- Alarm #32001: Over voltage

To configure voltage alarm thresholds:

1 Select **Faults > Voltage Alarm Configuration.** The Voltage Alarm Configuration page opens.

> **Note**
>
> You can also open the Voltage Alarm Configuration page by selecting **Platform > PM & Statistics > Voltage** and clicking **Thresholds**.

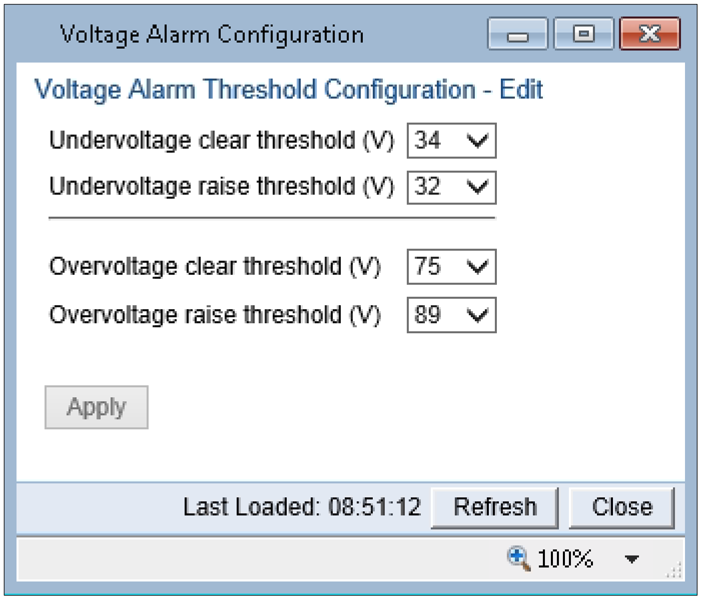


▼ Voltage Alarm Threshold Configuration

Undervoltage clear threshold (V)	Undervoltage raise threshold (V)	Overvoltage clear threshold (V)	Overvoltage raise threshold (V)
34	32	75	89

Figure 307 Voltage Alarm Configuration Page

2 Click **Edit**. The Voltage Alarm Configuration – Edit page opens.



Voltage Alarm Threshold Configuration - Edit

Undervoltage clear threshold (V) 34

Undervoltage raise threshold (V) 32

Overvoltage clear threshold (V) 75

Overvoltage raise threshold (V) 89

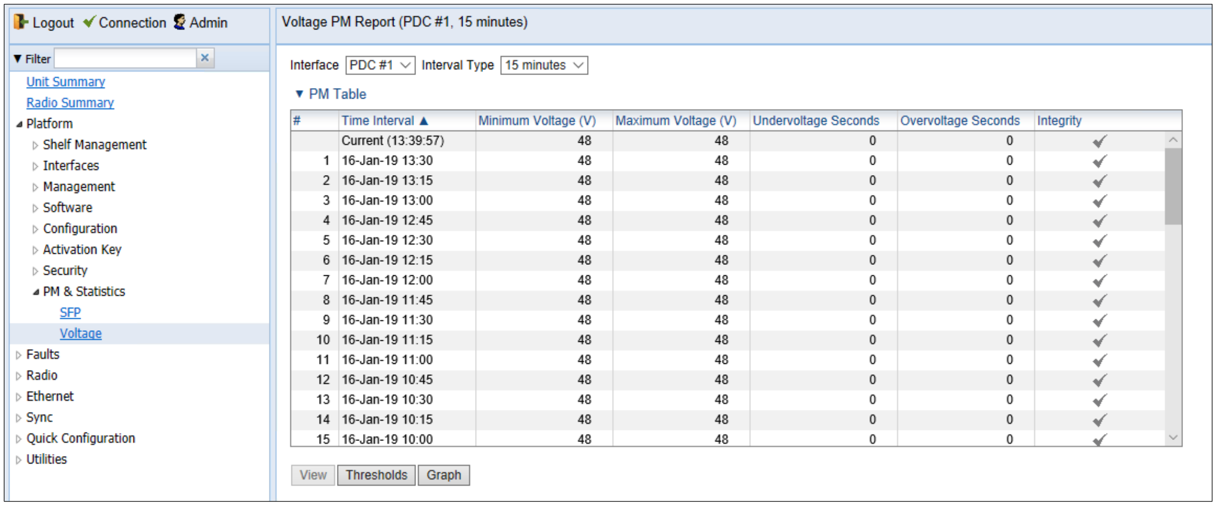
Figure 308 Voltage Alarm Configuration – Edit Page

3 Select the thresholds you want in the **Undervoltage clear threshold (V)**, **Undervoltage raise threshold (V)**, **Overvoltage clear threshold (V)**, and **Overvoltage raise threshold (V)** fields. The configurable values for these thresholds are 0-100V.

4 Click **Apply**.

To display voltage PMs:

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



Voltage PM Report (PDC #1, 15 minutes)

Interface PDC #1 Interval Type 15 minutes

▼ PM Table

#	Time Interval ▲	Minimum Voltage (V)	Maximum Voltage (V)	Undervoltage Seconds	Overvoltage Seconds	Integrity
	Current (13:39:57)	48	48	0	0	✓
1	16-Jan-19 13:30	48	48	0	0	✓
2	16-Jan-19 13:15	48	48	0	0	✓
3	16-Jan-19 13:00	48	48	0	0	✓
4	16-Jan-19 12:45	48	48	0	0	✓
5	16-Jan-19 12:30	48	48	0	0	✓
6	16-Jan-19 12:15	48	48	0	0	✓
7	16-Jan-19 12:00	48	48	0	0	✓
8	16-Jan-19 11:45	48	48	0	0	✓
9	16-Jan-19 11:30	48	48	0	0	✓
10	16-Jan-19 11:15	48	48	0	0	✓
11	16-Jan-19 11:00	48	48	0	0	✓
12	16-Jan-19 10:45	48	48	0	0	✓
13	16-Jan-19 10:30	48	48	0	0	✓
14	16-Jan-19 10:15	48	48	0	0	✓
15	16-Jan-19 10:00	48	48	0	0	✓

Figure 309 Voltage PM Report Page

2. In the **Interface** field, select the power input for which to display PMs.
3. In the **Interval Type** field:
   - To display reports for the past 24 hours, in 15 minute intervals, select **15 minutes**.
   - To display reports for the past month, in daily intervals, select **24 hours**.

Table 83 Voltage PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Minimum Voltage (V)	The lowest voltage during the measured period.
Maximum Voltage (V)	The highest voltage during the measured period.
Undervoltage Seconds	The number of seconds the unit was in an undervoltage state during the measured period.
Overvoltage Seconds	The number of seconds the unit was in an overvoltage state during the measured period.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred during the interval.

Uploading Unit Info

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

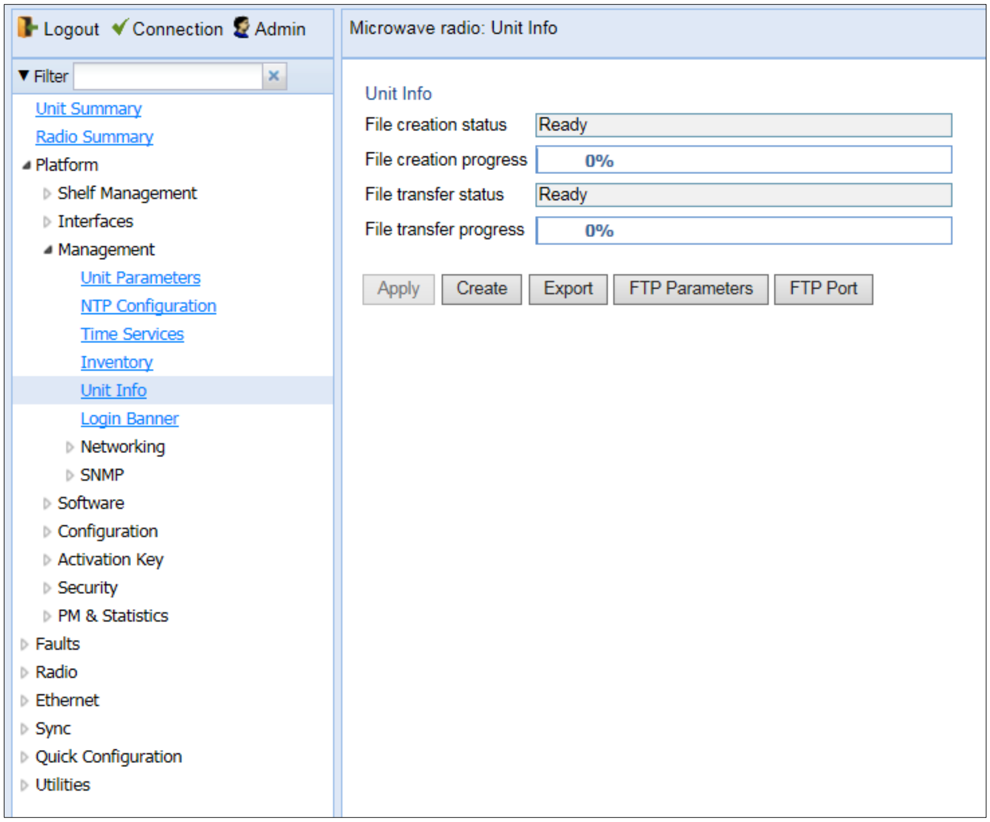
When uploading a Unit Information file, the PTP 850 functions as an FTP or SFTP client. You must install FTP or SFTP server software on the PC or laptop you are using to perform the upload. For details, see Installing and Configuring an FTP or SFTP Server.

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

To generate and upload a Unit Information file:

1. Install and configure an FTP server on the PC or laptop you are using to perform the upload. See Installing and Configuring an FTP or SFTP Server.
2. Select **Platform > Management > Unit Info**. The Unit Info page opens.

Figure 310 Unit Info Page



Microwave radio: Unit Info

Unit Info

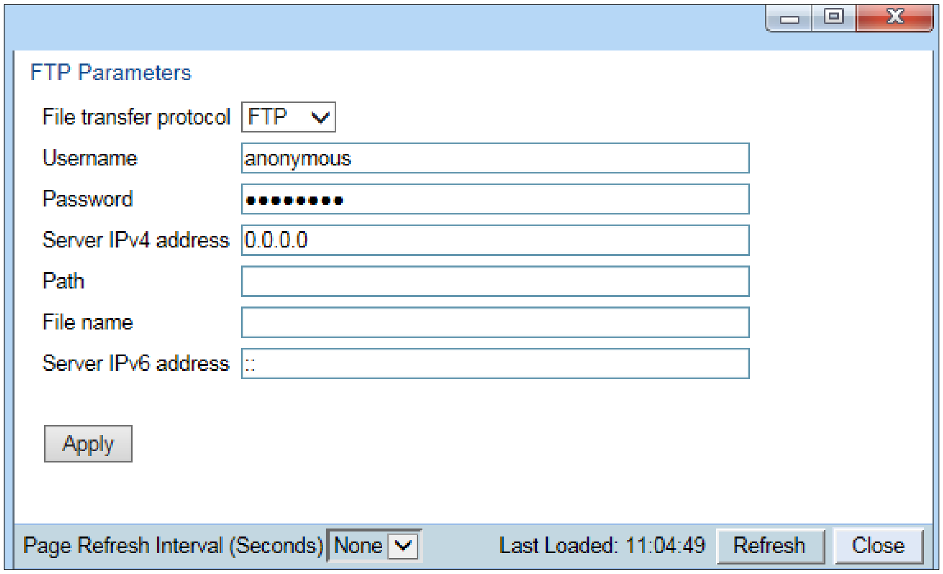
File creation status: Ready

File creation progress: 0%

File transfer status: Ready

File transfer progress: 0%

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



FTP Parameters

File transfer protocol: FTP

Username: anonymous

Password: ••••••••

Server IPv4 address: 0.0.0.0

Path:

File name:

Server IPv6 address: ::

Page Refresh Interval (Seconds): None

Last Loaded: 11:04:49

4. In the **File transfer protocol** field, select the file transfer protocol you want to use (**FTP** or **SFTP**).
5. In the **Username in server** field, enter the user name you configured in the FTP server.
6. In the **Password in server** field, enter the password you configured in the FTP server. If you did not configure a password for your FTP user, simply leave this field blank.
7. If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the FTP server in the **Server IPv4 address** field. See Defining the IP Protocol Version for Initiating Communications.
8. If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the FTP server in the **IPv6 Server Address** field. See Defining the IP Protocol Version for Initiating Communications.
9. In the **Path** field, enter the directory path to which you are uploading the file. Enter the path relative to the FTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
10. In the **File Name** field, enter the name you want to give to the exported Unit Information file.
11. Click **Apply** to save your settings.
12. Click **Create** to create the Unit Information file. The following fields display the status of the file creation process:
    - **Unit Info File creation status** – Displays the file creation status. You must wait until the status is Success to upload the file. Possible values are:
    - **Ready** – The default value, which appears when no file is being created.
    - **Generating File** – The file is being generated.
    - **Success** – The file has been successfully created. You may now upload the file.
    - **Failure** – The file was not successfully created.

- **Unit Info File creation progress** – Displays the progress of the current Unit Information file creation operation.

13. Click **Export**. The upload begins. The following fields display the status of the upload process:
    - **File File transfer status** – Displays the status of any pending Unit Information file upload. Possible values are:
    - **Ready** – The default value, which appears when no file transfer is in progress.
    - **File-in-transfer** – The upload operation is in progress.
    - **Success** – The file has been successfully uploaded.
    - **Failure** – The file was not successfully uploaded.

    If you try to export the file before it has been created, the following error message appears: **Error #3-Invalid set value**.

    If this occurs, wait about two minutes then click **Export** again.

    - **File transfer progress** – Displays the progress of the current Unit Information file upload operation.

Performing Diagnostics

This section includes:

- Performing Radio Loopback
- Performing Ethernet Loopback
- Configuring Service OAM (SOAM) Fault Management (FM)

Performing Radio Loopback

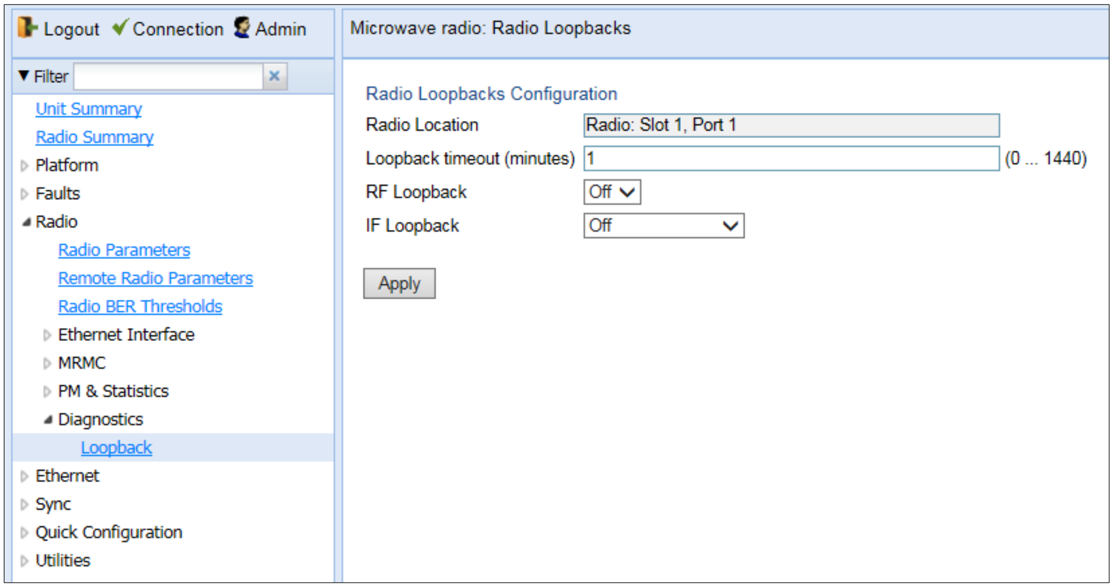
Note

To perform radio loopback, the radio must be set to its maximum TX power.

To perform loopback on a radio:

1. Select **Radio > Diagnostics > Loopback**. The Radio Loopbacks page opens.

Figure 311 Radio Loopbacks Page



Microwave radio: Radio Loopbacks

Radio Loopbacks Configuration

Radio Location: Radio: Slot 1, Port 1

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

RF Loopback: Off

IF Loopback: Off

2. In the **Loopback timeout (minutes)** field, enter the timeout, in minutes, for automatic termination of the loopback (0-1440). A value of 0 indicates that there is no timeout.
3. In the **RF loopback** field, select **On**.

Note

IF Loopback is planned for future release.

4. Click **Apply**.

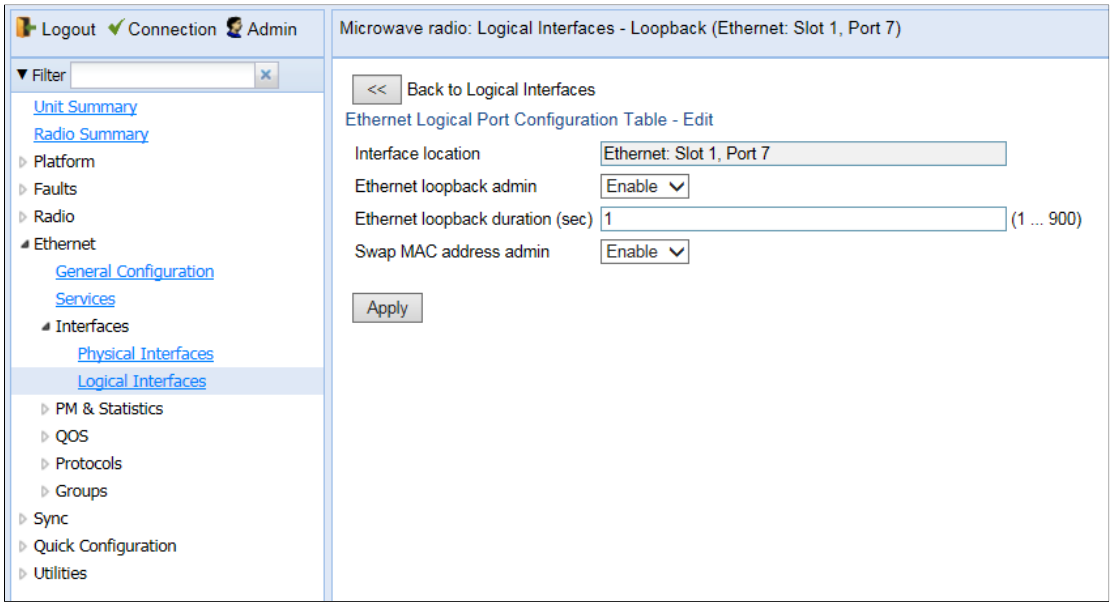
Performing Ethernet Loopback

Ethernet loopbacks can be performed on any logical Ethernet interface except a LAG. When Ethernet loopback is enabled on an interface, the system loops back all packets ingressing the interface. This enables loopbacks to be performed over the link from other points in the network.

To perform Ethernet loopback:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 184).
2. Select an interface in the Ethernet Logical Port Configuration table and click **Loopback**. The Logical Interfaces – Loopback page opens.

Figure 312 Logical Interfaces – Loopback Page



Microwave radio: Logical Interfaces - Loopback (Ethernet: Slot 1, Port 7)

Ethernet Logical Port Configuration Table - Edit

Interface location	Ethernet: Slot 1, Port 7
Ethernet loopback admin	Enable
Ethernet loopback duration (sec)	1 (1 ... 900)
Swap MAC address admin	Enable

3. In the **Ethernet loopback admin** field, select **Enable** to enable Ethernet loopback on the logical interface, or **Disable** to disable Ethernet loopback on the logical interface.
4. In the **Ethernet loopback duration (sec)** field, enter the loopback duration time (in seconds).
5. In the **Swap MAC address admin** field, select whether to swap DA and SA MAC addresses during the loopback. Swapping addresses prevents Ethernet loops from occurring. It is recommended to enable MAC address swapping if LLDP is enabled.
6. Click **Apply** to initiate the loopback.

Configuring Service OAM (SOAM) Fault Management (FM)

This section includes:

- SOAM Overview
- Configuring MDs
- Configuring MA/MEGs

- Configuring MEPs
- Displaying Remote MEPs
- Displaying Last Invalid CCMS
- Configuring MIPs with MHF Default
- Performing Loopback

SOAM Overview

The Y.1731 standards and the MEF-30 specifications define Service OAM (SOAM). SOAM is concerned with detecting, isolating, and reporting connectivity faults spanning networks comprising multiple LANs, including LANs other than IEEE 802.3 media.

Y.1731 Ethernet FM (Fault Management) consists of three protocols that operate together to aid in fault management:

- Continuity check
- Link trace
- Loopback

Note

Link trace is planned for future release.

PTP 850 utilizes these protocols to maintain smooth system operation and non-stop data flow.

The following are the basic building blocks of FM:

MD (Maintenance Domain) – An MD defines the management space on a network, typically owned and operated by a single entity, for which connectivity faults are managed via SOAM.

MA/MEG (Maintenance Association/Maintenance Entity Group) – An MA/MEG contains a set of MEPs or MIPs.

MEP (MEG End Points) – Each MEP is located on a service point of an Ethernet service at the boundary of the MEG. By exchanging CCMs (ContinuityCheck Messages), local and remote MEPs have the ability to detect the network status, discover the MAC address of the remote unit/port where the peer MEP is defined, and identify network failures.

MIP (MEG Intermediate Points) – Similar to MEPs, but located inside the MEG and can only respond to, not initiate, CCM messages.

CCM (Continuity Check Message) – MEPs in the network exchange CCMs with their peers at defined intervals. This enables each MEP to detect loss of connectivity or failure in the remote MEP.

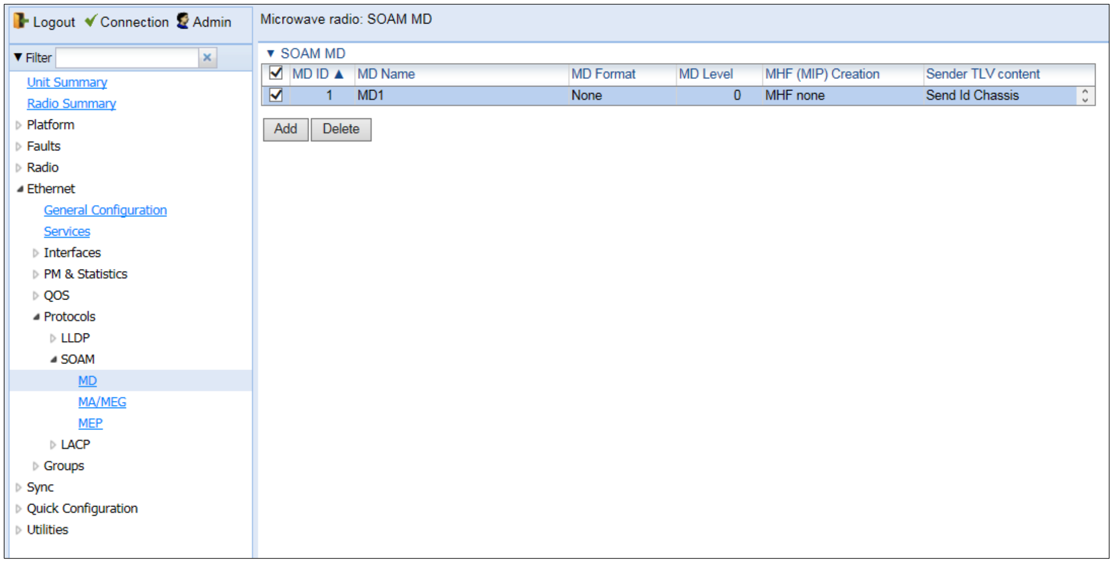
Configuring MDs

In the current release, you can define one MD, with an **MD Format** of **None**.

To add an MD:

1. Select **Ethernet** > **Protocols** > **SOAM** > **MD**. The SOAM MD page opens.

Figure 313 SOAM MD Page



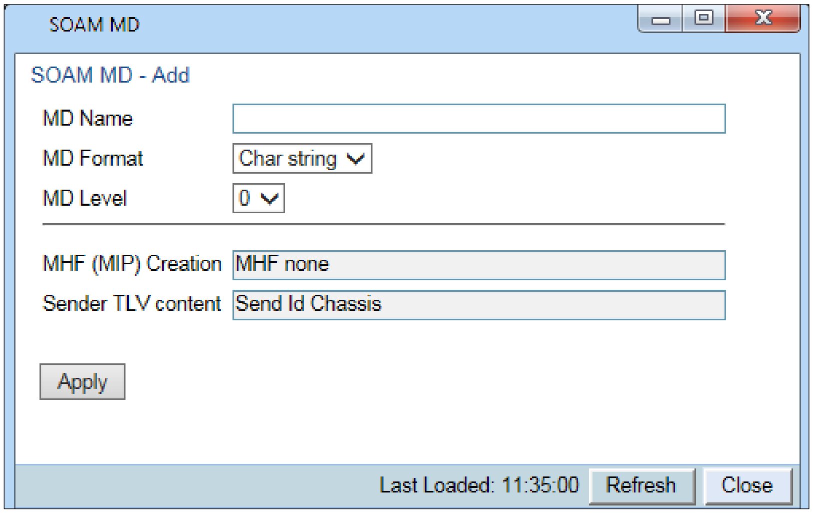
Microwave radio: SOAM MD

SOAM MD

☑	MD ID ▲	MD Name	MD Format	MD Level	MHF (MIP) Creation	Sender TLV content
☑	1	MD1	None	0	MHF none	Send Id Chassis

2. Click **Add**. The SOAM MD – Add page opens.

Figure 314 SOAM MD Page



SOAM MD - Add

MD Name

MD Format: Char string

MD Level: 0

MHF (MIP) Creation: MHF none

Sender TLV content: Send Id Chassis

Last Loaded: 11:35:00

3. In the **MD Name** field, enter an identifier for the MD (up to 43 alphanumeric characters). The MD Name should be unique over the domain.

4. In the **MD Format** field, select **None**.

> **Note**
>
> Support for MDs with the MD format Character String is planned for future release. In this release, the software enables you to configure such MDs, but they have no function.

5. In the **MD Level** field, select the maintenance level of the MD (1-7). The maintenance level ensures that the CFM frames for each domain do not interfere with each other. Where domains are nested, the encompassing domain must have a higher level than the domain it encloses. The maintenance level is carried in all CFM frames that relate to that domain. The **MD Level** must be the same on both sides of the link.

> **Note**
>
> In the current release, the MD level is not relevant to the SOAM functionality.

6. Click **Apply**, then **Close**.

The **MHF (MIP) Creation** field displays the contents of MHF format included in the CCMs sent in this MD (in the current release, this is **MHF none** and **MHF default**).

The **Sender TLV Content** field displays the contents of TLVs included in the CCMs sent in this MD (in the current release, this is only **Send ID Chassis**).

Configuring MA/MEGs

You can configure up to 64 MEP pairs per network element:

Fast MEGs have a CCM interval of 1 second.

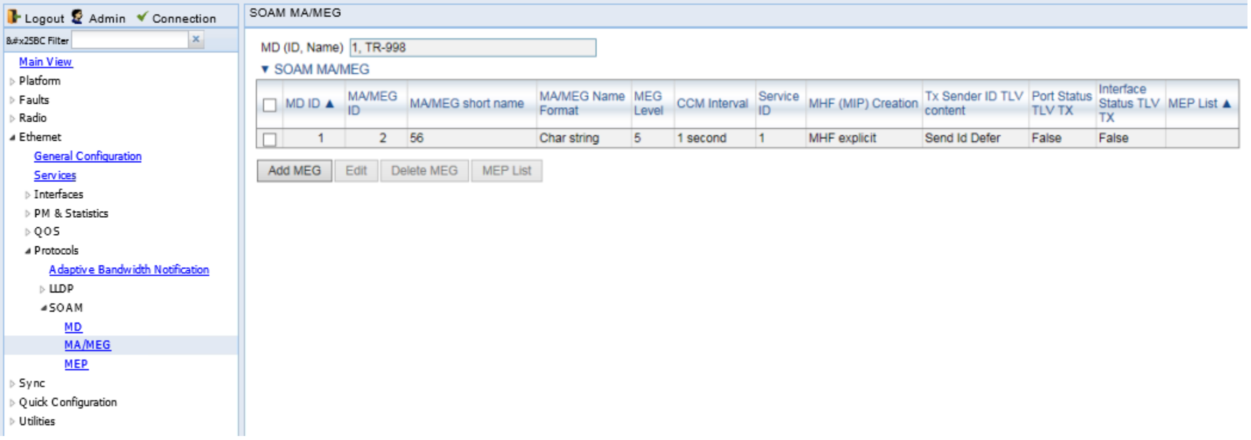
Slow MEGs have a CCM interval of 10 seconds, 1 minute, or 10 minutes.

You can configure up to 32 MEP pairs per network element.

To add a MEG:

1. Select **Ethernet > Protocols > SOAM > MA/MEG**. The SOAM MA/MEG page opens.

Figure 315 SOAM MA/MEG Page



SOAM MA/MEG

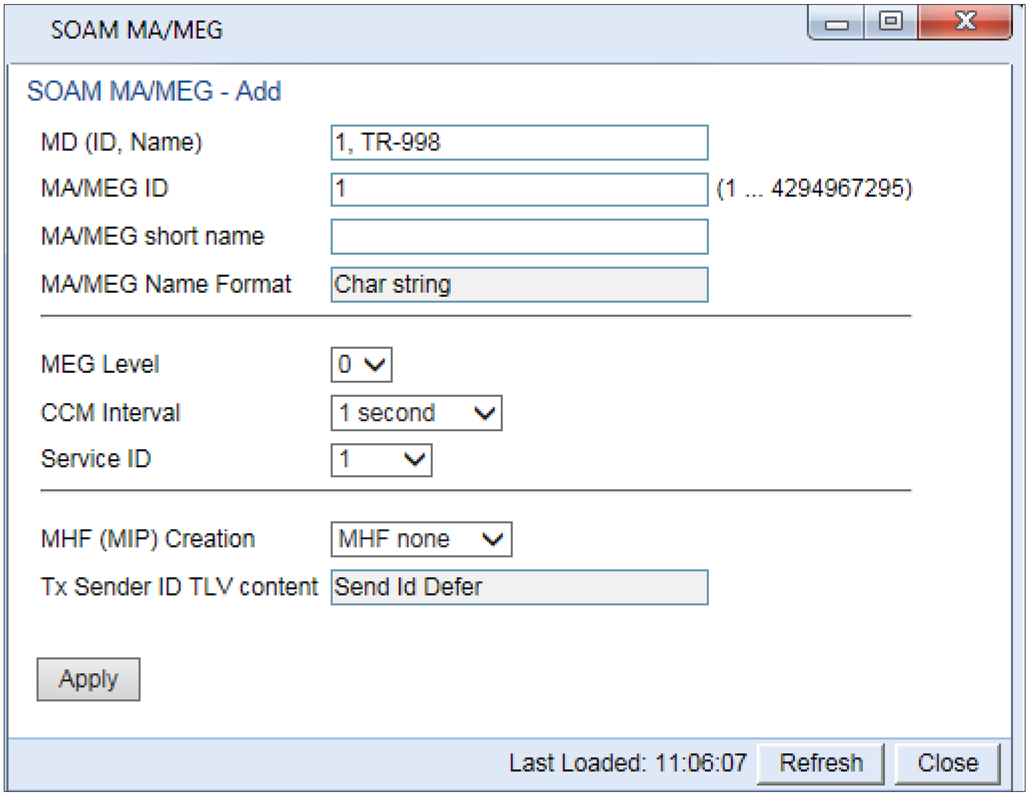
MD (ID, Name) 1, TR-998

▼ SOAM MA/MEG

□	MD ID ▲	MA/MEG ID	MA/MEG short name	MA/MEG Name Format	MEG Level	CCM Interval	Service ID	MHF (MIP) Creation	Tx Sender ID TLV content	Port Status TLV TX	Interface Status TLV TX	MEP List ▲
□	1	2	56	Char string	5	1 second	1	MHF explicit	Send Id Defer	False	False	

2. Click **Add MEG**. The SOAM MA/MEG – Add page opens.

Figure 316 SOAM MA/MEG – Add Page



SOAM MA/MEG

SOAM MA/MEG - Add

MD (ID, Name)	1, TR-998
MA/MEG ID	1 (1 ... 4294967295)
MA/MEG short name	
MA/MEG Name Format	Char string
MEG Level	0
CCM Interval	1 second
Service ID	1
MHF (MIP) Creation	MHF none
Tx Sender ID TLV content	Send Id Defer

Last Loaded: 11:06:07

3. Configure the fields described in *Table 84*.
4. Click **Apply**, then **Close**.

Table 85 describes the status (read-only) fields in the SOAM MA/MEG Component table.

Table 84 SOAM MA/MEG Configuration Parameters

Parameter	Definition
MD (ID, Name)	Select the MD to which you are assigning the MEP.
MA/MEG ID	Automatically generated by the system. You can change this value.
MA/MEG short name	Enter a name for the MEG (up to 44 alphanumeric characters).

Parameter	Definition
MEG Level	Select a MEG level (0-7). The MEG level must be the same for MEGs on both sides of the link. Higher levels take priority over lower levels. If MEGs are nested, the OAM flow of each MEG must be clearly identifiable and separable from the OAM flows of the other MEGs. In cases where the OAM flows are not distinguishable by the Ethernet layer encapsulation itself, the MEG level in the OAM frame distinguishes between the OAM flows of nested MEGs. Eight MEG levels are available to accommodate different network deployment scenarios. When customer, provider, and operator data path flows are not distinguishable based on means of the Ethernet layer encapsulations, the eight MEG levels can be shared among them to distinguish between OAM frames belonging to nested MEGs of customers, providers and operators. The default MEG level assignment among customer, provider, and operator roles is: • The customer role is assigned MEG levels 6 and 7. • The provider role is assigned MEG levels 3 through 5. • The operator role is assigned MEG levels: 0 through 2. The default MEG level assignment can be changed via a mutual agreement among customer, provider, and/or operator roles. The number of MEG levels used depends on the number of nested MEs for which the OAM flows are not distinguishable based on the Ethernet layer encapsulation.
CCM Interval	The interval at which CCM messages are sent within the MEG. Options are: • 1 second (default) • 10 seconds • 1 minute • 10 minutes It takes a MEP 3.5 times the CCM interval to determine a change in the status of its peer MEP. For example, if the CCM interval is 1 second, a MEP will detect failure of the peer 3.5 seconds after it receives the first CCM failure message. If the CCM interval is 10 minutes, the MEP will detect failure of the peer 35 minutes after it receives the first CCM failure message.
Service ID	Select an Ethernet service to which the MEG belongs. You must define the service and add service points before you configure the MEG.

Parameter	Definition
MHF (MIP) Creation	Determines whether MIPs are created on the MEG. Options are: • MHF none – No MIPs are created. • MHF default – MIPs are created automatically on any service point in the MEG's Ethernet service. • MHF explicit – MIPs are created on the service points of the MEG when a lower-level MEP exists on the service point. This option is usually used when the operator's domain is encompassed by another domain. MHF defer – No MIPs are created. Not used in the current release.

Table 85 SOAM MA/MEG Status Parameters

Parameter	Definition
MA/MEG Name Format	Reserved for future use. In the current release, this is Char String only.
Tx Sender ID TLV content	Reserved for future use. Sender ID TLV is not transmitted.
Port Status TLV TX	Reserved for future use. No Port Status TLV is transmitted in the CCM frame.
Interface Status TLV TX	Reserved for future use. No Interface Status TLV is transmitted in the CCM frame.
MEP List	Lists all local and remote MEPs that have been defined for the MEG.

Configuring MEPs

Each MEP is attached to a service point in an Ethernet service. The service and service point must be configured before you configure the MEP. See Configuring Ethernet Service(s).

Each MEP inherits the same VLAN, C-VLAN, or S-VLAN configuration as the service point on which it resides. See Configuring Service Points (CLI).Configuring Service Points

In order to set the VLAN used by CCM/LBM/LTM if the service point is defined ambiguously (for example PIPE, Bundle-C, Bundle-S, or All-to-One), the service point's C-VLAN/S-VLAN parameter should not be set to N.A.

To configure a MEP, you must:

1. Add MEPs to the relevant MA/MEG. In this stage, you add both local and remote MEPs. The only thing you define at this point is the MEP ID. See Adding Local and Remote MEPs.
2. Configure the local MEPs. At this point, you determine which MEPs are local MEPs. The system automatically defines the other MEPs you configured in the previous step as remote MEPs. See Configuring the Local MEPs.

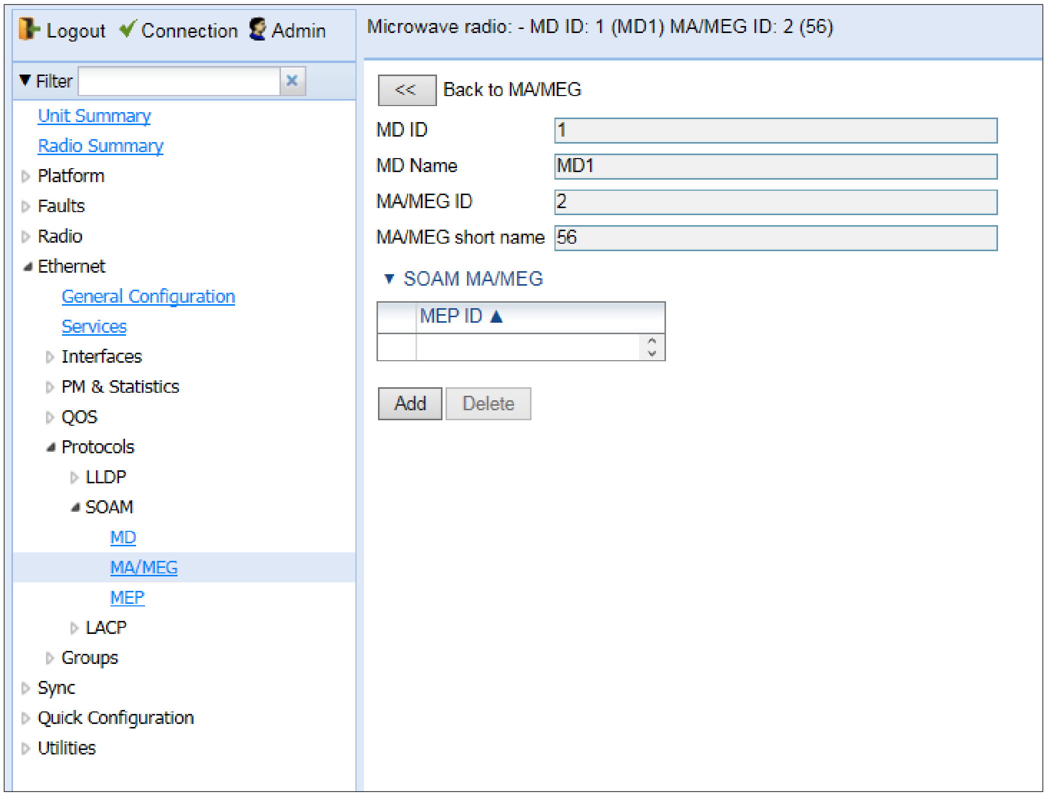
3. Enable the Local MEPs. See Enabling Local MEPs.

Adding Local and Remote MEPs

To add a MEP to the MA/MEG:

1. In the SOAM MA/MEG page, select a MA/MEG and click **MEP List**. The MEP List page opens.

Figure 317 MEP List Page

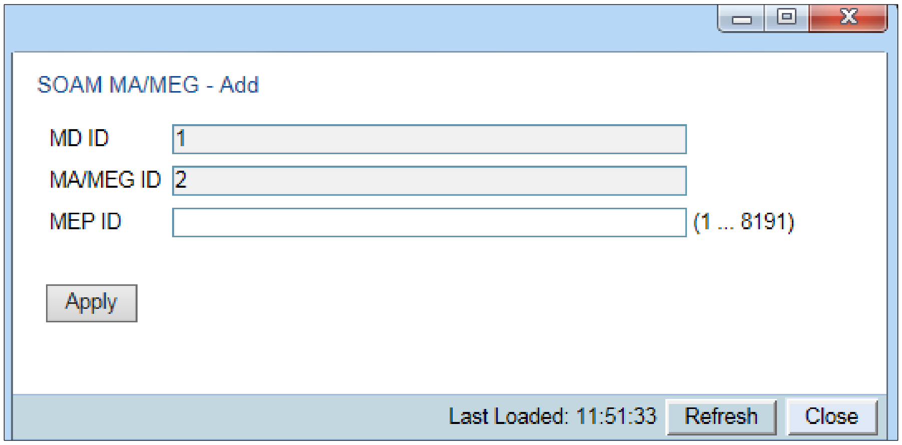


Microwave radio: - MD ID: 1 (MD1) MA/MEG ID: 2 (56)

MD ID	1
MD Name	MD1
MA/MEG ID	2
MA/MEG short name	56

2. Click **Add**. The Add MEP page opens.

Figure 318 Add MEP Page



SOAM MA/MEG - Add

MD ID	1	
MA/MEG ID	2	
MEP ID		(1 ... 8191)

Last Loaded: 11:51:33

3. In the **MEP ID** field, enter a MEP ID (1-8191).

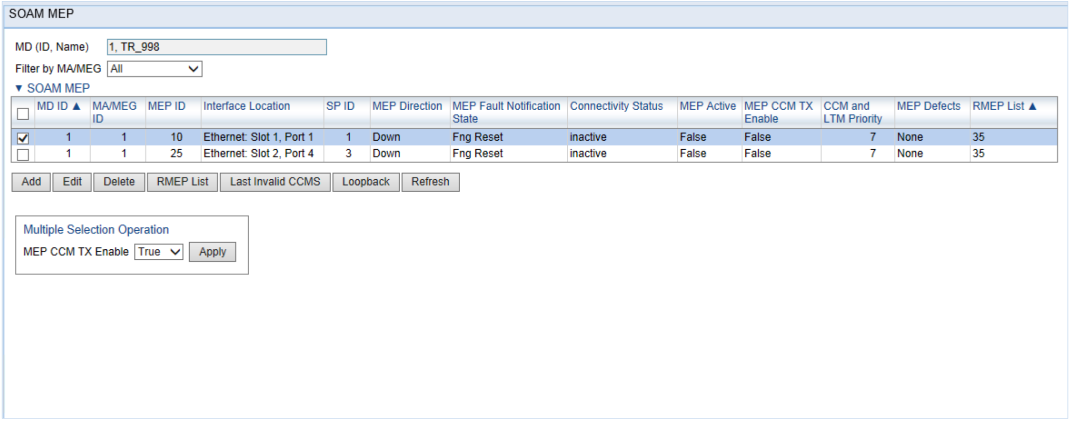
4. Click **Apply**, then **Close**.

Configuring the Local MEPs

Once you have added local and remote MEPs, you must define the MEPs and determine which are the local MEPs:

1. Select **Ethernet > Protocols > SOAM > MEP**. The SOAM MEP page opens. Table 86 lists and describes the parameters displayed in the SOAM MEP page.

Figure 319 SOAM MEP Page



SOAM MEP

MD (ID, Name) 1, TR_998

Filter by MA/MEG All

▼ SOAM MEP

□	MD ID ▲	MA/MEG ID	MEP ID	Interface Location	SP ID	MEP Direction	MEP Fault Notification State	Connectivity Status	MEP Active	MEP CCM TX Enable	CCM and LTM Priority	MEP Defects	RMEP List ▲
☑	1	1	10	Ethernet: Slot 1, Port 1	1	Down	Fng Reset	inactive	False	False	7	None	35
□	1	1	25	Ethernet: Slot 2, Port 4	3	Down	Fng Reset	inactive	False	False	7	None	35

Multiple Selection Operation

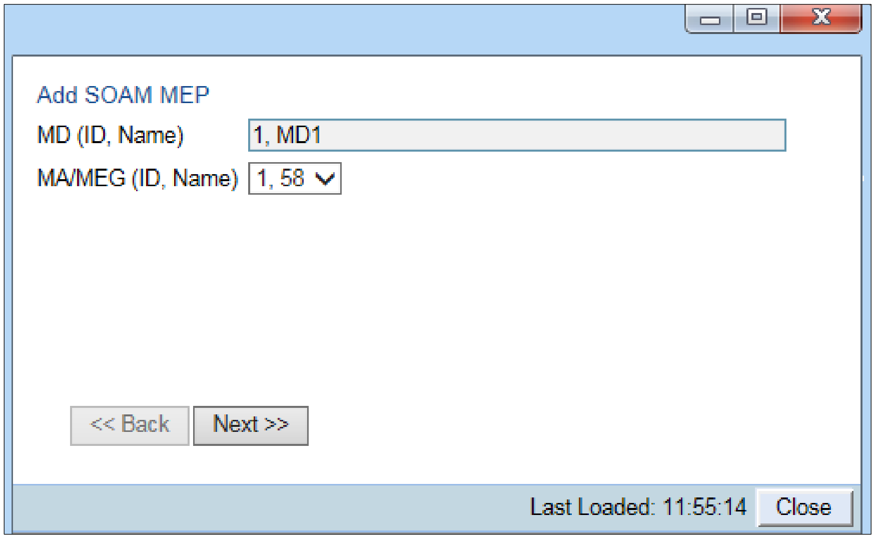
MEP CCM TX Enable True

Note

To display MEPs belonging to a specific MEG, select the MEG in the **Filter by MA/MEG** field near the top of the SOAM MEP page. To display all MEPs configured for the unit, select **All**.

2. Click **Add.** Page 1 of the Add SOAM MEP wizard opens.

Figure 320 Add SOAM MEP Wizard – Page 1



Add SOAM MEP

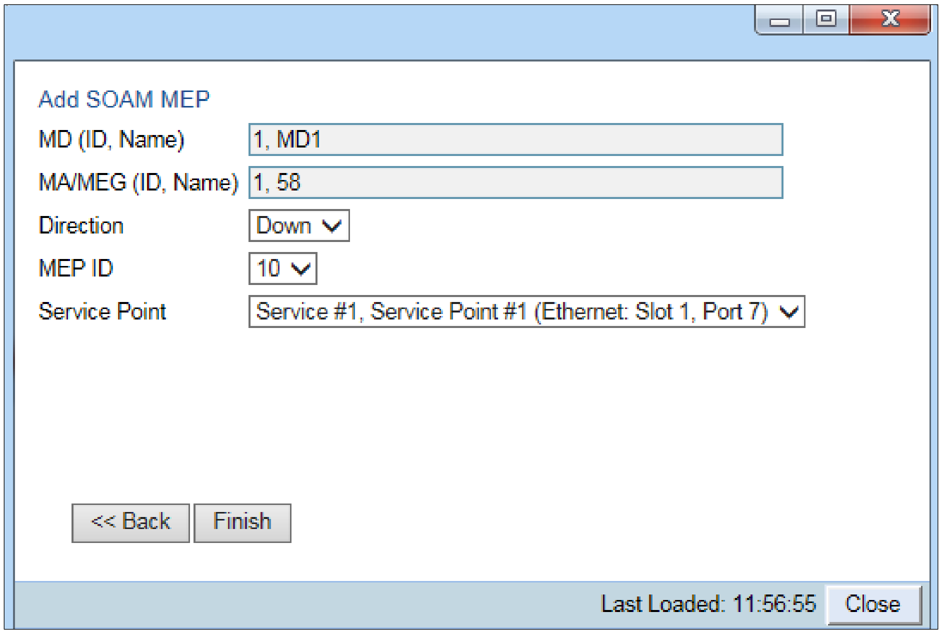
MD (ID, Name) 1, MD1

MA/MEG (ID, Name) 1, 58

Last Loaded: 11:55:14

3. In the **MEG Name** field, select an MA/MEG.
4. Click **Next.** Page 2 of the Add SOAM MEP wizard opens.

Figure 321 Add SOAM MEP Wizard – Page 2



Add SOAM MEP

MD (ID, Name) 1, MD1

MA/MEG (ID, Name) 1, 58

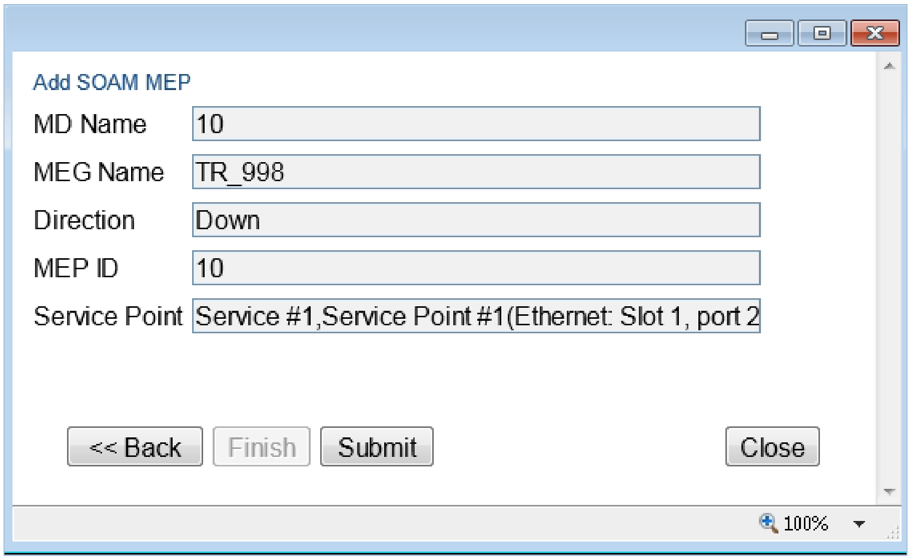
Direction Down

MEP ID 10

Service Point Service #1, Service Point #1 (Ethernet: Slot 1, Port 7)

5. In the **Direction** field, select **Up** or **Down**.
6. In the **MEP ID** field, select a MEP ID from the list of MEPs you have added to the selected MEG.
7. In the **Service Point** field, select the service point on which you want to place the MEP.
8. Click **Finish**. The Add SOAM MEP wizard displays the parameters you have selected.

Figure 322 Add SOAM MEP Wizard –Summary Page



Add SOAM MEP

MD Name 10

MEG Name TR_998

Direction Down

MEP ID 10

Service Point Service #1,Service Point #1(Ethernet: Slot 1, port 2

9. Verify that you want to submit the displayed parameters and click **Submit**.

Table 86 SOAM MEP Parameters

Parameter	Definition
MD (ID, Name)	The MD ID and name are automatically generated by the system.

Parameter	Definition
MA/MEG (ID, Name)	The MA/MEG ID and name are automatically generated by the system.
MEP ID	The MEP ID.
Interface Location	The interface on which the service point associated with the MEP is located.
SP ID	The service point ID.
MEP Direction	**Up** or **Down**.
MEP Fault Notification State	The initial Indicates the status of the defect SOAM state machine. Possible values are: **Fng Reset** – Initial state. **Fng Defect** – Transient state when a defect is detected. **Fng Defect Reported** – The defect state is steady (stable). **Fng Defect Clearing** – Transient state when a defect is in the process of being cleared. **Fng Defect Cleared** – The defect has been cleared (Transient state).
Connectivity Status	Indicates whether a MEP can exchange PDU (CCM, Loopback, LTR) with its remote MEP. A MEP with some defect or an inactive MEP cannot exchange PDUs. Possible values are: **inactive** – At least one of the MEPremote MEPs is enabled (**True**).in rMEPFailed status (not discovered). **active** – All remote MEPs are discovered correctly and have an rMEPOk status.
MEP Active	Indicates whether the MEP is enabled (**True**) or disabled (**False**).
MEP CCM TX Enable	Indicates whether the MEP is sending CCMs (**True/False**).
CCM and LTM Priority	The p-bit included in CCMs and/or LTM frames sent by this MEP (0 to 7).
MEP Defects	Indicates if a defect has been detected by the MEP level.
RMEP List	Once you have configured at least one local MEP, all other MEPs that you have added but not configured as local MEPs are displayed here, and are considered to be remote MEPs.

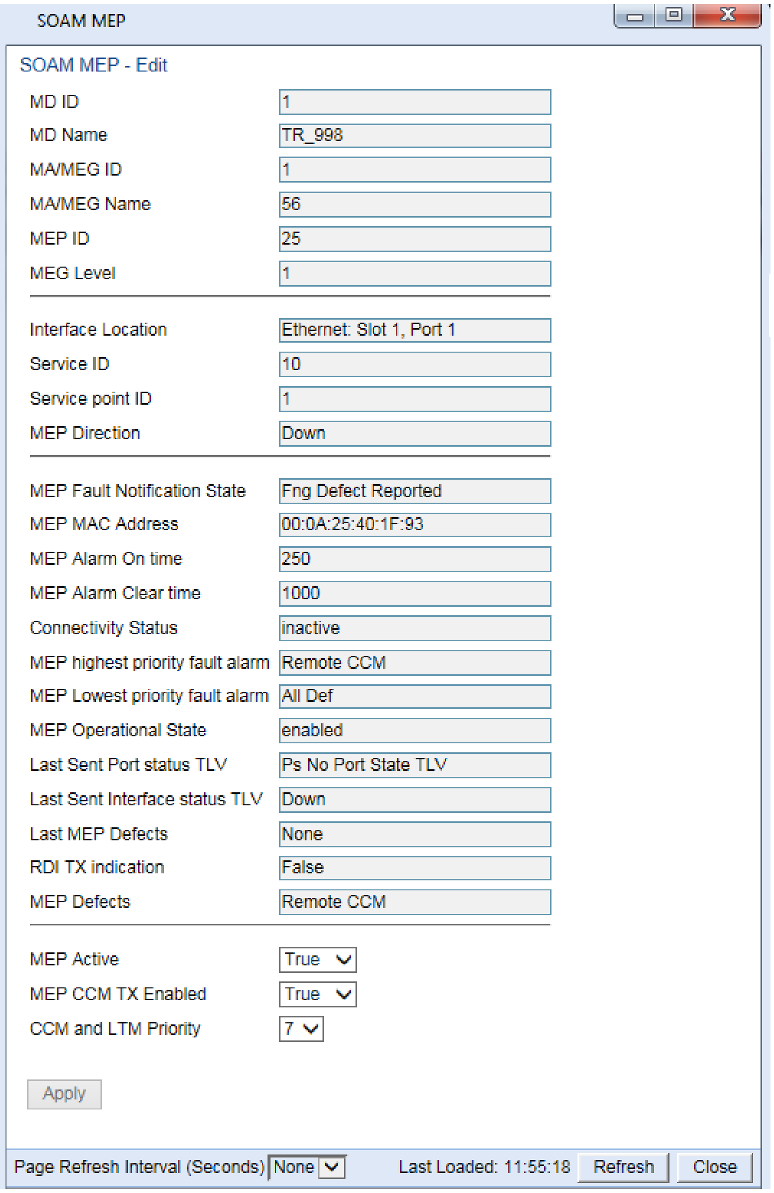
Enabling Local MEPs

Once you have added a MEP and defined it as a local MEP, you must enable the MEP.

To enable a MEP:

1. In the SOAM MEP page (Figure 319), select the MEP you want to enable.
2. Click **Edit**. The SOAM MEP - Edit page opens.

Figure 323 SOAM MEP - Edit Page



SOAM MEP

SOAM MEP - Edit

MD ID	1
MD Name	TR_998
MA/MEG ID	1
MA/MEG Name	56
MEP ID	25
MEG Level	1
Interface Location	Ethernet: Slot 1, Port 1
Service ID	10
Service point ID	1
MEP Direction	Down
MEP Fault Notification State	Fng Defect Reported
MEP MAC Address	00:0A:25:40:1F:93
MEP Alarm On time	250
MEP Alarm Clear time	1000
Connectivity Status	inactive
MEP highest priority fault alarm	Remote CCM
MEP Lowest priority fault alarm	All Def
MEP Operational State	enabled
Last Sent Port status TLV	Ps No Port State TLV
Last Sent Interface status TLV	Down
Last MEP Defects	None
RDI TX indication	False
MEP Defects	Remote CCM
MEP Active	True
MEP CCM TX Enabled	True
CCM and LTM Priority	7

Page Refresh Interval (Seconds) None

Last Loaded: 11:55:18

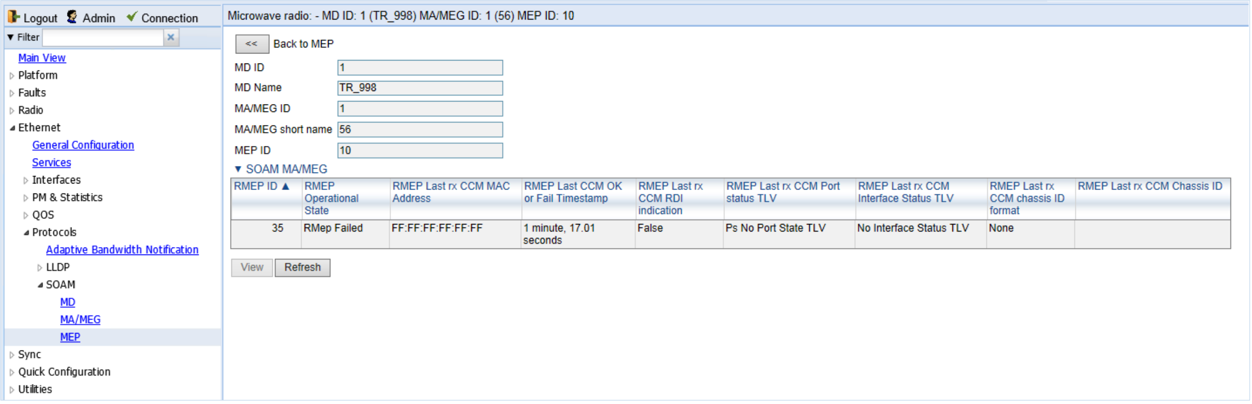
3. In the **MEP Active** field, select **True**.
4. In the **MEP CCM TX Enable** field, select **True**.
5. In the **CCM and LTM Priority** field, select the p-bit that will be included in CCMs sent by this MEP (0 to 7). It is recommended to select 7.
6. Click **Apply**, then **Close**.

Displaying Remote MEPs

To display a list of remote MEPs (RMEPs) and their parameters:

1. Select **Ethernet > Protocols > SOAM > MEP**. The SOAM MEP page opens (Figure 319).
2. Select a MEP and click **RMEP List**. The SOAM MEP DB table is displayed.

Figure 324 SOAM MEP DB Table



Microwave radio: - MD ID: 1 (TR_998) MA/MEG ID: 1 (56) MEP ID: 10

MD ID: 1
MD Name: TR_998
MA/MEG ID: 1
MA/MEG short name: 56
MEP ID: 10

RMEP ID ▲	RMEP Operational State	RMEP Last rx CCM MAC Address	RMEP Last CCM OK or Fail Timestamp	RMEP Last rx CCM RDI indication	RMEP Last rx CCM Port status TLV	RMEP Last rx CCM Interface Status TLV	RMEP Last rx CCM chassis ID format	RMEP Last rx CCM Chassis ID
35	RMep Failed	FF:FF:FF:FF:FF:FF	1 minute, 17.01 seconds	False	Ps No Port State TLV	No Interface Status TLV	None	

Table 87 lists and describes the parameters displayed in the SOAM MEP DB table. To return to the SOAM MEP page, click **Back to MEP**.

Note

To display these parameters in a separate window for a specific remote MEP, select the RMEP ID and click View.

Table 87 SOAM MEP DB Table Parameters

Parameter	Definition
RMEP ID	The remote MEP ID.
RMEP Operational State	The operational state of the remote MEP.
RMEP Last rx CCM MAC Address	The MAC Address of the interface on which the remote MEP is located.
RMEP Last CCM OK or Fail Timestamp	The timestamp marked by the remote MEP indicated the most recent CCM OK or failure it recorded. If none, this field indicates the amount of time since SOAM was activated.
RMEP Last rx CCM RDI Indication	Displays the state of the RDI (Remote Defect Indicator) bit in the most recent CCM received by the remote MEP: • True – RDI was received in the last CCM. • False – No RDI was received in the last CCM.

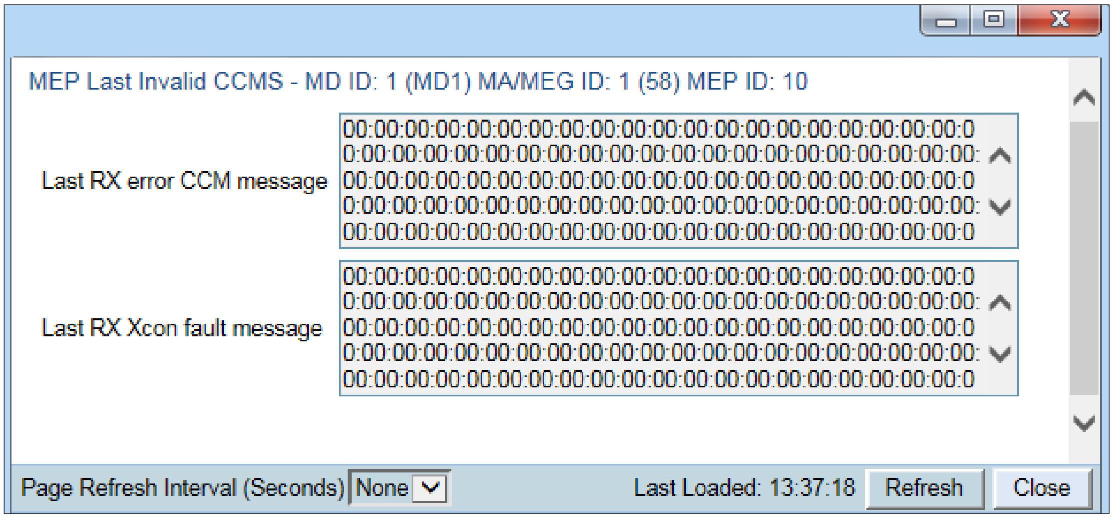
Parameter	Definition
RMEP Last rx CCM Port Status TLV	The Port Status TLV in the most recent CCM received from the remote MEP. Reserved for future use.
RMEP Last rx CCM Interface Status TLV	Displays the operational status of the interface on which the remote MEP has been defined.
RMEP Last rx CCM Chassis ID Format	Displays the format of the remote chassis (always the MAC address).
RMEP Last rx CCM Chassis ID	Displays the MAC address of the remote chassis.

Displaying Last Invalid CCMS

To display the entire frame of the last CCM error message and the last CCM cross-connect error message received by a specific local MEP:

1. Select **Ethernet > Protocols > SOAM > MEP**. The SOAM MEP page opens (Figure 319).
2. Select a MEP and click **Last Invalid CCMS**. The MEP Last Invalid CCMS page opens.

Figure 325 MEP Last Invalid CCMS Page



MEP Last Invalid CCMS - MD ID: 1 (MD1) MA/MEG ID: 1 (58) MEP ID: 10

Last RX error CCM message

```
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0
0:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0
0:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0
```

Last RX Xcon fault message

```
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0
0:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0
0:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0
```

Page Refresh Interval (Seconds) None

Last Loaded: 13:37:18

The **Last RX error CCM message** field displays the frame of the last CCM that contains an error message received by the MEP.

The **Last RX Xcon fault message** field displays the frame of the last CCM that contains a cross-connect error message received by the MEP.

Note

A cross-connect error occurs when a CCM is received from a remote MEP that has not been defined locally.

Configuring MIPs with MHF Default

If you configure a MEG with the MHF default option, MIPS are created automatically on all service points of the service to which the MEG is attached. These MIPs cannot be displayed in the Web EMS, but can be displayed via CLI. See Displaying MEP and Remote MEP Attributes (CLI).

Creating MIPs is subject to the following limitations:

Once you have created a MEG that contains MIPS, i.e., a MEG with the MHF default attribute, you cannot create a MEG with the MHF none attribute on the same or higher level on the same Ethernet Service. However, you can create MEGs with the MHF none attribute on the same service on lower levels then the MEG with the MHF default attribute.

MEPs cannot be attached to a MEG with the MHF default attribute.

The Ethernet service and service points must already be defined before creating the MEG with the MHF default attribute in order for MIPs to be created on the service points.

To configure MEGs with MIPs:

1 Create a MEG with the MHF none attribute on the intended Ethernet service. See Configuring MA/MEGs.

2 Select the MEG and click **Edit**. The SOAM MA/MEG – Edit page opens.

3 In the **MIP Creation** field, select **MHF Default**.

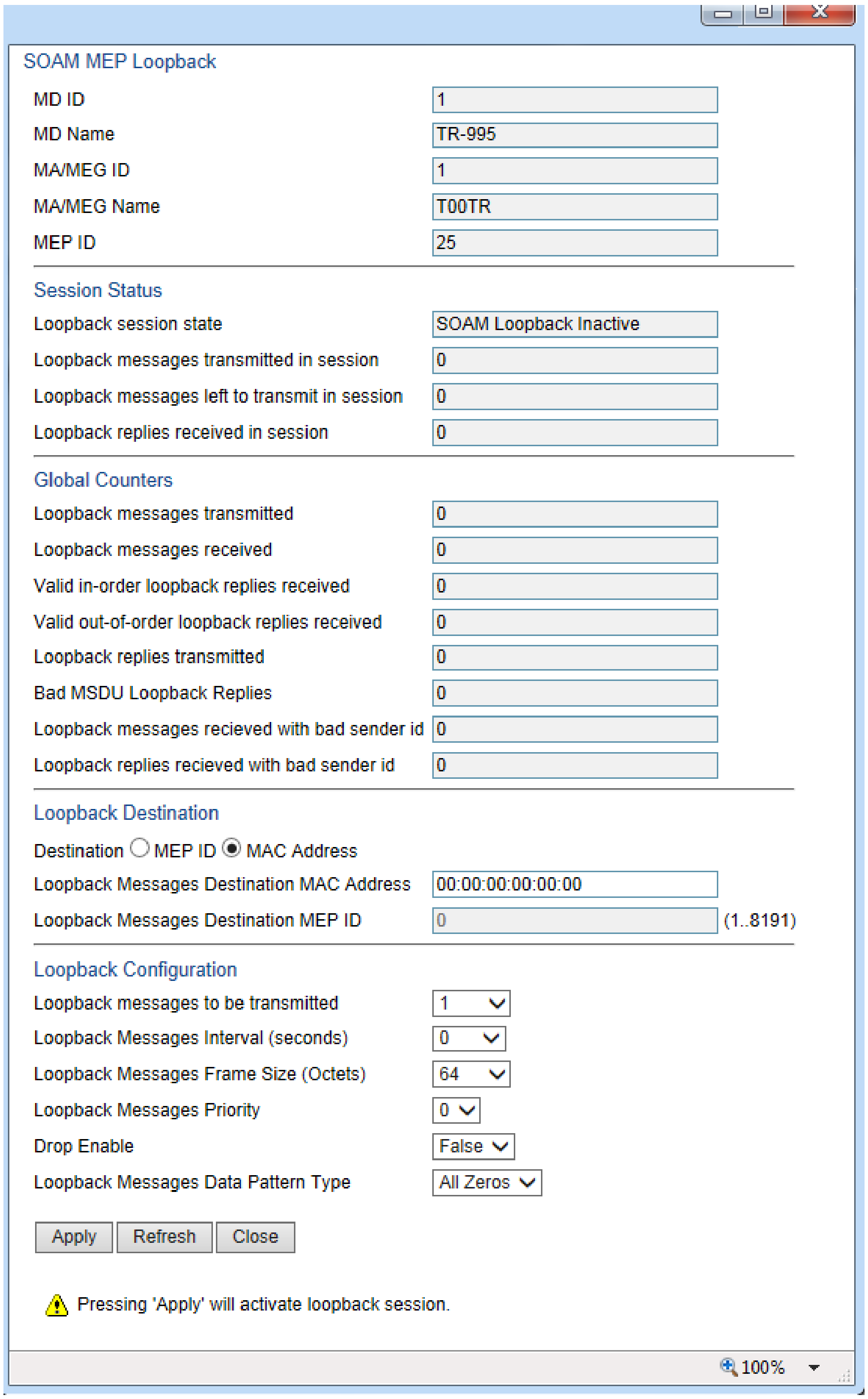
4 Click **Apply**, then **Close**.

Performing Loopback

To perform loopback on a MEP:

1. In the SOAM MEP page (Figure 319), select the MEP on which you want to perform the loopback.
2. Click **Loopback**. The SOAM MEP – Loopback page opens.

Figure 326 SOAM MEP Loopback Page



SOAM MEP Loopback

MD ID	1
MD Name	TR-995
MA/MEG ID	1
MA/MEG Name	T00TR
MEP ID	25

Session Status

Loopback session state	SOAM Loopback Inactive
Loopback messages transmitted in session	0
Loopback messages left to transmit in session	0
Loopback replies received in session	0

Global Counters

Loopback messages transmitted	0
Loopback messages received	0
Valid in-order loopback replies received	0
Valid out-of-order loopback replies received	0
Loopback replies transmitted	0
Bad MSDU Loopback Replies	0
Loopback messages recieved with bad sender id	0
Loopback replies recieved with bad sender id	0

Loopback Destination

Destination ○ MEP ID ● MAC Address

Loopback Messages Destination MAC Address	00:00:00:00:00:00
Loopback Messages Destination MEP ID	0 (1..8191)

Loopback Configuration

Loopback messages to be transmitted	1
Loopback Messages Interval (seconds)	0
Loopback Messages Frame Size (Octets)	64
Loopback Messages Priority	0
Drop Enable	False
Loopback Messages Data Pattern Type	All Zeros

Pressing 'Apply' will activate loopback session.

3. In the Loopback Destination area, select from the following options:

   - **MEP ID** – If you select **MEP ID**, you must enter the MEP ID of the MEP on the interface to which you want to perform the loopback in the **Loopback Messages Destination MEP ID** field. If you select **MEP ID**, the loopback will only be activated if CCMs have already been received from the MEP. For this reason, it is recommended to initiate loopback via MAC address.

- ○ **MAC Address** (default) – If you select **MAC Address**, you must enter the MAC address of the interface to which you want to send the loopback in the **Loopback Messages Destination MAC Address**. If you are not sure what the interface's MAC address is, you can get it from the Interface Manager by selecting **Platform > Management > Interface Manager.**

4. In the **Loopback messages to be transmitted** field, select the number of loopback messages to transmit (0 – 1024). If you select 0, loopback will not be performed.
5. In the **Loopback Messages Interval** field, select the interval (in seconds) between each loopback message (0.1 – 60). You can select in increments of 1/10 second. However, the lowest possible interval is 1 second. If you select a smaller interval, the actual interval will still be 1 second.
6. In the **Loopback Messages Frame Size** field, select the frame size for the loopback messages (64 – 1516). Note that for tagged frames, the frame size will be slightly larger than the selected frame size.
7. In the **Loopback Messages Priority** field, select a value (0 – 7) for the priority bit for tagged frames.
8. In the **Drop Enable** field, choose the value of the DEI field for tagged loopback frames (**True** or **False**). The default value is **False.**
9. In the **Loopback Messages Data Pattern Type** field, select the type of data pattern to be sent in an OAM PDU Data TLV. Options are **All Zeros** and **All Ones**. The default value is **All Zeros**.
10. Click **Apply** to begin the loopback. The **Loopback session state** field displays the status of the loopback:
    - ○ **SOAM Loopback Complete** – The loopback has been successfully completed.
    - ○ **SOAM Loopback Stopped** – The loopback has been manually stopped.
    - ○ **SOAM Loopback Failed** – The loopback failed.
    - ○ **SOAM Loopback Active** – The loopback is currently active.
    - ○ **SOAM Loopback Inactive** – No loopback has been initiated.

The remote interface will answer and the loopback session will be completed if either of the following is true:

A remote MEP has been defined on the destination interface.

A MIP has been defined on the destination interface. See Configuring MIPs with MHF Default.

Note

To manually stop a loopback, you must use the CLI. Enter the following command in root view:

root> ethernet soam loopback stop meg-id <meg-id> mep-id <mep-id>

Chapter 15: Web EMS Utilities

This section includes:

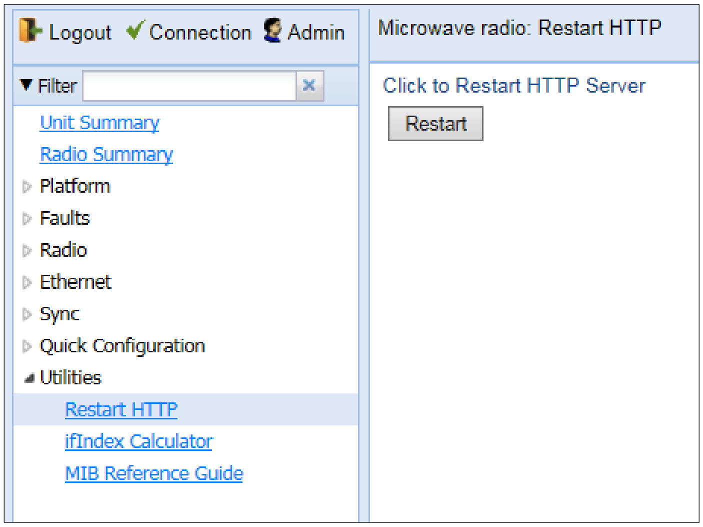
- Restarting the HTTP Server
- Calculating an ifIndex
- Displaying, Searching, and Saving a list of MIB Entities

Restarting the HTTP Server

To restart the unit’s HTTP server:

1 Select **Utilities > Restart HTTP**. The Restart HTTP page opens.

Figure 327 Restart HTTP Page



2 Click **Restart**. The system prompts you for confirmation.

3 Click **OK**. The HTTP server is restarted, and all HTTP sessions are ended. After a few seconds, the Web EMS prompts you to log in again.

Calculating an ifIndex

The ifIndex calculator enables you to:

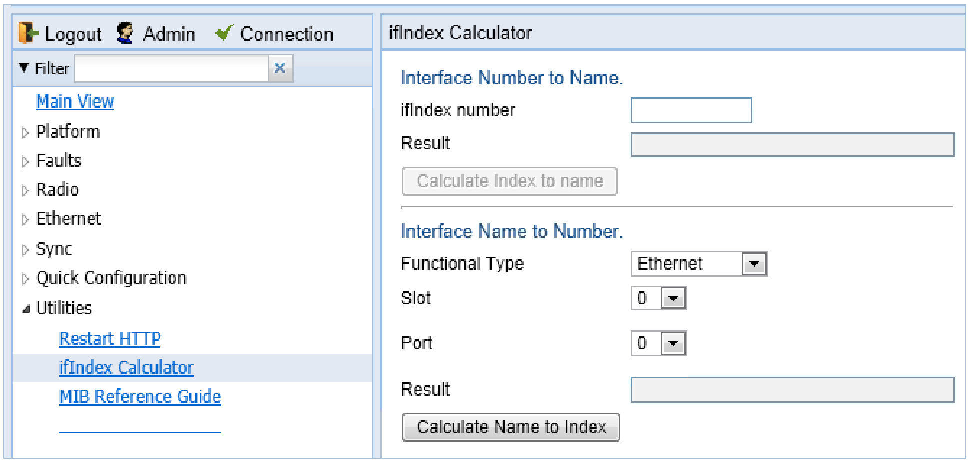
Calculate the ifIndex for any object in the system.

Determine the object represented by any valid ifIndex.

To use the ifIndex calculator:

1 Select **Utilities > ifCalculator**. The ifIndex Calculator page opens.

Figure 328 ifIndex Calculator Page



If you have an ifIndex and you want to determine which hardware item in the unit it represents, enter the number in the **ifIndex number** field and click **Calculate Index to name**. A description of the object appears in the **Result** field.

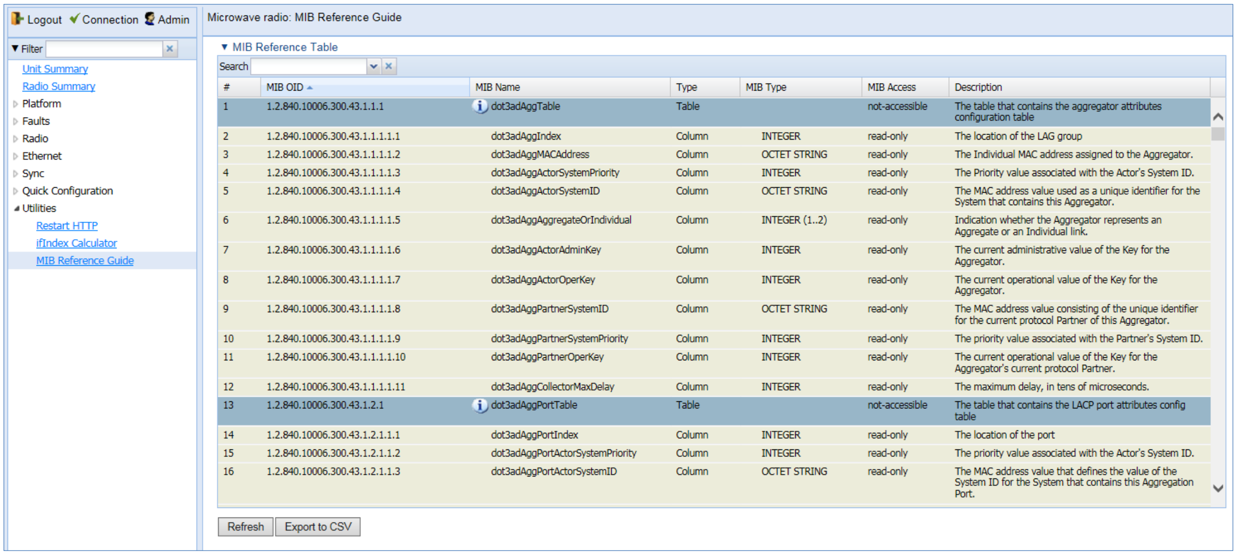
To determine the ifIndex of a hardware item in the unit, such as an interface, card, or slot, select the object type in the **Functional Type** field, select the **Slot** and **Port** (if relevant), and click **Calculate Name to Index**. The object’s ifIndex appears in the **Result** field.

Displaying, Searching, and Saving a list of MIB Entities

To display a list of entities in the PTP 850 private MIB:

1 Select **Utilities > ifCalculator**. The ifIndex Calculator page opens.

Figure 329 MIB Reference Table Page



#	MIB OID	MIB Name	Type	MIB Type	MIB Access	Description
1	1.2.840.10006.300.43.1.1.1	dot3adAggTable	Table		not-accessible	The table that contains the aggregator attributes configuration table
2	1.2.840.10006.300.43.1.1.1.1.1	dot3adAggIndex	Column	INTEGER	read-only	The location of the LAG group
3	1.2.840.10006.300.43.1.1.1.1.2	dot3adAggMACAddress	Column	OCTET STRING	read-only	The Individual MAC address assigned to the Aggregator.
4	1.2.840.10006.300.43.1.1.1.1.3	dot3adAggActorSystemPriority	Column	INTEGER	read-only	The Priority value associated with the Actor's System ID.
5	1.2.840.10006.300.43.1.1.1.1.4	dot3adAggActorSystemID	Column	OCTET STRING	read-only	The MAC address value used as a unique identifier for the System that contains this Aggregator.
6	1.2.840.10006.300.43.1.1.1.1.5	dot3adAggAggregateOrIndividual	Column	INTEGER (1..2)	read-only	Indication whether the Aggregator represents an Aggregate or an Individual link.
7	1.2.840.10006.300.43.1.1.1.1.6	dot3adAggActorAdminKey	Column	INTEGER	read-only	The current administrative value of the Key for the Aggregator.
8	1.2.840.10006.300.43.1.1.1.1.7	dot3adAggActorOperKey	Column	INTEGER	read-only	The current operational value of the Key for the Aggregator.
9	1.2.840.10006.300.43.1.1.1.1.8	dot3adAggPartnerSystemID	Column	OCTET STRING	read-only	The MAC address value consisting of the unique identifier for the current protocol Partner of this Aggregator.
10	1.2.840.10006.300.43.1.1.1.1.9	dot3adAggPartnerSystemPriority	Column	INTEGER	read-only	The priority value associated with the Partner's System ID.
11	1.2.840.10006.300.43.1.1.1.1.10	dot3adAggPartnerOperKey	Column	INTEGER	read-only	The current operational value of the Key for the Aggregator's current protocol Partner.
12	1.2.840.10006.300.43.1.1.1.1.11	dot3adAggCollectorMaxDelay	Column	INTEGER	read-only	The maximum delay, in tens of microseconds.
13	1.2.840.10006.300.43.1.2.1	dot3adAggPortTable	Table		not-accessible	The table that contains the LACP port attributes config table
14	1.2.840.10006.300.43.1.2.1.1.1	dot3adAggPortIndex	Column	INTEGER	read-only	The location of the port
15	1.2.840.10006.300.43.1.2.1.1.2	dot3adAggPortActorSystemPriority	Column	INTEGER	read-only	The priority value associated with the Actor's System ID.
16	1.2.840.10006.300.43.1.2.1.1.3	dot3adAggPortActorSystemID	Column	OCTET STRING	read-only	The MAC address value that defines the value of the System ID for the System that contains this Aggregation Port.

Note

Some of the entities listed in the Table may not be relevant to the particular unit you are using. This may occur because of activation key restrictions, minor differences between hardware types, or simply because a certain feature is not used in a particular configuration.

To search for a text string, enter the string in the Search field and press <Enter>. Items that contain the string are displayed in yellow. Searches are not case-sensitive.

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

Chapter 16: Getting Started (CLI)

This section includes:

General (CLI)

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

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

- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0

Caution

If the connection over the link is established with identical IP addresses, an IP address conflict will occur and remote connection to the element on the other side of the link may be lost.

Establishing a Connection (CLI)

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

Note

The PTP 850 IP address, as well as the password, should be changed before the system is set in operation. See Changing the Management IP Address (CLI) and Changing Your Password (CLI).

PC Setup (CLI)

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

Note

The PTP 850 IP address, as well as the password, should be changed before operating the system is set in operation. See Changing the Management IP Address (CLI) and Changing Your Password (CLI).

Logging On (CLI)

Use a telnet connection to manage the PTP 850 via CLI. You can use any standard telnet client, such as PuTTy or ZOC Terminal. Alternatively, you can simply use the `telnet <ip address>` command from the CMD window of your PC or laptop.

The default IP address of the unit is 192.168.1.1. Establish a telnet connection to the unit using the default IP address.

When you have connected to the unit, a login prompt appears. For example:

```
login:
```

At the prompt, enter the default login user name: `admin`

A password prompt appears. Enter the default password: `admin`

The root prompt appears. For example:

```
login as: admin

admin@192.168.1.1's password:

Last login: Sat Apr  1 01:46:26 from 192.168.1.10

root>
```

General CLI Commands

To display all command levels available from your current level, press <TAB> twice. For example, if you press <TAB> twice at the root level, the following is displayed:

```
root>
auto-state-propagation    ethernet   exit   multi-carrier-abc
platform        quit        radio      radio-groups
switch-back    switch-to     wait
```

Some of these are complete commands, such as `quit` and `exit`. Others constitute the first word or phrase for a series of commands, such as `ethernet` and `radio`.

Similarly, if you enter the word “platform” and press <TAB> twice, the first word or phrase of every command that follows platform is displayed:

```
root> platform
activation-key     configuration   if-manager      management
security      software                 status
sync        unit-info      unit-info-file
root> platform
```

To auto-complete a command, press <TAB> once.

Use the up and down arrow keys to navigate through recent commands.

Use the ? key to display a list of useful commands and their definitions.

> At the prompt, or at any point in entering a command, enter the word `help` to `display` a list of available commands. If you enter `help` at the prompt, a list of all commands is displayed. If you enter `help after entering part of a command, a list of commands that start with the portion of the command you have already entered is displayed.`

To scroll up and down a list, use the up and down arrow keys.

To end the list and return to the most recent prompt, press the letter `q`.

To ping another network device, enter one of the following commands:

```
root> ping ipv4-address <x.x.x.x> count <number of echo packets>
packet-size <packet-size>

root> ping ipv6-address <ipv6> count <number of echo packets>
packet-size <packet-size>
```

The optional `count` parameter determines how many packets are sent. This parameter can be an integer from 1 to 1000. The default value is 4.

The optional `packet-size` parameter determines the size of each packet, in bytes. This parameter can be an integer from 64 to 1480. The default value is 64.

The `ping` command is available from all views (e.g., root, interface views, group views).

Changing Your Password (CLI)

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

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

To change your password, enter the following command in root view:

```
root> platform security access-control password edit own-password
```

The system will prompt you to enter your existing password. The system will then prompt you to enter the new password.

If Enforce Password Strength is activated, the password must meet the following criteria:

Password length must be at least eight characters.

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

A password cannot be repeated within five changes in password.

See Configuring the Password Security Parameters (CLI).

Configuring In-Band Management (CLI)

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

> Note
>
> Before configuring in-band management, it is recommended to review the configuration recommendations for in-band management listed in Configuration Tips.

Each PTP 850E unit includes a pre-defined management service with Service ID 1025. The management service is a multipoint service that connects the two local management ports and the network element host CPU in a single service. In order to enable in-band management, you must add at least one service point to the management service, in the direction of the remote site or sites from which you want to access the unit for management. For instructions on adding service points, see Configuring Service Points (CLI).

After adding service points, you must enable in-band management using the following command in root view:

```
root> platform management in-band state set admin enable
```

To display the current in-band management admin status, enter the following command in root view:

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

```
root> platform management in-band state show
```

Changing the Management IP Address (CLI)

Related Topics:

Defining the IP Protocol Version for Initiating Communications (CLI)

Configuring the Remote Unit's IP Address (CLI)

You can enter the unit's address in IPv4 format and/or in IPv6 format. The unit will receive communications whether they were sent to its IPv4 address or its IPv6 address.

To set the unit's IP address in IPv4 format, enter the following command in root view to configure the IP address, subnet mask, and default gateway:

```
root> platform management ip set ipv4-address <ipv4-address> subnet <subnet> gateway
<gateway> name <name> description <name>
```

Table 88 IP Address (IPv4) CLI Parameters

Parameter	Input Type	Permitted Values	Description
ipv4-address	Dotted decimal format.	Any valid IPv4 address.	The IP address for the unit.
subnet	Dotted decimal format.	Any valid subnet mask.	The subnet mask for the unit.
gateway	Dotted decimal format.	Any valid IPv4 address.	The default gateway for the unit (optional).
name	Text String.		Enter a name (optional).
description	Text String.		Enter a description (optional).

To set the unit's IP address in IPv6 format, enter the following command in root view to configure the IP address, subnet mask, and default gateway:

```
root> platform management ip set ipv6-address <ipv6-address> prefix-length
<prefix-length> gateway <gateway>
```

Note

It is recommended not to configure addresses of type FE:80::/64 (Link Local addresses) because traps are not sent for these addresses.

Table 89 IP Address (IPv6) CLI Parameters

Parameter	Input Type	Permitted Values	Description
ipv6-address	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The IP address for the unit.
prefix-length	Number.	1-128	The prefix-length for the unit.
gateway	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The default gateway for the unit (optional).

Examples

The command below sets the following parameters:

IPv4 Address - 192.168.1.160

Subnet Mask – 255.255.0.0

Default Gateway – 192.168.1.100

```
root> platform management ip set ipv4-address 192.168.1.160 subnet
255.255.0.0 gateway 192.168.1.100
```

The command below sets the following parameters:

IPv6 Address - FE80:0000:0000:0000:0202:B3FF:FE1E:8329

Prefix length – 64

Default Gateway - FE80:0000:0000:0000:0202:B3FF:FE1E:8329

```
root> platform management ip set ipv6-address
FE80:0000:0000:0000:0202:B3FF:FE1E:8329 prefix-length 64 gateway
FE80:0000:0000:0000:0202:B3FF:FE1E:8329
```

Configuring the Activation Key (CLI)

This section includes:

- Activation Key Overview (CLI)
- Viewing the Activation Key Status Parameters (CLI)
- Entering the Activation Key (CLI)
- Activating a Demo Activation Key (CLI)
- Displaying a List of Activation-Key-Enabled Features (CLI)

Activation Key Overview (CLI)

PTP 850 offers a pay-as-you-grow concept in which future capacity growth and additional functionality can be enabled with activation keys. For purposes of the activation keys, each PTP 850 chassis is considered a distinct device, regardless of which cards are included in the chassis. Each device contains a single unified activation key cipher.

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

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

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

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

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

Viewing the Activation Key Status Parameters (CLI)

To display information about the currently installed activation key, enter the following command in root view:

```
root> platform activation-key show all
```

Entering the Activation Key (CLI)

To enter the activation key, enter the following command in root view.

```
root> platform activation-key set key string <key string>
```

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

To set the default activation key, enter the following command in root view:

```
root> platform activation-key set key string “Default Activation Key”
```

> **Note:** Make sure to enter the command using the exact syntax above, including the spaces and quotation marks, or an error will be returned.

Activating a Demo Activation Key (CLI)

To activate the demo activation key, enter the following command in root view:

```
root> platform activation-key set demo admin enable
```

To display the current status of the demo activation key, enter the following command in root view:

```
root> platform activation-key show demo status
```

Activation Key Reclaim (CLI)

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

A composite type activation key provides free activation keys when certain activation keys are purchased. For example, if a customer purchases an activation key for one GB ethernet port, two FE ethernet port activation keys are also provided. If the customer reclaims the activation key, the customer only gets credit for the original activation key, not for the composite items.

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

For instructions on how to reclaim an activation key, refer to the User Guide for the Cambium Activation Key Management System, Rev A.15 or later, Chapter 7, Reclaiming an Activation Key. During the activation key reclaim procedure, you will need to obtain a Validation Number from the PTP 850E unit. To display the Validation Number, enter the following command in root view:

```
root> platform activation-key show all
```

Displaying a List of Activation-Key-Enabled Features (CLI)

To display a list of features that your current activation key supports, and usage information about these features, enter the following command in root view:

```
root> platform activation-key show usage all
```

To display a list of the radio capacities that your current activation key supports and their usage information, enter the following command in root view:

```
root> platform activation-key show usage radio
```

Setting the Time and Date (Optional) (CLI)

Related Topics:

Configuring NTP (CLI)

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

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

Note

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

To set the UTC time, enter the following command in root view:

```
root> platform management time-services utc set date-and-time <date-and-time>
```

To set the local time offset relative to UTC, enter the following command in root view:

```
root> platform management time-services utc set offset hours-offset <hours-offset> minutes-offset <minutes-offset>
```

To display the local time configurations, enter the following command in root view:

```
root> platform management time-services show status
```

Table 90 Local Time Configuration CLI Parameters

Parameter	Input Type	Permitted Values	Description

date-and-time	Number	dd-mm-yyyy,hh:mm:ss
		where:
		dd = date
		mm = month
		yyyy= year
		hh = hour
		mm = minutes
		ss = seconds
			Sets the UTC time.

hours-offset	Number	-12 – 13	The required hours offset (positive or negative) relative to GMT. This is used to offset the clock relative to GMT, according to the global meridian location.

Parameter	Input Type	Permitted Values	Description
minutes-offset	Number	0 – 59	The required minutes relative to GMT. This is used to offset the clock relative to GMT, according to the global meridian location.

The following command sets the GMT date and time to January 30, 2014, 3:07 pm and 58 seconds:

```
root>  platform management time-services utc set date-and-time 30-01-2014,15:07:58
```

The following command sets the GMT offset to 13 hours and 32 minutes:

```
root> platform management time-services utc set offset hours-offset 13 minutes-offset 32
```

Setting the Daylight Savings Time (CLI)

To set the daylight savings time parameters, enter the following command in root view:

```
root> platform management time-services daylight-savings-time set start-date-month <start-date-month> start-date-day <start-date-day> end-date-month <end-date-month> end-date-day <end-date-day> offset <offset>
```

Table 91: Daylight Savings Time CLI Parameters

Parameter	Input Type	Permitted Values	Description
start-date-month	Number	1 – 12	The month when Daylight Savings Time begins.
start-date-day	Number	1 – 31	The date in the month when Daylight Savings Time begins.
end-date-month	Number	1 – 12	The month when Daylight Savings Time ends.
end-date-day	Number	1 – 31	The date in the month when Daylight Savings Time ends.
offset	Number	0 – 23	The required offset, in hours, for Daylight Savings Time. Only positive offset is supported.

The following command configures daylight savings time as starting on May 30 and ending on October 1, with an offset of 20 hours.

```
root> platform management time-services daylight-savings-time set start-date-month 5 start-date-day 30 end-date-month 10 end-date-day 1 offset 20
```

Enabling the Interfaces (CLI)

By default:

- Ethernet traffic interfaces are disabled and must be manually enabled.
- The Ethernet management interface is enabled.
- Radio interfaces are enabled.

Note

In relase 11.3,

For PTP 850C, Ethernet Slot 1, Ports 1, 2, 3, and 4 are supported.

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

For PTP 850S, Ethernet Slot 1, Ports 1 through 3 are supported when a CSFP module is used with P2. When a standard SFP module is used with P2, Ports 1 and 2 are supported.

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

In a 4x1/10G configuration the QSFP port can provide four Ethernet interfaces: Eth3, Eth4, Eth 5, and Eth6. In this configuration, a QSFP transceiver is attached to the QSFP port, and an MPO-MPO cable is connected between the transceiver and a splitter on the other side of the link. The splitter splits the traffic between four Ethernet cables connecting the splitter to the customer equipment.

To enable or disable an interface, enter the following command in root view:

```
root> platform if-manager set interface-type <interface-type> slot <slot>
port <port> admin <admin>
```

To display the status of all the interfaces in the unit, enter the following command in root view:

```
root> platform if-manager show interfaces
```

Table 92 Interface Configuration CLI Parameters

Parameter	Input Type	Permitted Values	Description
interface-type	Variable	ethernet radio	ethernet – an Ethernet traffic interface. radio – a radio interface.
slot	Number	Ethernet: 1 Radio: • PTP 850C and PTP 850E: 1 • PTP 850S: 2	The slot on which the interface is located.

Parameter	Input Type	Permitted Values	Description
port	Number	Ethernet: • PTP 850C: 1, 3-4 • PTP 850S: 1-3 • PTP 850E: 1-7 Radio: • PTP 850C: 1-2 PTP 850E and PTP 850S: 1 Management: 1	The specific interface you want to enable or disable.
admin	Variable	up down	Enter **up** to enable the interface or **down** to disable the interface.

The following command enables Ethernet port 7:

```
root> platform if-manager set interface-type ethernet slot 1 port 7 admin
up
```

The following command enables radio interface:

```
root> platform if-manager set interface-type radio slot 1 port 1 admin up
```

The following command disables the radio interface:

```
root> platform if-manager set interface-type radio slot 1 port 1 admin down
```

The following command disables the management interface:

```
root> platform if-manager set interface-type management slot 1 port 1 admin
down
```

PTP 850S Management Interface (CLI)

The PTP 850S management port (Port 1) can be used for traffic as well as management and PoE. For general information and limitations regarding this port, see *PTP 850S Management Interface*.

To use the PTP 850S management port for traffic, you should perform the following configurations:

- An egress Service Bundle Shaper (Shaper ID 256) is attached to this service point. This Shaper cannot be edited, but it can and must be either detached or disabled on the port in order for the port to support 1G traffic. See *Attaching a Shaper Profile to a Service Bundle for PTP 850S (CLI)*.
- Change the port speed from its default value of 100 Mbps to 1 Gbps. See *Configuring Ethernet Interfaces (CLI)*.
- Enable the LOC alarm (Alarm ID 401) for the management port. By default, this alarm is disabled on the management port and must be manually enabled when using the port for traffic.

To enable the LOC alarm:

1. Use the following command to enter management port view:

```
root> ethernet interfaces mng slot 1 port 1
```

2. In port view, use the following command:

```
eth type mng [1/1]> loc-alarm-supported set yes
```

If at some point you stop using the management port for traffic and use it instead exclusively for management, enter the following command in port view to disable the LOC alarm:

```
eth type mng [1/1]> loc-alarm-supported set no
```

To display the current LOC alarm status for the management port, enter the following command in port view:

```
eth type mng [1/1]> loc-alarm-supported show
```

Configuring the Radio (MRMC) Script(s) (CLI)

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

Note

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

Displaying Available MRMC Scripts (CLI)

To display all scripts that are available for a specific radio carrier in your unit:

Use the following command to enter radio view:

```
root> radio slot 1 port 1
```

Enter the following command in radio view:

```
radio[1/1]>mrmc script show script-type <script-type> acm-support <acm-support>
```

Note

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

Table 93 MRMC Script CLI Parameters

Parameter	Input Type	Permitted Values	Description
script-type	Variable	Normal asymmetrical	Determines the type of scripts to be displayed: • **normal** – Scripts for symmetrical bandwidth. • **asymmetrical** – Scripts for asymmetrical bandwidth. **Note:** Asymmetrical scripts are not supported in this release.
acm-support	Boolean	Yes no	Determines whether to display scripts that support Adaptive Coding Modulation (ACM). In ACM mode, a range of profiles determines Tx and Rx rates. This allows the radio to modify its transmit and receive levels in response to environmental conditions.

The following command displays available symmetrical (normal) scripts:

```
radio [1/1]>mrmc script show script-type normal acm-support yes
Script    |Script-Name
ID#       |
----------------------------------------------------
<5703>      |mdN_A250250N_5_5703
<5704>      |mdN_A500500N_5_5704
<5706>      |mdN_A10001000N_5_5706
<5710>      |mdN_A20002000N_5_5710
----------------------------------------------------
radio [1/1]>
```

Assigning an MRMC Script to a Radio Carrier (CLI)

Once you have a list of valid scripts, you can assign a script to the radio carrier. The command syntax differs depending on whether you are assigning a script with ACM support or a script without ACM support.

Note

When you enter a command to change the script, a prompt appears

informing you that changing the script will reset the unit and affect traffic. To continue, enter yes. Changing the maximum or minimum profile does not reset the radio interface.

When using an 80 or 112 MHz script with PTP 850C, the same script must be assigned to both carriers. The system cannot be configured to operate with the 80 or 112 MHz script on one of the carriers and a different script on the other carrier.

To assign a script with ACM enabled, enter the following command in radio view:

```
radio[1/1]> mrmc set acm-support script-id <script-id> modulation adaptive
max-profile <max-profile> min-profile <min-profile>
```

To assign a script without ACM enabled, enter the following command in radio view:

```
radio[1/1]> mrmc set acm-support script-id <script-id> modulation fixed
profile <profile>
```

To display the current MRMC script configuration, enter the following command in radio view:

```
radio[1/1]> mrmc show script-configuration
```

Table 94: MRMC Script Assignation to Radio Carrier CLI Parameters

Parameter	Input Type	Permitted Values	Description
script-id	Number		The ID of the script you want to assign to the radio carrier.
modulation	Variable	adaptive fixed	Determines whether ACM is enabled (adaptive) or disabled (fixed).
max-profile	Number		Adaptive ACM mode only: The maximum profile for the script. For example, if you select a maximum profile of 5, the system will not climb above profile 5, even if channel fading conditions allow it.

Parameter	Input Type	Permitted Values	Description
min-profile	Number		Adaptive ACM mode only: The minimum profile for the script. For example, if you select a minimum profile of 3, the system will not go below profile 3 regardless of the channel fading conditions. The minimum profile cannot be greater than the maximum profile, but it can be equal to it. If you do not include this parameter in the command, the minimum profile is set at the default value of 2.
profile	Number		Fixed ACM mode only: The profile in which the system will operate

Note

For a list and description of available profiles, see ***Error! Reference source not found.***. N ote that Profiles 0 and 1 require a special activation key (SL-ACMB). These profiles are used with ACMB, which is an enhancement of ACM that provides further flexibility to mitigate fading at BPSK by reducing the channel spacing to one half or one quarter of the original channel bandwidth when fading conditions make this appropriate.

The following command assigns MRMC script ID 5703, with ACM enabled, a minimum profile of 3, and a maximum profile of 9, to the radio carrier:

```
radio[1/1]>mrmc set acm-support script-id 5703 modulation adaptive max-
profile 9 min-profile 3
```

The following command assigns MRMC script ID 5704, with ACM disabled and a profile of 5, to the radio carrier:

```
radio[1/1]>mrmc set acm-support script-id 5704 modulation fixed profile 5
```

The following command assigns MRMC script ID 5710, with ACM enabled, minimum profile of 2, and a maximum profile of 8, to the radio carrier:

```
radio[1/1]>mrmc set acm-support script-id 5710 modulation max-profile 8
min-profile 2
```

Configuring the Radio Parameters (CLI)

In order to establish a radio link, you must:

- Enter radio view.
- Verify that the radio is muted (the **Mute Status** should be **On**).
- Configure the radio frequencies.

Note

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

- Configure the TX level.
- Set **Mute Admin** to **Off**.
- Verify that the radio is unmuted (the **Mute Status** should be **Off**).

Entering Radio View (CLI)

To view and configure radio parameters, you must first enter the radio's view level in the CLI.

To enter a radio's view level, enter the following command in root view:

```
root> radio slot <slot> port <port>
```

The following prompt appears:

```
radio[1/1]>
```

Muting and Unmuting a Radio (CLI)

To mute or unmute the radio, enter the following command:

```
radio[x/x]>rf mute set admin <admin>
```

To configure a timed mute, enter the following command in radio view:

```
radio[1/1]> rf mute set admin on-with-timer timeout-value <1-1440>
```

When the timer expires, the radio is automatically unmuted. A timed mute provides a fail-safe mechanism for maintenance operations that eliminates the possibility of accidently leaving the radio muted after the maintenance has been completed. By default, the timer is 10 minutes.

Note

In contrast to an ordinary mute, a timed mute is not persistent. This means that if the unit is reset, the radio is not muted when the unit comes back online, even if the timer had not expired.

To display the mute status of a radio, enter the following command in radio view:

```
radio[1/1]>rf mute show status
```

The following command mutes the radio:

```
radio[1/1]>rf mute set admin on
```

The following command unmutes the radio:

```
radio[1/1]>rf mute set admin off
```

The following command configures a timed mute. This mute will automatically expire in 30 minutes.

```
radio[1/1]> rf mute set admin on-with-timer timeout-value 30
```

Configuring the Transmit (TX) Frequency (CLI)

To set the transmit (TX) frequency of a radio, enter the following command in radio view. This command includes an option to set the remote RX frequency in parallel:

```
radio[1/1]>rf set tx-frequency <0-4294967295> local-remote <enable|disable>
```

Note: System release 10.6 does not support the ability to set the remote RX frequency.

The following command sets the TX frequency of the radio in an PTP 850E unit to 71000000 KHz, and sets the RX frequency of the remote unit to the same value.

```
radio[1/1]> rf set tx-frequency 71000000 local-remote enable
```

The following command sets the TX frequency of the radio in an PTP 850E unit to 71000000 KHz, but does not set the RX frequency of the remote unit.

```
radio[1/1]> rf set rx-frequency 71000000 local-remote disable
```

Configuring the Transmit (TX) Level (CLI)

To set the transmit (TX) level of a radio, enter the following command in radio view:

```
radio[1/1]>rf set tx-level <-50-50>
```

To display the maximum transmit (TX) level of a radio, enter the following command in radio view:

```
radio[1/1]>rf show max-tx-level
```

The following command sets the TX level of the radio to 10 dBm:

```
radio[1/1]>rf set tx-level 10
```

When Adaptive TX power is enabled, this command determines the maximum TX level.

Enabling ACM with Adaptive Transmit Power (CLI)

When Adaptive TX Power is enabled, the radio adjusts its TX power dynamically based on the current modulation. When the modulation is at a high level, the TX power is adjusted to the level required with the high modulation. If the modulation goes down to a lower level, the TX power increases to compensate for the lower modulation. The TX level configured by the `rf set tx-level` command determines the maximum TX level, but the actual TX level as shown in the Operational TX Level (dBm) field can be expected to be lower when the radio is operating at high modulations requiring less TX power.

To enable Adaptive TX Power, enter the following command in radio view:

```
radio[1/1]>rf adaptive-power admin enable
```

To disable Adaptive TX Power for a radio, enter the following command in radio view:

```
radio[1/1]>rf adaptive-power admin disable
```

To display whether Adaptive TX Power is enabled, enter the following command in radio view:

```
radio[1/1]>rf adaptive-power show status
```

The output of this command is:

```
radio [x/x]>rf adaptive-power show status

RF adaptive power admin status: [enable/disable]
RF adaptive power operational status: [up/down]
```

`RF adaptive power operational status: Up` means the feature is enabled and fully functional for that radio link.

Note

Adaptive TX Power only operates when the MRMC script is configured to Adaptive mode. If the script is configured to Fixed mode (or Adaptive mode with the Minimum and Maximum Profile set to the same value), you can set `adaptive-power` to `enable`, but the `adaptive power operational status` will be `down`.

Configuring the RSL Threshold Alarm (CLI)

You can enable an alarm to be triggered in the event that the RSL falls beneath a defined threshold. This alarm is alarm ID 1610, Radio Receive Signal Level is below the configured threshold. By default, the alarm is disabled.

To enable the RSL threshold alarm, enter the following command in radio view:

```
radio[x/x]> rf rsl-degradation set admin enable
```

To disable the RSL threshold alarm, enter the following command in radio view:

```
radio[x/x]> rf rsl-degradation set admin disable
```

To set the threshold of the RSL threshold alarm, enter the following command in radio view:

```
radio[x/x]> rf rsl-degradation set threshold <-99-0>
```

The default threshold is -68 dBm.

To display the current alarm configuration, enter the following command in radio view:

```
radio[x/x]> rf rsl-degradation show status
```

The following commands enable the RSL threshold alarm for radio carrier 1 and set the threshold to -55 dBm.

```
root> radio slot 2 port 1
radio [2/1]>rf rsl-degradation set admin enable
radio [2/1]>rf rsl-degradation set threshold -55
radio [2/1]>rf rsl-degradation show status

RSL degradation alarm admin: enable
RSL degradation threshold: -55

radio [2/1]>
```

The alarm is cleared when the RSL goes above the configured threshold. The alarm is masked if the radio interface is disabled, the radio does not exist, or a communication-failure alarm (Alarm ID #1703) is raised.

Creating Service (s) for Traffic (CLI)

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

Configuring CPRI (CLI)

Optionally, PTP 850E can be used with a CPRI module. The CPRI module is inserted in the PTP 850E's QSFP port (P4), and provides up to 10 Gbps capacity for CPRI traffic. The CPRI module converts CPRI signals to Ethernet and Ethernet to CPRI in accordance with Radio over Ethernet (RoE) standard IEEE 1914.3 and CPRI specification v7.0. For more details, see the Technical Description for PTP 850E.

Note: Support for CPRI is planned for future release.

CPRI Configuration Overview (CLI)

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

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

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

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

Setting the QSFP Mode to CPRI (CLI)

To set the QSFP mode of the QSFP port to CPRI, enter the following command in root view:

```
root> platform qsfp expected set slot 1 id 1 type CPRI
```

Creating an Ethernet Service for CPRI Traffic (CLI)

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

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

Use the following syntax to create a service point on the CPRI interface:

```
service[x]> sp add sp-type pipe int-type <dot1q|s-tag> spid <1-
32> interface cpri slot 1 port 1 sp-name <string> vlan <1-4097>
```

For example:

```
service[1]>sp add sp-type pipe int-type dot1q spid 1 interface
cpri slot 1 port 1 sp-name Test
```

Configuring Synchronization for CPRI Traffic (CLI)

Synchronization for the CPRI module should be configured as follows:

- If the CPRI module is connected to a Baseband Unit (BBU), CPRI Slot 1 Port 1 should be configured as the lowest priority synchronization source. Use the following command syntax to configure the CPRI module as a synchronization source:

```
platform sync source add cpri-interface slot 1 port 1 priority
<1-16> quality <automatic|prc|ssu-a|ssu-b|g.813/8262>
```

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

For instructions on configuring the Synchronization source, see *Configuring the Sync Source (CLI)*

Configuring the CPRI Parameters (CLI)

To configure the CPRI parameters:

1. Go to CPRI module view by entering the following command in root view:

```
root>cpri slot 1 port 1

CPRI slot[1] port[1]>
```

2. Enter the following command to configure the bit rate option for the CPRI module. This parameter must be set to the same value on both sides of the CPRI link.

```
CPRI slot[1] port[1]> cpri option set value <3|5|7>
```

The following options are available:

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

3. Enter the following command to configure the system mode. This parameter must be set to the same value on both sides of the CPRI link.

```
CPRI slot[1] port[1]> mode set value <line-code-
aware|tunneling>
```

The following options are available:

- **line-code-aware** – (default)
- **tunneling** – Only works with **normal-operation** as the sub mode. Does not work with bit rate option **7**.

4. Enter the following command to configure the sub-mode. This parameter must be set to the same value on both sides of the CPRI link.

```
CPRI slot[1] port[1]>lca submode set value <normal-
operation|special-characters>
```

The following options are available:

- **normal-operation** – (default)
- **special-characters** – Only works with **line-code-aware** as the system mode.

5. Enter the following command to configure the number of bytes that must be in the buffer before a CPRI signal is transmitted. This parameter must be set to the same value on both sides of the CPRI link.

```
CPRI slot[1] port[1]>buffer size set <1500-20000>
```

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

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

6. Enter the following command to configure the RoE payload length, in bytes. This includes only CPRI data, not the RoE header. The default value is 512. This parameter must be set to the same value on both sides of the CPRI link.

```
CPRI slot[1] port[1]>roe payload set size <64-1488>
```

The available options depend on the mode and sub-mode configuration, as follows:

- When the mode is **line-code-aware** and the sub-mode is **normal-operation**, supported values are 256, 512, and 1024.
- When the mode is **line-code-aware** and the sub-mode is **special characters**, supported values are 512 and 1024.
- When the mode is **tunneling** and the sub-mode is **normal-operation**, supported values are multiples of 16 within a range of 64 to 1488.

7. Enter the following command to configure the destination MAC address:

```
CPRI slot[1] port[1]> mac set destination address <MAC-address>
```

- If the CPRI module is connected to a BBU, enter the MAC address of the CPRI module connected to the RRH.
- If the CPRI module is connected to a RRH, enter the MAC address of the CPRI module connected to the BBU.

8. Enter the following command to configure an ID to be used in the RoE conversion:

```
CPRI slot[1] port[1]> flow ID set value <0-10>
```

The default is 1. This parameter must be set to the same value on both sides of the CPRI link.

9. Enter the following command to configure whether the TX is turned off if a fault is discovered.

```
CPRI slot[1] port[1]>turn off TX at fault set to <yes|no>
```

If this parameter is set to **yes**, the TX is turned off if a fault is discovered. The default value is **no**.

Enabling the CPRI Port (CLI)

You must enable the CPRI port (CPRI Slot 1 Port 1). To enable the CPRI port, enter the following command in root view:

```
root> platform if-manager set interface-type cpri slot 1 port 1
admin up
```

Chapter 17: Configuration Guide (CLI)

System Configurations (CLI)

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

Table 95 System Configurations (CLI)

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

Configuring Multi-Carrier ABC (CLI)

This option is only relevant for PTP 850C.

- Multi-Carrier ABC Overview (CLI)
- Configuring a Multi-Carrier ABC Group (CLI)
- Removing Members from a Multi-Carrier ABC Group (CLI)
- Deleting a Multi-Carrier ABC Group (CLI)

Multi-Carrier ABC Overview (CLI)

For an overview of Multi-Carrier ABC, see Multi-Carrier ABC Overview.

Configuring a Multi-Carrier ABC Group (CLI)

Note: Radio slot 2 port 1 should always be configured on channel 1 while Radio slot 2 port 2 should always be configured on channel 2.

To configure a Multi-Carrier ABC group:

1 Create the group by entering the following command in root view:

```
root> multi-carrier-abc create group group_id 1 slot 1 type
Enhanced
multi-carrier-abc enhanced-group-id [1] slot [1]>
```

2 Enter Multi-Carrier ABC Group view by entering the following command in root view:

```
root>multi-carrier-abc group-id 1 slot 1 type Enhanced
```

3 Add members to the group as follows:

- To add a radio interface to the group, enter the following command in Multi-Carrier ABC Group view. Repeat this command for each radio interface you want to add.

```
attach-member slot 1 port <1-2> channel-id <1-16>
```

- The Channel ID identifies the interface within the group.

4 Repeat for the second radio interface.

The following commands create a Multi-Carrier ABC group.

```
multi-carrier-abc create group group_id 1 slot 1 type Enhanced
multi-carrier-abc enhanced-group-id [1] slot [1]> attach-member
slot 1 port 1 channel-id 1
multi-carrier-abc enhanced-group-id [1] slot [1]> attach-member
slot 1 port 2 channel-id 2
multi-carrier-abc enhanced-group-id [1] slot [1]> exit
```

Removing Members from a Multi-Carrier ABC Group (CLI)

To remove members from a Multi-Carrier ABC group:

1 To remove an individual radio interface from the Multi-Carrier ABC group, go to Multi-Carrier ABC group view and enter the following command:

```
multi-carrier-abc enhanced-group-id [1] slot [1]> detach-member
channel-id <channel-id>
```

Deleting a Multi-Carrier ABC Group (CLI)

To delete a Multi-Carrier ABC group:

1 Remove the members from the group. See *Removing Members from a Multi- Carrier ABC Group (CLI)*.

2 Delete the group by entering the following command in root view:

```
root> multi-carrier-abc delete group group_id 1 slot 1 type
Enhanced
```

Configuring Multiband (CLI)

Multiband Overview (CLI)

For general information about Multiband and how it operates, see *Multiband Overview*.

Multiband Configuration (CLI)

To configure a Multiband node:

1 Connect the external switch to any operational traffic port on the PTP 850E.

2 Connect the Multiband port on the PTP 850E (Port 3, Eth2) to the paired unit. When the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, use the Eth2 port on the PTP 820C, PTP 820C-HP, or PTP 820S. When the paired unit is an PTP 820N or PTP 820A, use any SFP port on the PTP 820N or PTP 820A.

3 Verify that the **Admin** status of Eth2 on the PTP 850E is **Down**. See *Enabling the Interfaces (CLI)*.

4 Verify that no service points are configured on the Eth2 port of the PTP 850E. If there are service points on Eth2, remove them. See *Deleting a Service Point (CLI)*.

5 On the PTP 850E, configure a Multiband group that includes Eth2 and the radio: i Create the group by entering the following command in root view:

```
root>multi-carrier-abc create group group_id 1 slot 1 type
Enhanced
```

ii Enter Multi-Carrier ABC Group view by entering the following command in root view:

```
root>multi-carrier-abc group-id 1 slot 1 type Enhanced
multi-carrier-abc enhanced-group-id [1] slot [1]>
```

iii In Multi-Carrier ABC Group view, add the radio interface by entering the following command:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>attach-member
slot 1 port 1 channel-id 1
```

iv In Multi-Carrier ABC Group view, add the Ethernet interface by entering the following command:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>attach-eth-
member slot 1 port 2 channel-id 2
```

v In Multi-Carrier ABC Group view, use the following command to set the maximum traffic that the PTP 850E will pass to the paired unit:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-set-eth-
max-bandwidth slot 1 port 2 max-bandwidth <1-1000>
```

- When using Fixed ACM mode, set this parameter to the actual rate you want the paired unit to broadcast.
- When using Adaptive ACM mode, set this parameter to the maximum of the paired unit's capacity.

The default value is 1000 Mbps.

For example, the following command sets the maximum traffic to 900 Mbps:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-set-eth-
max-bandwidth slot 1 port 2 max-bandwidth 900


Maximum bandwith: 900 Mbps
```

Use the following command in Multi-Carrier ABC Group view to display the current maximum traffic setting:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-show-eth-
max-bandwidth slot 1 port 2
```

Note: The Maximum Bandwidth represents the L1 capacity of the radio link connected to the Ethernet member. The actual bandwidth that will be available for traffic is less due to overhead.

When using a third-party radio as the paired unit, it is particularly important to set this parameter properly in order to ensure optimal performance. Failure to properly set this parameter may lead to frequent pauses as the queue fills up during low capacity periods, such as when weather conditions cause the ACM profile to drop.

vi In Multi-Carrier ABC Group view, use the following command to set the bandwidth margin, in Mbps. This parameter deducts the specified throughput from the throughput the PTP 850E would otherwise pass to the paired unit. The purpose of this parameter is to provide a margin of safety that will avoid loss of traffic in the event that the ACM profile is reduced on the paired unit.

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-set-eth-
bandwidth-margin slot 1 port 2 bandwidth-margin 100 <5-100>
```

It is recommended to configure this parameter as follows:

- If the paired unit is an PTP 820 microwave radio, or a third-party device with a bandwidth notification mechanism that will inform the PTP 850E of an impending reduction of the ACM profile before the reduction takes place, it is recommended to leave this parameter at its default value of 5 Mbps.
- If the paired unit is a third-party device without a bandwidth notification mechanism that will inform the PTP 850E of an impending reduction of the ACM profile before the reduction takes place, it is recommended to

set this parameter to an amount equal to or greater than the largest throughput differential between any two adjacent profiles for the script configured on the paired unit.

The range of values is 5 to 100 Mbps.

For example, the following command sets the bandwidth margin to 100 Mbps:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-set-eth-
bandwidth-margin slot 1 port 2 bandwidth-margin 100
```

Use the following command in Multi-Carrier ABC Group view to display the current bandwidth margin:

```
abc-show-eth-bandwidth-margin slot 1 port 2
```

6 Enable the Eth2 interface. See *Enabling the Interfaces (CLI)*.

7 On the paired unit, configure a service between the port receiving traffic from the PTP 850E and the radio or Multi-Carrier ABC group.

Note: If the paired unit is an PTP 820C, PTP 820C-HP, PTP 820S, or third-party microwave radio, the service must be a Pipe service. If the paired unit is an PTP 820N or PTP 820A, any service type can be used. However, this service *must* be given higher priority than any other service attached to the interfaces used for Multiband.

8 On the paired unit, configure Automatic State Propagation with **ASP trigger by remote fault** enabled.

9 If the paired unit is an PTP 820 microwave radio, configure Radio BNM. Bandwidth Notification must be configured via the Web EMS. See *Multiband Configuration*, Step 10.

Multiband Overview (CLI)

For general information about Multiband and how it operates, see Multiband Overview.

Multiband Configuration (CLI)

To configure a Multiband node:

1. Connect the external switch to any operational traffic port on the PTP 850E.
2. Connect the Multiband port on the PTP 850E (Port 3, Eth2) to the paired unit. When the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, use the Eth2 port on the PTP 820C, PTP 820C-HP, or PTP 820S.
3. Verify that the **Admin** status of Eth2 on the PTP 850E is **Down**. See *Enabling the Interfaces (CLI)*.
4. Verify that no service points are configured on the Eth2 port of the PTP 850E. If there are service points on Eth2, remove them. See *Deleting a Service Point (CLI)*.
5. On the PTP 850E, configure a Multiband group that includes Eth2 and the radio:

- Create the group by entering the following command in root view:

```
root>multi-carrier-abc create group group_id 1 slot 1 type
Enhanced
```

- Enter Multi-Carrier ABC Group view by entering the following command in root view:

```
root>multi-carrier-abc group-id 1 slot 1 type Enhanced
multi-carrier-abc enhanced-group-id [1] slot [1]>
```

- In Multi-Carrier ABC Group view, add the radio interface by entering the following command:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>attach-member
slot 1 port 1 channel-id 1
```

- In Multi-Carrier ABC Group view, add the Ethernet interface by entering the following command:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>attach-eth-
member slot 1 port 2 channel-id 2
```

Note

The channel-id parameter must be set to 1 for the radio interface and 2 for the Ethernet interface.

- In Multi-Carrier ABC Group view, use the following command to set the maximum traffic that the PTP 850E will pass to the paired unit:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-set-eth-
max-bandwidth slot 1 port 2 max-bandwidth <1-1000>
```

  - When using Fixed ACM mode, set this parameter to the actual rate you want the paired unit to broadcast.
  - When using Adaptive ACM mode, set this parameter to the maximum of the paired unit’s capacity.

The default value is 1000 Mbps.

For example, the following command sets the maximum traffic to 900 Mbps:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-set-eth-
max-bandwidth slot 1 port 2 max-bandwidth 900


Maximum bandwidth: 900 Mbps
```

Use the following command in Multi-Carrier ABC Group view to display the current maximum traffic setting:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-show-eth-
max-bandwidth slot 1 port 2
```

Note

The Maximum Bandwidth represents the L1 capacity of the radio link connected to the Ethernet member. The actual bandwidth that will be available for traffic is less due to overhead.

> When using a third-party radio as the paired unit, it is particularly important to set this parameter properly in order to ensure optimal performance. Failure to properly set this parameter may lead to frequent pauses as the queue fills up during low capacity periods, such as when weather conditions cause the ACM profile to drop.

- In Multi-Carrier ABC Group view, use the following command to set the bandwidth margin, in Mbps. This parameter deducts the specified throughput from the throughput the PTP 850E would otherwise pass to the paired unit. The purpose of this parameter is to provide a margin of safety that will avoid loss of traffic in the event that the ACM profile is reduced on the paired unit.

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-set-eth-
bandwidth-margin slot 1 port 2 bandwidth-margin 100 <5-100>
```

It is recommended to configure this parameter as follows:

- If the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, or a third-party device with a bandwidth notification mechanism that will inform the PTP 850E of an impending reduction of the ACM profile before the reduction takes place, it is recommended to leave this parameter at its default value of 5 Mbps.
- If the paired unit is a third-party device without a bandwidth notification mechanism that will inform the PTP 850E of an impending reduction of the ACM profile before the reduction takes place, it is recommended to set this parameter to an amount equal to or greater than the largest throughput differential between any two adjacent profiles for the script configured on the paired unit.

The range of values is 5 to 100 Mbps.

For example, the following command sets the bandwidth margin to 100 Mbps:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>abc-set-eth-
bandwidth-margin slot 1 port 2 bandwidth-margin 100
```

Use the following command in Multi-Carrier ABC Group view to display the current bandwidth margin:

```
abc-show-eth-bandwidth-margin slot 1 port 2
```

1. Enable the Eth2 interface. See *Enabling the Interfaces (CLI)*.
2. If the paired unit is an PTP 820C or PTP 820C-HP, verify that XPIC is disabled on the PTP 820C or PTP 820C-HP.
3. On the paired unit, configure a Pipe service between the port receiving traffic from the PTP 850E and the radio or Multi-Carrier ABC group.
4. On the paired unit, configure Automatic State Propagation with **ASP trigger by remote fault** enabled.
5. If the paired unit is an PTP 820C, PTP 820C-HP, or PTP 820S, configure Radio BNM. For instructions, refer to the *User Guide for PTP 820 All-Outdoor Products*. Make sure to define a Name for the Radio BNM group.

> **Note:** If the paired unit is a third-party radio, enable 802.3X Flow Control.

Multiband Management (CLI)

The PTP 850E unit in a Multiband configuration can be managed normally, as in any other configuration. For in-band management of the PTP 850E, configure the management service on the PTP 850E Multiband group. See *Configuring In-Band Management (CLI).*

The following options are available for managing the paired unit in a Multiband configuration:

- Inband management via the PTP 850E
- Inband management directly from the external switch
- Out-of-Band management

For a detailed explanation of these options and their requirements, see Multiband Management.

Configuring Synchronization in a Multiband Node (CLI)

SyncE and 1588 Boundary Clock can be used in Multiband nodes. SyncE and 1588 Boundary Clock can be configured for both the PTP 850E and the unit paired with the PTP 850E. SyncE packets are carried between the units along with traffic; no special cables are required.

> Note
>
> When a third-party unit is paired with the PTP 850E, it is a prerequisite that the third-party radio unit support SyncE in order to provide synchronization for the Multiband node.

For details, see Configuring Synchronization in a Multiband Node.

For instructions on configuring SyncE, see Configuring the Sync Source (CLI).

Deleting a Multiband Group (CLI)

If you need to delete the Multiband group, you must first remove the group's members, then delete the group.

To remove members from a Multi-Carrier ABC group, go to Multi-Carrier ABC group view and enter the following command for each interface in the group:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>detach-member
channel-id <1-2>
```

After removing the members, enter the following command in root view:

```
root> multi-carrier-abc delete group group_id 1 slot 1 type Enhanced
```

Displaying Multiband Group Statistics (CLI)

To display general information about a Multiband group, including the group's TX and RX capacity, go to Multi-Carrier ABC group view and enter the following command:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>summary-show
```

To display port counters for a Multiband group, go to Multi-Carrier ABC group view and enter the following command:

```
multi-carrier-abc enhanced-group-id [1] slot [1]>show-ethernet-port-counters
```

Configuring XPIC (CLI)

Note

This section is only relevant for PTP 850E.

For a general explanation of XPIC in PTP 850E, see XPIC Overview.

Configuring the Radio Carriers for XPIC (CLI)

For PTP 850C, you must create and enable a single AMCC (XPIC) group on both sides of the link. The group must include both carriers on the PTP 850C unit, with opposite polarizations.

For PTP 850E, you must create and enable an AMCC group on each PTP 850E. Each group must include that unit’s radio carrier.

Configuring the Radio Carriers for XPIC an PTP 850C (CLI)

To configure the radio carriers for XPIC on an PTP 850C:

1 Configure the radio carrier in each unit on both ends of the link to the desired frequency channel. All radio carriers in the link must be configured to the same frequency channel.

2 Assign a script that supports XPIC to both radio carriers on both ends of the link. See Configuring the Radio (MRMC) Script(s) (CLI).

3 Create an AMCC (XPIC) group. To create an AMCC (XPIC) group, enter the following command:

```
root> amcc create group group_id 1 group_type xpic
group_sub_type external
```

The following should appear:

```
group_id 1, group_type xpic created
```

4 Attach the radio carrier to the AMCC (XPIC) group. To attach the radio carrier, enter the group view and attach the carrier using the following commands:

```
root>amcc group group_id 1 group_type xpic
xpic-group[1]>

xpic-group[1]>amcc attach slot 1 port 1 role <member-h|member-v>
```

The following should appear:

```
slot 1 port 1 role member h attached to group_id 1 group_type xpic
```

The **role** parameter can be `member-h` (Horizontal) or `member-v` (Vertical). Make sure the **role** you select matches the actual polarization of the PTP 850E unit, and that the **role** you configure in the paired unit is not the same as the role you configure here.

5 Enable the group. To enable the group, enter the following command in group view:

```
xpic-group[1]>set admin enable
```

The following should appear:

```
group_id 1 group_type xpic 'Admin Enabled'
```

Once you have configured XPIC on both units at both sides of the link, perform antenna alignment. For instructions, see Performing Antenna Alignment for XPIC.

Configuring the Radio Carriers for XPIC on an PTP 850E (CLI)

To configure the radio carriers for XPIC on an PTP 850E:

1. Configure the radio carrier in each unit on both ends of the link to the desired frequency channel. All radio carriers in the link must be configured to the same frequency channel.
2. Assign a script that supports XPIC to both radio carriers on both ends of the link. See *Configuring the Radio (MRMC) Script(s) (CLI)*.

3 Create an AMCC (XPIC) group. To create an AMCC (XPIC) group, enter the following command:

```
root> amcc create group group_id 1 group_type xpic
group_sub_type external
```

The following should appear:

```
group_id 1, group_type xpic created
```

4 Attach the radio carrier to the AMCC (XPIC) group. To attach the radio carrier, enter the group view and attach the carrier using the following commands:

```
root>amcc group group_id 1 group_type xpic
xpic-group[1]>

xpic-group[1]>amcc attach slot 1 port 1 role <member-h|member-v>
```

The following should appear:

```
slot 1 port 1 role member h attached to group_id 1 group_type xpic
```

The **role** parameter can be `member-h` (Horizontal) or `member-v` (Vertical). Make sure the **role** you select matches the actual polarization of the PTP 850E unit, and that the **role** you configure in the paired unit is not the same as the role you configure here.

5 Enable the group. To enable the group, enter the following command in group view:

```
xpic-group[1]>set admin enable
```

The following should appear:

```
group_id 1 group_type xpic 'Admin Enabled'
```

Once you have configured XPIC on both units at both sides of the link, perform antenna alignment. For instructions, see *Performing Antenna Alignment for XPIC*.

Deleting an AMCC (XPIC) Group

To delete an AMCC (XPIC) group:

1 Disable the group. To disable an AMCC (XPIC) group, enter the following command in group view:

```
xpic-group[1]>set admin disable
```

The following should appear:

```
group_id 1 group_type xpic 'Admin Disabled'
```

2 Remove the radio carrier from the group. To remove the radio carrier from the group, enter the following command in group view:

```
xpic-group[1]>amcc detach slot 1 port 1
```

The following should appear:

```
slot 1 port 1 detached from group_id 1 group_type xpic
```

3 1 Delete the group. To delete the group, enter the following command in root view:

```
root>amcc delete group group_id 1 group_type xpic
```

The following should appear:

```
group_id 1 group_type xpic deleted
```

Displaying XPIC Status (CLI)

To display basic information about an AMCC (XPIC) group, enter either of the following command in root view:

```
root>amcc show groups
```

If an XPIC group is configured on the unit, the following is displayed:

```
group_id 1 group_type xpic group_sub_type external
```

Alternatively, enter the following command in root view:

```
root>amcc show group_id 1 group_type xpic
```

If an XPIC group is configured on the unit, the following is displayed:

```
group_id 1 group_type xpic group_sub_type external
```

To display the Admin status of the XPIC group, enter the following command in group view:

```
xpic-group[1]>show admin
```

If the group is enabled, the following output is displayed:

```
group_id 1 group_type xpic 'Admin Enabled'
```

To display the role (polarization) assigned to the unit and the XPIC status of the unit, enter the following command in group view:

```
xpic-group[1]>show members
```

The following output indicates that the unit is assigned the Vertical role (v), and the status is normal:

```
slot 1 port 1 role member v state Idle
```

The following output indicates that the unit is assigned the Horizontal role (h), and the status is normal:

```
slot 1 port 1 role member h state Idle
```

To display the XPIC status of the unit, enter the following command in group view:

```
xpic-group[1]>show advanced-status
```

The following output indicates that the status is normal:

```
xpic state: IDLE
```

The following are the possible statuses:

- **IDLE** – XPIC is working properly.
- **INIT** – Indicates that the **Admin** state of the radio interface is **Down**. Go to the Interface Manager and set the **Admin** status of the radio interface to **Up**.
- **Configuration not supported** – Indicates that the MRMC script configured for the radio carrier does not support XPIC. See *Configuring the Radio (MRMC) Script(s) (CLI)*.
- **Single Channel** – Indicates one of the following:
    - The Clock Sharing cable is not connected to one of the units, or is defective.
    - The XPIC cable is not connected to one of the units, or is defective.
    - One of the PTP 850E units in the XPIC pair is down.

If this status appears, make sure that both units are up and check that all the cables are properly connected.

Configuring 1+1 HSB Unit Protection (CLI)

Note: This section is only relevant for PTP 850E.

This section includes:

- Configuring Ethernet Interface Protection (CLI)
- Configuring HSB Unit Protection (CLI)
- Configuring Revertive Protection (CLI)
- Viewing the Configuration of the Standby unit (CLI)
- Editing Standby Unit Settings (CLI)
- Viewing Link and Protection Status and Activity (CLI)
- Manually Switching to the Standby Unit (CLI)
- Disabling Automatic Switchover to the Standby Unit (CLI)
- Disabling Unit Protection (CLI)

For an overview of 1+1 HSB Unit Protection, see *1+1 HSB Unit Protection Overview*.

To configure unit protection, you must perform the following steps:

1. Configure Ethernet interface protection. See *Configuring Ethernet Interface Protection (CLI)*.
2. Configure HSB unit protection. See *Configuring HSB Unit Protection (CLI)*.
3. Optionally, you can configure revertive protection to ensure that the primary path is used whenever possible. See *Configuring Revertive Protection (CLI)*.

Configuring Ethernet Interface Protection (CLI)

The Ethernet interfaces can be protected in either of two ways:

- **Split Protection Mode** – For Port 5 (SFP+, Eth 7), an optical splitter is used to route traffic to Port 5 on each PTP 850E unit. For Port 4 (QSFP, Eth3-6), an optical splitter is used with MPO-MPO cables to route traffic to the QSFP splitter for each PTP 850E unit.

Note: For the QSFP port, Split Protection mode can only be used for 4x1/10Gbps configurations, not 1x40Gbps configurations. Support for Split Protection mode with 1x40Gbps is planned for future release.

- **Line Protection Mode** – Traffic is routed from two Ethernet ports on the external switch to a port on the active PTP 850E unit and a port on the standby PTP 850E unit. LACP protocol is used to determine which PTP 850E port is active and which port is standby, and traffic is only forwarded to the active port. Line Protection mode can be used with all PTP 850E Ethernet ports supported for traffic.

Configuring Split Ethernet Interface Protection Mode (CLI)

To configure split Ethernet interface protection mode:

1. For each Ethernet link, use an optical splitter to route traffic between the Ethernet port on the external switch and an Ethernet port on each PTP 850E unit or each QSFP splitter.
2. Proceed to *Configuring HSB Unit Protection (CLI)*.

Configuring Line Protection Mode (CLI)

To configure line protection mode:

1 Configure the Ethernet ports on the external switch in LACP mode. The external switch must support LACP.

Note: PTP 850 supports a special LACP implementation for purposes of line protection only. This LACP implementation is configured on the logical interface level, as described below. Regular LACP is configured as part of the LAG configuration, and is not supported with unit redundancy. See Configuring Link Aggregation (LAG) and LACP (Optional) (CLI).

2 For each Ethernet link, connect one port on the external switch to an Ethernet port on the active PTP 850E (or QSFP splitter), and the other port on the external switch to an Ethernet port on the standby PTP 850E (or QSFP splitter).

3 Enable LACP on each Ethernet interface connected to the external switch on the active PTP 850E:

i Go to interface view for the Ethernet interface connected to the external switch on the active PTP 850E.

ii In interface view, enter the following command:

```
eth type eth [1/x]>interface-mode-set interface-mode LACP
```

To disable LACP mode, enter the following command in Ethernet interface view:

```
eth type eth [1/x]>interface-mode-set interface-mode NONE
```

To display an interface’s current LACP setting, enter the following command in

Ethernet interface view:

```
eth type eth [1/x]>interface-mode-show
```

Configuring HSB Unit Protection (CLI)

To configure HSB unit protection:

Before enabling protection, you must:

1 Verify that both units have the same hardware part number (see *Displaying Unit Inventory (CLI)*) and the same software version (see *Viewing Current Software Versions (CLI)*). If the units do not have the same software version, upgrade each unit to the most recent software release (see *Configuring a Software Download (CLI)*).

2 Assign an IP address to each unit. For instructions, see *Changing the Management IP Address (CLI)*.

3 Establish a management connection to one of the units. You can select either unit; once you enable Protection Administration, the system will determine which unit becomes the Active unit.

4 To enable protection, enter the following command in root view:

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

The system configures itself for HSB protection:

- The system determines which unit is the Active unit based on a number of pre-defined criteria.
- When the system returns online, all management must be performed via the Active unit using the IP address you defined for that unit.
- The IP address you defined for the unit which is now the Standby unit is no longer valid, and the management port of the Standby unit becomes non- operational.
- Management of the Standby unit is performed via the Active unit, via the cable between the two Protection ports connecting the two units.
- HSB protection is enabled on both units.

5 Once you have enabled Protection Admin:

i Perform all necessary radio configurations on the Active unit, such as setting the frequency, assigning MRMC scripts, and unmuting the radio.

ii Perform all necessary Ethernet configurations on the Active unit, such as defining Ethernet services.

iii Enter the following command in root view to copy the configuration of the Active unit to the Standby unit:

```
root> platform management protection copy-to-mate
```

To keep the Standby unit up-to-date, after any change to the configuration of the Active unit enter the copy-to-mate command to copy the configuration to the Standby unit.

If you are unsure whether the Standby unit's configuration matches that of the Active unit, enter the following command in root view. The command output displays the list of mismatched parameters.

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

Configuring Revertive Protection (CLI)

To configure revertive mode, enter the following command in root view:

```
root> platform management protection revertive set admin
<enable|disable>
```

To set the active unit to be the primary unit, enter the following command in root view:

```
root> platform management protection revertive set primary yes
```

If you set the active unit to be the primary unit, you must enter the following command in the standby unit:

```
root> platform management protection revertive set primary no
```

See *Editing Standby Unit Settings (CLI)*.

To configure the revertive mode wait-to-restore timer (in seconds), enter the following command in root view:

```
root> platform management protection revertive set wtr <10-600>
```

To display the revertive mode settings, enter the following command in root view:

```
root> platform management protection revertive show
```

Viewing the Configuration of the Standby unit (CLI)

You can view the settings of the standby unit any time.

To view the settings of the standby unit, you can run show commands in the standby unit. To do so, first enter the mate/root context, as described in *Performing CLI operations on the Standby Unit (CLI)*, then run the relevant show command, and then switch back to the active unit.

Editing Standby Unit Settings (CLI)

Almost all settings of the standby unit are view-only. However, several settings are editable on the Standby unit. They must be configured separately for the Standby unit, and are not copied via copy-to-mate, nor do they trigger a configuration mismatch in the CLI.

In the Web EMS, failure to synchronize these configuration settings causes a configuration mismatch alarm.

The following settings must be configured separately on the standby unit:

- Revertive Mode – If Revertive Mode is enabled, you must set the `platform management protection revertive set primary` command in the standby unit to the opposite setting as the active unit. See *Configuring Revertive Protection (CLI)*.
- Setting the Unit Name. See *Configuring Unit Parameters (CLI)*.
- Disabling/enabling Radio TX-mute. See *Muting and Unmuting a Radio (CLI)*.
- Clearing the Radio and RMON counters. See *Displaying General Modem Status and Defective Block PMs (CLI)*.
- Setting the activation key configuration. See *Configuring the Activation Key (CLI)* and *Activating Demo Mode (CLI)*.
- Defining user accounts. See *Configuring User Accounts (CLI)*.
- Setting synchronization settings. See *Synchronization (CLI)*.

To configure these settings in the standby unit, first enter the mate/root context, as described in *Performing CLI operations on the Standby Unit (CLI)*, then run the relevant commands, and then switch back to the active unit

Performing CLI operations on the Standby Unit (CLI)

You can run CLI commands in the standby unit. To run

CLI commands in the standby unit:

1 Use the following command to enter view context for the standby unit:

```
root> switch-to mate

mate/root>
```

2 Enter the specific CLI command you want to run in mate/root context.

3 To switch back to the active unit, enter the following command:

```
mate/root> switch-back

root>
```

Viewing Link and Protection Status and Activity (CLI)

You can view link and protection status and activity any time.

- To view whether HSB protection is enabled or disabled, enter the following command in root view:

```
root> platform management protection show admin
```

- To view whether HSB protection is functional (available in practice), enter the following command in root view. Note that protection is not functional if MIMO is configured, or if the management connection to the mate is down.

```
root> platform management protection show operational-state
```

- To view protection activity, enter the following command in root view:

```
root> platform management protection show activity-state
```

- To view the status of the protection link to the mate, enter the following command in root view:

```
root> platform management protection show link-status
```

- To view the status of the last copy-to-mate operation, enter the following command in root view:

```
root> platform management protection show copy-to-mate status
```

Manually Switching to the Standby Unit (CLI)

At any point, you can manually switch to the Standby unit, provided that the highest protection fault level in the Standby unit is no higher than the highest protection fault level on the Active unit.

To manually switchover to the Standby unit enter the following in root view:

```
root> platform management protection set manual-switch
```

Disabling Automatic Switchover to the Standby Unit (CLI)

At any point, you can perform lockout, which disables automatic switchover to the standby unit.

To disable automatic switchover to the Standby unit, use the following command in root view:

```
root> platform management protection lockout set admin on
```

To re-enable automatic switchover to the standby unit, use the following command in root view:

```
root> platform management protection lockout set admin off
```

Disabling Unit Protection (CLI)

You can disable unit protection at any time. If you disable unit protection, keep in mind that while the unit that was formerly the active unit maintains its IP address, the unit that was formerly the standby unit is assigned the default IP address (192.168.1.1)

To disable protection, enter the following command in root view.

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

Configuring Link Aggregation (LAG) and LACP (Optional) (CLI)

Note

This section is only relevant for PTP 850S.

Link aggregation (LAG) enables you to group several physical Ethernet or radio interfaces into a single logical interface bound to a single MAC address. This logical interface is known as a LAG group. Traffic sent to the interfaces in a LAG group is distributed by means of a load balancing mechanism. PTP 850S uses a distribution function of up to Layer 4 in order to generate the most efficient distribution among the LAG physical ports.

This section explains how to configure LAG and includes the following topics:

- LAG Overview (CLI)
- Configuring a LAG Group (CLI)
- Configuring LACP (CLI)
- Viewing LAG Details (CLI)
- Editing and Deleting a LAG Group (CLI)
- Enabling and Disabling the LAG Group Shutdown in Case of Degradation Event Option (CLI)
- Configuring Enhanced LAG Distribution (CLI)
- Displaying LACP Parameters and Statistics (CLI)

LAG Overview (CLI)

Link aggregation (LAG) enables you to group several physical Ethernet or radio interfaces into a single logical interface bound to a single MAC address. This logical interface is known as a LAG group. Traffic sent to the interfaces in a LAG group is distributed by means of a load balancing mechanism. PTP 850S uses a distribution function of up to Layer 4 in order to generate the most efficient distribution among the LAG physical ports.

LAG can be used to provide interface redundancy, both on the same card (line protection) and on separate cards (line protection and equipment protection).

LAG can also be used to aggregate several interfaces in order to create a wider (aggregate) link. For example, LAG can be used to create a 4 Gbps channel.

You can create up to four LAG groups.

The following restrictions exist with respect to LAG groups:

- Only physical interfaces (including radio interfaces), not logical interfaces, can belong to a LAG group.
- Interfaces can only be added to the LAG group if no services or service points are attached to the interface.
- Any classification rules defined for the interface are overridden by the classification rules defined for the LAG group.

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

There are no restrictions on the number of interfaces that can be included in a LAG. It is recommended, but not required, that each interface in the LAG have the same parameters (e.g., speed, duplex mode).

> Note
>
> To add or remove an Ethernet interface to a LAG group, the interface must be in an administrative state of “down”. This restriction does not apply to radio interfaces. For instructions on setting the administrative state of an interface, see Enabling the Interfaces (CLI).

PTP 850S supports LACP, which expands the capabilities of static LAG and provides interoperability with third-party equipment that uses LACP. LACP improves the communication between LAG members. This improves error detection capabilities in situations such as improper LAG configuration or improper cabling. It also enables the LAG to detect uni-directional failure and remove the link from the LAG, preventing packet loss.

LACP is enabled as part of the LAG configuration process. It should only be used if the LAG is in a link with another LACP-enabled LAG.

> Note
>
> LACP can only be used with Ethernet interfaces. LACP cannot be used with Enhanced LAG Distribution or with the LAG Group Shutdown in Case of Degradation Event feature.

Configuring a LAG Group (CLI)

To create a LAG:

1 Go to interface view for the first interface you want to assign to the LAG and enter the following command:

```
eth type eth [x/x]> static-lag add lagid <lagid>
```

2 Repeat this process for each interface you want to assign to the LAG.

Configuring LACP (CLI)

To enable LACP on a LAG group, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> lacp admin set enable
```

To disable LACP on a LAG group, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> lacp admin set disable
```

To display whether or not LACP is enabled on a LAG group, go to interface view for the LAG and enter the following command:

```
eth group [lagx]>lacp admin show
```

The following commands enable LACP for LAG group 1:

```
root> ethernet interfaces group lag1
eth group [lag1]>lacp admin set enable
eth group [lag1]>
```

Viewing LAG Details (CLI)

To display the name of a LAG to which an interface belongs, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> static-lag show name
```

To enter interface view for a LAG, enter the following command in root view:

```
root> ethernet interfaces group <lagid>
```

To display details about a LAG, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> summary show
```

To display a LAG's operational state, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> operational state show
```

To display a list of interfaces that belong to a LAG, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> port static-lag show members
```

Editing and Deleting a LAG Group (CLI)

To remove a member Ethernet interface from a LAG, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> port static-lag remove member interface eth
slot <slot> port <port>
```

To remove a member radio interface from a LAG, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> port static-lag remove member interface radio
slot <slot> port <port>
```

To delete a LAG, go to interface view for the LAG and simply remove all the members, as described above.

Table 96 LAG Group CLI Parameters

Parameter	Input Type	Permitted Values	Description
lagid	Variable	lag1 lag2 lag3 lag4	The ID for the LAG.
slot	Number	1	
port	Number	Ethernet interface on PTP 850C: 1-4 Ethernet interface on PTP 850E: 1-7 Ethernet interface on PTP 850S: 1-3 Radio interface on an PTP 850C: 1-2 Radio interface on an PTP 850E or PTP 850S: 1 Management: 1	The port number of the interface.

For PTP 850C following commands create a LAG with the ID lag2. The LAG includes the Ethernet interfaces 1 and 2 and the radio interface:

```
root> platform if-manager set interface-type ethernet slot 1
port 1 admin down

root> platform if-manager set interface-type ethernet slot 1
port 2 admin down

root> ethernet interfaces eth slot 1 port 1

eth type eth [1/1]>

eth type eth [1/1]> static-lag add lagid lag2

eth type eth [1/1]> exit

root>

root> ethernet interfaces eth slot 1 port 2

eth type eth [1/2]>
eth type eth [1/2]> static-lag add lagid lag2

eth type eth [1/2]> exit

root>

root> ethernet interfaces radio slot 2 port 1

eth type radio[2/1]>

eth type radio[2/1]> static-lag add lagid lag2

eth type radio[2/1]> exit
```

```
root> platform if-manager set interface-type ethernet slot 1
port 2 admin up
```

For PTP 850E, the following commands create a LAG with the ID lag1. The LAG includes Ethernet interfaces 3, 4, and 7 and the radio:

```
root> platform if-manager set interface-type ethernet slot 1
port 3 admin down

root> ethernet interfaces eth slot 1 port 3

eth type eth [1/3]>

eth type eth [1/3]> static-lag add lagid lag1

eth type eth [1/3]> exit

root>

root> platform if-manager set interface-type ethernet slot 1
port 4 admin down

root> ethernet interfaces eth slot 1 port 4

eth type eth [1/4]>

eth type eth [1/4]> static-lag add lagid lag1

eth type eth [1/4]> exit

root> platform if-manager set interface-type ethernet slot 1
port 7 admin down

root> ethernet interfaces eth slot 1 port 7

eth type eth [1/7]>

eth type eth [1/7]> static-lag add lagid lag1

eth type eth [1/7]> exit

root> ethernet interfaces radio slot 1 port 1

eth type radio[1/1]>

eth type radio[1/1]> static-lag add lagid lag1

eth type radio[1/1]> exit

root> platform if-manager set interface-type ethernet slot 1
port 3 admin up

root> platform if-manager set interface-type ethernet slot 1
port 4 admin up
```

For PTP 850C, the following commands create a LAG with the ID lag1. The LAG includes Ethernet interfaces 3 and 4 and radio carrier 1:

```
root> platform if-manager set interface-type ethernet slot 1
port 3 admin down
root> ethernet interfaces eth slot 1 port 3
eth type eth [1/3]>
eth type eth [1/3]> static-lag add lagid lag1
eth type eth [1/3]> exit
root>

root> platform if-manager set interface-type ethernet slot 1
port 4 admin down
root> ethernet interfaces eth slot 1 port 4
eth type eth [1/4]>
eth type eth [1/4]> static-lag add lagid lag1
eth type eth [1/4]> exit
root> ethernet interfaces radio slot 1 port 1
eth type radio[1/1]>
eth type radio[1/1]> static-lag add lagid lag1
eth type radio[1/1]> exit
root> platform if-manager set interface-type ethernet slot 1
port 3 admin up
```

The following command displays the name of the LAG to which Ethernet port 1 belongs:

```
eth type eth [1/1]> static-lag show name

Static-lag group name: lag2
```

The following commands display details about the LAG:

```
root> ethernet interfaces group lag2

eth group [lag2]>

eth group [lag2]> port static-lag show members

Static-lag members

-------------------


Eth#[1/1]
Eth#[1/2]
Radio#[2/1]

eth group [lag2]> summary show

Group lag2 Summary:    Value
Port Description:

Port Admin state:     enable
Port Operational state:   down

Port Edge state:     non-edge-port
Member Port#(1)      1/1

Member Port#(2)      1/2
Member Port#(3)      1/1

eth group [lag2]> operational state show
```

The following commands remove port 2 on slot 1 from the LAG:

```
root> platform if-manager set interface-type ethernet slot 1
port 2 admin down

root> ethernet interfaces group lag2

eth group [lag2]>

eth group [lag2]> port static-lag remove member interface eth
slot 1 port 2
```

Enabling and Disabling the LAG Group Shutdown in Case of Degradation Event Option (CLI)

Note

LAG Group Shutdown in Case of Degradation Event cannot be used ith LACP.

A LAG group can be configured to be automatically closed in the event of LAG degradation. This option is used if you want traffic from the switch to be re-routed during such time as the link is providing less than a certain capacity.

By default, the LAG group shutdown in case of degradation event option is disabled. When enabled, the LAG is automatically closed in the event that any one or more ports in the LAG fail. When all ports in the LAG are again operational, the LAG is automatically re-opened.

Note

Failure of a port in the LAG also triggers a lag-degraded alarm, Alarm ID 100.

To enable the LAG group shutdown in case of degradation event option, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> static-lag set lag-degrade-admin admin enable
```

To disable the LAG group shutdown in case of degradation event option , go to interface view for the LAG and enter the following command:

```
eth group [lagx]> static-lag set lag-degrade-admin admin
disable
```

To display the current LAG group shutdown in case of degradation event option setting, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> static-lag show lag-degrade-admin
```

The following commands enable the LAG group shutdown in case of degradation event option for LAG group 1:

```
root> ethernet interfaces group lag1
eth group [lag1]>static-lag set lag-degrade-admin admin enable
eth group [lag1]>
```

Configuring Enhanced LAG Distribution (CLI)

You can change the distribution function by selecting from ten pre-defined LAG distribution schemes. The feature includes a display of the TX throughput for each interface in the LAG, to help you identify the best LAG distribution scheme for the specific link.

Note: Enhanced LAG distribution is only available for LAG groups that consist of exactly two interfaces. It cannot be used with LACP.

To configure enhanced LAG distribution, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> static-lag set df-pattern df <1-10>
```

The following commands set the LAG distribution scheme for LAG group 1 as distribution pattern 3.

```
root> ethernet interfaces group lag1
eth group [lag1]>static-lag set df-pattern df 3
```

The default LAG distribution pattern is 1.

To display the current LAG distribution scheme, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> static-lag show df-pattern
```

It is recommended to experiment with the various schemes by monitoring the TX port PMs for each interface in the LAG for each LAG distribution scheme. In the Web EMS, the page in which you configure enhanced LAG distribution also displays TX throughput PMs per interface. See *Configuring Enhanced LAG Distribution*. For information on monitoring Ethernet port PMs via the CLI, see *Displaying Ethernet Port PMs (CLI)*.

Displaying LACP Parameters and Statistics (CLI)

You can display the following LACP parameters and statistics:

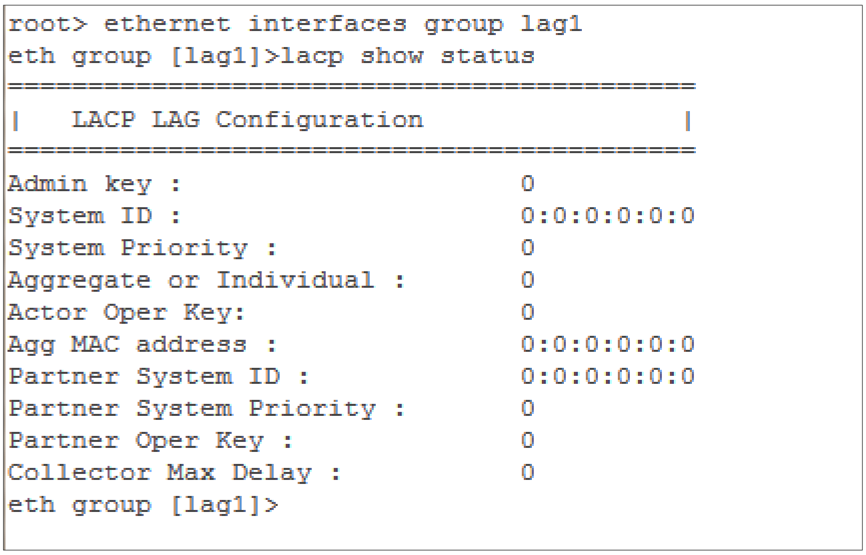
- LACP Aggregation (per LAG)
- LACP Port Status
- LACP Port Statistics
- LACP Port Debug Statistics

> Note
>
> PTP 850S does not support any LACP write parameters.

Displaying LACP Aggregation Status Parameters (CLI)

To display LACP aggregation status parameters, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> lacp show status
```



```
root> ethernet interfaces group lag1
eth group [lag1]>lacp show status
===========================================
|   LACP LAG Configuration                |
===========================================
Admin key :                     0
System ID :                     0:0:0:0:0:0
System Priority :               0
Aggregate or Individual :       0
Actor Oper Key:                 0
Agg MAC address :               0:0:0:0:0:0
Partner System ID :             0:0:0:0:0:0
Partner System Priority :       0
Partner Oper Key :              0
Collector Max Delay :           0
eth group [lag1]>
```

Table 97 LACP Aggregation Status Parameters (CLI

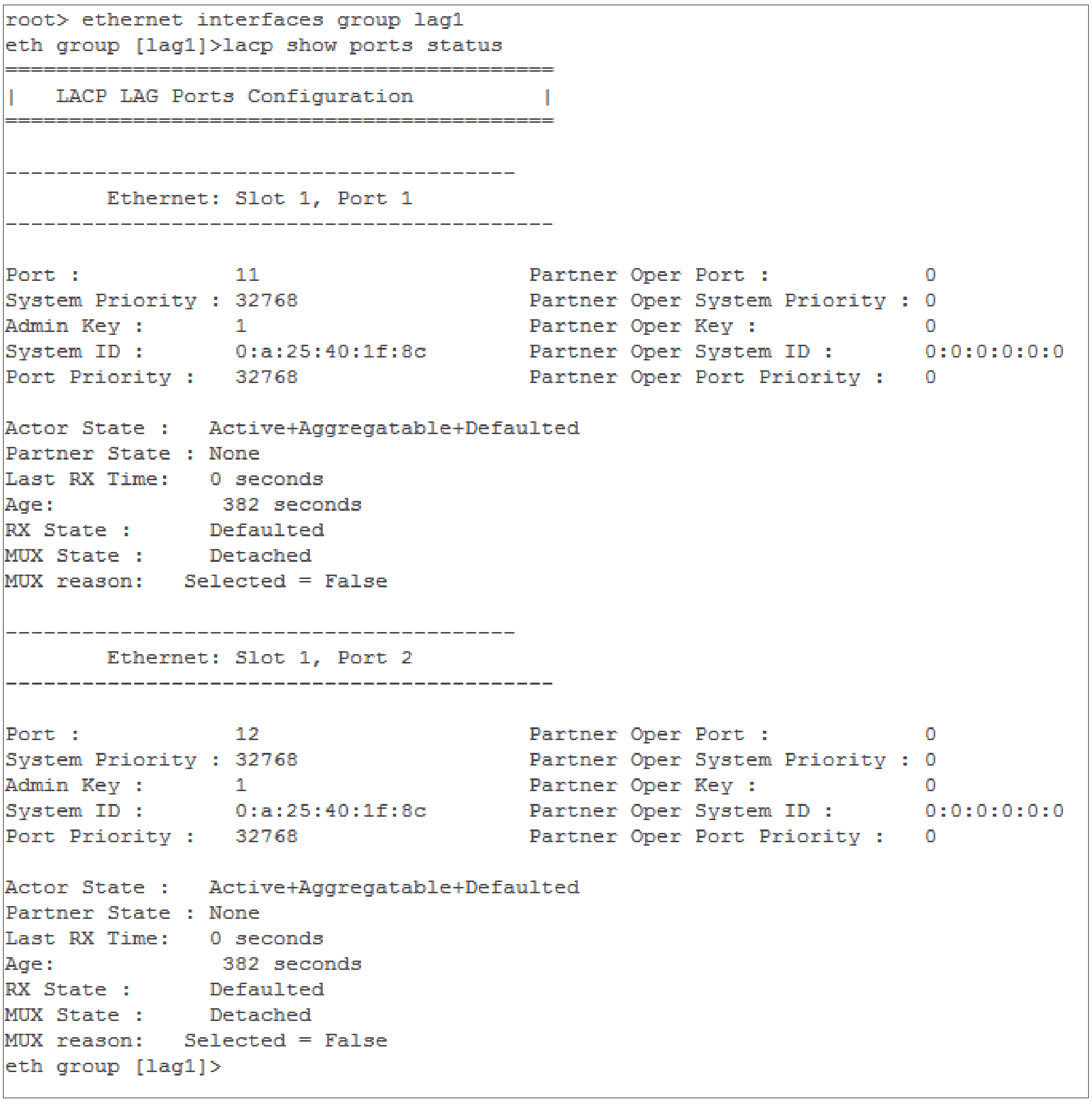
Parameter	Definition
Admin Key	The current administrative value of the key for the Aggregator.

System ID	The MAC address value used as a unique identifier for the system that contains this Aggregator.
System Priority	The priority value associated with the Actor's System ID.
Aggregate or Individual	Indicates whether the Aggregator represents an aggregate or an individual link.
Actor Oper Key	The current operational value of the Key for the Aggregator.
Agg MAC Address	The individual MAC address assigned to the Aggregator.
Partner System ID	The MAC address value consisting of the unique identifier for the current protocol Partner of this Aggregator.
Partner System Priority	The priority value associated with the Partner's System ID.
Partner Oper Key	The current operational value of the Key for the Aggregator's current Protocol partner.
Collector Max Delay	The maximum delay, in tens of microseconds.

Displaying LACP Port Status Parameters (CLI)

To display LACP port status parameters, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> lacp show ports status
```



```
root> ethernet interfaces group lag1
eth group [lag1]>lacp show ports status
===========================================
|   LACP LAG Ports Configuration          |
===========================================

----------------------------------------
        Ethernet: Slot 1, Port 1
-------------------------------------------

Port :            11                     Partner Oper Port :            0
System Priority : 32768                  Partner Oper System Priority : 0
Admin Key :       1                      Partner Oper Key :             0
System ID :       0:a:25:40:1f:8c        Partner Oper System ID :       0:0:0:0:0:0
Port Priority :   32768                  Partner Oper Port Priority :   0

Actor State :   Active+Aggregatable+Defaulted
Partner State : None
Last RX Time:   0 seconds
Age:             382 seconds
RX State :      Defaulted
MUX State :     Detached
MUX reason:   Selected = False

----------------------------------------
        Ethernet: Slot 1, Port 2
-------------------------------------------

Port :            12                     Partner Oper Port :            0
System Priority : 32768                  Partner Oper System Priority : 0
Admin Key :       1                      Partner Oper Key :             0
System ID :       0:a:25:40:1f:8c        Partner Oper System ID :       0:0:0:0:0:0
Port Priority :   32768                  Partner Oper Port Priority :   0

Actor State :   Active+Aggregatable+Defaulted
Partner State : None
Last RX Time:   0 seconds
Age:             382 seconds
RX State :      Defaulted
MUX State :     Detached
MUX reason:   Selected = False
eth group [lag1]>
```

Table 98 LACP Port Status Parameters (CLI)

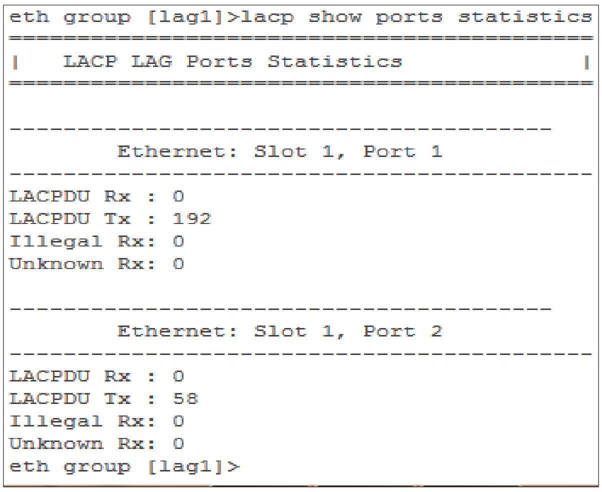
Parameter	Definition
System Priority	The priority value associated with the Actor’s System ID.
Admin Key	The current administrative value of the Key for the Aggregation Port.
System ID	The MAC Address value that defines the value of the System ID for the system that contains this Aggregation Port.
Port Priority	The priority value assigned to this Aggregation Port.
Actor State	The current operational values of the Actor’s state as transmitted by the Actor via LACPDUs.
Partner State	The current values of Actor State in the most recently received LACPDU transmitted by the protocol Partner.

Last RX Time	The value of a TimeSinceSystemReset (F.2.1) when the last LACPDU was received by this Aggregation port.
RX State	The state of the receive state machine for the Aggregation port. Possible values are: • **Current** – An LACPDU was received before expiration of the most recent timeout period. • **Expired** – No LACPDU was received before expiration of the most recent timeout period. **Defaulted** – No LACPDU was received during the two most recent timeout periods.
Mux State	The state of the Mux state machine for the Aggregation port. Possible values are Collecting, Distributing, Attached, and Detached.
Mux Reason	A text string indicating the reason for the most reason change in the state of the Mux machine.
Partner Oper Port	The operational port number assigned to this Aggregation port by the Aggregation port's port Partner.
Partner Oper System Priority	The operational value of priority associated with the Partner's System ID.
Partner Oper Key	The current operational value of the Key for the protocol Partner.
Partner Oper System ID	The MAC Address value representing the current value of the Aggregation Port's protocol Partner's System ID.
Partner Oper Port Priority	The Priority value assigned to this Aggregation port by the Partner.

Displaying LACP Port Statistics (CLI)

To display LACP port statistics, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> lacp show ports statistics
```



```
eth group [lag1]>lacp show ports statistics
===========================================
|   LACP LAG Ports Statistics             |
===========================================

----------------------------------------
        Ethernet: Slot 1, Port 1
-------------------------------------------
LACPDU Rx : 0
LACPDU Tx : 192
Illegal Rx: 0
Unknown Rx: 0

----------------------------------------
        Ethernet: Slot 1, Port 2
-------------------------------------------
LACPDU Rx : 0
LACPDU Tx : 58
Illegal Rx: 0
Unknown Rx: 0
eth group [lag1]>
```

Table 99 LACP Port Statistics (CLI)

Parameter	Definition
LACPDU RX	The number of LACPDUs that this port has received.
LACPDU TX	The number of LACPDUs that this port has transmitted.
Illegal RX	The number of illegal protocol frames that this port has received.
Unknown RX	The number of unknown protocol frames that this port has received.

Chapter 18: Unit Management (CLI)

This section includes:

- Defining the IP Protocol Version for Initiating Communications (CLI)
- Configuring the Remote Unit’s IP Address (CLI)
- Configuring SNMP (CLI)
- Configuring the Internal Ports for FTP or SFTP (CLI)
- Upgrading the Software (CLI)
- Backing Up and Restoring Configurations (CLI)
- Setting the Unit to the Factory Default Configuration (CLI)
- Performing a Hard (Cold) Reset (CLI)
- Configuring Unit Parameters (CLI)
- Configuring NTP (CLI)
- Displaying Unit Inventory (CLI)
- Displaying SFP DDM and Inventory Information (CLI)

Related topics:

- Setting the Time and Date (Optional) (CLI)
- Uploading Unit Info (CLI)
- Changing the Management IP Address (CLI)

Defining the IP Protocol Version for Initiating Communications (CLI)

You can specify which IP protocol the unit will use when initiating communications, such as downloading software, sending traps, pinging, or exporting configurations. The options are IPv4 or IPv6.

To define which IP protocol the unit will use when initiating communications, enter the following command in root view:

```
root> platform management ip set ip-address-family <ipv4|ipv6>
```

To show the IP protocol version the unit will use when initiating communications, enter the following command in root view:

```
root> platform management ip show ip-address-family
```

Configuring the Remote Unit’s IP Address (CLI)

You can configure the remote unit’s IP address, subnet mask and default gateway in IPv4 format and/or in IPv6 format. The remote unit will receive communications whether they were sent to its IPv4 address or its IPv6 address.

Note

Release 10.6 does not support the ability to configure the remote IP address.

Configuring the Remote Radio's IP Address in IPv4 format (CLI)

To set the remote radio’s IP Address, enter the following command in radio view:

```
radio[x/x]>remote-unit set ip-address <ipv4-address>
```

To display the remote radio’s IP Address, enter the following command in radio view:

```
radio[x/x]>remote-unit show ip-address
```

To set the remote radio’s subnet mask, enter the following command in radio view:

```
radio[x/x]>remote-unit set subnet-mask IP <subnet-mask>
```

To display the remote radio’s subnet mask, enter the following command in radio view:

```
radio[x/x]>remote-unit show subnet-mask
```

To set the remote radio’s default gateway, enter the following command in radio view:

```
radio[x/x]>remote-unit set default-gateway IP <ipv4-address>
```

To display the remote radio’s default gateway, enter the following command in radio view:

```
radio[x/x]>remote-unit show default-gateway
```

Table 100 Remote Unit IP Address (IPv4) CLI Parameters

Parameter	Input Type	Permitted Values	Description
ipv4-address	Dotted decimal format.	Any valid IPv4 address.	Sets the default gateway or IP address of the remote radio.
subnet-mask	Dotted decimal format.	Any valid subnet mask.	Sets the subnet mask of the remote radio.

The following command sets the default gateway of the remote radio as 192.168.1.20:

```
radio[1/1]>remote-unit set default-gateway IP 192.168.1.20
```

The following commands set the IP address of the remote radio as 192.168.1.1, with a subnet mask of 255.255.255.255.

```
radio[1/1]>remote-unit set ip-address 192.168.1.1
radio[1/1]>remote-unit set subnet-mask IP 255.255.255.255
```

Configuring the Remote Radio's IP Address in IPv6 format (CLI)

To set the remote radio's IP Address, enter the following command in radio view:

```
radio[x/x]>remote-unit set ip-address-ipv6 <ipv6-address>
```

To display the remote radio's IP Address, enter the following command in radio view:

```
radio[x/x]>remote-unit show ip-address-ipv6
```

To set the remote radio's prefix length , enter the following command in radio view:

```
radio[x/x]>remote-unit set prefix-length <prefix-length >
```

To display the remote radio's prefix-length, enter the following command in radio view:

```
radio[x/x]>remote-unit show prefix-length
```

To set the remote radio's default gateway, enter the following command in radio view:

```
radio[x/x]>remote-unit set default-gateway-ipv6 IPv6 <ipv6-address>
```

To display the remote radio's default gateway, enter the following command in radio view:

```
radio[x/x]>remote-unit show default-gateway-ipv6
```

Table 101 Remote Unit IP Address (IPv6) CLI Parameters

Parameter	Input Type	Permitted Values	Description
ipv6-address	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	Sets the default gateway or IP address of the remote radio.
prefix-length	Number	1-128	Sets the prefix length of the remote radio. It should be different for each RADIUS client.

The following command sets the default gateway of the remote radio as The following command sets the default gateway of the remote radio as FE80:0000:0000:0000:0202:B3FF:FE1E:8329:

```
radio[1/1]>remote-unit set default-gateway-ipv6 IPv6
FE80:0000:0000:0000:0202:B3FF:FE1E:8329
```

The following commands set the IP address of the remote radio as FE80:0000:0000:0000:0202:B3FF:FE1E:8329, with a prefix length of 64:

```
radio[1/1]>remote-unit set ip-address-ipv6
FE80:0000:0000:0000:0202:B3FF:FE1E:8329
```

```
radio[1/1]>remote-unit set prefix-length 64
```

Configuring SNMP (CLI)

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

PTP 850Eupports the following MIBs:

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

Access to the unit is provided by making use of the community and context fields in SNMPv1 and SNMPv2c/SNMPv3, respectively.

This section includes:

- Configuring Basic SNMP Settings (CLI)
- Configuring SNMPv3 (CLI)
- Displaying the SNMP Settings (CLI)
- Configuring Trap Managers (CLI)

Configuring Basic SNMP Settings (CLI)

To enable SNMP, enter the following command in root view:

```
root> platform security protocols-control snmp admin set <admin>
```

To specify the SNMP version, enter the following command in root view:

```
root> platform security protocols-control snmp version set <version>
```

To specify the SNMP read and write communities, enter the following command in root view:

```
root> platform security protocols-control snmpv1v2 set read-
community <read-community> write-community <write-community>
```

Table 102 Basic SNMP CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin	Variable	enable disable	Select **enable** to enable SNMP monitoring, or **disable** to disable SNMP monitoring.
version	Variable	v1 v2 v3	Specifies the SNMP version.
read-community	Text String	Any valid SNMP read community.	The community string for the SNMP read community.
write-community	Text String	Any valid SNMP write community.	The community string for the SNMP write community.

The following commands enable SNMP v2 on the unit, and set the read community to “public” and the write community to “private”:

```
root> platform security protocols-control snmp admin set enable
root> platform security protocols-control snmp version set v2
root> platform security protocols-control snmpv1v2 set read-
community public write-community private
```

Configuring SNMPv3 (CLI)

The following commands are relevant for SNMPv3.

To block SNMPv1 and SNMPv2 access so that only SNMPv3 access will be enabled, enter the following command in root view:

```
root> platform security protocols-control snmp v1v2-block set <set-
block>
```

To add an SNMPv3 user, enter the following command in root view:

```
root> platform security protocols-control snmp v3-authentication add
v3-user-name <v3-user-name> v3-user-password <v3-user-password> v3-
security-mode <v3-security-mode> v3-encryption-mode <v3-encryption-
mode> v3-auth-algorithm <v3-auth-algorithm> v3-access-mode <v3-
access-mode>
```

To remove an SNMP v3 user, enter the following command in root view:

```
root> platform security protocols-control snmp v3-authentication
remove v3-user-name <v3-user-name>
```

To display all SNMP v3 users and their authentication parameters, enter the following command in root view:

```
root> platform security protocols-control snmp v3-authentication
show
```

Table 103 SNMPv3 CLI Parameters

Parameter	Input Type	Permitted Values	Description
set-block	Variable	yes no	yes – SNMPv1 and SNMPv2 access is blocked. no – SNMPv1 and SNMPv2 access is not blocked.
v3-user-name	Text String		A SNMPv3 user name.
v3-user-password	Text String	Must be at least eight characters.	An SNMPv3 user password.
v3-security-mode	Variable	authNoPriv authPriv noAuthNoPriv	Defines the security mode to be used for this user.

Parameter	Input Type	Permitted Values	Description
v3-encryption-mode	Variable	None DES AES	Defines the encryption (privacy) protocol to be used for this user.
v3-auth-algorithm	Variable	None SHA MD5	Defines the authentication algorithm to be used for this user.
v3-access-mode	Variable	readWrite readOnly	Defines the access permission level for this user.

The following commands enable SNMP v2 on the unit, and set the read community to “public” and the write community to “private”:

```
root> platform security protocols-control snmp admin set enable

root> platform security protocols-control snmp version set v2

root> platform security protocols-control snmpv1v2 set read-
community public write-community private
```

The following commands enable SNMP v3 on the unit, block SNMP v1 and SNMP v2 access, and define an SNMPv3 user with User Name=Geno, Password=abcdefgh, security mode authPriv, encryption mode DES, authentication algorithm SHA, and read-write access:

```
root> platform security protocols-control snmp admin set enable

root> platform security protocols-control snmp version set v3

root> platform security protocols-control snmp v1v2-block set yes

root> platform security protocols-control snmp v3-authentication add
v3-user-name geno v3-user-password abcdefgh v3-security-mode
authPriv v3-encryption-mode DES v3-auth-algorithm SHA v3-access-mode
readWrite
```

Displaying the SNMP Settings (CLI)

To display the general SNMP parameters, enter the following command in root view:

```
root> platform security protocols-control snmp show-all
```

To display all SNMP v3 users and their authentication parameters, enter the following command in root view:

```
root> platform security protocols-control snmp v3-authentication
show
```

To display the current MIB version used in the system, enter the following command in root view:

```
root> platform security protocols-control snmp show-mib-version
```

To display details about the current MIB version used in the system, enter the following command in root view:

```
root> platform security protocols-control snmp show-mib-version-
table
```

To display the SNMP read and write communities, enter the following command in root view:

```
root> platform security protocols-control snmpv1v2 show
```

Configuring Trap Managers (CLI)

To display the current SNMP trap manager settings, enter the following command in root view:

```
root> platform security protocols-control snmp trap-manager show
```

To modify the settings of an SNMP trap manger, enter the following command in root view:

```
root> platform security protocols-control snmp trap-manager set
manager-id <manager-id> manager-admin <manager-admin> manager-
ipv4 <manager-ipv4> manager-ipv6<manager-ipv6> manager-port
<manager-port> manager-community <manager-community> manager-v3-user
<manager-v3-user> manager-description <manager-description>
```

To enable an SNMP trap manger without modifying its parameters, enter the following command in root view:

```
root> platform security protocols-control snmp trap-manager admin
manager-id <manager-id> manager-admin <manager-admin>
```

To specify the number of minutes between heartbeat traps, enter the following command in root view:

```
root> platform security protocols-control snmp trap-manager
heartbeat manager-id <manager-id> manager-heartbeat <manager-
heartbeat>
```

Table 104 Trap Managers CLI Parameters

Parameter	Input Type	Permitted Values	Description
manager-id	Number.	1 – 4	Enter the Manager ID of the trap manager you want to modify.
manager-admin	Variable.	enable disable	Enter **enable** or **disable** to enable or disable the trap manager.
manager-ipv4	Dotted decimal format.	Any valid IPv4 address.	If the IP protocol selected in platform management ip set ip-address-family is IPv4, enter the destination IPv4 address. Traps will be sent to this IP address.
manager-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	If the IP protocol selected in platform management ip set ip-address-family is IPv6, enter the destination IPv6 address. Traps will be sent to this IP address.
manager-port	Number.	70 – 65535	Enter the number of the port through which traps will be sent.
manager-community	Text String.	Any valid SNMP read community.	Enter the community string for the SNMP read community.

Parameter	Input Type	Permitted Values	Description
manager-v3-user	Text String.	The name of a V3 user defined in the system.	If the SNMP Trap version selected in platform security protocols-control snmp version set is V3, enter the name of a V3 user defined in the system. **Note**: Make sure that an identical V3 user is also defined on the manager's side
manager-description	Text String.		Enter a description of the trap manager (optional).
manager-heartbeat	Number.	0 – 1440	Specifies the number of minutes between heartbeat traps. If you enter 0, no heartbeat traps will be sent. **Note**: To reduce unnecessary traffic, heartbeat traps are only sent if no other trap was sent during the Heartbeat Period.

The following commands enable trap manager 2, and assign it IP address 192.168.1.250, port 164, and community "private", with a heartbeat of 12 minutes.

```
root> platform security protocols-control snmp trap-manager set
manager-id 2 manager-admin enable manager-ip 192.168.1.250 manager-
port 164 manager-community private manager-description text

root> platform security protocols-control snmp trap-manager
heartbeat manager-id 2 manager-heartbeat 12
```

Configuring the Internal Ports for FTP or SFTP (CLI)

By default, the following PTP 850 ports are used for FTP and SFTP when the PTP 850 unit is acting as an FTP or SFTP client (e.g., software downloads, configuration file backup and restore operations):

FTP – 21

SFTP – 22

To change the port for either protocol, enter the following command in root view:

```
root> platform management file-transfer port-config protocol
<ftp|sftp> port-number <0-65535>
```

To display the ports that are currently configured for FTP and SFTP, enter the following command in root view:

```
root> platform management file-transfer port-show
```

These ports are configured globally, rather than per specific operation.

The following sequence of commands displays the current (default) FTP and SFTP port settings, changes the FTP port to 125 and the SFTP port to 126, and shows the new FTP and SFTP port settings.

```
root>platform management file-transfer port-show

Port config table:
==================
File transfer    File transfer port

protocol         number
=====================================
ftp              21
sftp             22

root> platform management file-transfer port-config protocol ftp
port-number 125

root> platform management file-transfer port-config protocol sftp
port-number 126

root>platform management file-transfer port-show

Port config table:
==================
File transfer    File transfer port

protocol         number
=====================================

ftp              125
sftp             126

root>
```

Upgrading the Software (CLI)

PTP 850 software and firmware releases are provided in a single bundle that includes software and firmware for all components in the system. Software is first downloaded to the system, then installed. After installation, a reset is automatically performed on all components whose software was upgraded.

This section includes:

- Software Upgrade Overview (CLI)
- Viewing Current Software Versions (CLI)
- Configuring a Software Download (CLI)
- Downloading a Software Package (CLI)
- Installing and Upgrading Software (CLI)

Software Upgrade Overview (CLI)

The PTP 850 software installation process includes the following steps:

1. **Download** – The files required for the installation or upgrade are downloaded from a remote server.
2. **Installation** – The downloaded software and firmware files are installed in all modules and components of the PTP 850 that are currently running an older version.
3. **Reset** – The PTP 850 is restarted in order to boot the new software and firmware versions.

Software and firmware releases are provided in a single bundle that includes software and firmware for all components in the system. When you download a software bundle, the system verifies the validity of the bundle. The system also compares the files in the bundle to the files currently installed in the PTP 850 and its components, so that only files that need to be updated are actually downloaded. A message is displayed for each file that is actually downloaded.

Note

When downloading an older version, all files in the bundle may be downloaded, including files that are already installed.

Software bundles can be downloaded via HTTP, HTTPS, FTP or SFTP. After the software download is complete, you can initiate the installation.

Note

Before performing a software upgrade, it is important to verify that the system date and time are correct. See Setting the Time and Date (Optional) (CLI).

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

Viewing Current Software Versions (CLI)

To display all current software versions, enter the following command in root view:

```
root> platform software show versions
```

Configuring a Software Download (CLI)

You can download software using HTTP, HTTPS, FTP, or SFTP.

When downloading software via HTTP or HTTPS, the PTP 850 functions as the server, and you can download the software directly to the PTP 850 unit.

> **Note**
>
> HTTP/HTTPS software download is only supported using the Web EMS. For instructions, see Downloading and Installing Software.

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

To set the file transfer protocol you want to use (FTP or SFTP), enter the following command:

```
root> platform software download version protocol <ftp|sftp>
```

If the IP protocol selected in platform management ip set ip-address-family is IPv4, enter the following command:

```
root> platform software download channel server set server-ip
<server-ipv4> directory <directory> username <username> password
<password>
```

If the IP protocol selected in platform management ip set ip-address-family is IPv6, enter the following command:

```
root> platform software download channel server-ipv6 set server-ip
<server-ipv6> directory <directory> username <username> password
<password>
```

To display the software download channel configuration, enter one of the following commands:

```
root> platform software download channel server show
root> platform software download channel server-ipv6 show
```

Table 105 Software Download CLI Parameters

Parameter	Input Type	Permitted Values	Description
server-ipv4	Dotted decimal format.	Any valid IPv4 address.	The IPv4 address of the PC or laptop you are using as the FTP server.
server-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The IPv6 address of the PC or laptop you are using as the FTP server.

Parameter	Input Type	Permitted Values	Description
directory	Text String.		The directory path from which you are downloading the files. Enter the path relative to the FTP user's home directory, not the absolute path. To leave the path blank, enter //. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
server-username	Text String.		The user name you configured in the FTP server.
server-password	Text String.		The password you configured in the FTP server. If you did not configure a password for your FTP user, simply omit this parameter.

The following command configures a download from IP address 192.168.1.242, in the directory “current”, with user name “anonymous” and password “12345.”

```
root> platform software download channel server set server-
ip 192.168.1.242 directory \current username anonymous password
12345
```

Downloading a Software Package (CLI)

To initiate a software download, enter the following command in root view:

```
root> platform software download version protocol ftp
```

The following prompt appears:

```
You are about to perform a software management operation. This may
cause a system reset.

Are you sure? (yes/no)
```

Enter `Yes` at the prompt. When the prompt appears again, enter the following command to check the download status:

```
root> platform software download status show
```

Once the following message appears, proceed with the installation:

```
DOWNLOAD VERSION status: download success, process percentage: 100
```

If the software version on the FTP or SFTP server has already been downloaded
to the unit, the following message appears:

```
DOWNLOAD VERSION status: all components exist, process
percentage: 0
```

Installing and Upgrading Software (CLI)

To install or upgrade the software, enter the following command in root view after downloading the software bundle:

```
root> platform software install version
```

If you wish to delay the start of installation, enter instead the following command. The time you enter in HH:MM format is the amount of time to delay until the start of the installation process:

```
root> platform software install version timer-countdown <hh:mm>
```

The following prompt appears:

```
Software version to be installed:

Are you sure? (yes/no)
```

To display the status of a software installation or upgrade, enter the following command:

```
root> platform software install status show
```

Important Notes:

DO NOT reboot the unit during software installation process. As soon as the process is successfully completed, the unit will reboot itself.

Sometimes the installation process can take up to 30 minutes.

Only in the event that software installation was not successfully finished and more than 30 minutes have passed can the unit be rebooted.

If you configured delayed installation, you can do any of the following:

Abort the current delayed installation. To do so, enter the following command:

```
root> platform software install abort-timer
```

Show the time left until the installation process begins. To do so, enter the following command:

```
root> platform software install time-to-install
```

Show the original timer as configured for a delayed installation. To do so, enter the following command:

```
root> platform software install show-time
```

Backing Up and Restoring Configurations (CLI)

You can import and export PTP 850 configuration files. This enables you to copy the system configuration to multiple PTP 850 units. You can also backup and save configuration files.

Configuration files can only be copied between units of the same type, i.e., PTP 850E to PTP 850E to PTP 850E.

Note that you can also write CLI scripts that will automatically execute a series of commands when the configuration file is restored. For information, refer to Editing CLI Scripts (CLI).

This section includes:

- Configuration Management Overview (CLI)
- Setting the Configuration Management Parameters (CLI)
- Backing up and Exporting a Configuration File (CLI)
- Importing and Restoring a Configuration File (CLI)
- Editing CLI Scripts (CLI)

Configuration Management Overview (CLI)

System configuration files consist of a zip file that contains three components:

A binary configuration file used by the system to restore the configuration.

A text file which enables users to examine the system configuration in a readable format. The file includes the value of all system parameters at the time of creation of the backup file.

An additional text file which enables you to write CLI scripts in order to make desired changes in the backed-up configuration. This file is executed by the system after restoring the configuration.

The system provides three restore points to manage different configuration files. Each restore point contains a single configuration file. Files can be added to the restore points by creating backups of the current system state or by importing them from an external server. For example, you may want to use one restore point to keep a last good configuration, another to import changes from an external server, and the third to store the current configuration.

You can apply a configuration file to the system from any of the restore points.

You must configure from 1 to 3 restore points:

When you import a configuration file, the file is saved to the selected restore point, and overwrites whichever file was previously held in that restore point.

When you export a configuration file, the file is exported from the selected restore point.

When you backup the current configuration, the backup configuration file is saved to the selected restore point, and overwrites whichever file was previously held in that restore point.

When you restore a configuration, the configuration file in the selected restore point is the file that is restored.

Setting the Configuration Management Parameters (CLI)

When importing and exporting configuration files, the PTP 850 functions as an FTP or SFTP client. You must install FTP or SFTP server software on the PC or laptop you are using to perform the import or export. For details, see Installing and Configuring an FTP or SFTP Server.

Note

Before importing or exporting a configuration file, you must verify that the system date and time are correct. See Setting the Time and Date (Optional) (CLI).

To set the FTP or SFTP parameters for configuration file import and export, enter one of the following commands in root view:

If the IP protocol selected in platform management ip set ip-address-family is IPv4, enter the following command:

```
root> platform configuration channel server set ip-address <server-ipv4> directory <directory> filename <filename> username <username> password <password>
```

If the IP protocol selected in platform management ip set ip-address-family is IPv6, enter the following command:

```
root> platform configuration channel server-ipv6 set ip-address <server-ipv6> directory <directory> filename <filename> username <username> password <password>
```

To set the file transfer protocol you want to use (FTP or SFTP), enter the following command:

```
root>platform configuration channel set protocol <ftp|sftp>
```

To display the FTP channel parameters for importing and exporting configuration files, enter one of the following commands in root view:

```
root> platform configuration channel server show

root> platform configuration channel server-ipv6 show
```

Table 106 Configuration Management CLI Parameters

Parameter	Input Type	Permitted Values	Description
server-ipv4	Dotted decimal format.	Any valid IPv4 address.	The IPv4 address of the PC or laptop you are using as the FTP server.
server-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The IPv6 address of the PC or laptop you are using as the FTP server.

Parameter	Input Type	Permitted Values	Description
directory	Text String.		The location of the file you are downloading or uploading. If the location is the root shared folder, it should be left empty. If the location is a sub-folder under the root shared folder, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
filename	Text String.		The name of the file you are importing, or the name you want to give the file you are exporting. **Note**: You must add the suffix .zip to the file name. Otherwise, the file import may fail. You can export the file using any name, then add the suffix .zip manually.
username	Text String.		The user name you configured in the FTP server.
password	Text String.		The password you configured in the FTP server. If you did not configure a password for your FTP user, simply omit this parameter.

The following command configures the FTP channel for configuration file import and export to IP address 192.168.1.99, in the directory “current”, with file name “version_8_backup.zip”, user name “anonymous”, and password “12345.”

```
root> platform configuration channel server set server-ip 192.168.1.99
directory \current filename version_8_backup.zip username anonymous
password 12345
```

Backing up and Exporting a Configuration File (CLI)

To save the current configuration as a backup file to one of the restore points, enter the following command in root view:

```
root> platform configuration configuration-file add <restore-point>
```

To export a configuration from a restore point to the external server location, enter the following command in root view:

```
root> platform configuration configuration-file export <restore-point>
```

Table 107 Configuration Backup and Restore CLI Parameters

Parameter	Input Type	Permitted Values	Description
restore-point	Variable	restore-point-1 restore-point-2 restore-point-3	Identifies the restore point to or from which to perform the backup operation.

The following commands save the current configuration as a configuration at Restore Point 1, and export the file to the external server location:

```
root> platform configuration configuration-file add restore-point-1
root> platform configuration configuration-file export restore-point-1
```

Importing and Restoring a Configuration File (CLI)

You can import a configuration file from an external PC or laptop to one of the restore points. Once you have imported the file, you can restore the configuration. Restoring a saved configuration does not change the unit's FIPS mode.

Note

In order to import a configuration file, you must configure the FTP channel parameters and restore points, as described in Setting the Configuration Management Parameters and Backing up and Exporting a Configuration File.

To import a configuration file, enter the following command in root view:

```
root> platform configuration configuration-file import <restore-point>
```

To restore a configuration from a restore point to become the active configuration file, enter the following command in root view:

```
root> platform configuration configuration-file restore <restore-point>
```

Table 108 Configuration Import and Restore CLI Parameters

Parameter	Input Type	Permitted Values	Description
restore-point	Variable	restore-point-1 restore-point-2 restore-point-3	Identifies the restore point to or from which to perform the backup operation.

The following commands import a configuration file from an external PC or laptop to Restore Point 2 on the PTP 850, and restore the file to be the system configuration file for the PTP 850:

```
root> platform configuration configuration-file import restore-point-2
root> platform configuration configuration-file restore restore-point-2
```

Editing CLI Scripts (CLI)

The configuration file package includes a text file that enables you to write CLI scripts in a backed-up configuration that are executed after restoring the configuration.

To edit a CLI script:

1. Back up the current configuration to one of the restore points. See Backing up and Exporting a Configuration File (CLI).
2. Export the configuration from the restore point to a PC or laptop. See Backing up and Exporting a Configuration File (CLI).
3. On the PC or laptop, unzip the file *Configuration_files.zip*.
4. Edit *the cli_script.txt* file using clish commands, one per line.
5. Save and close the *cli_script.txt* file, and add it back into the *Configuration_files.zip* file.
6. Import the updated *Configuration_files.zip* file back into the unit. See Importing and Restoring a Configuration File (CLI).
7. Restore the imported configuration file. See Importing and Restoring a Configuration File (CLI). The unit is automatically reset. During initialization, the CLI script is executed, line by line.

Note

If any specific command in the CLI script requires reset, the unit is reset when that that command is executed. During initialization following the reset, execution of the CLI script continues from the following command.

Setting the Unit to the Factory Default Configuration (CLI)

To restore the unit to its factory default configuration, while retaining the unit's IP address settings and logs, enter the following commands in root view:

```
root> platform management set-to-default
```

The following prompt appears:

```
WARNING: All database and configuration will be lost, unit will be
restart.
Are you sure? (yes/no):yes
```

At the prompt, type `yes`.

Note

This does not change the unit's IP address or FIPS configuration.

Performing a Hard (Cold) Reset (CLI)

To initiate a hard (cold) reset on the unit, enter the following command in root view:

```
root> platform management chassis reset
```

The following prompt appears:

```
You are about to reset the shelf
Are you sure? :(yes/no):
```

Enter `yes`. The unit is reset.

Resetting the Remote Unit (CLI)

To initiate a hard (cold) reset on the remote unit, go to radio view and enter the following command:

```
radio [1/1]>remote-unit reset unit
```

The following prompt appears:

```
Are you sure you want to reset the remote unit
Are you sure? (yes/no):
```

Enter `yes`. The unit is reset.

Configuring Unit Parameters (CLI)

You can view and configure system information:

To configure a name for the unit, enter the following command in root view:

```
root> platform management system-name set name <name>
```

To define a location for the unit, enter the following command in root view:

```
root> platform management system-location set name <name>
```

To define a contact person for questions pertaining to the unit, enter the following command in root view:

```
root> platform management system-contact set name <name>
```

To define the unit's latitude coordinates, enter the following command in root view:

```
root> platform management system-latitude set <latitude>
```

To define the unit's longitude coordinates, enter the following command in root view:

```
root> platform management system-longitude set <longitude>
```

To define the type of measurement unit you want the system to use, enter the following command in root view:

```
root> platform management set unit_measure_format <unit_measure_format>
```

To display the type of measurement unit used by the system, enter the following command in root view:

```
root> platform management show unit_measure_format
```

Table 109 Unit Parameters CLI Parameters

Parameter	Input Type	Permitted Values	Description
name	Text	Up to 64 characters.	Defines the name of the unit.
latitude	Text	Up to 256 characters.	Defines the latitude coordinates of the unit.
longitude	Text	Up to 256 characters.	Defines the longitude coordinates of the unit.
unit_measure_format	Variable	metric imperial	Defines the measurement units of the unit.

The following commands configure a name, location, contact person, latitude coordinates, longitude coordinates, and units of measurements for the PTP 850:

```
root> platform management system-name set name "My-System-Name"
root> platform management system-location set name "My-System-Location"
root> platform management system-contact set name "John Doe"
root> platform management system-latitude set 40
root> platform management system-longitude set 73
root> platform management set unit_measure_format metric
```

Configuring NTP (CLI)

PTP 850 supports Network Time Protocol (NTP). NTP distributes Coordinated Universal Time (UTC) throughout the system, using a jitter buffer to neutralize the effects of variable latency.

You can configure up to four NTP servers. Each server can be configured using IPv4 or IPv6. When multiple servers are configured, the unit chooses the best server according to the implementation of Version 4.2.6p1 of the NTPD (Network Time Protocol Daemon). The servers are continually polled. The polling interval is determined by the NTPD, to achieve maximum accuracy consistent with minimum network overhead.

To configure NTP, enter the following command in root view:

```
root> platform management ntp set admin <admin> ntp-version <ntp-version>
ntp-server-ip-address-1 <ntp-server-ip-address>
```

To display the current NTP configuration, enter the following command in root view:

```
root> platform management ntp show status
```

Table 110 NTP CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin	Variable.	enable disable	Enter **enable** or **disable** to enable or disable the NTP server.
ntp-version	Variable.	v3 v4	Enter the NTP version you want to use. NTPv4 provides interoperability with NTP v3 and with SNTP.
ntp-server-ip-address	Dotted decimal format.	Any valid IP address.	Enter the IP address of the NTP server.

The following command enables NTP, using NTP v4, and sets the IP address of the NTP server as 62.90.139.210.

```
root> platform management ntp set admin enable ntp-version ntpv4 ntp-
server-ip-address-1
```

Displaying Unit Inventory (CLI)

To view inventory information, such as the part number and serial number of the unit hardware, enter the following command in root view:

```
root> platform management inventory show-info
```

For example:

```
root> platform management inventory show info
```

```
System information:
card-name : PTP 850
Subtype : 350
part number : 22-0001-0|
serial number : F493606212
company name : Cambium Networks
product name : AODU DC, All-outdoor, dual radio carriers in one product
product description : AODU DC, All-outdoor, dual radio carriers in one
product
root>
```

Displaying SFP DDM and Inventory Information (CLI)

Static and dynamic monitoring is available for SFP, SFP+, and QSFP modules used in ports P3 (Eth2), P4 (Eth3, Eth4, Eth5, Eth6), and P5 (Eth7).

Dynamic monitoring (DDM) PMs are also available.

Note

DDM parameters are not relevant for electrical SFPs.

The following alarms are available in connection with SFP DDM and inventory monitoring. The polling interval for these alarms is one minute.

- Alarm #803- SFP port RX power level is too low.
- Alarm #804 – SFP port RX power level is too high.
- Alarm #805- SFP port TX power level is too low.
- Alarm #806 – SFP port TX power level is too high.

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

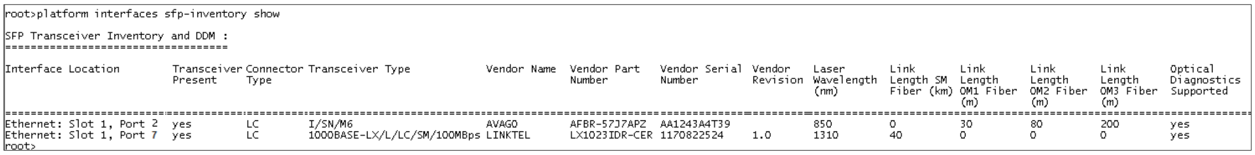
If there is no signal on the interface, a Loss of Carrier alarm (LOC) is raised, and this alarm masks the DDM alarms.

Displaying Static Information about an SFP Module (CLI)

To display static information about an SFP module, enter the following command in root view:

```
root> platform interfaces sfp-inventory show
```

For example:



```
root>platform interfaces sfp-inventory show

SFP Transceiver Inventory and DDM :
===================================

Interface Location        TransceiverConnector Transceiver Type            Vendor Name   Vendor Part   Vendor Serial   Vendor    Laser       Link       Link       Link       Link       Optical
                          Present    Type                                                Number        Number          Revision  Wavelength  Length SM  Length     Length     Length     Diagnostics
                                                                                                                                 (nm)        Fiber (km) OM1 Fiber  OM2 Fiber  OM3 Fiber  Supported
                                                                                                                                                        (m)        (m)        (m)
==================================================================================================================================================================================================
Ethernet: Slot 1, Port 2  yes        LC        I/SN/M6                     AVAGO         AFBR-57J7APZ  AA1243A4T39               850         0          30         80         200        yes
Ethernet: Slot 1, Port 7  yes        LC        1000BASE-LX/L/LC/SM/100MBps LINKTEL       LX1023IDR-CER 1170822524      1.0       1310        40         0          0          0          yes
root>
```

Table 111 SFP Inventory Parameters (CLI)

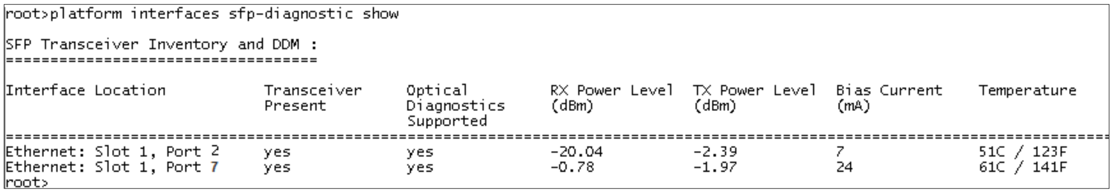
Parameter	Description
Transceiver Present	Indicates whether an SFP module is attached to the interface.
Connector Type	Always displays LC.
transceiver Type	Displays a description of the SFP module.
Vendor Name	Displays the name of the SFP's vendor.
Vendor Part Number	Displays the vendor's part number for the SFP module.
Vendor Serial Number	Displays the vendor's serial number for the SFP module.
Vendor Revision	Displays the revision number of the serial number provided by the vendor for the SFP module.
Laser Wavelength (nm)	Display's the SFP module's laser wavelength. For CSFP modules, two wavelengths are displayed. This parameters is not relevant for copper SFPs.
Link Length SM Fiber (km)	The maximum length of the cable (in km) for single mode fiber cables.
Link Length OM1 Fiber (m)	The maximum length of the cable (in meters) for OM1 multi-mode fiber cables.
Link Length OM2 Fiber (m)	The maximum length of the cable (in meters) for OM2 multi-mode fiber cables.
Link Length OM3 Fiber (m)	The maximum length of the cable (in meters) for OM3 multi-mode fiber cables.
Optical Diagnostics Supported	Displays whether the SFP module supports DDM monitoring. For modules that do not support DDM monitoring, the parameters described in Table 90 are not available.

Displaying Dynamic (DDM) Information about an SFP Module (CLI)

To display dynamic information about an SFP module, enter the following command in root view:

```
root> platform interfaces sfp-diagnostic show
```

For example:



```
root>platform interfaces sfp-diagnostic show

SFP Transceiver Inventory and DDM :
===================================

Interface Location          Transceiver     Optical         RX Power Level  TX Power Level  Bias Current    Temperature
                            Present         Diagnostics     (dBm)           (dBm)           (mA)
                                            Supported
==========================================================================================================================
Ethernet: Slot 1, Port 2    yes             yes             -20.04          -2.39           7               51C / 123F
Ethernet: Slot 1, Port 7    yes             yes             -0.78           -1.97           24              61C / 141F
root>
```

Table 112 SFP Digital Diagnostic Monitoring (DDM) Parameters (CLI)

Parameter	Description
Transceiver Present	Indicates whether an SFP module is attached to the interface.
RX Power Level (dBm)	The SFP module’s current RX power signal strength (in dBm).
TX Power Level (dBm)	The SFP module’s current TX power signal strength (in dBm).
Bias Current (mA)	The laser bias current of the SFP module (in mA)
Temperature	The current temperature of the SFP module (displayed in both C° and F°).

Note

Tx Power level DDM is not supported for QSFP (P4) – not part of the standard.

If no signal is being received, RX Power Level is displayed as -40 dBm.

If the Admin status of the port is Down, the TX Power Level is displayed as -40 DBm and the Bias Current is displayed as 0 mA.

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

Displaying DDM PMs about an SFP Module (CLI)

DDM PMs can be displayed for 15-minute and 24-hour intervals. For each interval, the following PMs are displayed:

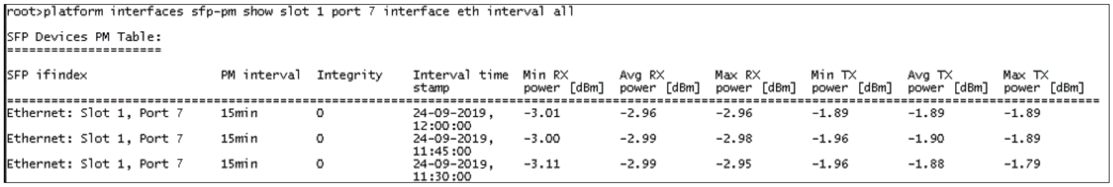
- Minimum RX power during the interval (dBm)
- Average RX power during the interval (dBm)
- Maximum RX power during the interval (dBm)
- Minimum TX power during the interval (dBm)
- Average TX power during the interval (dBm)

- Maximum TX power during the interval (dBm)

To display DDM PMs, enter the following command in root view:

```
root> platform interfaces sfp-pm show slot <slot> port <port>
interface eth interval <15min|24h|all>
```

For example:



```
root>platform interfaces sfp-pm show slot 1 port 7 interface eth interval all

SFP Devices PM Table:
=====================

SFP ifindex                  PM interval  Integrity    Interval time  Min RX        Avg RX        Max RX        Min TX        Avg TX        Max TX
                                                       stamp          power [dBm]   power [dBm]   power [dBm]   power [dBm]   power [dBm]   power [dBm]
=========================================================================================================================================================
Ethernet: Slot 1, Port 7     15min        0            24-09-2019,    -3.01         -2.96         -2.96         -1.89         -1.89         -1.89
                                                       12:00:00
Ethernet: Slot 1, Port 7     15min        0            24-09-2019,    -3.00         -2.99         -2.98         -1.96         -1.90         -1.89
                                                       11:45:00
Ethernet: Slot 1, Port 7     15min        0            24-09-2019,    -3.11         -2.99         -2.95         -1.96         -1.88         -1.79
                                                       11:30:00
```

The Integrity column indicates whether the PM is valid:

- 0 indicates a valid entry.
- 1 indicates an invalid entry. This can be caused by any of the following events that occurred during the interval
  - LOC alarm
  - Changing the Admin status of the interface
  - Unit reset

> Note
>
> No entries are displayed if the SFP device does not support DDM, or if the Admin status of the interface is Down.

DDM PMs are not persistent, which means they are not saved in the event of unit reset. RX and TX power levels are collected five times per 15-minute interval. 15-minute PM data is saved for 24 hours. 24-hour PM data, which is updated every 15 minutes, is saved for 30 days.

Chapter 19: Radio Configuration (CLI)

This section includes:

- Viewing and Configuring the Remote Radio Parameters (CLI)
- Configuring and Viewing Radio PMs and Statistics (CLI)

Related topics:

- Entering Radio View (CLI)
- Muting and Unmuting a Radio (CLI)
- Configuring the Transmit (TX) Level (CLI)
- Configuring the Transmit (TX) Frequency (CLI)
- Configuring the Radio (MRMC) Script(s) (CLI)
- System Configurations (CLI)
- Configuring 1+1 HSB Unit Protection (CLI)
- Configuring Multiband (CLI)
- Configuring XPIC (CLI)
- Configuring Link Aggregation (LAG) and LACP (Optional) (CLI)

Note

For convenience, this User Guide generally shows the radio prompt as `radio[1/1]>`.

Viewing and Configuring the Remote Radio Parameters (CLI)

This section includes:

- Displaying Communication Status with the Remote Radio (CLI)
- Displaying Remote Radio's Location (CLI)
- Muting and Unmuting the Remote Radio (CLI)
- Displaying the Remote Radio's RX Level (CLI)
- Configuring the Remote Radio's TX Level (CLI)
- Displaying the Remote Unit's Most Severe Alarm (CLI)

Related topics:

Configuring the Remote Unit's IP Address (CLI)

Displaying Communication Status with the Remote Radio (CLI)

To display the communication status with the remote radio, enter the following command:

```
radio[x/x]>remote-unit communication status show
```

Displaying Remote Radio's Location (CLI)

To display the remote radio's slot ID (location in the chassis), enter the following command in radio view. The slot ID of the remote radio will generally be 1, unless there is no communication with the remote unit. In that case, it will be -1.

```
radio[1/1]>remote-unit show slot-id
```

Muting and Unmuting the Remote Radio (CLI)

To mute or unmute the remote radio, enter the following command in radio view:

```
radio[x/x]>remote-unit mute set admin <admin>
```

To display the mute status of the remote radio, enter the following command in radio view:

```
radio[x/x]>remote-unit mute show status
```

Table 113 Remote Radio Mute/Unmute CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin	Variable	on off	Mutes (on) or unmutes (off) the remote unit.

The following command mutes the remote radio:

```
radio[2/1]>remote-unit mute set admin on
```

The following command unmutes the remote radio:

```
radio[2/1]>remote-unit mute set admin off
```

Displaying the Remote Radio's RX Level (CLI)

To display the remote radio's RX level, enter the following command in radio view:

```
radio[x/x]>remote-unit show rx-level
```

Configuring the Remote Radio's TX Level (CLI)

To set the transmit (TX) level of the remote radio, enter the following command in radio view:

```
radio[x/x]>remote-unit set tx-level <tx-level>
```

To display the transmit (TX) level of the remote radio, enter the following command in radio view:

```
radio[x/x]>remote-unit show tx-level
```

Table 114 Remote Radio TX Level CLI Parameters

Parameter	Input Type	Permitted Values	Description
tx-level	Number	Depends on the frequency and unit type.	The desired TX signal level (TSL), in dBm.

The following command sets the TX level of the remote radio to 10 dBm:

```
radio[2/1]>remote-unit set tx-level 10
```

Configuring Remote ATPC (CLI)

To set the RX reference level for ATPC on the remote radio, enter the following command in radio view:

```
radio[x/1]>remote-unit atpc set ref-level <ref-level>
```

To display the RX reference level for ATPC on the remote radio, enter the following command in radio view:

```
radio[x/1]>remote-unit atpc show ref-level
```

Table 115 Remote Radio ATPC CLI Parameters

Parameter	Input Type	Permitted Values	Description
ref-level	Number	-70 - -30	The RX reference level for the ATPC mechanism.

The following command sets the ATPC RX reference level of the remote radio to -55:

```
radio[2/1]>remote-unit atpc set ref-level -55
```

Displaying the Remote Unit’s Most Severe Alarm (CLI)

To display the most severe alarm currently raised in the unit, enter the following command in radio view:

```
radio[x/x]>remote-unit show most-severe-alarm
```

Configuring ATPC and ATPC Override Timer (CLI)

Note

This section is only relevant for PTP 850S.

ATPC is a closed-loop mechanism by which each carrier changes the TX power according to the indication received across the link, in order to achieve a desired RSL on the other side of the link.

With ATPC, if the radio increases its TX power up to the configured TX power, it can lead to a period of sustained transmission at maximum power, resulting in unacceptable interference with other systems.

In order to minimize interference, PTP 850S provides an ATPC override mechanism. When ATPC override is enabled, a timer begins when ATPC raises the TX power to its maximum. When the timer expires, the radio enters ATPC override state. In ATPC override state, the radio transmits no higher than the pre-determined ATPC override TX level, and an ATPC override alarm is raised. The radio remains in ATPC override state until the ATPC override state is manually cancelled by the user (or until the unit is reset). The radio then returns to normal ATPC operation.

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

Note

When canceling an ATPC override state, you should ensure that the underlying problem has been corrected. Otherwise, ATPC may be overridden again.

To enable or disable ATPC, enter the following command in radio view:

```
radio[x/1]>atpc set admin <admin>
```

To display whether or not ATPC is enabled, enter the following command in radio view:

```
radio[x/1]>atpc show admin
```

To set the RX reference level for ATPC, enter the following command in radio view

```
radio[x/1]>atpc set rx-level atpc_ref_rx_level <rx-level>
```

To display the RX reference level for ATPC, enter the following command in radio view:

```
radio[x/1]>atpc show rx-level
```

To set an ATPC override timer, enter the following command in radio view:

```
radio[x/1]>atpc set override timeout <timeout>
```

Note

The next command actually enables ATPC override. However, it is recommended to set the timer before enabling ATPC override. Failure to do so can lead to unexpected reduction of the TX power with corresponding loss of capacity if TX override is enabled with the timer set to a lower-than-desired value.

To enable ATPC override, enter the following command in radio view. ATPC must be enabled before you enable ATPC override.

```
radio[x/1]>atpc override set admin <override admin>
```

To display whether or not ATPC override is enabled, enter the following command in radio view:

```
radio[x/1]>atpc override show admin
```

To display the ATPC override timeout, enter the following command in radio view:

```
radio[x/1]>atpc show override timeout
```

To set the TX power to be used when the unit is in an ATPC override state, enter the following command in radio view:

```
radio[x/1]>atpc set override-tx-level <override-tx-level>
```

To display the ATPC override TX power, enter the following command in radio view:

```
radio[x/1]>atpc show override tx-level
```

To display the current ATPC override state, enter the following command in radio view:

```
radio[x/1]>atpc show override
```

Possible values are:

Normal – ATPC override is enabled, and there is no override.

Disabled – ATPC override is not enabled.

Override – ATPC override has been activated.

To cancel ATPC override, enter the following command in radio view:

```
radio[x/x]>atpc set override-cancel
```

Table 116 Radio ATPC CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin	Variable	enable disable	Enables or disables ATPC mode.
rx-level	Number	-70 - -30	The RSL reference level for the ATPC mechanism. When ATPC is enabled, it adjusts the TX power dynamically to preserve this RSL level.
timeout	Number	0-1800	The amount of time, in seconds, the timer counts from the moment the radio reaches its maximum configured TX power until ATPC override goes into effect.
override admin	Variable	enable disable	Enables or disables ATPC override.
override-tx- lev	Number	-50 - 50	The TX power, in dBm, to be used when the unit is an ATPC override state. The range of values depend on the frequency, MRMC script, and radio type.

The following commands enable ATPC mode and ATPC override, with an RSL reference level of -55, an ATPC override timeout of 15 minutes, and an override TX level of 18 dBm:

```
radio[2/1]>atpc set admin enable
radio[2/1]>atpc set rx-level atpc_ref_rx_level -55
radio[2/1]>atpc set override timeout 900
radio[2/1]>atpc override set admin enable
radio[2/1]> atpc set override-tx-level 18
```

Configuring Header De-Duplication (CLI)

Note: This section is only relevant for PTP 850S.

Header De-Duplication identifies traffic flows and replaces header fields with a flow ID. The Header De-Duplication module includes an algorithm for learning each new flow, and implements compression on the flow type starting with the next frame of that flow type.

You can determine the depth to which the compression mechanism operates, from Layer 2 to Layer 4. You must balance the depth of compression against the number of flows in order to ensure maximum efficiency. Multi-Layer (Enhanced) compression supports up to 256 flow types.

Note: The Header De-Duplication configuration must be identical on both sides of the link.

To configure Header De-Duplication, enter the following command in radio view:

```
radio[2/1]> compression header-compression set <mode>
```

To clear Ethernet port counters, including both Frame Cut-Through and Header De-Duplication counters, enter the following command in radio view:

```
radio[x/x]>clear-ethernet-port-counters
```

Table 117 Header De-Duplication CLI Parameters

Parameter	Input Type	Permitted Values	Description
mode	Variable	Disabled Layer2 MPLS Layer3 Layer4 Tunnel Tunnel-Layer3 Tunnel-Layer4	Disabled - Header De-Duplication is disabled. Layer2 - Header De-Duplication operates on the Ethernet level. MPLS - Header De-Duplication operates on the Ethernet and MPLS levels. Layer3 - Header De-Duplication operates on the Ethernet and IP levels. Layer4 - Header De-Duplication operates on all supported layers up to Layer 4. Tunnel - Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel layer for packets carrying GTP or GRE frames. Tunnel-Layer3 - Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel and T-3 layers for packets carrying GTP or GRE frames.

			Tunnel-Layer4 - Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel, T-3, and T- 4 layers for packets carrying GTP or GRE frames.

The following command enables Layer 2 Header De-Duplication on the radio:

```
root> radio slot 2 port 1

radio[2/1]> compression header-compression set Layer2
```

Displaying Header De-Duplication Information (CLI)

To display the current Header De-Duplication configuration, enter the following command in radio view:

```
radio[x/1]> compression show-configuration
```

To display counters for Header De-Duplication, enter the following command in radio view:

```
radio[x/1]> compression header-compression show-counters
```

The following counters are displayed:

- TX in octet count - Bytes on the TX side before Header De-Duplication.
- TX out octet count - Bytes on the TX side that were compressed by Header De-Duplication.
- TX frame in count - Frames on the TX side before Header De-Duplication.
- TX frame out compressed count - Frames on the TX side that were compressed by Header De-Duplication.
- TX frame uncompressed count - The number of frames on the TX side that were not compressed due to exclusion rules.

Note: The use of exclusion rules for Header De-Duplication is planned for future release.

- TX frame uncompressed other count - Frames on the TX side that were not compressed for reasons other than the use of exclusion rules.
- TX out frame learning count - The number of frames that have been used to learn unique data flows. Once a particular flow type has been learned, subsequent frames with that flow type are compressed by Header De- Duplication.
- TX out number of active flows in count - The number of Header De- Duplication flows that are active on the TX side.

Configuring Frame Cut-Through (CLI)

Note: This section is only relevant for PTP 850S.

Using the Frame Cut-Through feature, frames assigned to queues with 4th priority pre-empt frames already in transmission over the radio from other queues. After the 4th queue frames have been transmitted, transmission of the pre-empted frames resumes.

Notes: The Frame Cut-Through configuration must be identical on both sides of the link.

Frame Cut-Through cannot be used together with 1588 Transparent Clock.

To enable Frame Cut-Through, enter the following command in radio view:

```
radio[x/1]> cut-through mode yes
```

To disable Frame Cut-Through, enter the following command in radio view:

```
radio[x/1]> cut-through mode no
```

To display whether Frame Cut-Through is currently enabled or disabled, enter the following command in radio view:

```
radio[x/1]> cut-through show-mode
```

To display the number of frames and bytes that have been transmitted via Frame Cut-Through, enter the following command in radio view:

```
radio[x/1]> cut-through show-counters
```

Configuring AES-256 Payload Encryption (CLI)

Notes: This feature is only relevant for PTP 850E units.

This feature is not supported with 2+0 XPIC and Multiband links.

This feature requires:

- Requires an activation key. If no valid AES activation key has been applied to the unit, AES will not operate on the unit. See *Configuring the Activation Key (CLI)*.

Note: In order for the AES activation key to become active, you must reset the unit after configuring a valid AES activation key. Until the unit is reset, an alarm will be present if you enable AES. This is not the case for other activation keys.

PTP 850E supports AES-256 payload encryption, using a dual-key encryption mechanism:

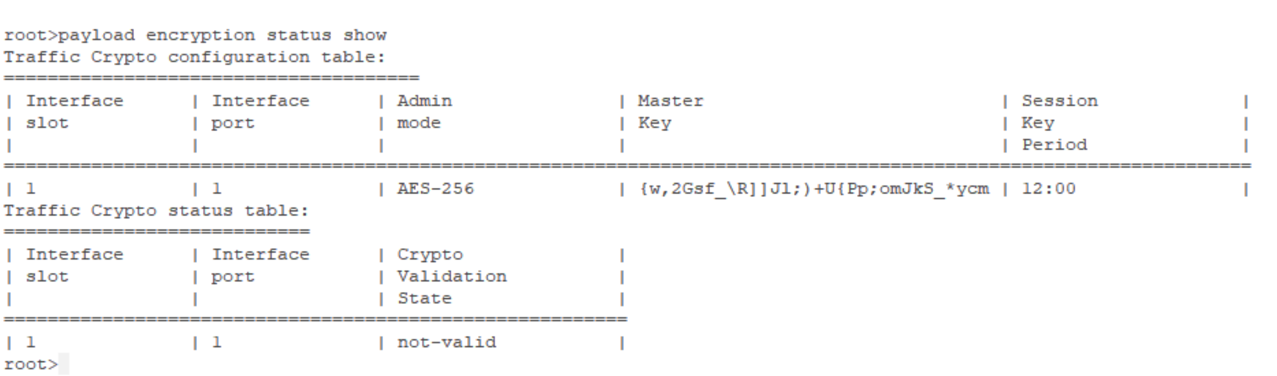
- The user provides a master key. The master key can also be generated by the system upon user command. The master key is a 32-byte symmetric encryption key. The same master key must be manually configured on both ends of the encrypted link.
- The session key is a 32-byte symmetric encryption key used to encrypt the actual data. Each link uses two session keys, one for each direction. For each direction, the session key is generated by the transmit side unit and propagated automatically, via a Key Exchange Protocol, to the other side of the link. The Key Exchange Protocol exchanges session keys by encrypting them with the master key, using the AES-256 encryption algorithm. Session keys are regenerated at user-configured intervals.

The first KEP exchange that takes place after a new master key is configured causes traffic to be blocked for up to one minute, until the Crypto Validation State becomes Valid. Subsequent KEP exchanges that take place when a session key expires do not affect traffic. KEP exchanges have no effect upon ACM, RSL, and MSE.

To display the current payload encryption status for all available radio links on the unit, enter the following command in root view:

```
root> payload encryption status show
```

The following is a sample output of this command in which payload encryption is enabled but not operational.



```
root>payload encryption status show
Traffic Crypto configuration table:
======================================
| Interface      | Interface      | Admin                | Master                            | Session              |
| slot           | port           | mode                 | Key                               | Key                  |
|                |                |                      |                                   | Period               |
==================================================================================================================
| 1              | 1              | AES-256              | {w,2Gsf_\R]]J1;)+U{Pp;omJkS_*ycm | 12:00                |
Traffic Crypto status table:
============================
| Interface      | Interface      | Crypto               |
| slot           | port           | Validation           |
|                |                | State                |
=========================================================
| 1              | 1              | not-valid            |
root>
```

> Note
>
> The Crypto Validation State field indicates whether the interface is functioning properly, with AES-256 encryption. In order for this field to display Valid, both the interface itself and AES-256 encryption must be enabled, the hardware must be in place and functioning properly, initialization must be finished, and AES-256 encryption must be functioning properly, with no loopback on the interface.

To configure payload encryption:

1 Verify that both the local and remote units are running with no alarms. If any alarm is present, take corrective actions to clear the alarms before proceeding.

2 If the link is using in-band management, identify which unit is local and which unit is remote from the management point of view.

3 To configure AES on a radio carrier, you must first enter traffic enc`ryption view for the specific radio. To enter Payload Encryption view, enter the following command in root view:

```
root> payload encryption slot 1 port 1
```

To display the payload encryption mode of the radio interface, enter the following command in Payload Encryption view:

```
Payload Encryption [1/1]> payload encryption mode show
```

The following display indicates that payload encryption is enabled on radio interface 1:

```
Payload Encryption [1/1]> payload encryption mode show
Admin Mode: AES-256
```

The following display indicates that payload encryption is disabled:

```
Payload Encryption [1/1]> payload encryption mode show
Admin Mode: Disable
```

4 Configure the master key on the remote unit by doing one of the following:

- Enter a master key manually.
- Generate the master key automatically.

You must use the same master key on both sides of the link. This means that if you generate a master key automatically on one side of the link, you must copy that key and for use on the other side of the link. Once payload encryption has been enabled on both sides of the link, the Key Exchange Protocol periodically verifies that both ends of the link have the same master key. If a mismatch is detected, an alarm is raised and traffic transmission is stopped for the mismatched carrier at both sides of the link. The link becomes non-valid and traffic stops being forwarded.

To define the master key manually, enter the following command in Payload Encryption view:

```
Payload Encryption [1/1]> payload encryption mkey
```

When you press **<Enter>**, the following prompt appears:

```
Please enter key:
```

Enter the master key and press **<Enter>.** The master key must be between 8 and 32 ASCII characters. The characters *do not* appear as you type them. To display the master key and verify that you typed it correctly, enter the `payload encryption status show` command described above. You can copy the master key from the output of this command.

To generate the master key automatically, enter the following command in Payload Encryption view:

```
Payload Encryption [1/1]> master key generate
```

A random master key is generated. You must copy and paste this key to the other end of the link to ensure that both sides of the link have the same master key. To display and copy the master key, enter the `traffic encryption status show` command described above. You can copy the master key from the output of this command.

5 On the local unit, follow the procedure described in Step 4 to configure the same master key configured on the remote unit also on the local unit.

6 Enable payload encryption on the remote unit:

i Enter the following command in Payload Encryption view:

```
Payload Encryption [1/1]> payload encryption mode admin AES-256
```

This step will cause the link status to be Down until payload encryption is successfully enabled on the local unit. However, the RSL measured on the link should remain at an acceptable level.

To disable payload encryption, enter the following command in Payload Encryption view:

```
Payload Encryption [1/1]> payload encryption mode admin Disable
```

ii The session key is automatically regenerated at defined intervals. To set the session key regeneration interval, enter the following command in Payload Encryption view:

```
Payload Encryption [x/x]> payload encryption session-key period
set <00:03-12:00>
```

Enter the regeneration interval in hours and minutes (HH:MM). For example, the following command configures radio interface 1 to regenerate the session key every 4 hours and 15 minutes:

```
Payload Encryption [1/1]> payload encryption session-key period
set 04:15
```

To display the session key regeneration interval, enter the following command in Payload Encryption view:

```
Payload Encryption [1/1]> payload encryption session-key period
show
```

7 Enable payload encryption on the local unit by following the procedure described in Step 6. Verify that on both the local and remote active units, the link status returns to Up and user traffic is restored. In links using in-band management, verify also that in-band management returns.

8 Verify that there are no alarms on the link.

You can set all master keys defined on the unit to zero value. To zeroize the master keys, enter the following command in root view:

```
root> payload encryption key zeroize
```

Note: Any time payload encryption fails, the Operational status of the link is Down until payload encryption is successfully restored.

Configuring and Viewing Radio PMs and Statistics (CLI)

This section includes:

- Displaying General Modem Status and Defective Block PMs (CLI)
- Displaying Excessive BER (Aggregate) PMs (CLI)
- Displaying BER Level and Configuring BER Parameters (CLI)
- Configuring RSL Thresholds (CLI)
- Configuring TSL Thresholds (CLI)
- Displaying RSL and TSL Levels (CLI)
- Configuring the Signal Level Threshold (CLI)
- Configuring the MSE Thresholds and Displaying the MSE PMs (CLI)
-
- Configuring the XPI Thresholds **and Displaying the XPI PMs (CLI)**

> **Note:** This section is only relevant for PTP 850C and PTP 850E.

To configure the modem XPI threshold for calculating XPI Exceed Threshold seconds, enter the following command in radio view:

```
radio[x/x]>modem set threshold-xpi-exceed threshold <threshold>
```

To display the currently configured XPI threshold, enter the following command in radio view:

```
radio[x/x]>modem show threshold-xpi-below
```

Table 143: XPI Threshold CLI Parameters

Parameter	Input Type	Permitted Values	Description
threshold	Number	0-99	The XPI threshold.

To display XPI PMs in 15-minute intervals, enter the following command in radio view:

```
radio[x/x]>modem pm-xpi show interval 15min
```

The following is a partial sample output of the modem pm-xpi show interval 15min command:

```
radio [x/x]>modem pm-xpi show interval 15min


Modem XPI PM Table:
===================


Interval   Integrity   Min XPI (dB)   Max XPI (dB)   XPI below
                             threshold
                             seconds
```

```
1     1      55.00     0.00      0
2     1      55.00     0.00      0
3     1      55.00     0.00      0
4     1      55.00     0.00      0
5     1      55.00     0.00      0
6     1      55.00     0.00      0
7     1      55.00     0.00      0
8     1      55.00     0.00      0
9     1      55.00     0.00      0
10    1      55.00     0.00      0
11    1      55.00     0.00      0
12    1      55.00     0.00      0
13    1      55.00     0.00      0
14    1      55.00     0.00      0
15    1      55.00     0.00      0
16    1      55.00     0.00      0
17    1      55.00     0.00      0
18    1      55.00     0.00      0
19    1      55.00     0.00      0
20    1      55.00     0.00      0

radio [x/x]>
```

To display XPI PMs in daily intervals, enter the following command in radio view:

```
radio[x/x]>modem pm-xpi show interval 24hr
```

The following is a partial sample output of the `modem pm-xpi show interval  24hr` command:

```
1      1       55.00      0.00       0
2      1       55.00      0.00       0
3      1       55.00      0.00       0
4      1       55.00      0.00       0
5      1       55.00      0.00       0
6      1       55.00      0.00       0
7      1       55.00      0.00       0
8      1       55.00      0.00       0
9      1       55.00      0.00       0
10     1       55.00      0.00       0
11     1       55.00      0.00       0
12     1       55.00      0.00       0
13     1       55.00      0.00       0
14     1       55.00      0.00       0
15     1       55.00      0.00       0
16     1       55.00      0.00       0
17     1       55.00      0.00       0
18     1       55.00      0.00       0
19     1       55.00      0.00       0
20     1       55.00      0.00       0
```

Table 144: XPI PMs (CLI)

Parameter	Description
Interval	The number of the interval: 1-30 for daily PM reports, and 1-96 for 15 minute PM reports.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. "1" in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.
Min XPI (dB)	Indicates the lowest XPI value in dB, measured during the interval.
Max XPI (dB)	Indicates the highest XPI value in dB, measured during the interval.

XPI Below Threshold Seconds	Indicates the number of seconds the XPI value was lower than the XPI threshold during the interval.

The following command sets the XPI threshold to 15:

```
radio[x/x]>modem set threshold-xpi-below threshold 15
```

Displaying ACM PMs and Configuring ACM Profile Thresholds (CLI)

For each radio carrier, you can display the minimum and maximum ACM profile and the minimum and maximum bitrate (throughput) per 15-minute or daily intervals.

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

- **Threshold 1** – When the ACM profile goes beneath this threshold, Alarm ID 1313 (Major) is raised. The alarm is cleared when the ACM profile is at or above this threshold.
- **Threshold 2** – When the ACM profile goes beneath this threshold, Alarm ID 1314 (Critical) is raised. The alarm is cleared when the ACM profile is at or above this threshold.

To define the ACM thresholds, enter the following command in radio view:

```
radio [x/x]>mrmc pm-acm set threshold1 <threshold1> threshold2
<threshold2>
```

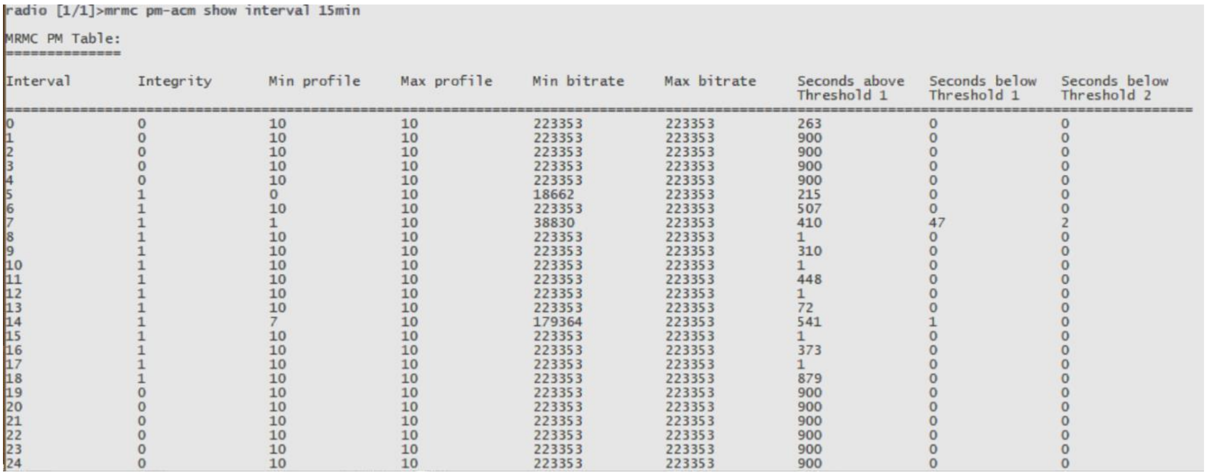
To display the ACM thresholds, enter the following command in radio view:

```
radio [x/x]>mrmc pm-acm get thresholds
```

To display ACM PMs in 15-minute intervals, enter the following command in radio view:

```
radio [x/x]>mrmc pm-acm show interval 15min
```

The following is a partial sample output of the `modem pm-acm show interval 15min` command:

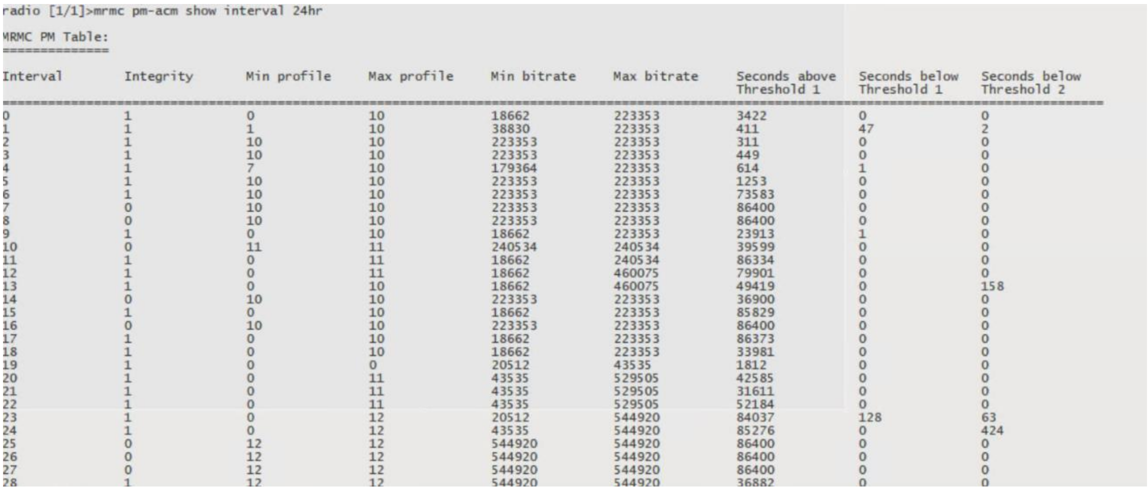


```
radio [1/1]>mrmc pm-acm show interval 15min

MRMC PM Table:
==============

Interval       Integrity      Min profile    Max profile    Min bitrate    Max bitrate    Seconds above  Seconds below  Seconds below
                                                                                          Threshold 1    Threshold 1    Threshold 2
=====================================================================================================================================
0              0              10             10             223353         223353         263            0              0
1              0              10             10             223353         223353         900            0              0
2              0              10             10             223353         223353         900            0              0
3              0              10             10             223353         223353         900            0              0
4              0              10             10             223353         223353         900            0              0
5              1              0              10             18662          223353         215            0              0
6              1              10             10             223353         223353         507            0              0
7              1              1              10             38830          223353         410            47             2
8              1              10             10             223353         223353         1              0              0
9              1              10             10             223353         223353         310            0              0
10             1              10             10             223353         223353         1              0              0
11             1              10             10             223353         223353         448            0              0
12             1              10             10             223353         223353         1              0              0
13             1              10             10             223353         223353         72             0              0
14             1              7              10             179364         223353         541            1              0
15             1              10             10             223353         223353         1              0              0
16             1              10             10             223353         223353         373            0              0
17             1              10             10             223353         223353         1              0              0
18             1              10             10             223353         223353         879            0              0
19             0              10             10             223353         223353         900            0              0
20             0              10             10             223353         223353         900            0              0
21             0              10             10             223353         223353         900            0              0
22             0              10             10             223353         223353         900            0              0
23             0              10             10             223353         223353         900            0              0
24             0              10             10             223353         223353         900            0              0
```

To display ACM PMs in daily intervals, enter the following command in radio view:

```
radio [x/x]>mrmc pm-acm show interval 24hr
```

The following is sample output of the modem pm-acm show interval 24hr command:



```
radio [1/1]>mrmc pm-acm show interval 24hr

MRMC PM Table:
==============

Interval        Integrity       Min profile     Max profile     Min bitrate     Max bitrate     Seconds above   Seconds below   Seconds below
                                                                                                Threshold 1     Threshold 1     Threshold 2
=============================================================================================================================================
0               1               0               10              18662           223353          3422            0               0
1               1               1               10              38830           223353          411             47              2
2               1               10              10              223353          223353          311             0               0
3               1               10              10              223353          223353          449             0               0
4               1               7               10              179364          223353          614             1               0
5               1               10              10              223353          223353          1253            0               0
6               1               10              10              223353          223353          73583           0               0
7               0               10              10              223353          223353          86400           0               0
8               0               10              10              223353          223353          86400           0               0
9               1               0               10              18662           223353          23913           1               0
10              0               11              11              240534          240534          39599           0               0
11              1               0               11              18662           240534          86334           0               0
12              1               0               11              18662           460075          79901           0               0
13              1               0               10              18662           460075          49419           0               158
14              0               10              10              223353          223353          36900           0               0
15              1               0               10              18662           223353          85829           0               0
16              0               10              10              223353          223353          86400           0               0
17              1               0               10              18662           223353          86373           0               0
18              1               0               10              18662           223353          33981           0               0
19              1               0               0               20512           43535           1812            0               0
20              1               0               11              43535           529505          42585           0               0
21              1               0               11              43535           529505          31611           0               0
22              1               0               11              43535           529505          52184           0               0
23              1               0               12              20512           544920          84037           128             63
24              1               0               12              43535           544920          85276           0               424
25              0               12              12              544920          544920          86400           0               0
26              0               12              12              544920          544920          86400           0               0
27              0               12              12              544920          544920          86400           0               0
28              1               12              12              544920          544920          36882           0               0
```

Table 145: ACM PMs and ACM Profile Thresholds (CLI)

Parameter	Description
threshold1	The higher ACM profile threshold (0-15). The default value is 0.
threshold2	The lower ACM profile threshold (0-15). The default value is 0.
Interval	The number of the interval: 1-30 for daily PM reports, and 1-96 for 15 minute PM reports.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. "1" in the column indicates that the values are not reliable due to a possible power surge or power failure
Min profile	Indicates the minimum ACM profile that was measured during the interval.
Max profile	Indicates the maximum ACM profile that was measured during the interval.
Min bitrate	Indicates the minimum total radio throughput (Mbps), delivered during the interval.
Max bitrate	Indicates the maximum total radio throughput (Mbps), delivered during the interval.

Displaying General Modem Status and Defective Block PMs (CLI)

To display the general status of the modem, enter the following command in radio view:

```
radio[x/x]>modem show status
```

The following is a sample output of the `modem show status` command:

```
MSE[db]: -99.00
Defective Blocks count: 0

Current Tx profile: 0
Current Tx QAM: 4
Current Tx rate(Kbps): 43389
Current Rx profile: 0
Current Rx QAM: 4
Current Rx rate(Kbps): 43389
```

A value of 0 in the MSE (Db) field means that the modem is not locked.

To clear all radio PMs in the system, enter the following command in root view:

```
root> radio pm clear all
```

To clear defective blocks counters for a radio, enter the following command in radio view:

```
radio[x/x]>modem clear counters
```

Displaying Excessive BER (Aggregate) PMs (CLI)

You can display modem BER (Bit Error Rate) PMs in either 15-minute or daily intervals.

To display modem BER PMs in 15-minute intervals, enter the following command in radio view:

```
radio [x/x]>framer pm-aggregate show interval 15min
```

The following is a partial sample output of the `framer pm-aggregate show interval 15min` command:

```
radio [2/1]>framer pm-aggregate show interval 15min
Modem BER PM table:
===================

Interval    Integrity    ES      SES       UAS        BBE
===========================================================
0           1            0       0         333         0
1           1            0       0         900         0
2           1            0       0         900         0
3           1            0       0         900         0
4           1            0       0         900         0
5           1            0       0         900         0
6           1            0       0         900         0
7           1            0       0         900         0
8           1            0       0         900         0

radio [2/1]>
```

To display modem BER PMs in daily intervals, enter the following command:

```
radio [x/x]>framer pm-aggregate show interval 24hr
```

The following is a sample output of the `framer pm-aggregate show interval 24hr` command:

```
radio [2/1]>framer pm-aggregate show interval 24hr

Modem BER PM table:
===================

Interval    Integrity    ES         SES          UAS       BBE
===============================================================
0           1            0          0            53843     0
4           1            0          0            37061     0
5           1            0          0            4034       0
6           1            0          0            85971     0
8           1            0          0            46171     0
11          1            0          0            24184     0
15          1            0          0            85978     0
17          1            0          0            54979     0

radio [2/1]>
```

Table 118 Aggregate PMs (CLI)

Parameter	Description
Interval	The number of the interval: 1-30 for daily PM reports, and 1-96 for 15 minute PM reports.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. "1" in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.
ES	Indicates the number of seconds in the measuring interval during which errors occurred.
SES	Indicates the number of severe error seconds in the measuring interval.
UAS	Indicates the Unavailable Seconds value of the measured interval. The value can be between 0 and 900 seconds (15 minutes).
BBE	Indicates the number of background block errors during the measured interval.

Displaying BER Level and Configuring BER Parameters (CLI)

To display the current BER level, enter the following command:

```
radio [x/x]>modem show ber
```

The `excessive-ber` parameter determines whether or not excessive BER is propagated as a fault and considered a system event. For example, if `excessive-ber` is enabled, excessive BER can trigger a protection switchover.

To enable or disable Excessive BER Admin, enter the following command in root view:

```
root> radio excessive-ber set admin <admin>
```

To display the current setting for `excessive-ber`, enter the following command in root view:

```
root> radio excessive-ber show admin
```

To set the level above which an excessive BER alarm is issued for errors detected over the radio link, enter the following command:

```
radio [x/x]>modem excessive-ber set threshold <threshold>
```

To display the excessive BER threshold, enter the following command:

```
radio [x/x]>modem excessive-ber show threshold
```

Table 119 Excessive BER CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin	Variable	enable disable	Enables or disables propagation of excessive BER as a fault.
threshold	Variable	1e -3 1e -4 1e -5	The level above which an excessive BER alarm is issued for errors detected over the radio link.

The following command enables `excessive-ber`:

```
root> radio excessive-ber set admin enable
```

The following command sets the excessive BER threshold to 1e-5:

```
radio [2/1]>modem excessive-ber set threshold 1e-5
```

Configuring RSL Thresholds (CLI)

You can set two RSL (RX Signal Level) thresholds. The number of seconds during which the RSL exceeds these thresholds are counted as RSL Exceed Threshold Seconds. See Displaying RSL and TSL Levels (CLI).

To set the RSL thresholds, enter the following command:

```
radio [x/x]>rf pm-rsl set threshold1 <threshold1> threshold2 <threshold2>
```

Table 120 RSL Thresholds CLI Parameters

Parameter	Input Type	Permitted Values	Description
threshold1	Number	-75 - -15	The first RSL threshold (dBm).
threshold2	Number	-75 - -15	The second RSL threshold (dBm).

The following command sets the RSL thresholds to -30 dBm and -60 dBm, respectively.

```
radio [2/1]>rf pm-rsl set threshold1 -30 threshold2 -60
```

Configuring TSL Thresholds (CLI)

The number of seconds during which the TX Signal Level exceeds the TSL threshold are counted as TSL Exceed Threshold Seconds. See Displaying RSL and TSL Levels (CLI).

To set the TSL threshold, enter the following command:

```
radio [x/x]>rf pm-tsl set threshold -15
```

Table 121 TSL Thresholds CLI Parameters

Parameter	Input Type	Permitted Values	Description
threshold	Number	-10 - 34	The TSL threshold (dBm).

The following command sets the TSL threshold to 10 dBm:

```
radio [2/1]>rf pm-tsl set threshold 10
```

Displaying RSL and TSL Levels (CLI)

You can display the RSL (RX Signal Level) and TSL (TX Signal Level) PMs in either 15-minute or daily intervals.

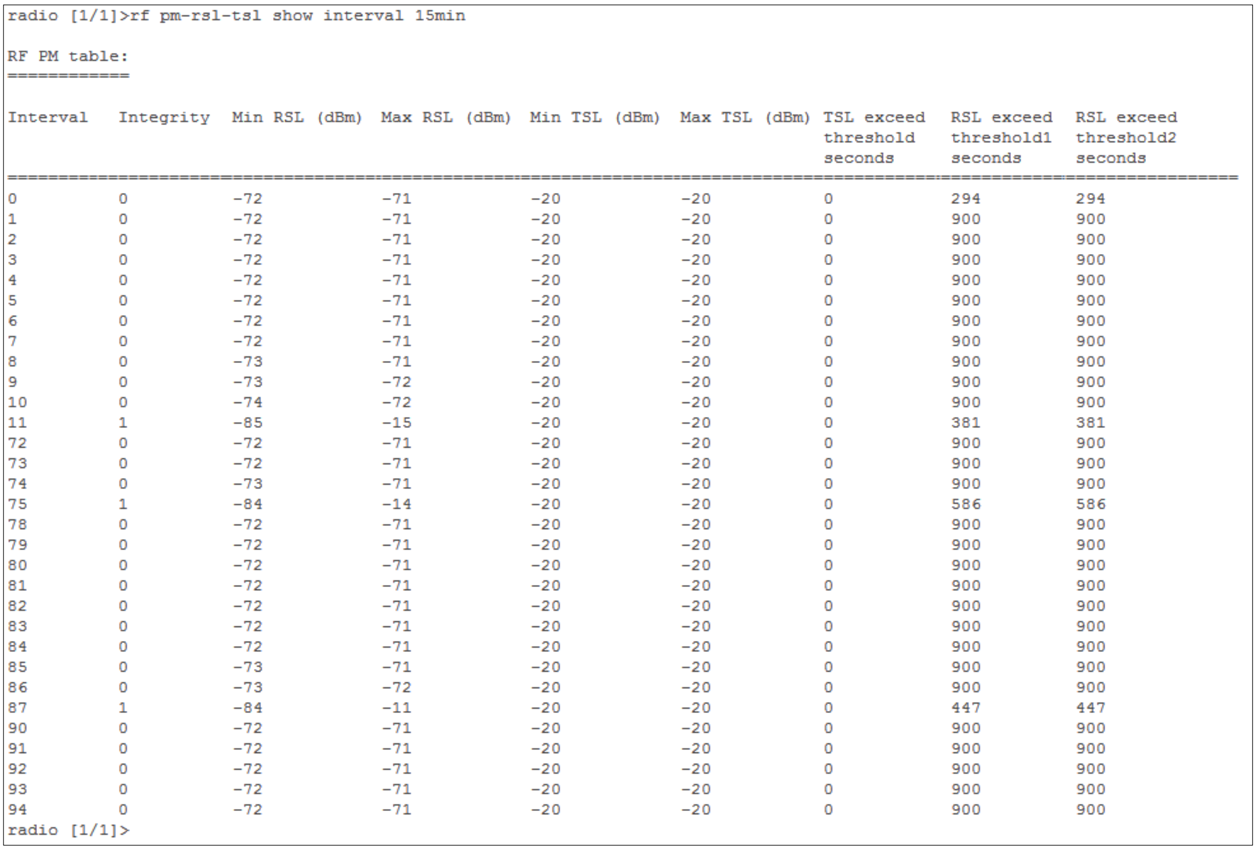
To display RSL and TSL PMs in 15-minute intervals, enter the following command:

```
radio [x/x]>rf pm-rsl-tsl show interval 15min
```

To display RSL and TSL PMs in daily intervals, enter the following command:

```
radio [x/x]>rf pm-rsl-tsl show interval 24hr
```

The following is the output format of the rf pm-rsl-tsl show commands:



```
radio [1/1]>rf pm-rsl-tsl show interval 15min

RF PM table:
============

Interval      Integrity     Min RSL (dBm)      Max RSL (dBm)      Min TSL (dBm)      Max TSL (dBm)     TSL exceed      RSL exceed      RSL exceed
                                                                                                       threshold       threshold1      threshold2
                                                                                                       seconds         seconds         seconds
===========================================================================================================================================================
0             0             -72                -71                -20                -20               0               294             294
1             0             -72                -71                -20                -20               0               900             900
2             0             -72                -71                -20                -20               0               900             900
3             0             -72                -71                -20                -20               0               900             900
4             0             -72                -71                -20                -20               0               900             900
5             0             -72                -71                -20                -20               0               900             900
6             0             -72                -71                -20                -20               0               900             900
7             0             -72                -71                -20                -20               0               900             900
8             0             -73                -71                -20                -20               0               900             900
9             0             -73                -72                -20                -20               0               900             900
10            0             -74                -72                -20                -20               0               900             900
11            1             -85                -15                -20                -20               0               381             381
72            0             -72                -71                -20                -20               0               900             900
73            0             -72                -71                -20                -20               0               900             900
74            0             -73                -71                -20                -20               0               900             900
75            1             -84                -14                -20                -20               0               586             586
78            0             -72                -71                -20                -20               0               900             900
79            0             -72                -71                -20                -20               0               900             900
80            0             -72                -71                -20                -20               0               900             900
81            0             -72                -71                -20                -20               0               900             900
82            0             -72                -71                -20                -20               0               900             900
83            0             -72                -71                -20                -20               0               900             900
84            0             -72                -71                -20                -20               0               900             900
85            0             -73                -71                -20                -20               0               900             900
86            0             -73                -72                -20                -20               0               900             900
87            1             -84                -11                -20                -20               0               447             447
90            0             -72                -71                -20                -20               0               900             900
91            0             -72                -71                -20                -20               0               900             900
92            0             -72                -71                -20                -20               0               900             900
93            0             -72                -71                -20                -20               0               900             900
94            0             -72                -71                -20                -20               0               900             900
radio [1/1]>
```

Table 122 RSL and TSL PMs (CLI)

Parameter	Description
Interval	The number of the interval: 1-30 for daily PM reports, and 1-96 for 15 minute PM reports.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. "1" in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.
Min RSL (dBm)	The minimum RSL (Received Signal Level) that was measured during the interval.
Max RSL (dBm)	The maximum RSL (Received Signal Level) that was measured during the interval.
Min TSL (dBm)	The minimum TSL (Transmit Signal Level) that was measured during the interval.
Max TSL (dBm)	The maximum TSL (Transmit Signal Level) that was measured during the interval.
TSL exceed threshold seconds	The number of seconds the measured TSL exceeded the threshold during the interval. See Configuring TSL Thresholds (CLI).
RSL exceed threshold1 seconds	The number of seconds the measured RSL exceeded RSL threshold 1 during the interval. See Configuring RSL Thresholds (CLI).
RSL exceed threshold2 seconds	The number of seconds the measured RSL exceeded RSL threshold 2 during the interval. See Configuring RSL Thresholds (CLI).

Configuring the Signal Level Threshold (CLI)

To set the BER (Bit Error Rate) level above which a Signal Degrade alarm is issued for errors detected over the radio link, enter the following command:

```
radio [x/x]>modem signal-degrade set threshold 1e-7
```

To display the Signal Degrade BER threshold, enter the following command:

```
radio [x/x]>modem signal-degrade show threshold
```

Table 123 Signal Level Threshold CLI Parameters

Parameter	Input Type	Permitted Values	Description
threshold	Variable	1e -6 1e -7 1e -8 1e -9 1e -10	The BER level above which a Signal Degrade alarm is issued for errors detected over the radio link.

The following command sets the Signal Degrade threshold at 1e-7:

```
radio [2/1]>modem signal-degrade set threshold 1e-7
```

Configuring the MSE Thresholds and Displaying the MSE PMs (CLI)

To configure the MSE (Mean Square Error) threshold, enter the following command:

```
radio [x/x]>modem set mse-exceed threshold <threshold>
```

To display the currently configured MSE threshold, enter the following command:

```
radio [x/x]>modem show threshold-mse-exceed
```

Table 124 MSE CLI Parameters

Parameter	Input Type	Permitted Values	Description
threshold	Number	-99 - -1	The MSE threshold.

To display MSE (Mean Square Error) PMs in 15-minute intervals, enter the following command:

```
radio [x/x]>modem pm-mse show interval 15min
```

The following is a partial sample output of the `modem pm-mse show interval 15min` command:

```
radio [2/1]>modem pm-mse show interval 15min


Modem MSE PM Table:
===================

Interval   Integrity    Min MSE (dB)   Max MSE (dB)   Exceed
                                                      threshold
                                                      seconds
===============================================================
0          1            0.00           0.00           708
1          1            0.00           0.00           900
2          1            0.00           0.00           900
3          1            0.00           0.00           900
4          1            0.00           0.00           900
5          1            0.00           0.00           900
6          1            0.00           0.00           900
7          1            0.00           0.00           900
8          1            0.00           0.00           900
9          1            0.00           0.00           900
10         1            0.00           0.00           900


radio [2/1]>
```

To display MSE (Mean Square Error) PMs in daily intervals, enter the following command:

```
radio [x/x]>modem pm-mse show interval 24hr
```

The following is sample output of the `modem pm-mse show interval 24hr` command:

```
radio [2/1]>modem pm-mse show interval 24hr

Modem MSE PM Table:
===================

Interval   Integrity    Min MSE (dB)   Max MSE (dB)   Exceed
                                                      threshold
                                                      seconds
===============================================================
0          1            0.00           0.00           63745
4          1            0.00           0.00           37062
5          1            0.00           0.00           3495
6          1            0.00           0.00           85976
8          1            0.00           0.00           46173
11         1            0.00           0.00           24185
15         1            0.00           0.00           85988
17         1            0.00           0.00           54981

radio [2/1]>modem
```

Table 125 MSE PMs (CLI)

Parameter	Description
Interval	The number of the interval: 1-30 for daily PM reports, and 1-96 for 15 minute PM reports.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. "1" in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time. A 1 and a 0 value in the **Max MSE** field may also indicate that the modem was unlocked.
Min MSE (dB)	Indicates the minimum MSE in dB, measured during the interval. A 0 in this field and a 1 in the **Integrity** field may also indicate that the modem was unlocked during the entire interval.
Max MSE (dB)	Indicates the maximum MSE in dB, measured during the interval. A 0 in this field and a 1 in the **Integrity** field may also indicate that the modem was unlocked.
Exceed Threshold Seconds	Indicates the number of seconds the MSE exceeded the MSE PM threshold during the interval.

The following command sets the MSE threshold to -30:

```
radio [2/1]>modem set mse-exceed threshold -30
```

Configuring the XPI Thresholds and Displaying the XPI PMs (CLI)

Note: This section is only relevant for PTP 850C and PTP 850E.

To configure the modem XPI threshold for calculating XPI Exceed Threshold seconds, enter the following command in radio view:

```
radio[x/x]>modem set threshold-xpi-exceed threshold <threshold>
```

To display the currently configured XPI threshold, enter the following command in radio view:

```
radio[x/x]>modem show threshold-xpi-below
```

Table 143: XPI Threshold CLI Parameters

Parameter	Input Type	Permitted Values	Description
threshold	Number	0-99	The XPI threshold.

To display XPI PMs in 15-minute intervals, enter the following command in radio view:

```
radio[x/x]>modem pm-xpi show interval 15min
```

The following is a partial sample output of the modem pm-xpi show interval 15min command:

```
radio [x/x]>modem pm-xpi show interval 15min


Modem XPI PM Table:
===================


Interval  Integrity  Min XPI (dB)  Max XPI (dB)   XPI below
                           threshold
                           seconds

1     1      55.00     0.00      0
2     1      55.00     0.00      0
3     1      55.00     0.00      0
4     1      55.00     0.00      0
5     1      55.00     0.00      0
6     1      55.00     0.00      0
7     1      55.00     0.00      0
8     1      55.00     0.00      0
9     1      55.00     0.00      0
10    1      55.00     0.00      0
11    1      55.00     0.00      0
12    1      55.00     0.00      0
13    1      55.00     0.00      0
14    1      55.00     0.00      0
15    1      55.00     0.00      0
16    1      55.00     0.00      0
17    1      55.00     0.00      0
18    1      55.00     0.00      0
19    1      55.00     0.00      0
20    1      55.00     0.00      0

radio [x/x]>
```

To display XPI PMs in daily intervals, enter the following command in radio view:

```
radio[x/x]>modem pm-xpi show interval 24hr
```

The following is a partial sample output of the `modem pm-xpi show interval 24hr` command:

```
radio [x/x]>modem pm-xpi show interval 24hr


Modem XPI PM Table:
===================


Interval   Integrity   Min XPI (dB)   Max XPI (dB)   XPI below
                             threshold
                             seconds


1     1      55.00     0.00      0
2     1      55.00     0.00      0
3     1      55.00     0.00      0
4     1      55.00     0.00      0
5     1      55.00     0.00      0
6     1      55.00     0.00      0
7     1      55.00     0.00      0
8     1      55.00     0.00      0
9     1      55.00     0.00      0
10    1      55.00     0.00      0
11    1      55.00     0.00      0
12    1      55.00     0.00      0
13    1      55.00     0.00      0
14    1      55.00     0.00      0
15    1      55.00     0.00      0
16    1      55.00     0.00      0
17    1      55.00     0.00      0
18    1      55.00     0.00      0
19    1      55.00     0.00      0
20    1      55.00     0.00      0
```

Table 144: XPI PMs (CLI)

Parameter	Description
Interval	The number of the interval: 1-30 for daily PM reports, and 1-96 for 15 minute PM reports.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. "1" in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.
Min XPI (dB)	Indicates the lowest XPI value in dB, measured during the interval.
Max XPI (dB)	Indicates the highest XPI value in dB, measured during the interval.

XPI Below Threshold Seconds	Indicates the number of seconds the XPI value was lower than the XPI threshold during the interval.

The following command sets the XPI threshold to 15:

```
radio[x/x]>modem set threshold-xpi-below threshold 15
```

Displaying ACM PMs and Configuring ACM Profile Thresholds (CLI)

For each radio carrier, you can display the minimum and maximum ACM profile and the minimum and maximum bitrate (throughput) per 15-minute or daily intervals.

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

- **Threshold 1** – When the ACM profile goes beneath this threshold, Alarm ID 1313 (Major) is raised. The alarm is cleared when the ACM profile is at or above this threshold.
- **Threshold 2** – When the ACM profile goes beneath this threshold, Alarm ID 1314 (Critical) is raised. The alarm is cleared when the ACM profile is at or above this threshold.

To define the ACM thresholds, enter the following command in radio view:

```
radio [x/x]>mrmc pm-acm set threshold1 <threshold1> threshold2
<threshold2>
```

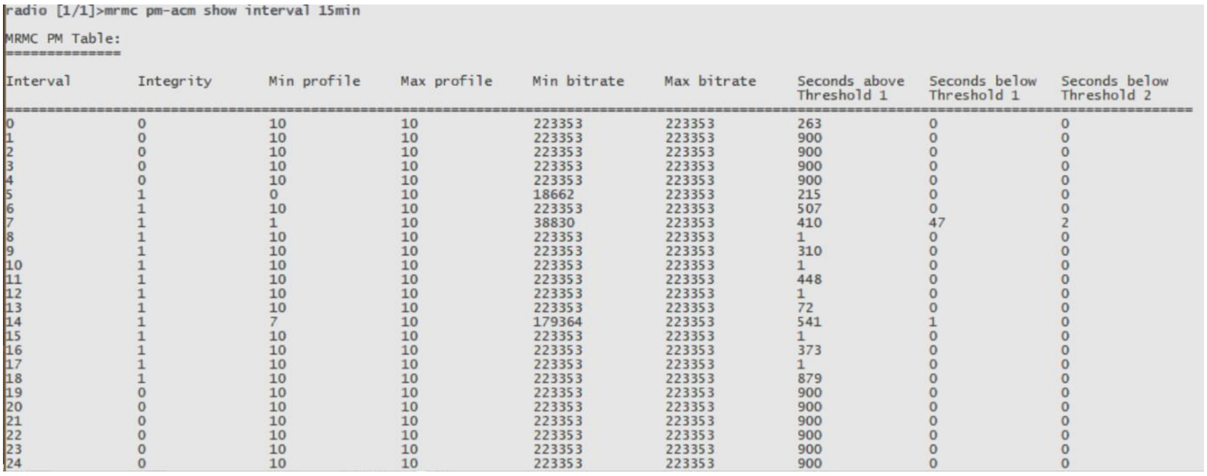
To display the ACM thresholds, enter the following command in radio view:

```
radio [x/x]>mrmc pm-acm get thresholds
```

To display ACM PMs in 15-minute intervals, enter the following command in radio view:

```
radio [x/x]>mrmc pm-acm show interval 15min
```

The following is a partial sample output of the `modem pm-acm show interval 15min` command:

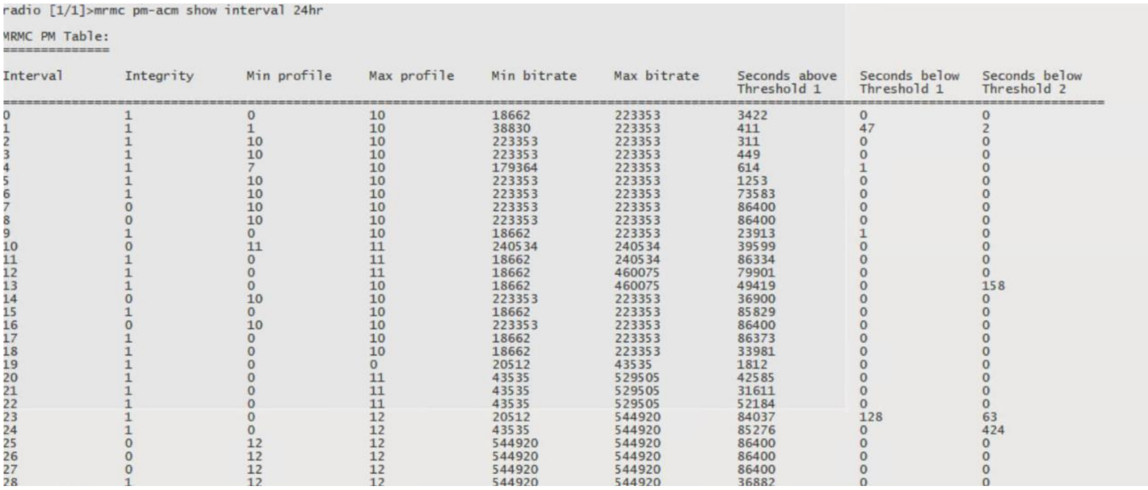


```
radio [1/1]>mrmc pm-acm show interval 15min

MRMC PM Table:
==============

Interval        Integrity       Min profile     Max profile     Min bitrate     Max bitrate     Seconds above   Seconds below   Seconds below
                                                                                                Threshold 1     Threshold 1     Threshold 2
=============================================================================================================================================
0               0               10              10              223353          223353          263             0               0
1               0               10              10              223353          223353          900             0               0
2               0               10              10              223353          223353          900             0               0
3               0               10              10              223353          223353          900             0               0
4               0               10              10              223353          223353          900             0               0
5               1               0               10              18662           223353          215             0               0
6               1               10              10              223353          223353          507             0               0
7               1               1               10              38830           223353          410             47              2
8               1               10              10              223353          223353          1               0               0
9               1               10              10              223353          223353          310             0               0
10              1               10              10              223353          223353          1               0               0
11              1               10              10              223353          223353          448             0               0
12              1               10              10              223353          223353          1               0               0
13              1               10              10              223353          223353          72              0               0
14              1               7               10              179364          223353          541             1               0
15              1               10              10              223353          223353          1               0               0
16              1               10              10              223353          223353          373             0               0
17              1               10              10              223353          223353          1               0               0
18              1               10              10              223353          223353          879             0               0
19              0               10              10              223353          223353          900             0               0
20              0               10              10              223353          223353          900             0               0
21              0               10              10              223353          223353          900             0               0
22              0               10              10              223353          223353          900             0               0
23              0               10              10              223353          223353          900             0               0
24              0               10              10              223353          223353          900             0               0
```

To display ACM PMs in daily intervals, enter the following command in radio view:

```
radio [x/x]>mrmc pm-acm show interval 24hr
```

The following is sample output of the modem pm-acm show interval 24hr command:



```
radio [1/1]>mrmc pm-acm show interval 24hr

MRMC PM Table:
==============

Interval        Integrity       Min profile     Max profile     Min bitrate     Max bitrate     Seconds above   Seconds below   Seconds below
                                                                                                Threshold 1     Threshold 1     Threshold 2
===========================================================================================================================================
0               1               0               10              18662           223353          3422            0               0
1               1               1               10              38830           223353          411             47              2
2               1               10              10              223353          223353          311             0               0
3               1               10              10              223353          223353          449             0               0
4               1               7               10              179364          223353          614             1               0
5               1               10              10              223353          223353          1253            0               0
6               1               10              10              223353          223353          73583           0               0
7               0               10              10              223353          223353          86400           0               0
8               0               10              10              223353          223353          86400           0               0
9               1               0               10              18662           223353          23913           1               0
10              0               11              11              240534          240534          39599           0               0
11              1               0               11              18662           240534          86334           0               0
12              1               0               11              18662           460075          79901           0               0
13              1               0               10              18662           460075          49419           0               158
14              0               10              10              223353          223353          36900           0               0
15              1               0               10              18662           223353          85829           0               0
16              0               10              10              223353          223353          86400           0               0
17              1               0               10              18662           223353          86373           0               0
18              1               0               10              18662           223353          33981           0               0
19              1               0               0               20512           43535           1812            0               0
20              1               0               11              43535           529505          42585           0               0
21              1               0               11              43535           529505          31611           0               0
22              1               0               11              43535           529505          52184           0               0
23              1               0               12              20512           544920          84037           128             63
24              1               0               12              43535           544920          85276           0               424
25              0               12              12              544920          544920          86400           0               0
26              0               12              12              544920          544920          86400           0               0
27              0               12              12              544920          544920          86400           0               0
28              1               12              12              544920          544920          36882           0               0
```

Table 145: ACM PMs and ACM Profile Thresholds (CLI)

Parameter	Description
threshold1	The higher ACM profile threshold (0-15). The default value is 0.
threshold2	The lower ACM profile threshold (0-15). The default value is 0.
Interval	The number of the interval: 1-30 for daily PM reports, and 1-96 for 15 minute PM reports.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. "1" in the column indicates that the values are not reliable due to a possible power surge or power failure
Min profile	Indicates the minimum ACM profile that was measured during the interval.
Max profile	Indicates the maximum ACM profile that was measured during the interval.
Min bitrate	Indicates the minimum total radio throughput (Mbps), delivered during the interval.
Max bitrate	Indicates the maximum total radio throughput (Mbps), delivered during the interval.

Chapter 20: Ethernet Services and Interfaces (CLI)

This section includes:

- Configuring Ethernet Services (CLI)
- Setting the MRU Size and the S-VLAN Ethertype (CLI)
- Configuring Ethernet Interfaces (CLI)
- Configuring Automatic State Propagation and Link Loss Forwarding (CLI)
- Viewing Ethernet PMs and Statistics (CLI)

Related topics:

- Configuring Link Aggregation (LAG) and LACP (Optional) (CLI)
- Performing Ethernet Loopback (CLI)
- Ethernet Protocols (CLI)

Configuring Ethernet Services (CLI)

This section includes:

Ethernet Services Overview (CLI)

Users can define the following number of Ethernet services:

- PTP 850C and PTP 850E: Up to 1024.
- PTP 850S: Up to 64.

Each service constitutes a virtual bridge that defines the connectivity between logical ports in the PTP 850 network element.

This version of PTP 850 supports the following service types:

-

> **Note**
>
> In release 10.6, only P2P and MNG services are supported. In release 10.9, Multipoint services are also supported.

In addition to user-defined services, PTP 850 contains a pre-defined management service (Service ID 257). By default, this service is operational.

> **Note**
>
> You can use the management service for in-band management. For instructions on configuring in-band management, see Mate Management Access (IP Forwarding) (CLI)

A service point is a logical entity attached to a physical or logical interface. Service points define the movement of frames through the service. Each service point includes both ingress and egress attributes. A Point-to-Point or Multipoint service can hold up to 32 service points. A Management service can hold up 30 service points.

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

General Guidelines for Provisioning Ethernet Services (CLI)

When provisioning Ethernet services, it is recommended to follow these guidelines:

- Use the same Service ID for all service fragments along the path of the service.

- Do not re-use the same Service ID within the same region. A region is defined as consisting of all PTP 850 devices having Ethernet connectivity between them.
- Use meaningful EVC IDs.

Give the same EVC ID (service name) to all service fragments along the path of the service.

Do not reuse the same EVC ID within the same region.

It is recommended to follow these guidelines for creating service points:

Always use SNP service points on NNI ports and SAP service points on UNI ports.

For each logical interface associated with a specific service, there should never be more than a single service point.

The transport VLAN ID should be unique per service within a single region. That is, no two services should use the same transport VLAN ID.

Defining Services (CLI)

Use the commands described in the following sections to define a service and its parameters. After defining the service, you must add service points to the service in order for the service to carry traffic.

Adding a Service (CLI)

To add a service, enter the following command in root view:

```
root> ethernet service add type <service type> sid <sid> admin <service
admin mode> evc-id <evc-id> description <evc-description>
```

Table 126 Adding Ethernet Service CLI Parameters

Parameter	Input Type	Permitted Values	Description
service type	Variable	p2p mp	Defines the service type: p2p - Point-to-Point mp - Multipoint
sid	Number	PTP 850C and PTP 850E: Any unused value from 1- 4095 PTP 850S: Any unused value from 1-256	A unique ID for the service. Once you have added the service, you cannot change the Service ID. Service ID 257 is reserved for a pre-defined management service.

Parameter	Input Type	Permitted Values	Description
service admin mode	Variable	Operational reserved	The administrative state of the service: operational - The service is functional. reserved - The service is disabled until this parameter is changed to operational. In this mode, the service occupies system resources but is unable to receive and transmit data.
evc-id	Text String	Up to 20 characters.	Defines an Ethernet Virtual Connection (EVC) ID. This parameter does not affect the network element's behavior, but is used by the NMS for topology management.
evc-description	Text String	Up to 64 characters.	A text description of the service. This parameter does not affect the network element's behavior, but is used by the NMS for topology management.

The following command adds a Multipoint service with Service ID 18.

```
root> ethernet service add type mp sid 18 admin operational evc-id Ring_1
description east_west
```

The following command adds a Point-to-Point service with Service ID 10.

```
root> ethernet service add type p2p sid 10 admin operational evc-id
Ring_1 description east_west
```

These services are immediately enabled, although service points must be added to the services in order for the services to carry traffic.

Entering Service View (CLI)

To view service details and set the service's parameters, you must enter the service's view level in the CLI.

To enter a service's view level:

```
root> ethernet service sid <sid>
```

Table 127 Entering Ethernet Service View CLI Parameters

Parameter	Input Type	Permitted Values	Description
sid	Number	Any unused value from 1-256	A unique ID for the service. Once you have added the service, you cannot change the Service ID. Service ID 257 is reserved for a pre-defined management service.

The following command enters service view for the service with Service ID 10:

```
root> ethernet service sid 10
```

The following prompt appears:

```
service[10]>
```

Showing Service Details (CLI)

To display the attributes of a service, go to service view for the service and enter the following command:

```
service[SID]>service info show
```

For example:

```
service[1]>service info show
```

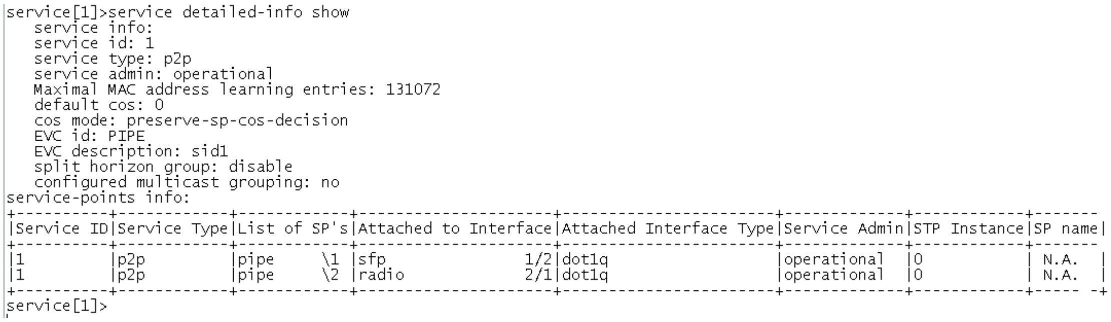
```
service info:
service id: 1
service type: p2p
service admin: operational
Maximal MAC address learning entries: 131072
default cos: 0
cos mode: preserve-sp-cos-decision
EVC id: N.A.
EVC description: N.A.
split horizon group: disable
configured multicast grouping: no
```

```
service[1]>
```

To display the attributes of a service and its service points, go to service view for the service and enter the following command:

```
service[SID]>service detailed-info show
```

For example:



```
service[1]>service detailed-info show
   service info:
   service id: 1
   service type: p2p
   service admin: operational
   Maximal MAC address learning entries: 131072
   default cos: 0
   cos mode: preserve-sp-cos-decision
   EVC id: PIPE
   EVC description: sid1
   split horizon group: disable
   configured multicast grouping: no
service-points info:
+----------+------------+------------+---------------------+-----------------------+-------------+------------+-------
|Service ID|Service Type|List of SP's|Attached to Interface|Attached Interface Type|Service Admin|STP Instance|SP name|
+----------+------------+------------+---------------------+-----------------------+-------------+------------+-------
|1         |p2p         |pipe      \1 |sfp               1/2|dot1q                  |operational  |0           | N.A.  |
|1         |p2p         |pipe      \2 |radio             2/1|dot1q                  |operational  |0           | N.A.  |
+----------+------------+------------+---------------------+-----------------------+-------------+------------+----- -+
service[1]>
```

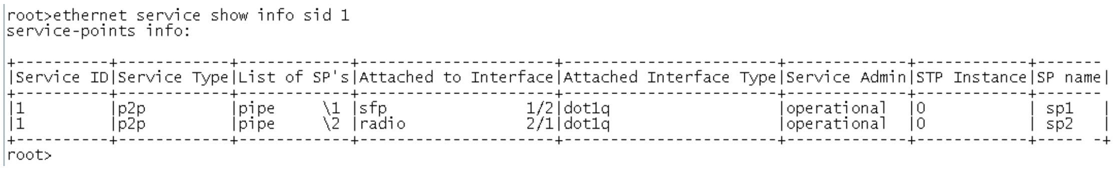
To display a list of service points and their attributes, enter the following command in root view:

```
root>ethernet service show info sid <sid>
```

Table 128 Displaying Ethernet Service Details CLI Parameters

Parameter	Input Type	Permitted Values	Description
sid	Number	Any defined Service ID.	None

For example:



```
root>ethernet service show info sid 1
service-points info:

+----------+------------+------------+---------------------+-----------------------+-------------+------------+-------
|Service ID|Service Type|List of SP's|Attached to Interface|Attached Interface Type|Service Admin|STP Instance|SP name|
+----------+------------+------------+---------------------+-----------------------+-------------+------------+-------
|1         |p2p         |pipe     \1 |sfp               1/2|dot1q                  |operational  |0           | sp1   |
|1         |p2p         |pipe     \2 |radio             2/1|dot1q                  |operational  |0           | sp2   |
+----------+------------+------------+---------------------+-----------------------+-------------+------------+----- -+
root>
```

Configuring a Service's Operational State (CLI)

To change the operational state of a service, go to service view for the service and enter the following command:

```
service[SID]>service admin set <service admin mode>
```

To display a service's admin mode, go to service view for the service and enter the following command:

```
Service[SID]> service admin show state
```

Table 129 Ethernet Service Operational State CLI Parameters

Parameter	Input Type	Permitted Values	Description
service admin mode	Variable	Operational reserved	The administrative state of the service: operational - The service is functional. reserved - The service is disabled until this parameter is changed to Operational. In this mode, the service occupies system resources but is unable to receive and transmit data.

The following command sets Service 10 to be operational:

```
service[10]>service admin set operational
```

Configuring a Service's CoS Mode and Default CoS (CLI)

The CoS mode determines whether or not frames passing through the service have their CoS modified at the service level. The CoS determines the priority queue to which frames are assigned.

The CoS of frames traveling through a service can be modified on the interface level, the service point level, and the service level. The service level is the highest priority, and overrides CoS decisions made at the interface and service point levels. Thus, by configuring the service to apply a CoS value to frames in the service, you can define a single CoS for all frames traveling through the service.

To set a service's CoS mode, go to service view for the service and enter the following command:

```
service[SID]>service cos-mode set cos-mode <cos-mode>
```

If the CoS mode is set to `default-cos`, you must define the Default CoS. Use the following command to define the Default CoS:

```
service[SID]>service default-cos set cos <cos>
```

Table 130 Ethernet Service CoS Mode CLI Parameters

Parameter	Input Type	Permitted Values	Description
cos-mode	Variable	default-cos preserve-sp-cos-decision	**default cos** - Frames passing through the service are assigned the default CoS defined below. This CoS value overrides whatever CoS may have been assigned at the service point or interface level. **preserve-sp-cos-decision** - The CoS of frames passing through the service is not modified by the service.
cos	Number	0 – 7	This value is assigned to frames at the service level if cos-mode is set to default-cos. Otherwise, this value is not used, and frames retain whatever CoS value they were assigned at the service point or logical interface level.

The following commands configure Service 10 to assign a CoS value of 7 to frames traversing the service:

```
service[10]>service cos-mode set cos-mode default-cos
service[10]>service default-cos set cos 7
```

The following command configures Service 10 to preserve the CoS decision made at the interface or service point level for frames traveling through the service:

```
service[10]>service cos-mode set cos-mode preserve-sp-cos-decision
```

Configuring a Service’s EVC ID and Description (CLI)

To add or change the EVC ID of a service, go to service view for the service and enter the following command:

```
service[SID]>service evcid set <evcid>
```

To display a service’s EVC ID, go to service view for the service and enter the following command:

```
service[SID]>service evcid show
```

To add or change the EVC description of a service, go to service view for the service and enter the following command:

```
service[SID]>service description set <evc description>
```

To display a service’s EVC description, go to service view for the service and enter the following command:

```
service[SID]>service description show
```

Table 131 Ethernet Service EVC CLI Parameters

Parameter	Input Type	Permitted Values	Description
evcid	Text String	Up to 20 characters.	Defines an Ethernet Virtual Connection (EVC) ID. This parameter does not affect the network element’s behavior, but is used by the NMS for topology management.
evc description	Text String	Up to 64 characters.	A text description of the service. This parameter does not affect the network element’s behavior, but is used by the NMS for topology management.

The following commands add the EVC ID "East_West" and the EVC description "Line_to_Radio" to Service 10:

```
service[10]>service evcid set East_West
service[10]>service description set Line_to_Radio
```

Deleting a Service (CLI)

Before deleting a service, you must first delete any service points attached to the service (refer to Deleting a Service Point (CLI)).

Use the following command to delete a service:

```
root>ethernet service delete sid <sid>
```

Use the following command to delete a range of services:

```
root>ethernet service delete sid <sid> to <sid>
```

Table 132 Deleting Ethernet Service CLI Parameters

Parameter	Input Type	Permitted Values	Description
sid	Number	Any defined Service ID.	The Service ID.

The following command deletes Service 10:

```
root>ethernet service delete sid 10
```

The following command deletes Services 10 through 15:

```
root>ethernet service delete sid 10 to 15
```

Configuring Service Points (CLI)

This section includes:

- Service Points Overview (CLI)
- Service Point Classification (CLI)
- Adding a Service Point (CLI)
- Configuring Service Point Ingress Attributes (CLI)

- Configuring Service Point Egress Attributes (CLI)
- Displaying Service Point Attributes (CLI)
- Deleting a Service Point (CLI)

Service Points Overview (CLI)

Service points are logical interfaces within a service. A service point is a logical entity attached to a physical or logical interface. Service points define the movement of frames through the service. Each service point includes both ingress and egress attributes.

Each service point for a Point-to-Point or Multipoint service can be either a Service Access Point (SAP) or a Service Network Point (SNP). A Point-to-Point service can also use Pipe service points.

An SAP is equivalent to a UNI in MEF terminology and defines the connection of the user network with its access points. SAPs are used for Point-to-Point and Multipoint traffic services.

An SNP is equivalent to an NNI or E-NNI in MEF terminology and defines the connection between the network elements in the user network. SNPs are used for Point-to-Point and Multipoint traffic services.

A Pipe service point is used to create traffic connectivity between two ports in a port-based manner (Smart Pipe). In other words, all the traffic from one port passes to the other port.

Management services utilize Management (MNG) service points.

A Point-to-Point or Multipoint service can hold up to 32 service points. A management service can hold up to 30 service points.

Table 133 summarizes the service point types available per service type.

Table 133 Service Points per Service Type

		Service Point Type			
		MNG	SAP	SNP	Pipe
Service Type	Management	Yes	No	No	No
	Point-to-Point	No	Yes	Yes	Yes
	Multipoint	No	Yes	Yes	No

Table 134 shows which service point types can co-exist on the same interface.

Table 134 Service Point Types per Interface

	MNG	SAP	SNP	Pipe
MNG	Only one MNG SP is allowed per interface.	Yes	Yes	Yes
SAP	Yes	Yes	No	No
SNP	Yes	No	Yes	No

	MNG	SAP	SNP	Pipe
PIPE	Yes	No	No	Only one Pipe SP is allowed per interface.

Service Point Classification (CLI)

This section includes:

- Overview of Service Point Classification (CLI)
- SAP Classification (CLI)
- SNP Classification (CLI)
- Pipe Service Point Classification (CLI)
- MNG Service Point Classification (CLI)

Overview of Service Point Classification (CLI)

Service points connect the service to the network element interfaces. It is crucial that the network element have a means to classify incoming frames to the proper service point. This classification process is implemented by means of a parsing encapsulation rule for the interface associated with the service point. This rule is called the Interface Type, and is based on a key consisting of:

The Interface ID of the interface through which the frame entered.

The frame’s C-VLAN and/or S-VLAN tags.

The Interface Type provides a definitive mapping of each arriving frame to a specific service point in a specific service. Since more than one service point may be associated with a single interface, frames are assigned to the earliest defined service point in case of conflict.

SAP Classification (CLI)

SAPs can be used with the following Interface Types:

- All to one – All C-VLANs and untagged frames that enter the interface are classified to the same service point.
- Dot1q – A single C-VLAN is classified to the service point.
- QinQ – A single S-VLAN and C-VLAN combination is classified to the service point.
- Bundle C-Tag – A set of multiple C-VLANs is classified to the service point.
- Bundle S-Tag – A single S-VLAN and a set of multiple C-VLANs are classified to the service point.

SNP Classification (CLI)

- SNPs can be used with the following Attached Interface Types:
- Dot1q – A single C-VLAN is classified to the service point.
- S-Tag – A single S-VLAN is classified to the service point.

Pipe Service Point Classification (CLI)

- Pipe service points can be used with the following Attached Interface Types:

- Dot1q – All C-VLANs and untagged frames that enter the interface are classified to the same service point.
- S-Tag – All S-VLANs and untagged frames that enter the interface are classified to the same service point.

MNG Service Point Classification (CLI)

- Management service points can be used with the following Interface Types:
- Dot1q – A single C-VLAN is classified to the service point.
- S-Tag – A single S-VLAN is classified to the service point.
- QinQ – A single S-VLAN and C-VLAN combination is classified to the service point.

Table 135 and Table 136 show which service point – Interface Type combinations can co-exist on the same interface.

Table 135 Legal Service Point – Interface Type Combinations per Interface – SAP and SNP

	SP Type	SAP					SNP	
SP Type	**Attached Interface Type**	**802.1q**	**Bundle -C**	**Bundle -S**	**All to One**	**Q in Q**	**802.1q**	**S-Tag**
SAP	**802.1q**	Yes	Yes	No	No	No	No	No
	Bundle-C	Yes	Yes	No	No	No	No	No
	Bundle-S	No	No	Yes	No	Yes	No	No
	All to One	No	No	No	Only 1 All to One SP Allowed	No	No	No
	Q in Q	No	No	Yes	No	Yes	No	No
SNP	**802.1q**	No	No	No	No	No	Yes	No
	S-Tag	No	No	No	No	No	No	Yes
Pipe	**802.1q**	No	No	No	No	No	No	No
	S-Tag	No	No	No	No	No	No	No
MNG	**802.1q**	Yes	Yes	No	No	No	Yes	No
	Q in Q	No	No	Yes	No	Yes	No	No
	S-Tag	No	No	No	No	No	No	Yes

Table 136 Legal Service Point – Interface Type Combinations per Interface – Pipe and MNG

	SP Type	Pipe		MNG		
SP Type	**Attached Interface Type**	**802.1q**	**S-Tag**	**802.1q**	**Q in Q**	**S-Tag**
SAP	**802.1q**	No	No	Yes	No	No
	Bundle-C	No	No	Yes	No	No
	Bundle-S	No	No	No	Yes	No
	All to One	No	No	No	No	No
	Q in Q	No	No	No	Yes	No
SNP	**802.1q**	No	No	Yes	No	No
	S-Tag	No	No	No	No	Yes
Pipe	**802.1q**	Only one Pipe SP Allowed	No	Yes	No	No
	S-Tag	No	Only one Pipe SP Allowed	No	No	Yes
MNG	**802.1q**	Yes	No	Only 1 MNG SP Allowed	No	No
	Q in Q	No	No	No	Only 1 MNG SP Allowed	No
	S-Tag	No	Yes	No	No	Only 1 MNG SP Allowed

Adding a Service Point (CLI)

The command syntax for adding a service point depends on the interface type of the service point. The interface type determines which frames enter the service via this service point.

To add a service point with an All-to-One interface type, go to service view for the service and enter the following command:

```
service[SID]>sp add sp-type <sp-type> int-type all-to-one spid <sp-id>
[interface|group] <interface|group> slot <slot> port <port> sp-name <sp-
name>
```

To add a service point with a Dot1q interface type, go to service view for the service and enter the following command:

```
service[SID]>sp add sp-type <sp-type> int-type dot1q spid <sp-id>
[interface|group] <interface|group> slot <slot> port <port> vlan <vlan>
sp-name <sp-name>
```

To add a service point with an S-Tag interface type, go to service view for the service and enter the following command:

```
service[SID]>sp add sp-type <sp-type> int-type s-tag spid <sp-id>
[interface|group] <interface|group> slot <slot> port <port> vlan <vlan>
sp-name <sp-name>
```

To add a service point with a Bundle-C interface type, go to service view for the service and enter the following command:

```
service[SID]>sp add sp-type <sp-type> int-type bundle-c spid <sp-id>
[interface|group] <interface|group> slot <slot> port <port> sp-name <sp-
name>
```

To add a service point with a Bundle-S interface type, go to service view for the service and enter the following command:

```
service[SID]>sp add sp-type <sp-type> int-type bundle-s spid <sp-id>
[interface|group] <interface|group> slot <slot> port <port> [outer-
vlan <outer-vlan>|vlan <vlan>] sp-name <sp-name>
```

Note: In SAP service points, use the parameter `outer-vlan`. In SP service points, use the parameter `vlan`.

To add a service point with a Q-in-Q interface type, go to service view for the service and enter the following command:

```
service[SID]>sp add sp-type <sp-type> int-type qinq spid <sp-id>
[interface|group] <interface|group> slot <slot> port <port> outer-
vlan <outer-vlan> inner-vlan <inner-vlan> sp-name <sp-name>
```

To add a Pipe service point, go to service view for the service and enter the following command:

```
service[SID]>sp add sp-type pipe int-type <int-type> spid <sp-id>
[interface|group] <interface|group> slot <slot> port <port> sp-name <sp-
name>
```

Table 137 Add Service Point CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-type	Variable	sap snp pipe mng	SAP - Service Access Point SNP - Service Network Point PIPE - Pipe service point MNG - Management service point
int-type	Variable	all-to-one dot1q s-tag bundle-c-tag bundle-s-tag qinq	Determines which frames enter the service via this service point, based on the frame's VLAN tagging. Since more than one service point may be associated with a single interface, frames are assigned to the earliest defined service point in case of conflict. all-to-one - All C-VLANs and untagged frames that enter the interface are classified to the service point. Only valid for SAP service point types. dot1q - A single C-VLAN is classified to the service point. Valid for all service point types. s-tag - A single S- VLAN is classified to the service point. Valid for SNP and MNG service point types. bundle-c-tag - A set of multiple C-VLANs is classified to the service point. Only valid for SAP service point types. bundle-s-tag - A single S-VLAN and a set of multiple C-VLANs are classified to the service point. Only valid for SAP service point types. qinq - A single S-VLAN and C-VLAN combination is classified to the service point. Valid for SAP and MNG service point types.
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	This ID is unique within the service.

Parameter	Input Type	Permitted Values	Description
interface	Variable	eth radio	The Interface type for the service point: eth - An Ethernet interface. radio - A radio interface. When you are defining the service point on a group, such as a LAG, use the group parameter instead of the interface parameter.
group	Variable	rp1 rp2 rp3 rp4 lag1 lag2 lag3 lag4 mc-abc1 mc-abc2 mc-abc3 mc-abc4	When you are defining the service point on an HSB group (rp1 - rp-4), a LAG (lag1 - lag4), or a Multi-Carrier ABC group (mc-abc1 - mc-abc4), use this parameter instead of the interface parameter to identify the group. The group must be defined before you add the service point. **Note**: Multi-Carrier ABC and HSB protection are only relevant for PTP 850E units.
slot	Number	Ethernet: 1 Radio: 2	
port	Number	For an Ethernet interface: 1-3 For a radio interface in PTP 850E units: 1-2 For a radio interface in PTP 850E: 1	The port or radio carrier on which the service point is located.

Parameter	Input Type	Permitted Values	Description
vlan	Number or Variable	1-4094 (except 4092 which is reserved for the default management service), or Untagged	Defines the VLAN classified to the service point. This parameter should not be included for service points with an interface type of bundle-C-tag. For instructions on attaching a bundled VLAN, refer to Attaching a VLAN Bundle to a Service Point (CLI). This parameter is also not relevant for: Service points with an interface type of qinq and all-to-one. Pipe service points.
outer-vlan	Number	1-4094 (except 4092, which is reserved for the default management service), or Untagged	Defines the S-VLAN classified to the service point. This parameter is only relevant for service points with the interface type bundle-s-tag or qinq.
inner-vlan	Number	1-4094 (except 4092, which is reserved for the default management service), or Untagged	Defines the C-VLAN classified to the service point. This parameter is only relevant for service points with the interface type qinq.
sp-name	Text string	Up to 20 characters.	A descriptive name for the service point (optional).

The following command adds an SAP service point with Service Point ID 10 to Service 37, with interface type dot1q. This service point is located on radio carrier 1. VLAN ID 100 is classified to this service point.

```
service[37]>sp add sp-type sap int-type dot1q spid 10 interface radio
slot 2 port 1 vlan 100 sp-name Radio
```

The following command adds an SAP service point with Service Point ID 10 to Service 37, with interface type bundle-s-tag. This service point is located on radio carrier 2 in a PTP 850E unit. S-VLAN 100 is classified to the service point.

```
service[37]>sp add sp-type sap int-type bundle-s-tag spid 10 interface
radio slot 2 port 2 outer-vlan 100 sp-name Radio
```

The following command adds an SAP service point with Service Point ID 10 to Service 37, with interface type qinq. This service point is located on radio carrier 2 in a PTP 850E unit. S-VLAN 100 and C-VLAN 200 are classified to the service point.

```
service[37]>sp add sp-type sap int-type qinq spid 10 interface radio slot
2 port 2 outer-vlan 100 inner-vlan 200 sp-name Radio
```

The following command adds an SAP service point with Service Point ID 10 to Service 37, with interface type all-to-one. This service point is located on radio carrier 1. All traffic entering the system from that port is classified to the service point.

```
service[37]>sp add sp-type sap int-type all-to-one spid 10 interface
radio slot 2 port 1 sp-name "all-to-one"
```

The following command adds an SNP service point with Service Point ID 10 to Service 37, with interface type s-tag. This service point is located on radio carrier 1. S-VLAN 100 is classified to the service point.

```
service[37]>sp add sp-type snp int-type s-tag spid 10 interface radio
slot 2 port 1 vlan 100 sp-name Radio
```

The following command adds an SAP service point with Service Point ID 7 to Service 36, with interface type dot1q. This service point is connected to HSB group 1 (rp1). VLAN ID 100 is classified to the service point.

```
service[36]>sp add sp-type sap int-type dot1q spid 7 group rp1 vlan 100
sp-name test1
```

The following command adds a Pipe service point with Service Point ID 1 to Service 1, with interface type dot1q. This service point is connected to Eth1.

```
service[1]>sp add sp-type pipe int-type dot1q spid 1 interface eth slot 1
port 1 sp-name pipe_dot1q
```

The following commands create a Smart Pipe service between Eth1 and radio carrier 1. This service carries S-VLANs and untagged frames between the two interfaces:

```
root> ethernet service add type p2p sid 10 admin operational evc-id test
description east_west

root>

root> ethernet service sid 10

service[10]>

service[10]>sp add sp-type pipe int-type s-tag spid 1 interface eth slot
1 port 1 sp-name test1

service[10]>

service[10]>sp add sp-type pipe int-type s-tag spid 2 interface radio
slot 2 port 1 sp-name test2

service[10]>
```

Configuring Service Point Ingress Attributes (CLI)

A service point's ingress attributes are attributes that operate upon frames ingressing via the service point. This includes how the service point handles the CoS of ingress frames and how the service point forwards frames to their next destination within the service.

This section includes:

Enabling and Disabling Broadcast Frames (CLI)

CoS Preservation and Modification on a Service Point (CLI)
Enabling and Disabling Flooding (CLI)

Enabling and Disabling Broadcast Frames (CLI)

To determine whether frames with a broadcast destination MAC address are allowed to ingress the service via this service point, go to service view for the service and enter the following command:

```
service[SID]>sp broadcast set spid <sp-id> state <state>
```

Table 138 Enable/Disable Broadcast Frames CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
state	Variable	allow disable	Determines whether frames with a broadcast destination MAC address are allowed to ingress the service via this service point.

The following command allows frames with a broadcast destination MAC address to ingress Service 37 via Service Point 1.

```
service[37]>sp broadcast set spid 1 state allow
```

The following command prevents frames with a broadcast destination MAC address from ingressing Service 37 via Service Point 1.

```
service[37]>sp broadcast set spid 1 state disable
```

CoS Preservation and Modification on a Service Point (CLI)

The CoS of frames traversing a service can be modified on the logical interface, service point, and service level. The service point can override the CoS decision made at the interface level. The service, in turn, can modify the CoS decision made at the service point level.

To determine whether the service point modifies CoS decisions made at the interface level, go to service view for the service and enter the following command:

```
service[SID]> sp cos-mode set spid <sp-id> mode <cos mode>
```

If you set cos-mode to `sp-def-cos`, you must then configure a default CoS. This CoS is applied to frames that ingress the service point, but can be overwritten at the service level.
To configure the default CoS, go to service view for the service and enter the following command:

```
service[SID]>sp sp-def-cos set spid <sp-id> cos <cos>
```

Table 139 Service Point CoS Preservation CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
cos mode	Variable	sp-def-cos interface-decision	sp-def-cos - The service point re-defines the CoS of frames that pass through the service point, according to the Default CoS (below). This decision can be overwritten on the service level. interface-decision - The service point preserves the CoS decision made at the interface level. This decision can still be overwritten at the service level.
cos	Number	0 – 7	If cos-mode is sp-def-cos, this is the CoS assigned to frames that pass through the service point. This decision can be overwritten on the service level.

The following commands configure Service Point 1 in Service 37 to apply a CoS value of 5 to frames that ingress the service point:

```
service[37]>sp cos-mode set spid 1 mode sp-def-cos
service[37]>sp sp-def-cos set spid 1 cos 5
```

The following command configures Service Point 1 in Service 37 to preserve the CoS decision made at the interface level for frames that ingress the service point:

```
service[37]>sp cos-mode set spid 1 mode interface-decision
```

Enabling and Disabling Flooding (CLI)

The ingress service point for a frame can forward the frame within the service by means of flooding or dynamic MAC address learning in the service.

To enable or disable forwarding by means of flooding for a service point, go to service view for the service and enter the following command:

```
service[SID]>sp flooding set spid <sp-id> state <flooding state>
```

Table 140 Service Point Enable/Disable Flooding CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.

Parameter	Input Type	Permitted Values	Description
state	Variable	Allow disable	Determines whether incoming frames with unknown MAC addresses are forwarded to other service points via flooding.

The following command configures Service Point 1 in Service 37 to flood incoming frames with unknown MAC addresses to other service points:

```
service[37]>sp flooding set spid 1 state allow
```

The following command configures Service Point 1 in Service 37 not to flood incoming frames with unknown MAC addresses to other service points:

```
service[37]>sp flooding set spid 1 state disable
```

Configuring Service Point Egress Attributes (CLI)

A service point's egress attributes are attributes that operate upon frames ingressing via the service point. This includes VLAN preservation and marking attributes.

This section includes:

- Configuring VLAN and CoS Preservation (CLI)
- Configuring Service Bundles (CLI)
- Attaching a VLAN Bundle to a Service Point (CLI)

Configuring VLAN and CoS Preservation (CLI)

CoS and VLAN preservation determines whether the CoS and/or VLAN IDs of frames egressing the service via the service point are restored to the values they had when the frame entered the service.

This section includes:

- Configuring C-VLAN CoS Preservation (CLI)
- Configuring C-VLAN Preservation (CLI)
- Configuring S-VLAN CoS Preservation (CLI)

Configuring C-VLAN CoS Preservation (CLI)

To configure CoS preservation for C-VLAN-tagged frames, go to service view for the service and enter the following command:

```
service[SID]>sp cvlan-cos-preservation-mode set spid <sp-id> mode <c-
vlan cos preservation mode>
```

Table 141 C-VLAN CoS Preservation Mode CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
c-vlan cos preservation mode	Variable	enable disable	Select enable or disable to determine whether the original C-VLAN CoS value is preserved or restored for frames egressing the service point. enable - the C-VLAN CoS value of frames egressing the service point is the same as the value when the frame entered the service. disable - the C-VLAN CoS value of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking (see Configuring Marking (CLI)).

The following command enables C-VLAN CoS preservation for Service Point 1 on Service 37:

```
service[37]>sp cvlan-cos-preservation-mode set spid 1 mode enable
```

The following command disables C-VLAN CoS preservation for Service Point 1 on Service 37:

```
service[37]>sp cvlan-cos-preservation-mode set spid 1 mode disable
```

Configuring C-VLAN Preservation (CLI)

To configure VLAN preservation for C-VLAN-tagged frames, go to service view for the service and enter the following command:

```
service[SID]>sp cvlan-preservation-mode set spid <sp-id> mode <c-
vlan preservation mode>
```

Table 142 C-VLAN Preservation CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.

Parameter	Input Type	Permitted Values	Description
c-vlan preservation mode	Variable	enable disable	Determines whether the original C-VLAN ID is preserved or restored for frames egressing from the service point. enable - The C-VLAN ID of frames egressing the service point is the same as the C-VLAN ID when the frame entered the service. disable - The C-VLAN ID of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking (see Configuring Marking (CLI)).

The following command enables C-VLAN preservation for Service Point 1 on Service 37:

```
service[37]>sp cvlan-preservation-mode set spid 1 mode enable
```

The following command disables C-VLAN preservation for Service Point 1 on Service 37:

```
service[37]>sp cvlan-preservation-mode set spid 1 mode disable
```

Configuring S-VLAN CoS Preservation (CLI)

To configure CoS preservation for S-VLAN-tagged frames, go to service view for the service and enter the following command:

```
service[SID]>sp svlan-cos-preservation-mode set spid <sp-id> mode <s-
vlan cos preservation mode>
```

Table 143 S-VLAN CoS Preservation CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
s-vlan cos preservation mode	Variable	enable disable	Select enable or disable to determine whether the original S-VLAN CoS value is preserved or restored for frames egressing the service point. enable - the S-VLAN CoS value of frames egressing the service point is the same as the value when the frame entered the service. disable - the S-VLAN CoS value of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking (see Configuring Marking (CLI)).

The following command enables S-VLAN CoS preservation for Service Point 1 on Service 37:

```
service[37]>sp svlan-cos-preservation-mode set spid 1 mode enable
```

The following command disables S-VLAN CoS preservation for Service Point 1 on Service 37:

```
service[37]>sp svlan-cos-preservation-mode set spid 1 mode disable
```

Configuring Service Bundles (CLI)

You can use service bundles to personalize common sets of egress queue attributes that can be applied to multiple service points. In this version only one service bundle is supported.

To assign a service point to a service bundle, go to service view for the service and enter the following command:

```
service[SID]>sp egress-service-bundle set spid 1 service-bundle-id
<service-bundle-id>
```

Table 144 Service Bundle CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
service-bundle-id	Number	1 – 63 **Note**: In the current release, only Service Bundle 1 is supported.	The service bundle assigned to the service point.

The following command assigns Service Bundle 1 to Service Point 1 in Service 37.

```
service[37]>sp egress-service-bundle set spid 1 service-bundle-id 1
```

Attaching a VLAN Bundle to a Service Point (CLI)

For service points with an interface type of bundle-C-tag or bundle-S-tag, you must classify a group of VLANs (VLAN Bundle) to the service point.

To classify a VLAN Bundle to a bundle-c-tag or bundle s-tag service point, go to service view for the service and enter the following command:

```
service[SIP]>sp bundle cvlan attach spid <sp-id> vlan <vlan> to-vlan <to-vlan>
```

To remove a VLAN Bundle from a bundle-c-tag or bundle-s-tag service point, go to service view for the service and enter the following command:

```
service[SIP]>sp bundle cvlan remove spid <sp-id> vlan <vlan> to-vlan <to-vlan>
```

To remove untagged frames from a bundle-c-tag or bundle s-tag service point, go to service view for the service and enter the following command:

```
service[SIP]>sp bundle remove untagged spid <sp-id>
```

To display a service point's attributes, including the VLANs classified to a bundle service point, go to service view for the service to which the service point belongs and enter the following command:

```
service[SID]>sp service-point-info show spid <sp-id>
```

Table 145 VLAN Bundle to Service Point CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
vlan	Number	1-4094 (except 4092, which is reserved for the default management service)	The C-VLAN at the beginning of the range of the VLAN Bundle.
to-vlan	Number	1-4094 (except 4092, which is reserved for the default management service)	The C-VLAN at the end of the range of the VLAN Bundle.

The following command classifies C-VLANs 100 through 200 to Service Point 1 in Service 37:

```
service[37]>sp bundle cvlan attach spid 1 vlan 100 to-vlan 200
```

The following command removes C-VLANs 100 through 200 from Service Point 1 in Service 37:

```
service[37]>sp bundle cvlan remove spid 1 vlan 100 to-vlan 200
```

Displaying Service Point Attributes (CLI)

To display a service point's attributes, go to service view for the service to which the service point belongs and enter the following command:

```
service[SID]>sp service-point-info show spid <sp-id>
```

Table 146 Display Service Point Attributes CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.

The following command displays the attributes of Service Point 1 in Service 37:

```
service[37]>sp service-point-info show spid 1
```

Deleting a Service Point (CLI)

You can only delete a service point if no VLAN bundles are attached to the service point. This is only relevant if the interface type of the service point is bundle-c-tag or bundle-s-tag. For more information, refer to Attaching a VLAN Bundle to a Service Point (CLI).

To delete a service point from a service, go to service view for the service and enter the following command:

```
service[SID]>sp delete spid <sp-id>
```

Table 147 Delete Service Point Attributes CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.

The following command deletes Service Point 10 from Service 37:

```
service[37]>sp delete spid 10
```

Defining the MAC Address Forwarding Table for a Service (CLI)

This section includes:

- MAC Address Forwarding Table Overview (CLI)
- Setting the Maximum Size of the MAC Address Forwarding Table (CLI)
- Setting the MAC Address Forwarding Table Aging Time (CLI)
- Adding a Static MAC Address to the Forwarding Table (CLI)
- Displaying the MAC Address Forwarding Table (CLI)
- Flushing the MAC Address Forwarding Table (CLI)
- Enabling MAC Address Learning on a Service Point (CLI)

MAC Address Forwarding Table Overview (CLI)

PTP 850 performs MAC address learning per service. PTP 850 can learn up to 131,072 MAC addresses.

If necessary due to security issues or resource limitations, you can limit the size of the MAC address forwarding table. The maximum size of the MAC address forwarding table is configurable per service in granularity of 16 entries.

When a frame arrives via a specific service point, the learning mechanism checks the MAC address forwarding table for the service to which the service point belongs to determine whether that MAC address is known to the service. If the MAC address is not found, the learning mechanism adds it to the table.

In parallel with the learning process, the forwarding mechanism searches the service’s MAC forwarding table for the frame’s MAC address. If a match is found, the frame is forwarded to the service point associated with the MAC address. If not, the frame is flooded to all service points in the service.

Setting the Maximum Size of the MAC Address Forwarding Table (CLI)

To limit the size of the MAC address forwarding table for a specific service, go to service view for the service and enter the following command:

```
service[SID]>service mac-limit-value set <mac limit>
```

Table 148 MAC Address Forwarding Table Maximum Size CLI Parameters

Parameter	Input Type	Permitted Values	Description
mac limit	Number	16 to 131,072, in multiples of 16	The maximum MAC address table size for the service. This maximum only applies to dynamic, not static, MAC address table entries.

The following command limits the number of dynamic MAC address forwarding table entries for Service 10 to 128:

```
service[10]>service mac-limit-value set 128
```

Setting the MAC Address Forwarding Table Aging Time (CLI)

You can configure a global aging time for dynamic entries in the MAC address forwarding table. Once this aging time expires for a specific table entry, the entry is erased from the table.

To set the global aging time for the MAC address forwarding table, enter the following command:

```
root> ethernet service learning-ageing-time set time <time>
```

To display the global aging time for the MAC address forwarding table, enter the following command:

```
root> ethernet service learning-ageing-time show
```

Table 149 MAC Address Forwarding Table Aging Time CLI Parameters

Parameter	Input Type	Permitted Values	Description
time	Number	15 - 3825	The global aging time for the MAC address forwarding table, in seconds.

The following command sets the global aging time to 2500 seconds:

```
root> ethernet service learning-ageing-time set time 2500
```

Adding a Static MAC Address to the Forwarding Table (CLI)

You can add static entries to the MAC forwarding table. The global aging timer does not apply to static entries, and they are not counted with respect to the maximum size of the MAC address forwarding table. It is the responsibility of the user not to use all the entries in the table if the user also wants to utilize dynamic MAC address learning.

To add a static MAC address to the MAC address forwarding table, go to service view for the service to which you want to add the MAC address and enter the following command:

```
service[SID]>service mac-learning-table set-static-
mac <static mac> spid <sp-id>
```

To delete a static MAC address from the MAC address forwarding table, go to service view for the service from which you want to delete the MAC address and enter the following command:

```
service[SID]>service mac-learning-table del-static-
mac <static mac> spid <sp-id>
```

Table 150 Adding Static Address to MAC Address Forwarding Table CLI Parameters

Parameter	Input Type	Permitted Values	Description
static mac	Six groups of two hexadecimal digits		The MAC address.
sp-id	Number	1-32	The Service Point ID of the service point associated with the MAC address.

The following command adds MAC address 00:11:22:33:44:55 to the MAC address forwarding table for Service 10, and associates the MAC address with Service Point ID 1 on Service 10:

```
service[10]>service mac-learning-table set-static-
mac 00:11:22:33:44:55 spid 1
```

The following command deletes MAC address 00:11:22:33:44:55, associated with Service Point 1, from the MAC address forwarding table for Service 10:

```
service[10]>service mac-learning-table del-static-
mac 00:11:22:33:44:55 spid 1
```

Displaying the MAC Address Forwarding Table (CLI)

You can display the MAC address forwarding table for an interface, a service, or for the entire unit.

To display the MAC address forwarding table for a service, go to service view for the service and enter the following command:

```
service[SID]>service mac-learning-table show
```

To display the MAC address forwarding table for an interface, go to interface view for the interface and enter the following command:

```
eth type xxx[x/x]>mac-learning-table show
```

To display the MAC address forwarding table for the entire unit, enter the following command:

```
root> ethernet generalcfg mac-learning-table show
```

Example

To display the MAC address forwarding table for GbE 1, enter the following commands:

```
root> ethernet interfaces eth slot 1 port 1

eth type eth[1/1]>mac-learning-table show
```

Flushing the MAC Address Forwarding Table (CLI)

You can perform a global flush on the MAC address forwarding table. This erases all dynamic entries for all services. Static entries are not erased.

Note

The ability to flush the MAC address forwarding table per-service and per-interface is planned for future release.

To perform a global flush of the MAC address forwarding table, enter the following command:

```
root> ethernet service mac-learning-table set global-flush
```

Enabling MAC Address Learning on a Service Point (CLI)

You can enable or disable MAC address learning for specific service points. By default, MAC learning is enabled.

To enable or disable MAC address learning for a service point, go to service view for the service and enter the following command:

```
service[SID]>sp learning-state set spid <sp-id> learning <learning>
```

Table 151 Enabling MAC Address Learning CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32	The Service Point ID of the service point associated with the MAC address.
learning	Variable	Enable disable	Select enable or disable to enable or disable MAC address learning for frames that ingress via the service point. When enabled, the service point learns the source MAC addresses of incoming frames and adds them to the MAC address forwarding table.

The following command enables MAC address learning for Service Point 1 on Service 37:

```
service[37]>sp learning-state set spid 1 learning enable
```

The following command disables MAC address learning for Service Point 1 on Service 37:

```
service[37]>sp learning-state set spid 1 learning disable
```

Setting the MRU Size and the S-VLAN Ethertype (CLI)

The following parameters are configured globally for the PTP 850 switch:

S- VLAN Ethertype – Defines the ethertype recognized by the system as the S-VLAN ethertype.

C-VLAN Ethertype – Defines the ethertype recognized by the system as the C-VLAN ethertype. PTP 850 supports 0x8100 as the C-VLAN ethertype.

MRU – The maximum segment size defines the maximum receive unit (MRU) capability and the maximum transmit capability (MTU) of the system. You can configure a global MRU for the system.

Note

The MTU is determined by the receiving frame and editing operation on the frame.

This section includes:

Configuring the S-VLAN Ethertype (CLI)

Configuring the C-VLAN Ethertype (CLI)

Configuring the MRU (CLI)

Configuring the S-VLAN Ethertype (CLI)

To configure the S-VLAN Ethertype, enter the following command in root view:

```
root> ethernet generalcfg ethertype set svlan-value <ethertype>
```

To display the system S-VLAN ethertype, enter the following command in root view:

```
root> ethernet generalcfg ethertype show svlan
```

Table 152 Configure S-VLAN Ethertype CLI Parameters

Parameter	Input Type	Permitted Values	Description
ethertype	Hexadecimal	0x8100 0x88a8 0x9100 0x9200	Defines the ethertype recognized by the system as the S-VLAN ethertype.

Example

For example, the following command sets the system S-VLAN ethertype to 0x88a8:

```
root> ethernet generalcfg ethertype set svlan-value 0x88a8
```

Configuring the C-VLAN Ethertype (CLI)

The system C-VLAN Ethertype is set by the system as 0x8100.

To display the system C-VLAN ethertype, enter the following command in root view:

```
root> ethernet generalcfg ethertype show cvlan
```

Configuring the MRU (CLI)

To define the global size (in bytes) of the Maximum Receive Unit (MRU), enter the following command in root view:

```
root> ethernet generalcfg mru set size <size>
```

To display the system MRU, enter the following command in root view:

```
root> ethernet generalcfg mru show
```

Table 153 Configure MRU CLI Parameters

Parameter	Input Type	Permitted Values	Description
size	Number	64 to 9612	Defines the global size (in bytes) of the Maximum Receive Unit (MRU). Frames that are larger than the global MRU will be discarded.

Example

For example, the following command sets the system MRU to 9612:

```
root> ethernet generalcfg mru set size 9612
```

Configuring Ethernet Interfaces (CLI)

Related Topics:

Enabling the Interfaces (CLI)

Performing Ethernet Loopback (CLI)

Configuring Ethernet Services (CLI)

Quality of Service (QoS) (CLI)

P-20's switching fabric distinguishes between physical interfaces and logical interfaces. Physical and logical interfaces serve different purposes in the switching fabric. In some cases, a physical interface corresponds to a logical interface on a one-to-one basis. For some features, such as LAG, a group of physical interfaces can be joined into a single logical interface.

The basic interface characteristics, such as media type, port speed, duplex, and auto-negotiation, are configured on the physical interface level. Ethernet services, QoS, and OAM characteristics are configured on the logical interface level.

> **Note**
>
> You cannot change the configuration of the Management interface. By default, the Management interface has the following configuration:
>
> - Auto negotiation ON
> - Full Duplex
> - RJ45 - 100Mbps

This section includes:

- Entering Interface View (CLI)
- Displaying the Operational State of the Interfaces in the Unit (CLI)
- Viewing Interface Attributes (CLI)

To display an interface's attributes, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>summary show
```

To display an interface's current operational state (up or down), go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>operational state show
```

The following command shows the attributes of Eth 7:

```
eth type eth [1/7]>summary show
```

The following command shows the operational state of Eth 7:

```
eth type eth [1/7]>operational state show
```

Configuring the QSFP Interface on an PTP 850E (CLI)

The QSFP interface (P4) on an PTP 850E requires special configuration of the QSFP mode before configuring the normal physical interface parameters. Before changing the **QSFP Expected** parameter, you must verify that:

- The **Admin** status of Eth3, Eth4, Eth5, and Eth6 is **Down**. See *Enabling the Interfaces (CLI)*.

> **Note:** If the QSFP interface is already set to **40Gbps Ethernet**, Eth4, Eth5, and Eth6 do not appear in the Interface Manager, and are not relevant.

- No service point is attached to the interface. See *Configuring Service Points (CLI)*.
- No ASP pair is assigned to the interface. See *Configuring Automatic State Propagation and Link Loss Forwarding (CLI)*.
- No Policer is attached to the interface. See *Attaching a Rate Meter (Policer) to an Interface (CLI)*.
- No Shaper is attached to the interface. See *Configuring Shapers (CLI)*.
- The interface is not part of a LAG group. See *Configuring Link Aggregation (LAG) and LACP (Optional) (CLI)*.
- No synchronization is configured on the interface. See *Synchronization (CLI)*Synchronization.

To configure the QSFP interface, enter the following command in root view:

```
root> platform qsfp expected set slot 1 id 1 type <type>
```

To display the current parameters of the QSFP interface, enter the following command in root view:

```
root> platform qsfp expected show
```

The type parameter can be any of the following:

- **ETH** – Use this for 4x1/10 and 1x1/10 Gbps configurations. After entering the command, proceed to the following sections to configure the regular parameters of the interface or interfaces.
- **CPRI** – Reserved for future use.
- **ETH-40G** – Use this for 1x40 Gbps configurations. There is no need to configure the regular interface parameters because they are set:
  - Auto Negotiation is Off
  - Speed is 40 Gbps
  - Full Duplex

Note: The option **CPRI** is reserved for future use.

Configuring an Interface's Media Type (CLI)

- Configuring an Interface's Speed and Duplex State (CLI)
- Configuring an Interface's Auto Negotiation State (CLI)
- Configuring an Interface's IFG (CLI)
- Configuring an Interface's Preamble (CLI)
- Adding a Description for the Interface (CLI)

Entering Interface View (CLI)

To view interface details and set the interface's parameters, you must enter the interface's view level in the CLI.

Use the following command to enter an Ethernet interface's view level:

```
root> ethernet interfaces eth slot <slot> port <port>
```

Use the following command to enter the radio interface's view level:

```
root> ethernet interfaces radio slot <slot> port <port>
```

Use the following command to enter the view level of a group, such as a Multi-Carrier ABC group, an HSB protection group, or a LAG:

```
root> ethernet interfaces group <group>
```

Table 154 Entering Interface View CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	1	

Parameter	Input Type	Permitted Values	Description
port	Number	Ethernet: 1-7 Radio: 1	The port number of the interface.

Note

In release 10.6, only Ethernet 7 is supported, along with the radio interface. In release 10.9, Ethernet Slot 1, Ports 4 through 7 are also supported.

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

In a 4x1/10G configuration the QSFP port can provide four Ethernet interfaces: Eth3, Eth4, Eth 5, and Eth6. In this configuration, a QSFP transceiver is attached to the QSFP port, and an MPO-MPO cable is connected between the transceiver and a splitter on the other side of the link. The splitter splits the traffic between four Ethernet cables connecting the splitter to the customer equipment.

The following command enters interface view for Ethernet 7:

```
root> ethernet interfaces eth slot 1 port 7
```

The following prompt appears:

```
eth type eth [1/7]>
```

The following command enters interface view for the radio interface:

```
root> ethernet interfaces radio slot 1 port 1
```

The following prompt appears:

```
radio [1/1]>
```

Note

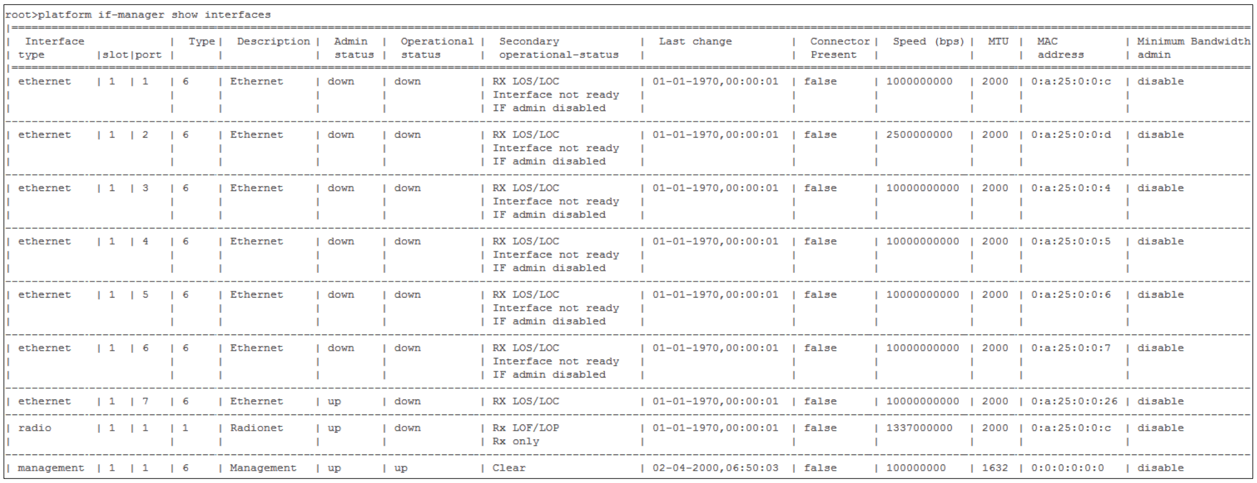
For simplicity, the examples in the following sections show the prompt for an Ethernet interface.

Displaying the Operational State of the Interfaces in the Unit (CLI)

To display a list of all interfaces in the unit and their operational states, enter the following command:

```
root> platform if-manager show interfaces
```

The following is a sample output of this command:



```
root>platform if-manager show interfaces
|==========================================================================================================================================================================
| Interface              | Type| Description | Admin  | Operational | Secondary             | Last change         | Connector| Speed (bps)| MTU | MAC          | Minimum Bandwidth
| type       |slot|port  |     |             | status | status      | operational-status    |                     | Present  |            |     | address      | admin
|==========================================================================================================================================================================
| ethernet   | 1  | 1    | 6   | Ethernet    | down   | down        | RX LOS/LOC            | 01-01-1970,00:00:01 | false    | 1000000000 | 2000| 0:a:25:0:0:c | disable
|                        |     |             |        |             | Interface not ready   |                     |          |            |     |              |
|                        |     |             |        |             | IF admin disabled     |                     |          |            |     |              |
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| ethernet   | 1  | 2    | 6   | Ethernet    | down   | down        | RX LOS/LOC            | 01-01-1970,00:00:01 | false    | 2500000000 | 2000| 0:a:25:0:0:d | disable
|                        |     |             |        |             | Interface not ready   |                     |          |            |     |              |
|                        |     |             |        |             | IF admin disabled     |                     |          |            |     |              |
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| ethernet   | 1  | 3    | 6   | Ethernet    | down   | down        | RX LOS/LOC            | 01-01-1970,00:00:01 | false    | 10000000000| 2000| 0:a:25:0:0:4 | disable
|                        |     |             |        |             | Interface not ready   |                     |          |            |     |              |
|                        |     |             |        |             | IF admin disabled     |                     |          |            |     |              |
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| ethernet   | 1  | 4    | 6   | Ethernet    | down   | down        | RX LOS/LOC            | 01-01-1970,00:00:01 | false    | 10000000000| 2000| 0:a:25:0:0:5 | disable
|                        |     |             |        |             | Interface not ready   |                     |          |            |     |              |
|                        |     |             |        |             | IF admin disabled     |                     |          |            |     |              |
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| ethernet   | 1  | 5    | 6   | Ethernet    | down   | down        | RX LOS/LOC            | 01-01-1970,00:00:01 | false    | 10000000000| 2000| 0:a:25:0:0:6 | disable
|                        |     |             |        |             | Interface not ready   |                     |          |            |     |              |
|                        |     |             |        |             | IF admin disabled     |                     |          |            |     |              |
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| ethernet   | 1  | 6    | 6   | Ethernet    | down   | down        | RX LOS/LOC            | 01-01-1970,00:00:01 | false    | 10000000000| 2000| 0:a:25:0:0:7 | disable
|                        |     |             |        |             | Interface not ready   |                     |          |            |     |              |
|                        |     |             |        |             | IF admin disabled     |                     |          |            |     |              |
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| ethernet   | 1  | 7    | 6   | Ethernet    | up     | down        | RX LOS/LOC            | 01-01-1970,00:00:01 | false    | 10000000000| 2000| 0:a:25:0:0:26| disable
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| radio      | 1  | 1    | 1   | Radionet    | up     | down        | Rx LOF/LOP            | 01-01-1970,00:00:01 | false    | 1337000000 | 2000| 0:a:25:0:0:c | disable
|                        |     |             |        |             | Rx only               |                     |          |            |     |              |
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| management | 1  | 1    | 6   | Management  | up     | up          | Clear                 | 02-04-2000,06:50:03 | false    | 100000000  | 1632| 0:0:0:0:0:0  | disable
```

Viewing Interface Attributes (CLI)

To display an interface's attributes, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>summary show
```

To display an interface's current operational state (up or down), go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>operational state show
```

The following command shows the attributes of Eth 7:

```
eth type eth [1/7]>summary show
```

The following command shows the operational state of Eth 7:

```
eth type eth [1/7]>operational state show
```

Configuring the QSFP Interface on an PTP 850E (CLI)

The QSFP interface (P4) on an PTP 850E requires special configuration of the QSFP mode before configuring the normal physical interface parameters. Before changing the **QSFP Expected** parameter, you must verify that:

- The **Admin** status of Eth3, Eth4, Eth5, and Eth6 is **Down**. See *Enabling the Interfaces (CLI)*.

Note: If the QSFP interface is already set to **40Gbps Ethernet**, Eth4, Eth5, and Eth6 do not appear in the Interface Manager, and are not relevant.

- No service point is attached to the interface. See *Configuring Service Points (CLI)*.
- No ASP pair is assigned to the interface. See *Configuring Automatic State Propagation and Link Loss Forwarding (CLI)*.
- No Policer is attached to the interface. See *Attaching a Rate Meter (Policer) to an Interface (CLI)*.
- No Shaper is attached to the interface. See *Configuring Shapers (CLI)*.

- The interface is not part of a LAG group. See *Configuring Link Aggregation (LAG) and LACP (Optional) (CLI)*.
- No synchronization is configured on the interface. See *Synchronization (CLI)*Synchronization.

To configure the QSFP interface, enter the following command in root view:

```
root> platform qsfp expected set slot 1 id 1 type <type>
```

To display the current parameters of the QSFP interface, enter the following command in root view:

```
root> platform qsfp expected show
```

The type parameter can be any of the following:

- **ETH** – Use this for 4x1/10 and 1x1/10 Gbps configurations. After entering the command, proceed to the following sections to configure the regular parameters of the interface or interfaces.
- **CPRI** – Reserved for future use.
- **ETH-40G** – Use this for 1x40 Gbps configurations. There is no need to configure the regular interface parameters because they are set:
  - Auto Negotiation is Off
  - Speed is 40 Gbps
  - Full Duplex

Note: The option **CPRI** is reserved for future use.

Configuring an Interface's Media Type (CLI)

The Media Type attribute defines the physical interface Layer 1 media type. Permitted values are RJ-45 and SFP.

Note

In System release 11.3,

For PTP 850C, Ethernet Slot 1, Ports 1, 2, 3, and 4 are supported.

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

To configure an Ethernet interface's Media Type, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>media-type state set <media type>
```

Table 155 Interface Media Type CLI Parameters

Parameter	Input Type	Permitted Values	Description
media type	Variable	rj45 sfp	Select the physical interface layer 1 media type: **RJ45** - An electrical (RJ-45) Ethernet interface. **SFP** - An optical (SFP) Ethernet interface.

Configuring an Interface's Speed and Duplex State (CLI)

To configure an Ethernet interface's maximum speed and duplex state, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>speed-and-duplex state set <speed-and-duplex state>
```

Table 156 Interface Speed and Duplex State CLI Parameters

Parameter	Input Type	Permitted Values	Description
speed-and-duplex state	Variable	'10hd' '10fd' '100hd' '100fd' '1000fd' '10000fd'	This parameter sets the maximum speed and the duplex state of the interface. For RJ-45 interfaces, any of the permitted values except 10000fd can be configured. For SFP interfaces, only '1000fd' is supported. **Note:** In relase 10.6, only Ethernet 7 (SFP+) is supported. In release 10.9, Ethernet Slot 1, Ports 4 through 7 are also supported.

Note

To use an SFP+ interface in 10G mode, the third-party switch must be running Pause Frame Flow Control, as defined in IEEE 802.3x. It is also recommended to configure shapers on the third-party switch so as to limit the packet flow from the switch to the PTP 850E unit to 2.5 Gbps.

After changing the speed of an SFP+ interface to or from 10000fd, you must reset the unit in order for the change to take effect.

Configuring an Interface’s Auto Negotiation State (CLI)

To configure an Ethernet interface’s auto-negotiation state, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>autoneg state set <autoneg state>
```

Table 157 Interface Auto Negotiation State CLI Parameters

Parameter	Input Type	Permitted Values	Description
autoneg state	Variable	On off	Enables or disables auto-negotiation on the physical interface. The default value is off. For Ports 3 to 6 (the QSFP ports), Auto Negotiation is not available, and the setting must remain off. For Port 7, if the Speed is set to 10000 (10G), Auto Negotiation is not available, and the setting must remain off. If the speed is set to 1000 (1G), Auto negotiation can be set to off (default) or on.

The following command enables auto negotiation for GbE 2:

```
eth type eth [1/2]>autoneg state set on
```

Configuring an Interface’s IFG (CLI)

The IFG attribute represents the physical port Inter-frame gap. Although you can modify the IFG field length, it is strongly recommended not to modify the default value of 12 bytes without a thorough understanding of how the modification will impact traffic.

To configure an Ethernet interface’s IFG, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>ifg set <ifg>
```

Table 158 Interface IFG CLI Parameters

Parameter	Input Type	Permitted Values	Description
ifg	Number	6 - 15	Sets the interface’s IFG (in bytes).

The following command sets the ifg for GbE 1 to 12:

```
eth type eth [1/1]>ifg set 12
```

The following displays the currently configured ifg for GbE 1:

```
eth type eth [1/1]>ifg get
```

Configuring an Interface’s Preamble (CLI)

Although you can modify an Ethernet interface’s preamble, it is strongly recommended not to modify the default value of 8 bytes without a thorough understanding of how the modification will impact traffic.

To configure an Ethernet interface’s preamble, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>preamble set <preamble>
```

Table 159 Interface Preamble CLI Parameters

Parameter	Input Type	Permitted Values	Description
preamble	Number	6 - 15	Sets the interface’s preamble (in bytes).

The following command sets the preamble for GbE 1 to 8:

```
eth type eth [1/1]>preamble set 8
```

The following command displays the current preamble for GbE 1:

```
eth type eth [1/1]>preamble get
```

Adding a Description for the Interface (CLI)

You can add a text description for an interface. To add a description, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>description set <description>
```

To delete a description, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>description delete
```

To display an interface’s description, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>description show
```

Table 160 Interface Description CLI Parameters

Parameter	Input Type	Permitted Values	Description
description	Text String	Up to 40 characters	Adds a text description to the interface.

The following command adds the description “Line” to GbE 1:

```
eth type eth [1/1]>description set Line
```

Configuring Automatic State Propagation and Link Loss Forwarding (CLI)

Automatic state propagation enables propagation of radio failures back to the Ethernet port. You can also configure Automatic State Propagation to close the Ethernet port based on a radio failure at the remote carrier.

Automatic state propagation is configured as pairs of interfaces. Each interface pair includes one Monitored Interface and one Controlled Interface.

Automatic state propagation is configured as pairs of interfaces. Each interface pair includes one Monitored Interface and one Controlled Interface. You can create multiple pairs using the same Monitored Interface and multiple Controlled Interfaces.

The Monitored Interface is a radio interface, a radio protection, or Multi-Carrier ABC group. The Controlled Interface is an Ethernet interface or LAG. An Ethernet interface can only be assigned to one Monitored interface.

Each Controlled Interface is assigned an LLF ID. If **ASP trigger by remote fault** is enabled on the remote side of the link, the ASP state of the Controlled Interface is propagated to the Controlled Interface with the same LLF ID at the remote side of the link. This means if ASP is triggered locally, it is propagated to the remote side of the link, but only to Controlled Interfaces with LLF IDs that match the LLF IDs of the affected Controlled Interfaces on the local side of the link.

Note

LLF requires an activation key. Without this activation key, only LLF ID 1 is available. See Configuring the Activation Key (CLI).

The following events in the Monitored Interface trigger ASP:

- Radio LOF
- Radio Excessive BER
- Radio LOC
- Remote Radio LOF
- Remote Excessive BER
- Remote LOC

The user can also configure the ASP pair so that Radio LOF, Radio Excessive BER, or loss of the Ethernet connection at the remote side of the link will also trigger ASP.

In addition, ASP is triggered if the Controlled Interface is a LAG, and the physical interfaces that belong to the LAG are set to **Admin = Down** in the Interface Manager.

When a triggering event takes place:

- If the Controlled Interface is an electrical GbE port, the port is closed.
- If the Controlled Interface is an optical GbE port, the port is muted.

The Controlled Interface remains closed or muted until all triggering events are cleared.

In addition, when a local triggering event takes place, the ASP mechanism sends an indication to the remote side of the link. Even when no triggering event has taken place, the ASP mechanism sends periodic update messages indicating that no triggering event has taken place.

A trigger delay time can be configured, so that when a triggering event takes place, the ASP mechanism does not propagate the event until this delay time has elapsed. A trigger delay from 0 to 10,000 ms can be set per LLD ID.

Note

It is recommended to configure both ends of the link to the same Automatic State Propagation configuration.

To configure propagation of a radio interface failure to an Ethernet port, use the following command:

```
root> auto-state-propagation add eth-port-to-radio eth-slot 1 eth-port
<eth-port> radio-slot 1 radio-port 1 llf-id <llf-id>
```

To enable automatic state propagation on an Ethernet port, determine whether remote interface failures are also propagated, enable ASP Management Safe (CSF) mode (optional), and set a trigger delay (optional), use the following command:

```
root> auto-state-propagation configure eth-port eth-slot 1 eth-port <eth-
port> asp-admin <asp-admin> remote-fault-trigger-admin <remote-fault-
trigger-admin> csf-mode-admin <csf-mode-admin> trigger-delay <trigger-
delay> llf-id <llf-id>
```

Note

In this command, the llf-id command is used optionally to change the LLF ID of the Ethernet port.

To delete automatic state propagation on an Ethernet port, use the following command:

```
root> auto-state-propagation delete eth-port eth-slot 1 eth-port <eth-
port>
```

To display all automatic state propagation configurations on the unit, use the following command:

```
root> auto-state-propagation show-config all
```

To display the automatic state propagation configuration for a specific Ethernet port, use the following command:

```
root> auto-state-propagation show-config eth-port eth-slot <eth-slot>
eth-port <eth-port>
```

Table 161: Automatic State Propagation to an Ethernet Port CLI Parameters

Parameter	Input Type	Permitted Values	Description
eth-port	Number	PTP 850S: 1-3 PTP 850E: 3-7	The interface to which you want to propagate faults from the selected radio or group.

Parameter	Input Type	Permitted Values	Description
llf-id	Number	1-31	An ID for Link Loss Forwarding (LLF). When **remote-fault-trigger-admin** is set to **enable**, ASP events at the other side of the link are propagated to Controlled Interfaces with LLF IDs that match the LLF IDs of affected Controlled Interfaces at the other side of the link. LLF IDs are unique per Monitored Interface. That is, if LLF ID 1 has been used for a Controlled Interface that is grouped with radio interface 1, that ID cannot be used again for another Controlled Interface grouped with radio interface 1. However, it *can* be used for Controlled Interface grouped with radio interface 2.
asp-admin	Variable	enable disable	Enables or disables automatic state propagation on the Ethernet interface.
remote-fault-trigger-admin	Variable	enable disable	Determines whether faults on the remote radio interface or group are propagated to the local Ethernet interface.
csf-mode-admin	Variable	enable disable	Enables or disables ASP Management Safe (CSF) mode. In ASP Management Safe mode, the ASP mechanism does not physically shut down the Controlled Interface when ASP is triggered. Instead, the ASP mechanism sends a failure indication message. This message is used to propagate the failure indication to external equipment.

Parameter	Input Type	Permitted Values	Description
trigger-delay	Number	0-10000	Sets a trigger delay time, in milliseconds. When a triggering event takes place, the ASP mechanism does not propagate the event until this delay time has elapsed. By default, the trigger-delay is 0 (no delay time). In XPIC configurations, it is recommended to configure a trigger-delay of 100 ms.

The following commands configure and enable automatic state propagation to propagate faults from radio interface 1 to Ethernet ports 1 and 2, and from radio interface 2 to Ethernet port 3. CSF mode is disabled. Faults on the remote carrier are propagated to the local Ethernet ports as follows:

- ○ A failure on the remote side of the link is propagated to any of local Ethernet ports 3 or 4 that share an LLF ID with an Ethernet interface in an ASP pair with the remote radio.
- ○ The trigger delay for Ethernet port 3 is 100 ms. There is no trigger delay for Ethernet port 4.

```
root> auto-state-propagation add eth-port-to-radio eth-slot 1 eth-port 1
radio-slot 2 radio-port 1 llf-id 1

root> auto-state-propagation add eth-port-to-radio eth-slot 1 eth-port 2
radio-slot 2 radio-port 2 llf-id 2

root> auto-state-propagation configure eth-port eth-slot 1 eth-port 1
asp-admin enable remote-fault-trigger-admin enable csf-mode-admin disable
trigger-delay 100

root> auto-state-propagation configure eth-port eth-slot 1 eth-port 2
asp-admin enable remote-fault-trigger-admin enable csf-mode-admin disable
trigger-delay 5000

root> auto-state-propagation add eth-port-to-radio eth-slot 1 eth-port 3
radio-slot 1 radio-port 2 llf-id 1

root> auto-state-propagation configure eth-port eth-slot 1 eth-port 3
asp-admin enable remote-fault-trigger-admin enable csf-mode-admin disable
```

Configuring Receipt of CSF PDUs (CLI)

When ASP Management Safe mode (CSF) is configured, the peer unit must be configured to receive CSF PDUs. To enable the unit to receive CSF PDUs, enter the following command in root view:

```
root> ethernet soam csf receive set admin enable ifc-down
<yes|no>
```

CSF receive must be enabled in order for G.8032 ERPI topology changes to be initiated upon receipt of a CSF PDU.

To disable this setting, enter the following command

```
root> ethernet soam csf receive set admin disable
```

The ifc-down parameter should usually be set to Yes. This means that all network protocols, LAG, and other unit modules will treat the interface on which the CSF PDU was received as Operation Status = Down. Also, a soam-csf-rdi-alarm will be raised to indicate that that relevant port is set to Operational Status = Down due to ASP triggered by the remote unit.

To display the current setting of this parameter, enter the following command:

```
root> ethernet soam csf receive show
```

Viewing Ethernet PMs and Statistics (CLI)

PTP 850 stores and displays statistics in accordance with RMON and RMON2 standards. You can display various peak TX and RX rates (in seconds) and average TX and RX rates (in seconds), both in bytes and in packets, for each measured time interval. You can also display the number of seconds in the interval during which TX and RX rates exceeded the configured threshold.

This section includes:

- Displaying Ethernet Port PMs (CLI)
- Clearing Ethernet Port PMs (CLI)
- Displaying RMON Statistics (CLI)
- Displaying Ethernet Port PMs (CLI)
- Clearing Ethernet Port PMs (CLI)

Displaying RMON Statistics (CLI)

PTP 850E stores and displays statistics in accordance with RMON and RMON2 standards.

To display RMON statistics for a physical interface, go to interface view for the interface and enter the following command:

To display RMON statistics for a physical interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rmon statistics show clear-on-read <clear-on-read>
layer-1 <layer-1>
```

Table 162 RMON Statistics CLI Parameters

Parameter	Input Type	Permitted Values	Description
clear-on-read	Boolean	yes no	If you enter yes, the statistics are cleared once you display them.
layer-1	Boolean	yes no	yes – Statistics are represented as Layer 1 statistics, including preamble and IFG. no – Statistics are represented as Layer 2 statistics.

The following commands bring you to interface view for Ethernet port 1, and clears the statistics after displaying them.

```
root> ethernet interfaces eth slot 1 port 1

eth type eth [1/1]>rmon statistics show clear-on-read yes layer-1 yes
```

The following commands bring you to interface view for radio interface 2, without clearing the statistics.

```
root> ethernet interfaces radio slot 2 port 1
eth type radio[2/2]>rmon statistics show clear-on-read no layer-1 no
```

Configuring Ethernet Port PMs and PM Thresholds (CLI)

To enable the gathering of PMs for an Ethernet interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm set admin <enable|disable>
```

You can configure thresholds and display the number of seconds these thresholds were exceeded during a specified interval.

To configure interface PM thresholds, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm set thresholds rx-layer1-rate-threshold <0-
4294967295> tx-layer1-rate-threshold <0-4294967295>
```

To display whether or not PM gathering is enabled for an Ethernet interface, as well as the configured thresholds, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show configuration
```

Table 163 Port PM Thresholds CLI Parameters

Parameter	Input Type	Permitted Values	Description
rx-layer1-rate-thershold	Number	0-4294967295	The exceed threshold for port RX PMs, in bytes per second.
tx-layer1-rate-thershold	Number	0-4294967295	The exceed threshold for port TX PMs, in bytes per second.

The following commands bring you to interface view for Ethernet port 1, enable PM gathering, and set the thresholds for RX and TX PMs at 850,000,000 bytes per second:

```
root> ethernet interfaces eth slot 1 port 1
eth type eth [1/1]>pm set admin enable
eth type eth [1/1]>pm set thresholds rx-layer1-rate-threshold 850000000
tx-layer1-rate-threshold 850000000
```

Displaying Ethernet Port PMs (CLI)

Note

The port PM results may be several pages long. Remember:
To view the next results page, press the space bar.
To end the list and return to the most recent prompt, press the letter q.

To display RX packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-packets interval 15min
```

To display RX packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-packets interval 24hr
```

To display RX broadcast packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bcast-packets interval 15min
```

To display RX broadcast packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bcast-packets interval 24hr
```

To display RX multicast packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-mcast-packets interval 15min
```

To display RX multicast packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-mcast-packets interval 24hr
```

To display Layer 1 RX PMs, in bytes per second, in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bytes-layer1 interval 15min
```

To display Layer 1 RX PMs, in bytes per second, in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bytes-layer1 interval 24hr
```

To display Layer 2 RX PMs, in bytes per second, in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bytes-layer2 interval 15min
```

To display Layer 2 RX PMs, in bytes per second, in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bytes-layer2 interval 24hr
```

To display TX packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-packets interval 15min
```

To display TX packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-packets interval 24hr
```

To display TX broadcast packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bcast-packets interval 15min
```

To display TX broadcast packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bcast-packets interval 24hr
```

To display TX multicast packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-mcast-packets interval 15min
```

To display TX multicast packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-mcast-packets interval 24hr
```

To display Layer 1 TX PMs, in bytes per second, in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bytes-layer1 interval 15min
```

To display Layer 1 TX PMs, in bytes per second, in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bytes-layer1 interval 24hr
```

To display Layer 2 TX PMs, in bytes per second, in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bytes-layer2 interval 15min
```

To display Layer 2 TX PMs, in bytes per second, in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bytes-layer2 interval 24hr
```

Table 164 Ethernet Port PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Invalid data flag	Indicates whether the values received during the measured interval are valid. An x in the column indicates that the values are not valid (for example, because of a power surge or power failure that occurred during the interval).
Peak RX Packets	The peak rate of RX packets per second for the measured time interval.
Average RX Packets	The average rate of RX packets per second for the measured time interval.
Peak RX Broadcast Packets	The peak rate of RX broadcast packets per second for the measured time interval.
Average RX Broadcast Packets	The average rate of RX broadcast packets per second for the measured time interval.

Parameter	Definition
Peak RX Multicast Packets	The peak rate of RX multicast packets per second for the measured time interval.
Average RX Multicast Packets	The average rate of RX multicast packets per second for the measured time interval.
Peak RX Bytes in Layer1	The peak RX rate, in bytes per second, for the measured time interval (including preamble and IFG).
Average RX Bytes in Layer1	The average RX rate, in bytes per second, for the measured time interval (including preamble and IFG).
RX Bytes Layer1 Exceed Threshold (sec)	The number of seconds during the measured time interval that the RX rate exceeded the configured threshold.
Peak RX Bytes in Layer2	The peak RX rate, in bytes per second, for the measured time interval (excluding preamble and IFG).
Average RX Bytes in Layer2	The average RX rate, in bytes per second, for the measured time interval (excluding preamble and IFG).
Peak TX Packets	The peak rate of TX packets per second for the measured time interval.
Average TX Packets	The average rate of TX packets per second for the measured time interval.
Peak TX Broadcast Packets	The peak rate of TX broadcast packets per second for the measured time interval.
Average TX Broadcast Packets	The average rate of TX broadcast packets per second for the measured time interval.
Peak TX Multicast Packets	The peak rate of TX multicast packets per second for the measured time interval.
Average TX Multicast Packets	The average rate of TX multicast packets per second for the measured time interval.
Peak TX Bytes in Layer1	The peak TX rate, in bytes per second, for the measured time interval (including preamble and IFG).
Average TX Bytes in Layer1	The average TX rate, in bytes per second, for the measured time interval (including preamble and IFG).
TX Bytes Layer1 Exceed Threshold (sec)	The number of seconds during the measured time interval that the TX rate exceeded the configured threshold.
Peak TX Bytes in Layer2	The peak TX rate, in bytes per second, for the measured time interval (excluding preamble and IFG).
Average TX Bytes in Layer2	The average TX rate, in bytes per second, for the measured time interval (excluding preamble and IFG).

Clearing Ethernet Port PMs (CLI)

To clear all PMs for an Ethernet interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm clear-all
```

Chapter 21: Quality of Service (QoS) (CLI)

This section includes:

- Configuring Classification (CLI)
- Configuring Policers (Rate Metering) (CLI)
- Configuring Marking (CLI)
- Configuring WRED (CLI)
- Configuring Shapers (CLI)
- Configuring Scheduling (CLI)
- Displaying Ingress Statistics (CLI)
- Displaying Ingress Statistics (CLI)

Configuring Classification (CLI)

This section includes:

- Classification Overview (CLI)
- Configuring Ingress Path Classification on a Logical Interface (CLI)
- Configuring VLAN Classification and Override (CLI)
-
- Configuring DSCP Classification (CLI)
- Configuring MPLS Classification (CLI)
- Configuring Ingress Path Classification on a Service Point (CLI)
- Configuring Ingress Path Classification on a Service (CLI)

Classification Overview (CLI)

PTP 850 supports a hierarchical classification mechanism. The classification mechanism examines incoming frames and determines their CoS and Color. The benefit of hierarchical classification is that it provides the ability to “zoom in” or “zoom out”, enabling classification at higher or lower levels of the hierarchy. The nature of each traffic stream defines which level of the hierarchical classifier to apply, or whether to use several levels of the classification hierarchy in parallel.

The hierarchical classifier consists of the following levels:

Logical interface-level classification

Service point-level classification

Service level classification

Configuring Ingress Path Classification on a Logical Interface (CLI)

Logical interface-level classification enables you to configure classification on a single interface or on a number of interfaces grouped tougher, such as a LAG group.

The classifier at the logical interface level supports the following classification methods, listed from highest to lowest priority. A higher level classification method supersedes a lower level classification method:

- VLAN ID
- MPLS EXP field
- DSCP bits (only considered if MPLS is not present, regardless of trust setting)
- 802.1p bits
- Default CoS

PTP 850 performs the classification on each frame ingressing the system via the logical interface. Classification is performed step by step from the highest priority to the lowest priority classification method. Once a match is found, the classifier determines the CoS and Color decision for the frame for the logical interface-level.

You can disable some of these classification methods by configuring them as un-trusted. For example, if MPLS classification is configured as un-trusted for a specific interface, the classification mechanism does not perform classification according to the MPLS EXP bits. This is useful, for example, if classification is based on 802.1p bits.

If no match is found at the logical interface level, the default CoS is applied to incoming frames at this level. In this case, the Color of the frame is assumed to be Green.

Configuring VLAN Classification and Override (CLI)

You can specify a specific CoS and Color for a specific VLAN ID. In the case of double-tagged frames, the match must be with the frame's outer VLAN. Permitted values are CoS 0 to 7 and Color Green or Yellow per VLAN ID. This is the highest classification priority on the logical interface level, and overrides any other classification criteria at the logical interface level.

To configure CoS and Color override based on VLAN ID, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>vlan-cos-override set outer-vlan-id <outer-vlan-id>
inner-vlan-id <inner-vlan-id> use-cos <use-cos> use-color <use-color>
```

To display configured VLAN-based CoS and Color override values, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>vlan-cos-override show outer-vlan-id <outer-vlan-id>
inner-vlan-id <inner-vlan-id>
```

To delete a set of VLAN-based CoS and Color override values, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>vlan-cos-override delete outer-vlan-id <outer-vlan-id>
inner-vlan-id <inner-vlan-id>
```

Table 165 VLAN Classification and Override CLI Parameters

Parameter	Input Type	Permitted Values	Description
outer-vlan-id	Number	1 – 4094	For double-tagged frames, the S-VLAN value mapped to the CoS and Color values defined in the command. For single-tagged frames, the VLAN value mapped to the CoS and Color values defined in the command.
inner-vlan-id	Number	1 – 4094	Optional. Include this parameter when you want to map double-tagged frames to specific CoS and Color values. When this parameter is included in the command, both the S-VLAN and the C-VLAN IDs must match the configured `outer-vlan-id` and `inner-vlan-id` values, respectively, in order for the defined CoS and Color values to be applied to the frame.

Parameter	Input Type	Permitted Values	Description
use-cos	Number	0 – 7	The CoS value applied to matching frames.
use-color	Variable	green yellow	The Color applied to matching frames.

The following command configures the classification mechanism on GbE 1 to override the CoS and Color values of frames with S-VLAN ID 10 and C-VLAN ID 30 with a CoS value of 6 and a Color value of Green:

```
eth type eth [1/1]>vlan-cos-override set outer-vlan-id 10 inner-vlan-id 30
use-cos 6 use-color green
```

The following command configures the classification mechanism on GbE 2 to override the CoS and Color values of frames with VLAN ID 20 with a CoS value of 5 and a Color value of Green:

```
eth type eth [1/2]>vlan-cos-override set outer-vlan-id 20 use-cos 5 use-
color green
```

The following command displays the CoS and Color override values for frames that ingress on GbE 1, with S-VLAN ID 10 and C-VLAN ID 20:

```
eth type eth [1/1]>vlan-cos-override show outer-vlan-id 10 inner-vlan-id 20
```

The following command displays all CoS and Color override values for frames that ingress on GbE 2:

```
eth type eth [1/2]>vlan-cos-override show all
```

The following command deletes the VLAN to CoS and Color override mapping for frames that ingress on GbE 1, with S-VLAN ID 10 and C-VLAN ID 20:

```
eth type eth [1/1]>vlan-cos-override delete outer-vlan-id 10 inner-vlan-id
20
```

Configuring DSCP Classification (CLI)

When DSCP classification is set to Trust mode, the interface performs QoS and Color classification according to a user-configurable DSCP to CoS and Color classification table. 802.1p classification has priority over DSCP Trust Mode, so that if a match is found on the 802.1p level, DSCP is not considered.

This section includes:

- Configuring Trust Mode for DSCP Classification (CLI)
- Modifying the DSCP Classification Table (CLI)

Configuring Trust Mode for DSCP Classification (CLI)

To define the trust mode for DSCP classification, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>classification set ip-dscp <ip-dscp>
```

To display the trust mode for DSCP classification, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>classification show 802.1p state
```

Table 166 Trust Mode for DSCP CLI Parameters

Parameter	Input Type	Permitted Values	Description
ip-dscp	Variable	trust un-trust	Select the interface's trust mode for DSCP classification: `trust` – The interface performs QoS and color classification according to a user-configurable table for DSCP to CoS and color classification. DSCP classification has priority over MPLS classification, so that if a match is found with the DSCP value of the ingressing frame, MPLS bits are not considered. `un-trust` – The interface does not consider DSCP during classification.

The following command enables DSCP trust mode for GbE 1:

```
eth type eth [1/1]>classification set ip-dscp trust
```

The following command disables DSCP trust mode for GbE 1:

```
eth type eth [1/1]>classification set ip-dscp un-trust
```

Modifying the DSCP Classification Table (CLI)

PTP 850 units have a DSCP classification table with 24 pre-defined entries. Each entry includes the following criteria:

- **DSCP** – The DSCP value to be mapped.
- **Binary** – The binary representation of the DSCP value.
- **Description** – A description of the DSCP value.
- **CoS** – The CoS assigned to frames with the designated DSCP value.
- **Color** – The Color assigned to frames with the designated DSCP value.

You can modify the Description, CoS, and Color for any of the pre-defined entries. You can also add and delete entries. The maximum number of entries is:

- PTP 850C and PTP 850E: 64.
- PTP 850S: 32

The following table shows the default values for the DSCP classification table.

Table 167 DSCP Classification Table Default Values

DSCP	DSCP (bin)	Description	CoS (Configurable)	Color (Configurable)
0 (default)	000000	BE (CS0)	0	Green
10	001010	AF11	1	Green
12	001100	AF12	1	Yellow
14	001110	AF13	1	Yellow
18	010010	AF21	2	Green
20	010100	AF22	2	Yellow
22	010110	AF23	2	Yellow

DSCP	DSCP (bin)	Description	CoS (Configurable)	Color (Configurable)
26	011010	AF31	3	Green
28	011100	AF32	3	Yellow
30	011110	AF33	3	Yellow
34	100010	AF41	4	Green
36	100100	AF42	4	Yellow
38	100110	AF43	4	Yellow
46	101110	EF	7	Green
8	001000	CS1	1	Green
16	010000	CS2	2	Green
24	011000	CS3	3	Green
32	100000	CS4	4	Green
40	101000	CS5	5	Green
48	110000	CS6	6	Green
56	111000	CS7	7	Green
51	110011	DSCP_51	6	Green
52	110100	DSCP_52	6	Green
54	110110	DSCP_54	6	Green
56	111000	CS7	7	Green

To modify the DSCP classification table, enter the following command:

```
root> ethernet qos dscp-mapping-tbl set dscp <dscp> cos <cos> color <color>
```

To display the DSCP classification table, enter the following command:

```
root> ethernet qos dscp-mapping-tbl show
```

Table 168 Modify DSCP Classification Table CLI Parameters

Parameter	Input Type	Permitted Values	Description
dscp	Number	0-63	The DSCP value to be mapped.
cos	Number	0 – 7	The CoS assigned to frames with the designated DSCP value.
color	Variable	green yellow	The Color assigned to frames with the designated DSCP value.

Example

The following command maps frames with DSCP value of 10 to CoS 1 and Green color:

```
root> ethernet qos dscp-mapping-tbl set dscp 10 cos 1 color green
```

Configuring MPLS Classification (CLI)

When MPLS classification is set to Trust mode, the interface performs QoS and Color classification according to a user-configurable MPLS EXP bit to CoS and Color classification table. Both 802.1p and DSCP classification have priority over MPLS Trust Mode, so that if a match is found on either the 802.1p or DSCP levels, MPLS bits are not considered.

This section includes:

- Configuring Trust Mode for MPLS Classification (CLI)
- Modifying the MPLS EXP Bit Classification Table (CLI)

Configuring Trust Mode for MPLS Classification (CLI)

To define the trust mode for MPLS classification, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>classification set mpls <mpls>
```

Note

For PTP 850C and PTP 850E, if you change the trust mode for MPLS, the trust mode for DSCP is automatically changed to the same setting.

To display the trust mode for MPLS classification, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>classification show mpls state
```

Table 169 Trust Mode for MPLS CLI Parameters

Parameter	Input Type	Permitted Values	Description
mpls	Variable	Trust un-trust	Select the interface's trust mode for MPLS bits: `trust` – The interface performs QoS and color classification according to a user-configurable table for MPLS EXP to CoS and color classification. `un-trust` – The interface does not consider MPLS bits during classification.

The following command enables MPLS trust mode for GbE 1:

```
eth type eth [1/1]>classification set mpls trust
```

The following command disables MPLS trust mode for GbE 1:

```
eth type eth [1/1]>classification set mpls un-trust
```

Modifying the MPLS EXP Bit Classification Table (CLI)

The following table shows the default values for the MPLS EXP bit classification table.

Table 170 MPLS EXP Bit Classification Table Default Values

MPLS EXP bits	CoS (Configurable)	Color (Configurable)
0	0	Yellow
1	1	Green
2	2	Yellow
3	3	Green
4	4	Yellow
5	5	Green
6	6	Green
7	7	Green

To modify the MPLS EXP bit classification table, enter the following command:

```
root> ethernet qos mpls-exp-bits-mapping-tbl set mpls-exp <mpls-exp> cos
<cos> color <color>
```

To display the MPLS EXP bit classification table, enter the following command:

```
root> ethernet qos mpls-mapping-tbl show
```

Table 171 MPLS EXP Bit Classification Table Modification CLI Parameters

Parameter	Input Type	Permitted Values	Description
mpls-exp	Number	0 – 7	The MPLS EXP bit to be mapped.
cos	Number	0 – 7	The CoS assigned to frames with the designated MPLS EXP bit value.
color	Variable	green yellow	The Color assigned to frames with the designated MPLS EXP bit value.

The following command maps frames with MPLS EXP bit value of 4 to CoS 4 and Yellow color:

```
root> ethernet qos mpls-exp-bits-mapping-tbl set mpls-exp 4 cos 4 color
yellow
```

Configuring 802.1p Classification (CLI)

When 802.1p classification is set to Trust mode, the interface performs QoS and Color classification according to user-configurable tables for 802.1q UP bit (C-VLAN frames) or 802.1AD UP bit (S-VLAN frames) to CoS and Color classification.

This section includes:

- Configuring Trust Mode for 802.1p Classification (CLI)
- Modifying the C-VLAN 802.1 UP and CFI Bit Classification Table (CLI)
- Modifying the S-VLAN 802.1 UP and DEI Bit Classification Table (CLI)

Configuring Trust Mode for 802.1p Classification (CLI)

To define the trust mode for 802.1p classification, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>classification set 802.1p <802.1p>
```

To display the trust mode for 802.1p classification, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>classification show 802.1p state
```

Table 172: 802.1p Trust Mode CLI Parameters

Parameter	Input Type	Permitted Values	Description
802.1p	Variable	trust un-trust	Enter the interface's trust mode for user priority (UP) bits: • **trust** – The interface performs QoS and color classification according to UP and CFI/DEI bits according to user-configurable tables for 802.1q UP bits (C-VLAN frames) or 802.1AD UP bits (S-VLAN frames). MPLS and DSCP classification have priority over 802.1p classification, so that if a match is found on the MPLS or DSCP level, 802.1p bits are not considered. • **un-trust** – The interface does not consider 802.1 UP bits during classification.

The following command enables 802.1p trust mode for Eth 7:

```
eth type eth [1/7]>classification set 802.1p trust
```

The following command disables 802.1p trust mode for GbE 1:

```
eth type eth [1/7]>classification set 802.1p un-trust
```

Modifying the C-VLAN 802.1 UP and CFI Bit Classification Table (CLI)

The following table shows the default values for the C-VLAN 802.1 UP and CFI bit classification table.

Table 173: C-VLAN 802.1 UP and CFI Bit Classification Table Default Values

802.1 UP	CFI	CoS (configurable)	Color (configurable)
0	0	0	Green
0	1	0	Yellow
1	0	1	Green
1	1	1	Yellow
2	0	2	Green
2	1	2	Yellow
3	0	3	Green
3	1	3	Yellow
4	0	4	Green
4	1	4	Yellow
5	0	5	Green
5	1	5	Yellow
6	0	6	Green
6	1	6	Yellow
7	0	7	Green
7	1	7	Yellow

To modify the C-VLAN 802.1 UP and CFI bit classification table, enter the following command:

```
root> ethernet qos 802.1q-up-bits-mapping-tbl set 802.1p <802.1p> cfi <cfi>
cos <cos> color <color>
```

To display the C-VLAN 802.1 UP and CFI bit classification table, enter the following command:

```
root> ethernet qos 802.1q-up-bits-mapping-tbl show
```

Table 174: C-VLAN 802.1 UP and CFI Bit Classification Table CLI Parameters

Parameter	Input Type	Permitted Values	Description
802.1p	Number	0 – 7	The User Priority (UP) bit to be mapped.
cfi	Number	0 – 1	The CFI bit to be mapped.
cos	Number	0 – 7	The CoS assigned to frames with the designated UP and CFI.
color	Variable	Green yellow	The Color assigned to frames with the designated UP and CFI.

The following command maps frames with an 802.1p UP bit value of 1 and a CFI bit value of 0 to CoS 1 and Green color:

```
root> ethernet qos 802.1q-up-bits-mapping-tbl set 802.1p 1 cfi 0 cos 1
color green
```

Modifying the S-VLAN 802.1 UP and DEI Bit Classification Table (CLI)

The following table shows the default values for the S-VLAN 802.1 UP and DEI bit classification table.

Table 175: S-VLAN 802.1 UP and DEI Bit Classification Table Default Values

802.1 UP	DEI	CoS (Configurable)	Color (Configurable)
0	0	0	Green
0	1	0	Yellow
1	0	1	Green
1	1	1	Yellow
2	0	2	Green
2	1	2	Yellow
3	0	3	Green
3	1	3	Yellow
4	0	4	Green
4	1	4	Yellow
5	0	5	Green
5	1	5	Yellow
6	0	6	Green
6	1	6	Yellow
7	0	7	Green
7	1	7	Yellow

To modify the S-VLAN 802.1 UP and DEI bit classification table, enter the following command:

```
root> ethernet qos 802.1ad-up-bits-mapping-tbl set 802.1p <802.1p> dei
<dei> cos <cos> color <color>
```

To display the S-VLAN 802.1 UP and CFI bit classification table, enter the following command:

```
root> ethernet qos 802.1ad-up-bits-mapping-tbl show
```

Table 176: S-VLAN 802.1 UP and DEI Bit Classification Table CLI Parameters

Parameter	Input Type	Permitted Values	Description
802.1p	Number	0 – 7	The User Priority (UP) bit to be mapped.
dei	Number	0 - 1	The DEI bit to be mapped.
cos	Number	0 – 7	The CoS assigned to frames with the designated UP and CFI.

Parameter	Input Type	Permitted Values	Description
color	Variable	green yellow	The Color assigned to frames with the designated UP and CFI.

The following command maps frames with an 802.1ad UP bit value of 7 and a DEI bit value of 0 to CoS 7 and Green color:

```
root> ethernet qos 802.1ad-up-bits-mapping-tbl set 802.1p 7 dei 0 cos 7
color green
```

Configuring MAC DA Classification (CLI)

Note: This section is only relevant for PTP 850S.

You can determine whether classification is performed by MAC DA in the service point's **CoS Mode** parameter. See *Classification Overview*.

To add an entry to the MAC DA classification table, enter the following command in root view:

```
root>ethernet generalcfg mac-da add mac <MAC address> color
<green|yellow>
```

To edit an entry to the MAC DA classification table, enter the following command in root view:

```
root>ethernet generalcfg mac-da edit mac <MAC address> color
<green|yellow>
```

To delete an entry to the MAC DA classification table, enter the following command in root view:

```
root>ethernet generalcfg mac-da delete mac <MAC address>
```

The following command adds MAC address 00:11:22:33:44:55 to the MAC DA classification table, with a CoS of 7 and the Color green.

```
root>ethernet generalcfg mac-da add mac 00:11:22:33:44:55 cos 7
color green
```

The following command changes the CoS assigned to this MAC address to 6.

```
root>ethernet generalcfg mac-da edit mac 00:11:22:33:44:55 cos
6 color green
```

The following command deletes this MAC address.

```
root>ethernet generalcfg mac-da delete mac 00:11:22:33:44:55
```

Configuring a Default CoS (CLI)

You can define a default CoS value for frames passing through the interface. This value can be overwritten on the service point and service level. The Color is assumed to be Green.

To define a default CoS value for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>classification set default-cos <default-cos>
```

To display the default CoS value for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>classification show default-cos
```

Table 177 Default CoS CLI Parameters

Parameter	Input Type	Permitted Values	Description
default-cos	Number	0 – 7	Enter the default CoS value for frames passing through the interface. This value can be overwritten on the service point and service level.

The following command sets the default CoS for GbE 1 as 7:

```
eth type eth [1/1]>classification set default-cos 7
```

Configuring Ingress Path Classification on a Service Point (CLI)

For instruction on configuring ingress path classification on a service point, see CoS Preservation and Modification on a Service Point (CLI).

Configuring Ingress Path Classification on a Service (CLI)

For instruction on configuring ingress path classification on a service, see Configuring a Service's CoS Mode and Default CoS (CLI).

Configuring Policers (Rate Metering) (CLI)

This section includes:

- Overview of Rate Metering (Policing) (CLI)
- Configuring Rate Meter (Policer) Profiles (CLI)
- Displaying Rate Meter Profiles (CLI)
- Deleting a Rate Meter Profile (CLI)
- Attaching a Rate Meter (Policer) to an Interface (CLI)
- Attaching a Rate Meter (Policer) to a Service Point and CoS (CLI)

To assign a rate meter (policer) profile to a service point, go to service view for the service and enter the following commands:

```
service[x]>sp rate-meter add capability spid <spid>
service[x]>sp rate-meter edit spid <spid> admin-state <admin-
state> profile-id <profile-id>
```

To change the rate meter (policer) profile for a service point, go to service view for the service and enter the following command:

```
service[x]>sp rate-meter edit spid <spid> admin-state <admin-
state> profile-id <profile-id>
```

To display the current rate meter (policer) profile for a service point, go to service view for the service and enter the following command:

```
service[x]>sp rate-meter show configuration spid <spid>
```

To assign a rate meter (policer) profile to a service point and CoS, go to service view for the service and enter the following commands:

```
service[x]>sp rate-meter add capability spid <spid>

service[x]>sp rate-meter edit spid <spid> cos <cos> admin-state
<admin-state> profile-id <profile-id>
```

To change the rate meter (policer) profile for a service point and CoS, go to service view for the service and enter the following command:

```
service[x]>sp rate-meter edit spid <spid> cos <cos> admin-state
<admin-state> profile-id <profile-id>
```

To display the current rate meter (policer) profile for a service point and CoS, go to service view for the service and enter the following command:

```
service[x]>sp rate-meter show configuration spid <spid> cos
<cos>
```

To delete the rate meter (policer) profile for a service point or service point/CoS combination, go to service view for the service and enter the following command:

```
service[x]>sp rate-meter delete spid <spid>
```

Table 202: Assigning Rate Meter for Service Point and Service Point/CoS CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
admin-state	Variable	enable disable	Enables or disables rate metering on unicast traffic flows from the logical interface.
profile-id	Number	1 – 250	Select from the rate meter profiles defined in the
cos	Number	0 – 7	The CoS value to which you are assigning the rate meter.

The following commands assign Rate Meter Profile 2 to service point 10 on service 5:

```
root> ethernet service sid 5

service[5]> sp rate-meter add capability spid 10

service[5]>sp rate-meter edit spid 10 admin-state enable
profile-id 2
```

The following commands assign Rate Meter Profile 4 to service point 10 and CoS 6 on service 5:

```
root> ethernet service sid 5

service[5]> sp rate-meter add capability spid 10

service[5]>sp rate-meter edit spid 10 cos 6 admin-state enable
profile-id 4
```

- Configuring the Line Compensation Value for a Rate Meter (Policer) (CLI)

Overview of Rate Metering (Policing) (CLI)

The PTP 850 switching fabric supports hierarchical policing on the logical interface level. You can define up to 250 rate meter (policer) profiles.

Note

Policing on the service point level, and the service point and CoS level, is planned for future release.

The PTP 850's policer mechanism is based on a dual leaky bucket mechanism (TrTCM). The policers can change a frame’s color and CoS settings based on CIR/EIR + CBS/EBS, which makes the policer mechanism a key tool for implementing bandwidth profiles and enabling operators to meet strict SLA requirements.

The output of the policers is a suggested color for the inspected frame. Based on this color, the queue management mechanism decides whether to drop the frame or to pass it to the queue.

Configuring Rate Meter (Policer) Profiles (CLI)

To add a rate meter (policer) profile, enter the following command:

```
root> ethernet qos rate-meter add profile-id <profile-id> cir <cir> cbs
<cbs> eir <eir> ebs <ebs> color-mode <color-mode> coupling-flag <coupling-
flag> rate-meter-profile-name <rate-meter-profile-name>
```

To edit an existing rate meter (policer) profile, enter the following command:

```
root> ethernet qos rate-meter edit profile-id <profile-id> cir <cir> cbs
<cbs> eir <eir> ebs <ebs> color-mode <color-mode> coupling-flag <coupling-
flag> rate-meter-profile-name <rate-meter-profile-name>
```

Table 178 Rate Meter Profile CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 – 250	A unique ID for the rate meter (policer) profile.
cir	Number	0, or 64,000 - 1,000,000,000	The Committed Information Rate (CIR) defined for the rate meter (policer), in bits per second. If the value is 0, all incoming CIR traffic is dropped.
cbs	Number	0 - 4096	The Committed Burst Rate (CBR) for the rate meter (policer), in Kbytes.
eir	Number	0, or 64,000 - 1,000,000,000	The Excess Information Rate (EIR) for the rate meter (policer), in bits per second. If the value is 0, all incoming EIR traffic is dropped.
ebs	Number	0 - 4096	The Excess Burst Rate (EBR) for the rate meter (policer), in Kbytes.
color-mode	Variable	color-blind color-aware	Determines how the rate meter (policer) treats frames that ingress with a CFI or DEI field set to 1 (yellow). Options are: `color aware` – All frames that ingress with a CFI/DEI field set to 1 (yellow) are treated as EIR frames, even if credits remain in the CIR bucket. `color blind` – All ingress frames are treated as green regardless of their CFI/DEI value. A color-blind policer discards any former color decisions.
coupling-flag	Variable	enable disable	When enabled, frames that ingress as yellow may be converted to green when there are no available yellow credits in the EIR bucket. Only relevant in `color-aware` mode.
rate-meter-profile-name	Text string	Up to 20 characters.	A description of the rate meter (policer) profile.

The following command creates a rate meter (policer) profile with Profile ID 50, named “64k.”

```
root> ethernet qos rate-meter add profile-id 50 cir 64000 cbs 5 eir 64000
ebs 5 color-mode color-blind coupling-flag disable rate-meter-profile-name
64k
```

This profile includes the following parameters:

- CIR – 64,000 bps
- CBS – 5 Kbytes
- CBS – 5 Kbytes
- EIR – 64,000 bps
- EBS – 5 Kbytes
- Color Blind mode
- Coupling Flag disabled

The following command edits the rate meter (policer) profile with Profile ID 50, and changes its name to “256 kBytes.”

```
root> ethernet qos rate-meter edit profile-id 50 cir 128000 cbs 5 eir
128000 ebs 5 color-mode color-aware coupling-flag enable rate-meter-
profile-name 256 kBytes
```

This edited profile includes the following parameters:

- CIR – 128,000 bps
- CBS – 5 Kbytes
- EIR – 128,000 bps
- EBS – 5 Kbytes
- Color Aware mode
- Coupling Flag enabled

Displaying Rate Meter Profiles (CLI)

You can display all configured rate meter (policer) profiles or a specific profile.

To display a specific profile, enter the following command:

```
root> ethernet qos rate-meter show profile-id <profile-id>
```

To display all configured profiles, enter the following command:

```
root> ethernet qos rate-meter show profile-id all
```

The following command displays the parameters of Rate Meter Profile 50:

```
root> ethernet qos rate-meter show profile-id 50
```

Deleting a Rate Meter Profile (CLI)

You cannot delete a rate meter (policer) profile that is attached to a logical interface. You must first remove the profile from the logical interface, then delete the profile.

To delete a rate meter (policer) profile, use the following command:

```
root> ethernet qos rate-meter delete profile-id <profile-id>
```

The following command deletes Rate Meter Profile 50:

```
root> ethernet qos rate-meter delete profile-id 50
```

Attaching a Rate Meter (Policer) to an Interface (CLI)

On the logical interface level, you can assign rate meter (policer) profiles as follows:

Per frame type (unicast, multicast, and broadcast)

Per frame ethertype

This section includes:

- Assigning a Rate Meter (Policer) for Unicast Traffic (CLI)
- Assigning a Rate Meter (Policer) for Unknown Multicast Traffic (CLI)
- Assigning a Rate Meter (Policer) per Ethertype (CLI)

Assigning a Rate Meter (Policer) for Unicast Traffic (CLI)

To assign a rate meter (policer) profile for unicast traffic to the interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter unicast add capability admin-state <admin-
state> profile-id <profile-id>
```

To change the rate meter (policer) profile for unicast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter unicast edit admin-state <admin-state>
profile-id <profile-id>
```

To display the current unicast rate meter (policer) profile for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter unicast show configuration
```

To delete the rate meter (policer) profile for unicast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter unicast delete
```

Table 179 Assigning Rate Meter for Unicast Traffic CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin-state	Variable	enable disable	Enables or disables rate metering on unicast traffic flows from the logical interface.
profile-id	Number	1 – 250	Select from the rate meter profiles defined in the system.

The following command assigns Rate Meter Profile 1 to unicast traffic on GbE 1, and enables rate metering on the port:

```
eth type eth [1/1]>rate-meter unicast add capability admin-state enable
profile-id 1
```

The following command changes the rate meter (policer) profile for unicast traffic on GbE 1 to 4:

```
eth type eth [1/1]>rate-meter unicast edit admin-state enable profile-id 4
```

Assigning a Rate Meter (Policer) for Unknown Unicast Traffic (CLI)

Unknown unicast packets are unicast packets with unknown destination MAC addresses To assign a rate meter (policer) profile for unknown unicast traffic to the interface, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>rate-meter unknown-unicast add capability admin-state
<admin-state> profile-id <profile-id>
```

To change the rate meter (policer) profile for unicast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>rate-meter unknown-unicast edit admin-state <admin-
state> profile-id <profile-id>
```

To display the current unicast rate meter (policer) profile for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>rate-meter unknown-unicast show configuration
```

To delete the rate meter (policer) profile for unicast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>rate-meter unknown-unicast delete
```

Table 180: Assigning Rate Meter for Unknown Unicast Traffic CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin-state	Variable	enable disable	Enables or disables rate metering on unknown unicast traffic flows from the logical interface.
profile-id	Number	1 – 250	Select from the rate meter profiles defined in the system.

The following command assigns Rate Meter Profile 1 to unknown unicast traffic on Eth 7, and enables rate metering on the port:

```
eth type eth [1/7]>rate-meter unknown-unicast add capability admin-state
enable profile-id 1
```

The following command changes the rate meter (policer) profile for unknown unicast traffic on Eth 7 to 4:

```
eth type eth [1/7]>rate-meter unknown-unicast edit admin-state enable
profile-id 4
```

Assigning a Rate Meter (Policer) for Multicast Traffic (CLI)

To assign a rate meter (policer) profile for multicast traffic to the interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter multicast add capability admin-state <admin-
state> profile-id <profile-id>
```

To change the rate meter (policer) profile for multicast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter multicast edit admin-state <admin-state>
profile-id <profile-id>
```

To display the current multicast rate meter (policer) profile for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter multicast show configuration
```

To delete the rate meter (policer) profile for multicast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter multicast delete
```

Table 181 Assigning Rate Meter for Multicast Traffic CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin-state	Variable	enable disable	Enables or disables rate metering on multicast traffic flows from the logical interface.
profile-id	Number	1 – 250	Select from the rate meter profiles defined in the system.

The following command assigns Rate Meter Profile 1 to multicast traffic on GbE 1, and enables rate metering on the port.

```
eth type eth [1/1]>rate-meter multicast add capability admin-state enable
profile-id 1
```

The following command changes the rate meter (policer) profile for multicast traffic on GbE 1 to 4:

```
eth type eth [1/1]>rate-meter multicast edit admin-state enable profile-id
4
```

Assigning a Rate Meter (Policer) for Unknown Multicast Traffic (CLI)

Unknown multicast packets are multicast packets with unknown destination MAC addresses. To assign a rate meter (policer) profile for unknown multicast traffic to the interface, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>rate-meter unknown-multicast add capability admin-state
<admin-state> profile-id <profile-id>
```

To change the rate meter (policer) profile for multicast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>rate-meter unknown-multicast edit admin-state <admin-
state> profile-id <profile-id>
```

To display the current multicast rate meter (policer) profile for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>rate-meter unknown-multicast show configuration
```

To delete the rate meter (policer) profile for multicast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]>rate-meter unknown-multicast delete
```

Table 182: Assigning Rate Meter for Multicast Traffic CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin-state	Variable	enable disable	Enables or disables rate metering on unknown multicast traffic flows from the logical interface.
profile-id	Number	1 – 250	Select from the rate meter profiles defined in the system.

The following command assigns Rate Meter Profile 1 to unknown multicast traffic on Eth 7, and enables rate metering on the port.

```
eth type eth [1/7]>rate-meter unknown-multicast add capability admin-state
enable profile-id 1
```

The following command changes the rate meter (policer) profile for unknown multicast traffic on Eth 7 to 4:

```
eth type eth [1/7]>rate-meter unknown-multicast edit admin-state enable
profile-id 4
```

Assigning a Rate Meter (Policer) for Broadcast Traffic (CLI)

To assign a rate meter (policer) profile for broadcast traffic to the interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter broadcast add capability admin-state <admin-
state> profile-id <profile-id>
```

To change the rate meter (policer) profile for broadcast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter broadcast edit admin-state <admin-state>
profile-id <profile-id>
```

To display the current broadcast rate meter (policer) settings for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter broadcast show configuration
```

To delete the rate meter (policer) profile for broadcast traffic, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter broadcast delete
```

Table 183 Assigning Rate Meter for Broadcast Traffic CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin-state	Variable	enable disable	Enables or disables rate metering on broadcast traffic flows from the logical interface.
profile-id	Number	1 – 250	Select from the rate meter profiles defined in the system.

The following command assigns Profile 1 to broadcast traffic on GbE 1, and enables rate metering on the port.

```
eth type eth [1/1]>rate-meter broadcast add capability admin-state enable
profile-id 1
```

The following command changes the rate meter (policer) profile for broadcast traffic on GbE 1 to 4:

```
eth type eth [1/1]>rate-meter broadcast edit admin-state enable profile-id
4
```

Assigning a Rate Meter (Policer) per Ethertype (CLI)

You can define up to three policers per Ethertype value.

To assign a rate meter (policer) profile for a specific Ethertype to an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter <ethertype#> add capability ethertype-value
<ethertype-value> admin-state <admin-state> profile-id <profile-id>
```

To change the rate meter (policer) profile for a specific Ethertype, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter <ethertype#> edit ethertype-value <ethertype-
value> admin-state <admin-state> profile-id <profile-id>
```

To display the current Ethertype rate meter (policer) settings for an interface, go to interface view for the interface and enter the following commands:

```
eth type eth [x/x]>rate-meter ethertype1 show configuration
eth type eth [x/x]>rate-meter ethertype2 show configuration
eth type eth [x/x]>rate-meter ethertype3 show configuration
```

To delete the rate meter (policer) profile for an Ethertype, go to interface view for the interface and enter one or more of the following commands:

```
eth type eth [x/x]>rate-meter ethertype1 delete
eth type eth [x/x]>rate-meter ethertype2 delete
eth type eth [x/x]>rate-meter ethertype3 delete
```

Table 184 Assigning Rate Meter per Ethertype CLI Parameters

Parameter	Input Type	Permitted Values	Description
ethertype#	Variable	ethertype1 ethertype2 ethertype3 I	Identifies which of three possible policer-per-Ethertype combinations you are defining.
ethertype-value	Hexadecimal	1-65535	Identifies the Ethertype to which the profile applies.
admin-state	Variable	enable disable	Enables or disables policing on broadcast traffic flows from the logical interface.
profile-id	Number	1 – 250	Select from the policer profiles defined in the system. For instructions on defining rate meter (policer) profiles, refer to Configuring Rate Meter (Policer) Profiles (CLI).

The following commands assign Rate Meter Profiles 1, 2, and 3 to Ethertypes 0x8000, 0x8100, and 0x9100, respectively, on GbE 1, and enable rate metering on the port.

```
eth type eth [1/1]>rate-meter ethertype1 add capability ethertype-value
0x8000 admin-state enable profile-id 1

eth type eth [1/1]>rate-meter ethertype2 add capability ethertype-value
0x8100 admin-state enable profile-id 2

eth type eth [1/1]>rate-meter ethertype3 add capability ethertype-value
0x9100 admin-state enable profile-id 3
```

The following commands change the rate meter (policer) profiles assigned in the examples above to 4, 5, and 6, respectively.

```
eth type eth [1/1]>rate-meter ethertype1 edit ethertype-value 0x8000 admin-
state enable profile-id 4

eth type eth [1/1]>rate-meter ethertype2 edit ethertype-value 0x8100 admin-
state enable profile-id 5

eth type eth [1/1]>rate-meter ethertype3 edit ethertype-value 0x9100 admin-
state enable profile-id 6
```

Attaching a Rate Meter (Policer) to a Service Point and CoS (CLI)

To assign a rate meter (policer) profile to a service point, go to service view for the service and enter the following commands:

```
service[x]>sp rate-meter add capability spid <spid>

service[x]>sp rate-meter edit spid <spid> admin-state <admin-
state> profile-id <profile-id>
```

To change the rate meter (policer) profile for a service point, go to service view for the service and enter the following command:

```
service[x]>sp rate-meter edit spid <spid> admin-state <admin-
state> profile-id <profile-id>
```

To display the current rate meter (policer) profile for a service point, go to service view for the service and enter the following command:

```
service[x]>sp rate-meter show configuration spid <spid>
```

To assign a rate meter (policer) profile to a service point and CoS, go to service view for the service and enter the following commands:

```
service[x]>sp rate-meter add capability spid <spid>

service[x]>sp rate-meter edit spid <spid> cos <cos> admin-state
<admin-state> profile-id <profile-id>
```

To change the rate meter (policer) profile for a service point and CoS, go to service view for the service and enter the following command:

```
service[x]>sp rate-meter edit spid <spid> cos <cos> admin-state
<admin-state> profile-id <profile-id>
```

To display the current rate meter (policer) profile for a service point and CoS, go to service view for the service and enter the following command:

```
service[x]>sp rate-meter show configuration spid <spid> cos
<cos>
```

To delete the rate meter (policer) profile for a service point or service point/CoS combination, go to service view for the service and enter the following command:

```
service[x]>sp rate-meter delete spid <spid>
```

Table 202: Assigning Rate Meter for Service Point and Service Point/CoS CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
admin-state	Variable	enable disable	Enables or disables rate metering on unicast traffic flows from the logical interface.
profile-id	Number	1 – 250	Select from the rate meter profiles defined in the
cos	Number	0 – 7	The CoS value to which you are assigning the rate meter.

The following commands assign Rate Meter Profile 2 to service point 10 on service 5:

```
root> ethernet service sid 5

service[5]> sp rate-meter add capability spid 10
service[5]>sp rate-meter edit spid 10 admin-state enable
profile-id 2
```

The following commands assign Rate Meter Profile 4 to service point 10 and CoS 6 on service 5:

```
root> ethernet service sid 5

service[5]> sp rate-meter add capability spid 10
service[5]>sp rate-meter edit spid 10 cos 6 admin-state enable
profile-id 4
```

Configuring the Line Compensation Value for a Rate Meter (Policer) (CLI)

A rate meter can measure CIR and EIR at Layer 1 or Layer 2 rates. Layer 1 capacity is equal to Layer 2 capacity plus 20 additional bytes for each frame due to the preamble and Inter Frame Gap (IFG). In most cases, the preamble and IFG equals 20 bytes, but other values are also possible. Line compensation defines the number of bytes to be added to each frame for purposes of CIR and EIR calculation. When Line Compensation is 20, the rate meter operates as Layer 1. When Line Compensation is 0, the rate meter operates as Layer 2. This parameter is very important to users that want to distinguish between Layer 1 and Layer 2 traffic.

To configure the rate meter (policer) line compensation value for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter-compensation-value set <value>
```

To display the rate meter (policer) line compensation value for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>rate-meter-compensation-value get
```

Table 185 Assigning Line Compensation Value for Rate Meter CLI Parameters

Parameter	Input Type	Permitted Values	Description
value	Number	0 – 32	Policers attached to the interface use this value to compensate for Layer 1 non-effective traffic bytes.

The following command sets the line compensation value for policers attached to GbE 1 to 20:

```
eth type eth [1/1]>rate-meter-compensation-value set 20
```

Displaying Rate Meter Statistics for an Interface (CLI)

Note: This section is only relevant for PTP 850S.

For the rate meter (policer) at the logical interface level, you can display the following statistics counters:

- Green Frames
- Green Bytes
- Yellow Frames
- Yellow Bytes
- Red Frames
- Red Bytes

Note: Rate meter (policer) counters are displayed in granularity of 64 bits.

The following commands display rate meter counters for the available frame types and Ethertypes:

```
eth type eth [x/x]>rate-meter unicast show statistics clear-on-read <clear-on-read> layer-1 <layer-1>

eth type eth [x/x]>rate-meter multicast show statistics clear-on-read <clear-on-read> layer-1 <layer-1>

eth type eth [x/x]>rate-meter broadcast show statistics clear-on-read <clear-on-read> layer-1 <layer-1>

eth type eth [x/x]>rate-meter ethertype1 show statistics clear-on-read <clear-on-read> layer-1 <layer-1>

eth type eth [x/x]>rate-meter ethertype2 show statistics clear-on-read <clear-on-read> layer-1 <layer-1>

eth type eth [x/x]>rate-meter ethertype3 show statistics clear-on-read <clear-on-read> layer-1 <layer-1>
```

Table 204: Displaying Rate Meter Statistics CLI Parameters

Parameter	Input Type	Permitted Values	Description
clear-on-read	Boolean	yes no	If you enter yes, the statistics are cleared once you display them.
layer 1	Boolean	yes no	yes – Statistics are represented as Layer 1 statistics, including preamble and IFG. no – Statistics are represented as Layer 2 statistics.

The following commands display rate meter counters for GbE 1, for each of the available frame types and Ethertypes. These commands clear the counters after displaying them.

```
eth type eth [1/1]>rate-meter unicast show statistics clear-on-read yes layer-1 no

eth type eth [1/1]>rate-meter multicast show statistics clear-on-read yes layer-1 no

eth type eth [1/1]>rate-meter broadcast show statistics clear-on-read yes layer-1 no

eth type eth [1/1]>rate-meter ethertype1 show statistics clear-on-read yes layer-1 no

eth type eth [1/1]>rate-meter ethertype2 show statistics clear-on-read yes layer-1 no

eth type eth [1/1]>rate-meter ethertype3 show statistics clear-on-read yes layer-1 no
```

Configuring Marking (CLI)

This section includes:

- Marking Overview (CLI)
- Configuring Marking Mode on a Service Point (CLI)
- Marking Table for C-VLAN UP Bits (CLI)
- Marking Table for S-VLAN UP Bits (CLI)

Marking Overview (CLI)

When enabled, PTP 850's marking mechanism modifies each frame's 802.1p UP bit and CFI/DEI bits according to the classifier decision. The CFI/DEI (color) field is modified according to the classifier and policer decision. The color is first determined by a classifier and may be later overwritten by a policer. Green color is represented by a CFI/DEI value of 0, and Yellow color is represented by a CFI/DEI value of 1. Marking is performed on egress frames that are VLAN-tagged.

The marking is performed according to global marking tables that describe the 802.1p UP bits and the CFI bits (for C-VLAN tags) or DEI bits (for S VLAN tags). The marking mode attribute in the service point egress attributes determines whether the frame is marked as Green or Yellow according to the calculated color.

Note

The calculated color is sent to the queue manager regardless of whether the marking bit is set.

Regular marking is only performed when:

The outer frame is S-VLAN, and S-VLAN CoS preservation is disabled

The outer frame is C-VLAN, and C-VLAN CoS preservation is disabled

If marking and CoS preservation for the relevant outer VLAN are both disabled, special marking is applied. Special marking means that marking is performed, but only according to the values defined for Green frames in the 802.1Q and 802.1AD marking tables.

When marking is performed, the C-VLAN or S-VLAN 802.1p UP bits are re-marked according to the calculated CoS and Color.

Configuring Marking Mode on a Service Point (CLI)

To enable or disable marking mode on a service point, go to service view for the service and enter the following command:

```
service[SID]>sp marking set spid <sp-id> mode <mode>
```

Table 186 Marking Mode on Service Point CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
mode	Variable	enable disable	Determines whether re-marking of the outer VLAN (C-VLAN or S-VLAN) of tagged frames that pass through the service point is enabled. If mode is set to enable, and CoS preservation for the relevant outer VLAN is set to disable, the service point re-marks the C-VLAN or S-VLAN 802.1p UP bits of egress frames according to the calculated CoS and Color, and the user-configurable 802.1Q and 802.1AD marking tables. If mode is set to enable and CoS preservation for the relevant outer VLAN is also set to enable, re-marking is not performed. If mode is set to disable and CoS preservation for the relevant outer VLAN is also set to disable, re-marking is applied, but only according to the values defined for Green frames in the 802.1Q and 802.1AD marking tables. For information about configuring CoS Preservation, refer to *CoS Preservation and Modification on a Service Point (CLI)*.

Examples

The following command enables marking mode on Service Point 3 on Service 2:

```
service[2]>sp marking set spid 3 mode enable
```

The following command disables marking mode on Service Point 3 on Service 2:

```
service[2]>sp marking set spid 3 mode disable
```

Marking Table for C-VLAN UP Bits (CLI)

When marking is performed, the following table is used by the marker to decide which CoS and Color to use as the egress CoS and Color bits for C-VLAN-tagged frames.

Table 187 Marking Table for C-VLAN UP Bits

CoS	Color	802.1q (Configurable)	CFI Color (Configurable)
0	Green	0	0
0	Yellow	0	1
1	Green	1	0
1	Yellow	1	1
2	Green	2	0
2	Yellow	2	1
3	Green	3	0
3	Yellow	3	1
4	Green	4	0
4	Yellow	4	1
5	Green	5	0
5	Yellow	5	1
6	Green	6	0
6	Yellow	6	1
7	Green	7	0
7	Yellow	7	1

To modify the 802.1q CoS and Color to UP and CFI bit mapping table, enter the following command in root view:

```
root> ethernet qos 802.1q-up-bits-marking-tbl set cos <cos> color <color>
802.1p <802.1p> cfi <cfi>
```

To display the 802.1q CoS and Color to UP and CFI bit mapping table, enter the following command in root view:

```
root> ethernet qos 802.1q-up-bits-marking-tbl show
```

Table 188 802.1q CoS and Color to UP and CFI Bit Mapping Table CLI Parameters

Parameter	Input Type	Permitted Values	Description
cos	Number	0 – 7	The CoS value to be mapped.
color	Variable	green yellow	The Color to be mapped.
802.1p	Number	0 – 7	The UP bit value assigned to matching frames.
cfi	Number	0 – 1	The CFI bit value assigned to matching frames.

Example

The following command maps CoS 0, Green, to 802.1p UP bit 0, and CFI bit 0:

```
root> ethernet qos 802.1q-up-bits-marking-tbl set cos 0 color green 802.1p
0 cfi 0
```

Marking Table for S-VLAN UP Bits (CLI)

When marking is performed, the following table is used by the marker to decide which CoS and Color to use as the egress CoS and Color bits for S-VLAN-tagged frames.

Table 189 802.1ad UP Marking Table (S-VLAN)

CoS	Color	802.1ad UP (Configurable)	DEI Color (Configurable)
0	Green	0	0
0	Yellow	0	1
1	Green	1	0
1	Yellow	1	1
2	Green	2	0
2	Yellow	2	1
3	Green	3	0
3	Yellow	3	1
4	Green	4	0
4	Yellow	4	1
5	Green	5	0
5	Yellow	5	1
6	Green	6	0
6	Yellow	6	1
7	Green	7	0
7	Yellow	7	1

To modify the 802.1ad CoS and Color to UP and DEI bit mapping table, enter the following command in root view:

```
root> ethernet qos 802.1ad-up-bits-marking-tbl set cos <cos> color <color>
802.1p <802.1p> dei <dei>
```

To display the 802.1q CoS and Color to UP and CFI bit mapping table, enter the following command in root view:

```
root> ethernet qos 802.1ad-up-bits-marking-tbl show
```

Table 190 802.1ad UP Marking Table (S-VLAN) CLI Parameters

Parameter	Input Type	Permitted Values	Description
cos	Number	0 – 7	The CoS value to be mapped.
color	Variable	green yellow	The Color to be mapped.

Parameter	Input Type	Permitted Values	Description
802.1p	Number	0 – 7	The UP bit value assigned to matching frames.
dei	Number	0 – 1	The DEI bit value assigned to matching frames.

Example

The following command marks CoS 5, Yellow, to 802.1p UP bit 5, and DEI bit 1:

```
root> ethernet qos 802.1ad-up-bits-marking-tbl set cos 5 color yellow
802.1p 5 dei 1
```

Configuring WRED (CLI)

This section includes:

- WRED Overview (CLI)
- Configuring WRED Profiles (CLI)
- Assigning a WRED Profile to a Queue (CLI)

WRED Overview (CLI)

Weighted Random Early Detection (WRED) enables differentiation between higher and lower priority traffic based on CoS. You can define up to 30 WRED profiles. Each profile contains a green traffic curve and a yellow traffic curve. These curves describe the probability of randomly dropping frames as a function of queue occupancy.

The system also includes two pre-defined read-only profiles. These profiles are assigned WRED profile IDs 31 and 32.

Profile number 31 defines a tail-drop curve and is configured with the following values:

- 100% Yellow traffic drop after 64kbytes occupancy.
- 100% Green traffic drop after 128kbytes occupancy.
- Yellow maximum drop is 100%
- Green maximum drop is 100%

Profile number 32 defines a profile in which all will be dropped. It is for internal use and should not be applied to traffic.

A WRED profile can be assigned to each queue. The WRED profile assigned to the queue determines whether or not to drop incoming frames according to the occupancy of the queue. As the queue occupancy grows, the probability of dropping each incoming frame increases as well. As a consequence, statistically more TCP flows will be restrained before traffic congestion occurs.

Configuring WRED Profiles (CLI)

To configure a WRED profile, enter the following command in root view:

```
root> ethernet qos wred-profile-tbl add profile-id <profile-id> green-min-
threshold <green-min-threshold> green-max-threshold <green-max-threshold>
green-max-drop <green-max-drop> yellow-min-threshold <yellow-min-threshold>
yellow-max-threshold <yellow-max-threshold> yellow-max-drop <yellow-max-
drop>
```

To edit an existing WRED profile, enter the following command in root view:

```
root> ethernet qos wred-profile-tbl edit profile-id <profile-id> green-min-
threshold <green-min-threshold> green-max-threshold <green-max-threshold>
green-max-drop <green-max-drop> yellow-min-threshold <yellow-min-threshold>
yellow-max-threshold <yellow-max-threshold> yellow-max-drop <yellow-max-
drop>
```

To display a WRED profile, enter the following command in root view:

```
root> ethernet qos wred-profile-tbl show profile-id <profile-id>
```

To delete a WRED profile, enter the following command in root view:

```
root> ethernet qos wred-profile-tbl delete profile-id <profile id>
```

You cannot delete a WRED profile that is assigned to a queue. You must first remove the WRED profile from the queue by replacing it with a different WRED profile. You can then delete the WRED profile.

Note

Each queue always has a WRED profile assigned to it. By default, WRED Profile 31 is assigned to every queue until a different profile is assigned.

Table 191 WRED Profile CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 - 30	A unique ID to identify the profile.
green-min-threshold	Number	24 - 8192	The minimum throughput of green frames for queues with this profile, in Kbytes. When this value is reached, the system begins dropping green frames in the queue.
green-max-threshold	Number	24 - 8192	The maximum throughput of green frames for queues with this profile, in Kbytes. When this value is reached, all green frames in the queue are dropped.
green-max-drop	Number	1 - 100	The maximum percentage of dropped green frames for queues with this profile.
yellow-min-threshold	Number	24 - 8192	The minimum throughput of yellow frames for queues with this profile, in Kbytes. When this value is reached, the system begins dropping yellow frames in the queue.
yellow-max-threshold	Number	0 - 8192	The maximum throughput of yellow frames for queues with this profile, in Kbytes. After this value is reached, all yellow frames in the queue are dropped.
yellow-max-drop	Number	1 - 100	The maximum percentage of dropped yellow frames for queues with this profile.

Examples

The following command adds a WRED profile.

```
root> ethernet qos wred-profile-tbl add profile-id 2 green-min-threshold
8000 green-max-threshold 8000 green-max-drop 100 yellow-min-threshold 8000
yellow-max-threshold 8000 yellow-max-drop 100
```

The new profile has the following parameters:

profile-id – 2

green-min-threshold – 8000 Kbytes

green-max-threshold – 8000 Kbytes

green-max-drop – 100%

yellow-min-threshold – 8000 Kbytes

yellow-max-threshold – 8000 Kbytes

yellow-max-drop – 100%

The following command edits the WRED profile created by the previous command:

```
root> ethernet qos wred-profile-tbl edit profile-id 2 green-min-threshold
8000 green-max-threshold 8000 green-max-drop 100 yellow-min-threshold 4000
yellow-max-threshold 4000 yellow-max-drop 100
```

The edited profile has the following parameters:

green-min-threshold – 8000 Kbytes

green-max-threshold – 8000 Kbytes

green-max-drop – 100%

yellow-min-threshold – 4000 Kbytes

yellow-max-threshold –4000 Kbytes

yellow-max-drop – 100%

Assigning a WRED Profile to a Queue (CLI)

To assign a WRED profile to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> wred set service-bundle-id <service-bundle-id> cos
<cos> profile-id <profile-id>
```

To display the WRED profile assigned to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> wred show profile-id service-bundle-id <service-bundle-
id> cos <cos>
```

Table 192 Assigning WRED Profile to Queue CLI Parameters

Parameter	Input Type	Permitted Values	Description
service-bundle-id	Number	1 – 63 **Note:** In the current release, only Service Bundle 1 is supported.	Assigns the WRED profile to a Service Bundle. Service Bundles are bundles of queues, grouped together in order to configure common egress characteristics for specific services.
cos	Number	0 – 7	Assigns the WRED profile to a queue in the designated service bundle.
profile-id	Number	1 – 32	A unique ID that identifies the profile.

Examples

The following command assigns WRED Profile 2 to the CoS 0 queue in Service Bundle 1, on GbE 1:

```
eth type eth [1/1]> wred set service-bundle-id 1 cos 0 profile-id 2
```

The following command displays the WRED profile assigned to the CoS 0 queue in Service Bundle 1, on GbE 1:

```
eth type eth [1/1]> wred show profile-id service-bundle-id 1 cos 0
```

Configuring Shapers (CLI)

Egress shaping abilities differ between PTP 850C and PTP 850E, on one hand, and PTP 850S, on the other. Therefore, it is presented separately for each product group:

- Configuring Shapers for PTP 850C and PTP 850E (CLI)
- Configuring Shapers for PTP 850S (CLI)

Configuring Shapers for PTP 850C and PTP 850E (CLI)

This section includes:

- Overview of Egress Shaping for PTP 850C and PTP 850E (CLI)
- Configuring Egress Line Compensation for Shaping for PTP 850C and PTP 850E (CLI)

Overview of Egress Shaping for PTP 850C and PTP 850E (CLI)

Egress shaping determines the traffic profile for each queue. PTP 850 can perform queue shaping on the queue level, using dual leaky bucket shaping. On the queue level, you can configure up to 32 single leaky bucket shaper profiles. If no profile is attached to the queue, no egress shaping is performed on that queue.

Note: You can enter any value within the permitted range. Based on the value you enter, the software automatically rounds off the setting according to the granularity. If you enter a value below the lowest granular value (except 0), the software adjusts the setting to the minimum.

You can attach one of the configured queue shaper profiles to each priority queue. If no profile is attached to the queue, no egress shaping is performed on that queue.

This section includes:

- Configuring Queue Shaper Profiles for PTP 850C and PTP 850E (CLI)
- Attaching a Shaper Profile to a Queue for PTP 850C and PTP 850E (CLI)

Configuring Queue Shaper Profiles (CLI)

To configure a queue shaper profile, enter the following command in root view:

```
root> ethernet qos queue-shaper-profile-tbl-broadband add profile-id
<profile-id> cir <cir> shaper-profile-name <shaper-profile-name> cbs <cbs>
eir <eir> ebs <ebs> burst-type <burst-type>
```

To edit the parameters of an existing queue shaper profile, enter the following command in root view:

```
root> ethernet qos queue-shaper-profile-tbl-broadband edit profile-id
<profile-id> cir <cir> shaper-profile-name <shaper-profile-name> cbs <cbs>
eir <eir> ebs <ebs> burst-type <burst-type>
```

Table 193: Queue Shaper Profiles CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 - 32	A unique ID that identifies the profile.
cir	Number	0 – 40000000	The Committed Information Rate (CIR) assigned to the profile (in kbps). If the value

Parameter	Input Type	Permitted Values	Description
			is 0, all incoming CIR traffic is dropped. Granularity is 81 kbps. The default value is 40000000 kbps.
shaper-profile-name	Text String	Up to 20 characters.	Granularity is 81 kbps. The default value is 40000000 kbps. A description of the profile.
cbs	Number	1 – 32	The Committed Burst Rate (CBR) for the shaper, in Kbytes. Permitted values are 1-32 KB. The default value is 16 KB.
eir	Number	40000000	The Excess Information Rate (EIR) for the shaper (in kbps). If the value is 0, all incoming EIR traffic is dropped. Granularity is 162 kbps. The default value is 40000000 kbps.
ebs	Number	1 – 32	The Excess Burst Rate (EBR) for the shaper, in Kbytes. Permitted values are 1-32 KB. The default value is 16 KB.
burst-type	Variable	short long	Only **short** is supported.

The following command creates Queue Shaper 1, named “p1,” with a CIR value of 16000 kbps, CBS of 16 KB, EIR of 16000 kbps, and EBR of 1:

```
root> ethernet qos queue-shaper-profile-tbl-broadband add profile-id 1 cir
16000 shaper-profile-name p1 cbs 16 eir 16000 ebs 1 burst-type short
```

The following command changes the CIR value of the profile created above from 16000 to 32000, and changes the profile name to p3:

```
root> ethernet qos queue-shaper-profile-tbl-broadband add profile-id 1 cir
32000 shaper-profile-name p3 cbs 16 eir 16000 ebs 1 burst-type short
```

To display the parameters of a queue shaper profile, enter the following command in root view:

```
root> ethernet qos queue-shaper-profile-tbl-broadband show profile-id
<profile-id>
```

To delete a queue shaper profile, enter the following command in root view:

```
root> ethernet qos queue-shaper-profile-tbl-broadband delete profile-id
<profile id>
```

You cannot delete a queue shaper profile if it is attached to a queue. You must first remove the profile from the queue. You can then delete the profile.

Attaching a Shaper Profile to a Queue (CLI)

You can attach one of the configured queue shaper profiles to each priority queue. If no profile is attached to the queue, no egress shaping is performed on that queue. Shapers are attached to queues based on the logical interface and service bundle to which the queue belongs, and the queue’s CoS value.

To attach a queue shaper profile to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> queue-shaper add capability service-bundle-id <service-
bundle-id> cos <cos> admin-state <admin-state> profile-id <profile-id>
```

To change the queue shaper profile attached to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> queue-shaper edit service-bundle-id <service-bundle-id>
cos <cos> admin-state <admin-state> profile-id <profile-id>
```

To display the queue shaper profile attached to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> queue-shaper show configuration service-bundle-id
<service-bundle-id> cos <cos>
```

To remove a queue shaper profile from a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> queue-shaper delete service-bundle-id <service-bundle-
id> cos <cos>
```

Table 194 Attaching Shaper Profile to Queue CLI Parameters

Parameter	Input Type	Permitted Values	Description
service-bundle-id	Number	1 – 63 **Note:** In the current release, only Service Bundle 1 is supported.	The service bundle to which you are attaching the queue shaper profile.
cos	Number	0 – 7	The CoS queue ID of the queue to which you want to assign the shaper. Queues are numbered according to CoS value.
admin-state	Variable	enable disable	Select `enable` to enable egress queue shaping on the queue, or `disable` to disable egress queue shaping on the queue. If you set shaping to `disable`, the shaper profile remains attached to the queue, but does not affect traffic.
profile-id	Number	1 – 32	Enter the ID of one of the configured queue shaper profiles.

The following command adds Queue Shaper Profile 5 to queues with CoS 0, on Service Bundle 1, on GbE 1, and enables shaping on these queues.

```
eth type eth [1/1]> queue-shaper add capability service-bundle-id 1 cos 0
admin-state enable profile-id 5
```

The following command changes the Queue Shaper Profile assigned in the previous command to Queue Shaper Profile 2:

```
eth type eth [1/1]> queue-shaper edit service-bundle-id 1 cos 0 admin-state
enable profile-id 2
```

Configuring Egress Line Compensation for Shaping for PTP 850C and PTP 850E (CLI)

You can configure a line compensation value for all the shapers under a specific logical interface. This value is used to compensate for Layer 1 non-effective traffic bytes on egress.

To set the egress line compensation value, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>shaping-compensation-value set <value>
```

To display the egress line compensation value, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>shaping-compensation-value get
```

Table 195 Egress Line Compensation for Shaping CLI Parameters

Parameter	Input Type	Permitted Values	Description
value	Number	0 – 26 (even numbers only)	Shapers attached to the interface use this value to compensate for Layer 1 non-effective traffic bytes on egress.

The following command sets the egress line compensation value to 0 on GbE 1:

```
eth type eth [1/1]>shaping-compensation-value set 0
```

Configuring Shapers for PTP 850S (CLI)

This section includes:

- Overview of Egress Shaping for PTP 850S (CLI)
- Configuring Queue Shapers for PTP 850S (CLI)
- Configuring Service Bundle Shapers for PTP 850S (CLI)
- Configuring Egress Line Compensation for Shaping for PTP 850S (CLI)

Overview of Egress Shaping for PTP 850S (CLI)

Egress shaping determines the traffic profile for each queue. PTP 850 performs egress shaping on the following levels:

- Queue level – Single leaky bucket shaping
- Service Bundle level – Dual leaky bucket shaping

Note: Single leaky bucket shaping on the interface level is planned for future release.

Configuring Queue Shapers for PTP 850S (CLI)

You can configure up to 32 single leaky bucket queue shaper profiles. The CIR value can be set to the following values:

- 16,000 – 32,000,000 bps – granularity of 16,000 bps
- 32,000,000 – 131,008,000 bps – granularity of 64,000 bps

Note: You can enter any value within the permitted range. Based on the value you enter, the software automatically rounds off the setting according to the granularity. If you enter a value below the lowest granular value (except 0), the software adjusts the setting to the minimum.

You can attach one of the configured queue shaper profiles to each priority queue. If no profile is attached to the queue, no egress shaping is performed on that queue.

This section includes:

- Configuring Queue Shaper Profiles for PTP 850S (CLI)
- Attaching a Shaper Profile to a Queue for PTP 850S (CLI)

Configuring Queue Shaper Profiles for PTP 850S (CLI)

To configure a queue shaper profile, enter the following command in root view:

```
root> ethernet qos queue-shaper-profile-tbl add profile-id
<profile-id> cir <cir> shaper-profile-name <shaper-profile-
name>
```

To edit the parameters of an existing queue shaper profile, enter the following command in root view:

```
root> ethernet qos queue-shaper-profile-tbl edit profile-id
<profile-id> cir <cir> shaper-profile-name <shaper-profile-
name> burst-type short
```

Note: The burst-type parameter is reserved for future use. However, you must enter this parameter in order for the command to execute.

To display the parameters of a queue shaper profile, enter the following command in root view:

```
root> ethernet qos queue-shaper-profile-tbl show profile-id
<profile-id>
```

To delete a queue shaper profile, enter the following command in root view:

```
root> ethernet qos queue-shaper-profile-tbl delete profile-id
<profile id>
```

You cannot delete a queue shaper profile if it is attached to a queue. You must first remove the profile from the queue. You can then delete the profile.

Table 215: Queue Shaper Profiles CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 - 32	A unique ID that identifies the profile.

cir	Number	16000 – 131008000	The Committed Information Rate (CIR) assigned to the profile (in bps).
shaper-profile-name	Text String	Up to 20 characters.	A description of the profile.

The following command creates Queue Shaper 1, named “p1”, with a CIR value of 16000 bps:

```
root> ethernet qos queue-shaper-profile-tbl add profile-id 1
cir 16000 shaper-profile-name p1
```

The following command changes the CIR value of the profile created above from 16000 to 32000, and changes the profile name to p3:

```
root> ethernet qos queue-shaper-profile-tbl edit profile-id 1
cir 32000 shaper-profile-name p3 burst-type short
```

Attaching a Shaper Profile to a Queue for PTP 850S (CLI)

You can attach one of the configured queue shaper profiles to each priority queue. If no profile is attached to the queue, no egress shaping is performed on that queue. Shapers are attached to queues based on the logical interface and service bundle to which the queue belongs, and the queue’s CoS value.

To attach a queue shaper profile to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> queue-shaper add capability service-bundle-
id <service-bundle-id> cos <cos> admin-state <admin-state>
profile-id <profile-id>
```

To change the queue shaper profile attached to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> queue-shaper edit service-bundle-id
<service-bundle-id> cos <cos> admin-state <admin-state>
profile-id <profile-id>
```

To display the queue shaper profile attached to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> queue-shaper show configuration service-
bundle-id <service-bundle-id> cos <cos>
```

To remove a queue shaper profile from a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> queue-shaper delete service-bundle-id
<service-bundle-id> cos <cos>
```

Table 216: Attaching Shaper Profile to Queue CLI Parameters

Parameter	Input Type	Permitted Values	Description

service-bundle-id	Number	1 – 63 **Note:** In the current release, only Service Bundle 1 is supported.	The service bundle to which you are attaching the queue shaper profile.
cos	Number	0 – 7	The CoS queue ID of the queue to which you want to assign the shaper. Queues are numbered according to CoS value.
admin-state	Variable	enable disable	Select `enable` to enable egress queue shaping on the queue, or `disable` to disable egress queue shaping on the queue. If you set shaping to `disable`, the shaper profile remains attached to the queue, but does not affect traffic.
profile-id	Number	1 – 32	Enter the ID of one of the configured queue shaper profiles.

The following command adds Queue Shaper Profile 5 to queues with CoS 0, on Service Bundle 1, on GbE 1, and enables shaping on these queues:

```
eth type eth [1/1]> queue-shaper add capability service-bundle-
id 1 cos 0 admin-state enable profile-id 5
```

The following command changes the Queue Shaper Profile assigned in the previous command to Queue Shaper Profile 2:

```
eth type eth [1/1]> queue-shaper edit service-bundle-id 1 cos 0
admin-state enable profile-id 2
```

Configuring Service Bundle Shapers for PTP 850S (CLI)

You can configure up to 256 dual leaky bucket service bundle shaper profiles. The profiles can be configured as follows:

Valid CIR values are:

0 – 32,000,000 bps, with granularity of 16,000 bps

32,000,000 – 1,000,000,000 bps, with granularity of 64,000 bps Valid PIR

values are:

16,000 – 32,000,000 bps, with granularity of 16,000 bps

32,000,000 – 1,000,000,000 bps, with granularity of 64,000 bps

Note: You can enter any value within the permitted range. Based on the

value you enter, the software automatically rounds off the setting according to the granularity. If you enter a value below the lowest granular value (except 0), the software adjusts the setting to the minimum.

You can attach one of the configured service bundle shaper profiles to each service bundle. If no profile is attached to the service bundle, no egress shaping is performed on that service bundle.

This section includes:

Configuring Service Bundle Shaper Profiles for PTP 850S (CLI)
Attaching a Shaper Profile to a Service Bundle for PTP 850S (CLI)

Configuring Service Bundle Shaper Profiles for PTP 850S (CLI)

To configure a service bundle shaper profile, enter the following command in root view:

```
root> ethernet qos service-bundle-shaper-profile-tbl add
profile-id <profile-id> cir <cir> pir <pir> shaper-profile-name
<shaper-profile-name>
```

To edit the parameters of an existing service bundle shaper profile, enter the following command in root view:

```
root> ethernet qos service-bundle-shaper-profile-tbl edit
profile-id <profile-id> cir <cir> pir <pir> shaper-profile-name
<shaper-profile-name>
```

To display the parameters of a service bundle shaper profile, enter the following command in root view:

```
root> ethernet qos service-bundle-shaper-profile-tbl show
profile-id <profile-id>
```

To display the parameters of all configured service bundle shaper profiles, enter the following command in root view:

```
root> ethernet qos service-bundle-shaper-profile-tbl show
profile-id all
```

To delete a service bundle shaper profile, enter the following command in root view:

```
root> ethernet qos service-bundle-shaper-profile-tbl delete
profile-id <profile-id>
```

You cannot delete a service bundle shaper profile if it is attached to a service bundle. You must first remove the profile from the service bundle. You can then delete the profile.

Table 217: Service Bundle Shaper Profiles CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 - 256	A unique ID that identifies the
cir	Number	1 - 1000000000	The Committed Information Rate (CIR) assigned to the profile (in
pir	Number	16000 - 1000000000	The Peak Information Rate (PIR) assigned to the
shaper-profile-name	Text String	Up to 20 character	A description of the profile.

The following command creates Service Bundle Shaper 1, named “p1”, with a CIR value of 100000000 bps and a PIR value of 200000000 bps:

```
root> ethernet qos service-bundle-shaper-profile-tbl add
profile-id 1 cir 100000000 pir 200000000 shaper-profile-name p1
```

The following command changes the CIR value in the Service Bundle Shaper created above from 100000000 bps to 110000000 bps:

```
root> ethernet qos service-bundle-shaper-profile-tbl edit
profile-id 1 cir 110000000 pir 200000000 shaper-profile-name p1
```

Attaching a Shaper Profile to a Service Bundle for PTP 850S (CLI)

You can attach one of the configured service bundle shaper profiles to each service bundle. If no profile is attached to the service bundle, no egress shaping is performed on that service bundle.

To attach a service bundle shaper profile to a service bundle, go to interface view for the service bundle and enter the following command:

```
eth type eth [x/x]> service-bundle-shaper add capability
service-bundle-id <service-bundle-id> admin-state <admin-state>
profile-id <profile-id>
```

To change the service bundle shaper profile attached to a service bundle, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> service-bundle-shaper edit service-bundle-
id <service-bundle-id> admin-state <admin-state> profile-id
<profile-id>
```

To display the service bundle shaper profile attached to a service bundle, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> service-bundle-shaper show configuration
service-bundle-id <service-bundle-id>
```

To remove a service bundle shaper profile from a service bundle, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> service-bundle-shaper delete service-
bundle-id <service-bundle-id>
```

Table 218: Attaching Shaper Profile to Service Bundle CLI Parameters

Parameter	Input Type	Permitted Values	Description
service-bundle-id	Number	1 – 63 **Note:** In the current release, only Service Bundle 1 is supported.	The service bundle to which you are attaching the queue shaper profile.
admin-state	Variable	enable disable	Select enable to `enable` egress shaping on the service bundle, or `disable` to disable egress shaping on the service bundle.
profile-id	Number	1 – 256	Enter the ID of one of the configured service bundle shaper profiles.

The following command adds Service Bundle Shaper Profile 5 to Service Bundle 1, on GbE 1, and enables shaping on this service bundle:

```
eth type eth [1/1]> service-bundle-shaper add capability
service-bundle-id 1 admin-state enable profile-id 5
```

The following command changes the Service Bundle Shaper Profile assigned in the previous command to Service Bundle 1, from 5 to 4:

```
eth type eth [1/1]> service-bundle-shaper edit service-bundle-
id 1 admin-state enable profile-id 4
```

Configuring Egress Line Compensation for Shaping for PTP 850S (CLI)

You can configure a line compensation value for all the shapers under a specific logical interface. This value is used to compensate for Layer 1 non-effective traffic bytes on egress.

To set the egress line compensation value, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>shaping-compensation-value set <value>
```

To display the egress line compensation value, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>shaping-compensation-value get
```

Table 219: Egress Line Compensation for Shaping CLI Parameters

Parameter	Input Type	Permitted Values	Description
value	Number	0 – 26 (even numbers only)	Shapers attached to the interface use this value to compensate for Layer 1 non-effective traffic bytes on egress.

The following command sets the egress line compensation value to 0 on GbE 1:

```
eth type eth [1/1]>shaping-compensation-value set 0
```

Configuring Scheduling (CLI)

This section includes:

Overview of Egress Scheduling (CLI)

Egress scheduling is responsible for transmission from the priority queues. PTP 850 uses a unique algorithm with a hierarchical scheduling model over the three levels of the egress path that enables compliance with SLA requirements.

The scheduler scans all the queues over all the service bundles, per interface, and determines which queue is ready to transmit. If more than one queue is ready to transmit, the scheduler determines which queue transmits first based on:

Queue Priority – A queue with higher priority is served before lower-priority queues.

Weighted Fair Queuing (WFQ) – If two or more queues have the same priority and are ready to transmit, the scheduler transmits frames from the queues based on a WFQ algorithm that determines the ratio of frames per queue based on a predefined weight assigned to each queue.

Configuring Queue Priority (CLI)

A priority profile defines the exact order for serving the eight priority queues in a single service bundle. When you attach a priority profile to an interface, all the service bundles under the interface inherit the profile.

The priority mechanism distinguishes between two states of the service bundle:

Green State – Committed state

Yellow state – Best effort state

Green State refers to any time when the service bundle rate is below the user-defined CIR. Yellow State refers to any time when the service bundle is above the user-defined CIR but below the PIR.

You can define up to four Green priority profiles, from 4 (highest) to 1 (lowest). An additional four Yellow priority profiles are defined automatically and cannot be changed or edited.

The following table provides a sample of an interface priority profile. This profile is also used as the default interface priority profile.

Table 196 Interface Priority Profile Example

Profile ID (1-9)			
CoS	Green Priority (user defined)	Yellow Priority (read only)	Description
0	1	1	Best Effort

Profile ID (1-9)			
CoS	Green Priority (user defined)	Yellow Priority (read only)	Description
1	2	2	Data Service 4
2	2	2	Data Service 3
3	2	2	Data Service 2
4	2	2	Data Service 1
5	3	3	Real Time 2 (Video with large buffer)
6	3	3	Real Time 1 (Video with small buffer)
7	4	4	Management (Sync, PDUs, etc.)

When the service bundle state is Green (committed state), the service bundle priorities are as defined in the Green Priority column. When the service bundle state is Yellow (best effort state), the service bundle priorities are system-defined priorities shown in the Yellow Priority column.

Note

CoS 7 is always marked with the highest priority and cannot be changed or edited, no matter what the service bundle state is, since it is assumed that only high priority traffic will be tunneled via CoS 7.

The system supports up to nine interface priority profiles. Profiles 1 to 8 are defined by the user, while profile 9 is the pre-defined read-only default interface priority profile.

Configuring Interface Priority Profiles (CLI)

To define an interface priority profile, enter the following command in root view:

```
root> ethernet qos port-priority-profile-tbl add profile-id <profile-id> cos0-priority <cos0-priority> description <description> cos1-priority <cos1-priority> description <description> cos2-priority <cos2-priority> description <description> cos3-priority <cos3-priority> description <description> cos4-priority <cos4-priority> description <description> cos5-priority <cos5-priority> description <description> cos6-priority <cos6-priority> description <description> cos7-priority <cos7-priority> description <description>
```

To edit an existing interface priority profile, enter the following command in root view:

```
root> ethernet qos port-priority-profile-tbl edit profile-id <profile-id> cos0-priority <cos0-priority> description <description> cos1-priority <cos1-priority> description <description> cos2-priority <cos2-priority> description <description> cos3-priority <cos3-priority> description <description> cos4-priority <cos4-priority> description <description> cos5-priority <cos5-priority> description <description> cos6-priority <cos6-priority> description <description> cos7-priority <cos7-priority> description <description>
```

To display the parameters of an interface priority profile, enter the following command in root view:

```
root> ethernet qos port-priority-profile-tbl show profile-id <profile-id>
```

To delete an interface priority profile, enter the following command in root view:

```
root> ethernet qos port-priority-profile-tbl delete profile-id <profile-id>
```

You can only delete an interface priority profile if the profile is not attached to any interface.

Table 197 Interface Priority Profile CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 – 8	A unique ID to identify the profile.
cos0-priority	Number	1 – 4	The Green priority for the CoS 0 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 0 egressing the service bundle to which the profile is assigned.
description	Text String	Up to 20 characters.	A description of the priority level.
cos1-priority	Number	1 – 4	The Green priority for the CoS 1 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 1 egressing the service bundle to which the profile is assigned.
cos2-priority	Number	1 – 4	The Green priority for the CoS 2 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 2 egressing the service bundle to which the profile is assigned.
cos3-priority	Number	1 – 4	The Green priority for the CoS 3 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 3 egressing the service bundle to which the profile is assigned.
cos4-priority	Number	1 – 4	The Green priority for the CoS 4 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 4 egressing the service bundle to which the profile is assigned.
cos5-priority	Number	1 – 4	The Green priority for the CoS 5 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 5 egressing the service bundle to which the profile is assigned.
cos6-priority	Number	1 – 4	The Green priority for the CoS 6 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 6 egressing the service bundle to which the profile is assigned.

Parameter	Input Type	Permitted Values	Description
cos7-priority	Number	1 – 4	The Green priority for the CoS 7 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 7 egressing the service bundle to which the profile is assigned.

Example

The following command configures a priority profile with Profile ID 1.

```
root> ethernet qos port-priority-profile-tbl add profile-id 1 cos0-priority
1 description c0_p1 cos1-priority 1 description c1_p1 cos2-priority 1
description c2_p1 cos3-priority 2 description c3_p2 cos4-priority 2
description c4_p2 cos5-priority 3 description c5_p3 cos6-priority 4
description c6_p4 cos7-priority 4 description c7_p4
```

This profile has the parameters listed in the following table.

Table 198 Interface Priority Sample Profile Parameters

CoS	Green Priority (user defined)	Yellow Priority (read only)	Description
0	1	1	c0_p1
1	1	1	c1_p1
2	1	1	c2_p1
3	2	1	c3_p2
4	2	1	c4_p2
5	3	1	c5_p3
6	4	1	c6_p4
7	4	4	c7_p4

The following command edits the profile you created in the previous command so that CoS 6 queues have a Green priority of 3 instead of 4, and a description of “c6_p3”.

```
root> ethernet qos port-priority-profile-tbl edit profile-id 1 cos0-
priority 1 description c0_p1 cos1-priority 1 description c1_p1 cos2-
priority 1 description c2_p1 cos3-priority 2 description c3_p2 cos4-
priority 2 description c4_p2 cos5-priority 3 description c5_p3 cos6-
priority 3 description c6_p3 cos7-priority 4 description c7_p4
```

Attaching a Priority Profile to an Interface (CLI)

To attach a priority profile to an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> priority set profile-id <profile-id>
```

To display which priority profile is attached to an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> port-priority show profile-id
```

Table 199 Attaching Priority Profile to Interface CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 – 9	Enter the ID of one of the configured logical interface priority profiles.

Examples

The following command attaches Interface Priority Profile 3 to GbE 1:

```
eth type eth [1/1]> priority set profile-id 3
```

The following is a sample output from the `port-priority show profile-id` command:

```
eth type eth [1/1]>port-priority show profile-id
Profile ID: 9
CoS   Priority               Priority                Description
     (when queue is green)  (when queue is yellow)
0     1                      1                       best effort
1     2                      1                       data service
2     2                      1                       data service
3     2                      1                       data service
4     2                      1                       data service
5     3                      1                       real time
6     3                      1                       real time
7     4                      4                       management
eth type eth [1/1]>
```

Configuring Weighted Fair Queuing (WFQ) (CLI)

This section includes:

Overview of WFQ for PTP 850C and PTP 850E (CLI)

Configuring a WFQ Profile for PTP 850S (CLI)

Attaching a WFQ Profile to an Interface (CLI)

Overview of WFQ for PTP 850C and PTP 850E (CLI)

The scheduler serves the queues based on their priority, but when two or more queues have data to transmit and their priority is the same, the scheduler uses Weighted Fair Queuing (WFQ) to determine the priorities within each priority. WFQ defines the transmission ratio, in bytes, between the queues. All the service bundles under the interface inherit the WFQ profile attached to the interface.

For each WFQ profile, you can determine the relative weights for both CIR and EIR traffic.

The system supports up to six WFQ interface profiles. Profile ID 1 is a pre-defined read-only profile, and is used as the default profile. Profiles 2 to 6 are user-defined profiles.

The following table provides an example of a WFQ profile.

Table 200 WFQ Profile Example

	Profile ID (1-7)	
CoS	**Queue Weight (Green)**	**Queue Weight (Yellow – not visible to users, and cannot be edited)**
0	15	20
1	15	20
2	15	20
3	15	20
4	15	20
5	15	20
6	15	20
7	20	20

You can attach one of the configured interface WFQ profiles to each interface. By default, the interface is assigned Profile ID 1, the pre-defined system profile.

Configuring a WFQ Profile for PTP 850C and PTP 850E (CLI)

To define a WFQ profile, enter the following command in root view:

```
root> ethernet qos wfq-weight-profile-tbl add profile-id <2-7>
cos0-weight <1-20> cos1-weight <1-20> cos2-weight <1-20> cos3-
weight <1-20> cos4-weight <1-20> cos5-weight <1-20> cos6-weight
<1-20> cos7-weight <1-20> cos0-eir-weight <1-20> cos1-eir-
weight <1-20> cos2-eir-weight <1-20> cos3-eir-weight <1-20>
cos4-eir-weight <1-20> cos5-eir-weight <1-20> cos6-eir-weight
<1-20> cos7-eir-weight <1-20>
```

To edit an existing WFQ profile, enter the following command in root view:

```
root> ethernet qos wfq-weight-profile-tbl edit profile-id <2-7>
cos0-weight <1-20> cos1-weight <1-20> cos2-weight <1-20> cos3-
weight <1-20> cos4-weight <1-20> cos5-weight <1-20> cos6-weight
<1-20> cos7-weight <1-20> cos0-eir-weight <1-20> cos1-eir-
weight <1-20> cos2-eir-weight <1-20> cos3-eir-weight <1-20>
cos4-eir-weight <1-20> cos5-eir-weight <1-20> cos6-eir-weight
<1-20> cos7-eir-weight <1-20>
```

To display the parameters of a WFQ profile, enter the following command in root view:

```
root> ethernet qos wfq-weight-profile-tbl show profile-id
<profile-id>
```

To delete a WFQ profile, enter the following command in root view:

```
root> ethernet qos wfq-weight-profile-tbl delete profile-id
<profile-id>
```

You can only delete a WFQ profile if the profile is not attached to any interface.

The following command configures a WFQ profile with Profile ID 2:

```
root>ethernet qos wfq-weight-profile-tbl add profile-id 2 cos0-
weight 15 cos1-weight 15 cos2-weight 15 cos3-weight 15 cos4-
weight 15 cos5-weight 15 cos6-weight 15 cos7-weight 20 cos0-
eir-weight 20 cos1-eir-weight 20 cos2-eir-weight 20 cos3-eir-
weight 20 cos4-eir-weight 20 cos5-eir-weight 20 cos6-eir-weight
20 cos7-eir-weight 20
```

This profile has the parameters listed in the following table.

Table 225: WFQ Sample Profile Parameters

CoS	Queue Weight (Green)	Queue Weight (Yellow)
0	15	20
1	15	20
2	15	20
3	15	20
4	15	20
5	15	20
6	15	20
7	20	20

The following command edits the profile you created in the previous command so that CoS 6 queues have a CIR weight of 20 instead of 15:

```
root>ethernet qos wfq-weight-profile-tbl add profile-id 2 cos0-
weight 15 cos1-weight 15 cos2-weight 15 cos3-weight 15 cos4-
weight 15 cos5-weight 15 cos6-weight 20 cos7-weight 20 cos0-
eir-weight 20 cos1-eir-weight 20 cos2-eir-weight 20 cos3-eir-
weight 20 cos4-eir-weight 20 cos5-eir-weight 20 cos6-eir-weight
20 cos7-eir-weight 20
```

Attaching a WFQ Profile to an Interface for PTP 850C and PTP 850E (CLI)

To attach a WFQ profile to an interface, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]> port-wfq set profile-id <profile-id>
```

To display which WFQ profile is attached to an interface, go to interface view for the interface and enter the following command:

```
eth type eth [1/x]> port-wfq show profile-id
```

Table 226: Attaching WFQ Profile to Interface CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 – 6	Enter the ID of one of the configured WFQ profiles.

The following command assigns WFQ Profile 3 to Eth 7:

```
eth type eth [1/7]> port-wfq set profile-id 3
```

The following is a sample display for the `port-wfq show profile-id` command:

```
eth type eth [1/7]>port-wfq show profile-id

Profile         1

CoS           Queue Weight
                (Green)

                 20
0                20
1                20
2                20
3                20
4                20
5                20
6                20
7

eth type eth [1/1]>
```

Configuring a WFQ Profile for PTP 850S (CLI)

To define a WFQ profile, enter the following command in root view:

```
root> ethernet qos wfq-weight-profile-tbl add profile-id <2-7>
cos0-weight <1-20> cos1-weight <1-20> cos2-weight <1-20> cos3-
weight <1-20> cos4-weight <1-20> cos5-weight <1-20> cos6-weight
<1-20> cos7-weight <1-20> cos0-eir-weight <1-20> cos1-eir-
weight <1-20> cos2-eir-weight <1-20> cos3-eir-weight <1-20>
cos4-eir-weight <1-20> cos5-eir-weight <1-20> cos6-eir-weight
<1-20> cos7-eir-weight <1-20>
```

To edit an existing WFQ profile, enter the following command in root view:

```
root> ethernet qos wfq-weight-profile-tbl edit profile-id <profile.id>
cos0-weight <cos0-weight> cos1-weight <cos1-weight> cos2-weight <cos2-
weight> cos3-weight <cos3-weight> cos4-weight <cos4-weight> cos5-weight
<cos5-weight> cos6-weight <cos6-weight> cos7-weight <cos7-weight>
```

To display the parameters of a WFQ profile, enter the following command in root view:

```
root> ethernet qos wfq-weight-profile-tbl show profile-id <profile-id>
```

To delete a WFQ profile, enter the following command in root view:

```
root> ethernet qos wfq-weight-profile-tbl delete profile-id <profile-id>
```

You can only delete WFQ profile if the profile is not attached to any interface.

Table 201 WFQ Profile CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	2 – 6	A unique ID to identify the profile.
cos0-weight	Number	1 - 20	The relative weight for the CoS 0 queue.
cos1- weight	Number	1 - 20	The relative weight for the CoS 1 queue.
cos2- weight	Number	1 - 20	The relative weight for the CoS 2 queue.
cos3- weight	Number	1 - 20	The relative weight for the CoS 3 queue.
cos4- weight	Number	1 - 20	The relative weight for the CoS 4 queue.
cos5- weight	Number	1 - 20	The relative weight for the CoS 5 queue.
cos6- weight	Number	1 - 20	The relative weight for the CoS 6 queue.
cos7- weight	Number	1 - 20	The relative weight for the CoS 7 queue.

Examples

The following command configures a WFQ profile with Profile ID 2.

```
root> ethernet qos wfq-weight-profile-tbl add profile-id 2 cos0-weight 15
cos1-weight 15 cos2-weight 15 cos3-weight 15 cos4-weight 15 cos5-weight 15
cos6-weight 15 cos7-weight 20
```

This profile has the parameters listed in the following table. Note that the yellow queue weight is constant and cannot be changed. This means that all best effort traffic (yellow) will always have the same weight, regardless of CoS.

Table 202 WFQ Sample Profile Parameters

CoS	Queue Weight (Green)	Queue Weight (Yellow – not visible to users, and cannot be edited)
0	15	20
1	15	20
2	15	20
3	15	20
4	15	20
5	15	20
6	15	20
7	20	20

The following command edits the profile you created in the previous command so that CoS 6 queues have a weight of 20 instead of 15:

```
root> ethernet qos wfq-weight-profile-tbl edit profile-id 2 cos0-weight 15
cos1-weight 15 cos2-weight 15 cos3-weight 15 cos4-weight 15 cos5-weight 15
cos6-weight 20 cos7-weight 20
```

Attaching a WFQ Profile to an Interface (CLI)

To attach a WFQ profile to an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> port-wfq set profile-id <profile-id>
```

To display which WFQ profile is attached to an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> port-wfq show profile-id
```

Table 203 Attaching WFQ Profile to Interface CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 – 6	Enter the ID of one of the configured WFQ profiles.

Examples

The following command assigns WFQ Profile 3 to GbE 1:

```
eth type eth [1/1]> port-wfq set profile-id 3
```

The following is a sample display for the `port-wfq show profile-id` command:

```
eth type eth [1/1]>port-wfq show profile-id

Profile ID: 1

CoS           Queue Weight
                (Green)

0                20
1                20
2                20
3                20
4                20
5                20
6                20
7                20

eth type eth [1/1]>
```

Displaying Ingress Statistics (CLI)

You can display the following statistics counters for ingress frames and bytes per interface and per service point:

- Green Frames
- Green Bytes
- Yellow Frames
- Yellow Bytes
- Red Frames
- Red Bytes

Note: Ingress statistics are displayed in granularity of 64 bits.

Service point statistics can be displayed for the service point in general or for specific CoS queues on the service point.

Displaying Ingress Statistics per Interface (CLI)

To display ingress statistics per interface, enter the following command in interface view:

```
eth type eth [x/x]>logical-port statistics show clear-in-read <yes|no>
```

The following commands display statistics for Ethernet interface Eth 7. These commands clear the counters after displaying them.

```
root>ethernet interfaces eth slot 1 port 7
eth type eth [1/7]>logical-port statistics show clear-on-read yes

_____________________________________________

| Green Packets         |                  0|

| Green Bytes           |                  0|

| Yellow Packets        |                  0|

| Yellow Bytes          |                  0|

| Red Packets           |                  0|

| Red Bytes             |                  0|

eth type eth [1/7]>
```

Displaying Ingress Statistics per Service Point (CLI)

To enable the collection of ingress statistics for a service point, enter the following command in service view:

```
service[x]>sp statistics set spid <1-32> admin-state <enable|disable>
```

To display ingress statistics for a service point, enter the following command in service view:

```
service[x]>sp statistics show spid <1-30> clear-on-read <yes|no> layer-1
<yes|no>
```

To enable the collection of ingress statistics for a specific CoS queue on a service point, enter the following command in service view:

```
service[x]>sp statistics set spid <1-32> cos <0-6> admin-state
<enable|disable>
```

To view ingress statistics for a specific CoS queue on a service point, enter the following command in service view:

```
service[x]>sp statistics show spid <1-30> cos <0-6> clear-on-read <yes|no>
layer-1 <yes|no>
```

Note: You cannot enable ingress statistics for both a service point and a CoS queue on the service point at the same time. You can, however, enable ingress statistics on multiple CoS queues at the same time.

The following commands enable and display statistics for service point 30 on service 10. These commands clear the counters after displaying them.

```
root>ethernet service sid 10
service[10]>sp statistics set spid 30 admin-state enable
service[10]>sp statistics show spid 30 clear-on-read yes layer-1 no

_____________________________________________

| Green Packets        |                   0|

| Green Bytes          |                   0|

| Yellow Packets       |                   0|

| Yellow Bytes         |                   0|

| Red Packets          |                   0|

| Red Bytes            |                   0|
|______________________|____________________|

service[10]>
```

The following commands enable and display statistics for CoS 1 of service point 1 on service 10. These commands clear the counters after displaying them.

```
root>ethernet service sid 10
service[10]>sp statistics set spid 1 cos 1 admin-state enable
service[10]>sp statistics show spid 1 cos 1 clear-on-read yes layer-1 no
_____________________________________________

| Green Packets        |                   0|

| Green Bytes          |                   0|

| Yellow Packets       |                   0|

| Yellow Bytes         |                   0|

| Red Packets          |                   0|

| Red Bytes            |                   0|
|______________________|____________________|

service[10]>
```

Displaying Egress PMs and Statistics (CLI)

PTP 850 collects egress PMs and statistics at the queue level and the service bundle level.

Displaying Queue-Level Statistics (CLI)

PTP 850 supports the following counters per queue at the queue level:

Transmitted Green Packets (64 bits counter)

Transmitted Green Bytes (64 bits counter)

Transmitted Green Bits per Second (32 bits counter)

Dropped Green Packets (64 bits counter)

Dropped Green Bytes (64 bits counter)

Transmitted Yellow Packets (64 bits counter)

Transmitted Yellow Bytes (64 bits counter)

Transmitted Yellow Bits per Second (32 bits counter)

Dropped Yellow Packets (64 bits counter)

Dropped Yellow Bytes (64 bits counter)

To display queue-level PMs, enter interface view for the interface and enter the following command:

```
eth type eth [x/x]> tm-queue show statistics service-bundle-id <service-
bundle-id> cos <cos> clear-on-read <clear-on-read> layer-1 <layer-1>
```

To clear queue-level PMs for a specific service bundle, enter interface view for the interface and enter the following command:

```
eth type eth [x/x]> tm-queue clear statistics service-bundle-id <service-
bundle-id>
```

Table 204 Egress Queue Level PMs CLI Parameters

Parameter	Input Type	Permitted Values	Description
service-bundle-id	Number	1 – 63 **Note**: In the current release, only Service Bundle 1 is supported.	The service bundle for which you want to display PMs.
cos	Number	0 - 7	The queue for which you want to display PMs.
clear-on-read	Boolean	yes no	If you enter yes, the statistics are cleared once you display them.
layer-1	Boolean	yes no	yes – Statistics are represented as Layer 1 statistics, including preamble and IFG. no – Statistics are represented as Layer 2 statistics.

The following command displays PMs for the CoS 0 queue in Service Bundle 1, on GbE 2. The PMs are cleared after they are displayed.

```
eth type eth [1/2]> tm-queue show statistics service-bundle-id 1 cos 0
clear-on-read yes layer-1 yes
```

The following command clears PMs for all queues in Service Bundle 1, on GbE 2.

```
eth type eth [1/2]> tm-queue clear statistics service-bundle-id 1
```

Configuring and Displaying Queue-Level PMs (CLI)

PTP 850E devices support advanced traffic PMs per CoS queue and service bundle. For each logical interface, you can configure thresholds for Green and Yellow traffic per queue. You can then display the following PMs for 15-minute and 24-hour intervals, per queue and color:

- Maximum bytes passed per second
- Minimum bytes passed per second
- Average bytes passed per second
- Maximum bytes dropped per second
- Minimum bytes dropped per second
- Average bytes dropped per second
- Maximum packets passed per second
- Minimum packets passed per second
- Average packets passed per second
- Maximum packets dropped per second
- Minimum packets dropped per second
- Average packets dropped per second
- Seconds bytes per second were over the configured threshold per interval

These PMs are available for any type of logical interface, including groups. To activate collection of these PMs, the user must add a PM collection rule on a logical interface and service bundle and set the relevant thresholds per CoS and Color. When the PM is configured on a group, queue traffic PMs are recorded for the group and not for the individual interfaces that belong to the group.

One collection rule is available per interface.

PMs for queue traffic are saved for 30 days, after which they are removed from the database. It is important to note that they are not persistent, which means they are not saved in the event of unit reset.

To configure and display queue-level PMs, you must first enter interface view. See *Entering Interface View (CLI).*

To display whether any service bundles are configured on an interface, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show configuration all
```

If no service bundles have been configured, the following output is displayed:

```
eth type eth [1/x]>pm tm-queue show configuration all
Num entries: 0
```

If a service bundle has been configured and enabled, the following output is displayed:

```
eth type eth [1/x]>pm tm-queue show configuration all
Service bundle: 1   Admin: enable
Num entries: 1
```

If a service bundle has been configured but it’s Admin status is disabled, the following output is displayed:

```
eth type eth [1/x]>pm tm-queue show configuration all
Service bundle: 1   Admin: disable
Num entries: 1
```

To configure a service bundle, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue create service-bundle-id <1-6> admin-state
<enable|disable>
```

To change the Admin state of a service bundle, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue set service-bundle-id <1-6> admin-state
<enable|disable>
```

To remove a service bundle, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue remove service-bundle-id <1-6>
```

For example:

```
eth type eth [1/7]>pm tm-queue remove service-bundle-id 1
WARNING: All PM history for that service bundle will be deleted.
Are you sure? (yes/no):yes
eth type eth [1/7]>
```

To display the threshold settings for a service bundle, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show configuration service-bundle-id <1-6>
```

For example:

```
eth type eth [1/7]>pm tm-queue show configuration service-bundle-id 1
Admin: enable
cos0 green  bytes passed threshold:     675000 bytes
cos1 green  bytes passed threshold:     675000 bytes
cos2 green  bytes passed threshold:     675000 bytes
cos3 green  bytes passed threshold:     675000 bytes
cos4 green  bytes passed threshold:     675000 bytes
cos5 green  bytes passed threshold:     675000 bytes
cos6 green  bytes passed threshold:     675000 bytes
cos7 green  bytes passed threshold:     675000 bytes
cos0 yellow bytes passed threshold:     675000 bytes
cos1 yellow bytes passed threshold:     675000 bytes
cos2 yellow bytes passed threshold:     100000 bytes
cos3 yellow bytes passed threshold:     675000 bytes
cos4 yellow bytes passed threshold:     675000 bytes
cos5 yellow bytes passed threshold:     675000 bytes
cos6 yellow bytes passed threshold:     675000 bytes
cos7 yellow bytes passed threshold:     675000 bytes
```

To set thresholds for green bytes, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue set service-bundle-id <1-6> cos <0-7> green-bytes-
passed-threshold <0-4294967295>
```

To set thresholds for yellow bytes, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue set service-bundle-id <1-6> cos <0-7> yellow-bytes-
passed-threshold <0-4294967295>
```

To display PMs for green bytes passed, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show counter green_bytes_passed service-bundle-id 1
cos <0-7> interval <15min|24hr>
```

To display PMs for green packets passed, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show counter green_packets_passed service-bundle-id
1 cos <0-7> interval <15min|24hr>
```

To display PMs for green bytes dropped, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show counter green_bytes_dropped service-bundle-id 1
cos <0-7> interval <15min|24hr>
```

To display PMs for green packets dropped, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show counter green_packets_dropped service-bundle-id
1 cos <0-7> interval <15min|24hr>
```

To display PMs for yellow bytes passed, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show counter yellow_bytes_passed service-bundle-id 1
cos <0-7> interval <15min|24hr>
```

To display PMs for yellow packets passed, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show counter yellow_packets_passed service-bundle-id
1 cos <0-7> interval <15min|24hr>
```

To display PMs for yellow bytes dropped, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show counter yellow_bytes_dropped service-bundle-id
1 cos <0-7> interval <15min|24hr>
```

To display PMs for yellow packets dropped, enter the following command in interface view:

```
eth type eth [1/x]> pm tm-queue show counter yellow_packets_dropped service-bundle-
id 1 cos <0-7> interval <15min|24hr>
```

The integrity column indicates whether the PM is valid:

- 0 indicates a valid entry.
- 1 indicates an invalid entry. This can occur for a number of reasons, including but not limited to a disconnected cable, a missing SFP module, muting of a radio interface, and an operational status of Down.

Displaying Service Bundle-Level Statistics (CLI)

PTP 850 supports the following counters per service bundle at the service bundle level:

Transmitted Green Packets (64 bits counter)

Transmitted Green Bytes (64 bits counter)

Transmitted Green Bits per Second (32 bits counter)

Dropped Green Packets (64 bits counter)

Dropped Green Bytes (64 bits counter)

Transmitted Yellow Packets (64 bits counter)

Transmitted Yellow Bytes (64 bits counter)

Transmitted Yellow Bits per Second (32 bits counter)

Dropped Yellow Packets (64 bits counter)

Dropped Yellow Bytes (64 bits counter)

To display service bundle-level PMs, enter interface view for the interface and enter the following command:

```
eth type eth [x/x]> tm-service-bundle show statistics service-bundle-id
<service-bundle-id> clear-on-read <clear-on-read> layer-1 <layer-1>
```

To clear service bundle-level PMs for all service bundles on an interface, enter interface view for the interface and enter the following command:

```
eth type eth [x/x]> tm-service-bundle clear statistics
```

Table 205 Egress Service Bundle Level PMs CLI Parameters

Parameter	Input Type	Permitted Values	Description
service-bundle-id	Number	1 – 63 **Note:** In the current release, only Service Bundle 1 is supported.	The service bundle for which you want to display PMs.
clear-on-read	Boolean	yes no	If you enter yes, the statistics are cleared once you display them.
layer-1	Boolean	yes no	• yes – Statistics are represented as Layer 1 statistics, including preamble and IFG. • no – Statistics are represented as Layer 2 statistics.

Examples

The following command displays service bundle PMs for Service Bundle 1, on GbE 1. The PMs are cleared after they are displayed.

```
eth type eth [1/1]> tm-service-bundle show statistics service-bundle-id 1
clear-on-read yes layer-1 yes
```

Chapter 22: Ethernet Protocols (CLI)

This section includes:

- Configuring G.8032 (CLI)
- Configuring MSTP (CLI)
- Configuring Ethernet Bandwidth Notification (ETH-BN) (CLI)
- Configuring LLDP (CLI)

Related Topics:

- Configuring Service OAM (SOAM) Fault Management (FM) (CLI)

Configuring G.8032 (CLI)

This section includes:

- Configuring the Destination MAC Address (CLI)
- Configuring ERPIs (CLI)
- Configuring the RPL Owner (CLI)
- Configuring Timers (CLI)
- Initiating a Manual or Forced Switch and Clearing the Switch or Initiating Reversion (CLI)
- Blocking or Unblocking R-APS Messages on a Service Point (CLI)
- Displaying the ERPI Attributes (CLI)

Note: P2P services are not affected by G.8032, and continue to traverse ports that are blocked by G.8032.

G.8032 cannot be configured on management ports, including management ports used for traffic (PTP 850S).

Configuring the Destination MAC Address (CLI)

To set the destination MAC address for PDUs generated by the node, enter the following command in root view:

```
root> ethernet generalcfg g8032-dest-mac-address set MAC <MAC
address>
```

To display the destination MAC address, enter the following command in root view:

```
root> ethernet generalcfg g8032-dest-mac-address show
```

To display the destination MAC address and the node ID, enter the following command in root view:

```
root> ethernet g8032 show-node-attributes
```

The node ID is the base MAC address for the node.

Table 233: G.8032 Destination MAC Address CLI Parameters

Parameter	Input Type	Permitted Values	Description
MAC address	Six groups of two hexadecimal digits	01:19:a7:00:00:x where x can be any number between 0 and 16.	The destination MAC address for PDUs generated by the node.

The following command sets the destination MAC address as 01:19:a7:00:00:02:

```
root> ethernet generalcfg g8032-dest-mac-address set MAC
01:19:a7:00:00:02
```

Configuring ERPIs (CLI)

You can configure up to 16 Ethernet Ring Protection instances (ERPIs). Each ERPI is associated with an Ethernet service defined in the system. An ERPI can be:

- **Ring**: A Ring is an Ethernet ring that is connected on two ports (East and West service points) to an interconnection node.
- **Sub-Ring**: A Sub-Ring is an Ethernet ring which is connected to another ring or network through the use of interconnection nodes (East and West service points). On their own, the Rub-Ring links do not form a closed physical loop. A closed loop may be formed by the sub-ring links and the link between interconnection nodes that is controlled by other ring or network.
- **Ring with Sub-Ring**: The ERPI includes both a ring, with East and West service points, and a connection to a sub-ring using a Sub-Ring service point.

Note: Service points on the PTP 820 side of the link must have a single, determinate VLAN. This means the service point type must be dot1q, s-tag, or QinQ. On the customer side, any service point type can be used.

To add a Ring ERPI, enter the following command in root view:

```
root> ethernet g8032 create-erpi erp-type ring erpi-id <erpi-
id> erpi-service-id <erpi-service-id> west-sp <west-sp> east-sp
<east-sp> level <level> version <version>
```

To add a Sub-Ring ERPI, enter the following command in root view:

```
root> ethernet g8032 create-erpi erp-type sub-ring erpi-id
<erpi-id> erpi-service-id <erpi-service-id> west-sp <west-sp>
east-sp <east-sp> level <level> version <version>
```

To add a Ring with Sub-Ring ERPI, enter the following command in root view:

```
root> ethernet g8032 create-erpi erp-type ring-with-sub-ring
erpi-id <erpi-id> erpi-service-id <erpi-service-id> west-sp
<west-sp> east-sp <east-sp> sub-ring-sp <sub-ring-sp> level
<level> version <version>
```

To assign a name to an ERPI, enter the following command in root view:

```
root> ethernet g8032 set-erpi-name erpi-id <erpi-id> erpi-name
<erpi-name>
```

To delete an ERPI, enter the following command in root view:

```
root> ethernet g8032 delete-erpi erpi-id 1
```

Table 234: G.8032 ERPI Configuration CLI Parameters

Parameter	Input Type	Permitted Values	Description
erpi-id	Number	1-64	A unique ID that identifies the ERPI.
erpi-service-	Number	1-4095	The ID of the Ethernet service to which the ERPI belongs.
west-sp	Number	1-32	The first endpoint for the ERPI. This can be any service point that has been configured for the

east-sp	Number	1-32	The second endpoint for the ERPI. This can be any service point that has been configured for
sub-ring-sp	Number	1-32	The service point that connects the Ring with the Sub- Ring. This can be any service point that has been configured for the service.
level	Number	0-7	Optional. The Maintenance Entity Group (MEG) level used for R-APS messages sent in the ERPI.
version	Number	1-2	Optional. The ERPI (G.8032) protocol version currently being used in the unit.
erpi-name	Text		A descriptive name for the ERPI.

The following commands create a Ring ERPI with ID 1, and name the ERPI "service_x". This ERPI is associated with Ethernet Service 1. The end points of the ERPI are Service Point 1 and Service Point 2. The ERPI is configured with MEG level 2:

```
root> ethernet g8032 create-erpi erp-type ring erpi-id 1 erpi-
service-id 1 west-sp 1 east-sp 2 level 2
root> ethernet g8032 set-erpi-name erpi-id 1 erpi-name
service_x
```

The following commands create a Sub-Ring ERPI with ID 10, and name the ERPI "Sub_ring". This ERPI is associated with Ethernet Service 20. The end points of the ERPI are Service Point 1 and Service Point 2. The ERPI is configured with MEG level 4:

```
root> ethernet g8032 create-erpi erp-type sub-ring erpi-id 10
erpi-service-id 20 west-sp 1 east-sp 2 level 4
root> ethernet g8032 set-erpi-name erpi-id 1 erpi-name Sub_ring
```

The following commands create a Ring with Sub-Ring ERPI with ID 20, and name the ERPI "RSRi". This ERPI is associated with Ethernet Service 30. The end points of the ERPI are Service Point 1 and Service Point 2, and the point of connection between the Ring and the Sub-Ring is Service Point 3. The ERPI is configured with MEG level 5:

```
root> ethernet g8032 create-erpi erp-type ring-with-sub-ring
erpi-id 20 erpi-service-id 30 west-sp 1 east-sp 2 sub-ring-sp 3
level 5
root> ethernet g8032 set-erpi-name erpi-id 1 erpi-name RSRi
```

The following command deletes ERPI 1:

```
root> ethernet g8032 delete-erpi erpi-id 1
```

Configuring the RPL Owner (CLI)

The RPL Owner Node is a node in the ERPI that is responsible for blocking traffic at one end of the ERPI. You can select one RPL per ERPI.

To set the RPL Owner Node, enter the following command in root view:

```
root> ethernet g8032 set-rpl-owner erpi-id <erpi-id> SP <SP>
```

To remove the RPL Owner Node, enter the following command in root view:

```
root> ethernet g8032 remove-rpl-owner erpi-id <erpi-id>
```

Table 235: G.8032 RPL Owner CLI Parameters

Parameter	Input Type	Permitted Values	Description
erpi-id	Number	1-64	The ID of the ERPI for which you want to set or delete the RPL owner.
SP	Number or Variable	east west sub-ring	Specifies the service point you want to designate as the RPL owner.

The following command sets the East service point as the RPL owner for ERPI 1:

```
root> ethernet g8032 set-rpl-owner erpi-id 1 SP east
```

The following command sets the Sub-Ring service point as the RPL owner for ERPI 20:

```
root> ethernet g8032 set-rpl-owner erpi-id 20 SP sub-ring
```

The following command removes the RPL owner for ERPI 1

Configuring Timers (CLI)

You can configure timers per ERPI to control the ERPI's switching and convergence parameters. The following timers are available:

- **Wait to Restore (WTR) Timer** – Defines a minimum time the system waits after signal failure is recovered before reverting to idle state, when the RPL can again be blocked.
- **Guard Time** – The guard time is the minimum time the system waits after recovery from a signal failure before accepting new R-APS messages. The Guard Time should be greater than the maximum expected forwarding delay for which one R-APS message circles around the ring.

Note: The Guard Time is used to prevent Ethernet ring nodes from acting upon outdated R-APS messages and prevents the possibility of forming a closed loop.

- **Hold-Off Time** – Determines the time period from failure detection to response. It is used to coordinate between recovery mechanisms (which mechanism takes place first).

To configure the WTR timer, enter the following command in root view:

```
root> ethernet g8032 set-wtr erpi-id <erpi-id> wtr <wtr>
```

To configure the guard time, enter the following command in root view:

```
root> ethernet g8032 set-guard-time erpi-id <erpi-id> guard-
time <guard-time>
```

To configure the hold-off, enter the following command in root view:

```
root> ethernet g8032 set-holdoff-time erpi-id <erpi-id>
holdoff-time <holdoff-time>
```

Table 236: G.8032 Timer Configuration CLI Parameters

Parameter	Input Type	Permitted Values	Description
erpi-id	Number	1-64	The ID of the ERPI for which you want to set
wtr	Number	1-12	The minimum time (in minutes) the system waits after signal failure is recovered before reverting to idle state.
guard-time	Number	10-2000, in multiples of 10	The minimum time (in msec) the system waits after recovery from a signal failure before accepting new R-APS messages.
holdoff-time	Number	0-10000, in multiples of 100	The minimum time (in msec) the system waits before reacting to a signal failure.

The following command sets the WTR timer for ERPI 1 to 2 minutes:

```
root> ethernet g8032 set-wtr erpi-id 1 wtr 2
```

The following command sets the guard time for ERPI 1 to 20 msecs:

```
root> ethernet g8032 set-guard-time erpi-id 1 guard-time 20
```

The following command sets the hold-off time for ERPI 1 to 1000 msecs:

```
root> ethernet g8032 set-holdoff-time erpi-id 1 holdoff-time
1000
```

Initiating a Manual or Forced Switch and Clearing the Switch or Initiating Reversion (CLI)

To initiate a forced switch, enter the following command in root view:

```
root> ethernet g8032 fs-erpi erpi-id <erpi-id> SP <SP>
```

To initiate a manual switch, enter the following command in root view:

```
root> ethernet g8032 ms-erpi erpi-id <erpi-id> SP <SP>
```

You can use a "clear" command to clear a forced or manual switch. You can also use a "clear" command to trigger convergence prior to the expiration of the relevant timer. To issue a "clear" command, enter the following command in root view:

```
root> ethernet g8032 clear-erpi erpi-id <erpi-id> SP <SP>
```

Table 237: G.8032 Switching and Reversion CLI Parameters

Parameter	Input Type	Permitted Values	Description
erpi-id	Number	1-64	The ID of the ERPI on which you want to perform or clear the switch or initiate convergence.
SP	Number or Variable	east west sub-ring	Specifies the service point on which to clear the manual or forced switch or to implement convergence.

The following command initiates a forced switch in the East service point of ERPI 1:

```
root> ethernet g8032 fs-erpi erpi-id 1 SP east
```

The following command initiates a manual switch in the Sub-Ring service point of ERPI 20:

```
root> ethernet g8032 ms-erpi erpi-id 20 SP sub-ring
```

The following command initiates convergence in the East service point of ERPI 1:

```
root> ethernet g8032 clear-erpi erpi-id 1 SP east
```

Blocking or Unblocking R-APS Messages on a Service Point (CLI)

To enable or disable transmission of R-APS messages on a service point, enter the following command in root view:

```
root> ethernet g8032 set-erpi-sp-tx-raps-cntrl erpi-id <erpi-
id> SP <SP> tx-raps <tx-raps>
```

Table 238: G.8032 Switching and Reversion CLI Parameters

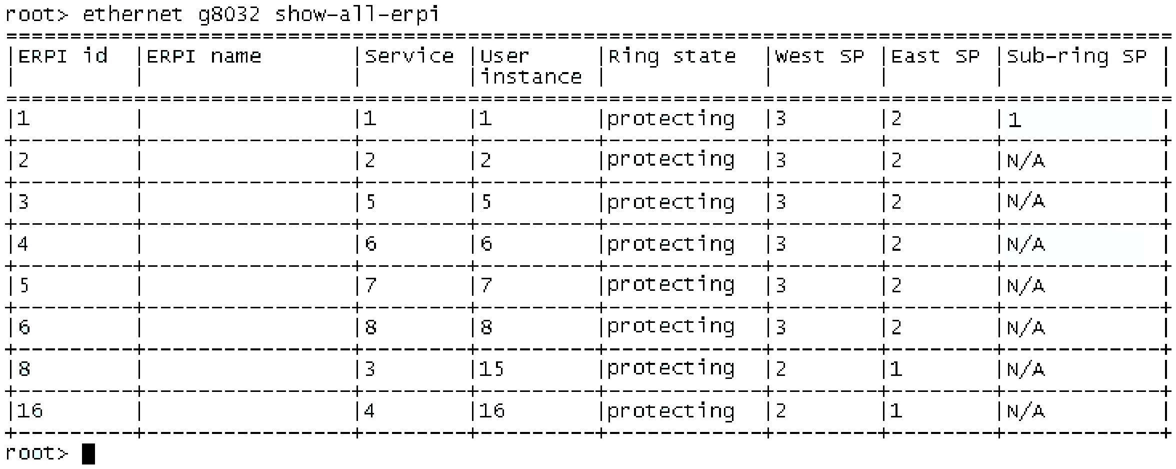
Parameter	Input Type	Permitted Values	Description
erpi-id	Number	1-64	The ID of the ERPI on which you want to perform or clear the switch or initiate convergence.
SP	Variable	east west sub-ring	Specifies the service point on which to clear the manual or forced switch or to implement convergence.
tx-raps	Variable	true false	`true` – R-APS message transmission is enabled on the service point. `false` – R-APS message transmission is blocked on the service point.

Displaying the ERPI Attributes (CLI)

To display a list of all ERPIs configured on the unit, enter the following command in root view:

```
root> ethernet g8032 show-all-erpi
```

The following is an example of this command's output.



```
root> ethernet g8032 show-all-erpi
==============================================================================================
|ERPI id   |ERPI name         |Service |User     |Ring state   |West SP  |East SP  |Sub-ring SP |
|          |                  |        |instance |             |         |         |            |
==============================================================================================
|1         |                  |1       |1        |protecting   |3        |2        |1           |
+----------+------------------+--------+---------+-------------+---------+---------+------------+
|2         |                  |2       |2        |protecting   |3        |2        |N/A         |
+----------+------------------+--------+---------+-------------+---------+---------+------------+
|3         |                  |5       |5        |protecting   |3        |2        |N/A         |
+----------+------------------+--------+---------+-------------+---------+---------+------------+
|4         |                  |6       |6        |protecting   |3        |2        |N/A         |
+----------+------------------+--------+---------+-------------+---------+---------+------------+
|5         |                  |7       |7        |protecting   |3        |2        |N/A         |
+----------+------------------+--------+---------+-------------+---------+---------+------------+
|6         |                  |8       |8        |protecting   |3        |2        |N/A         |
+----------+------------------+--------+---------+-------------+---------+---------+------------+
|8         |                  |3       |15       |protecting   |2        |1        |N/A         |
+----------+------------------+--------+---------+-------------+---------+---------+------------+
|16        |                  |4       |16       |protecting   |2        |1        |N/A         |
+----------+------------------+--------+---------+-------------+---------+---------+------------+
root> █
```

To display all ERPIs that include a service point on a specific port, enter the following command in root view:

```
root> ethernet g8032 show-all-port-erpi interface <interface>
slot <slot> port <port>
```

To display all ERPIs that include a service point on a specific group, enter the following command in root view:

```
root> ethernet g8032 show-all-port-erpi group <group>
```

The following command displays all ERPIs with a service point on LAG group 1:

```
root> ethernet g8032 show-all-port-erpi group lag1
```

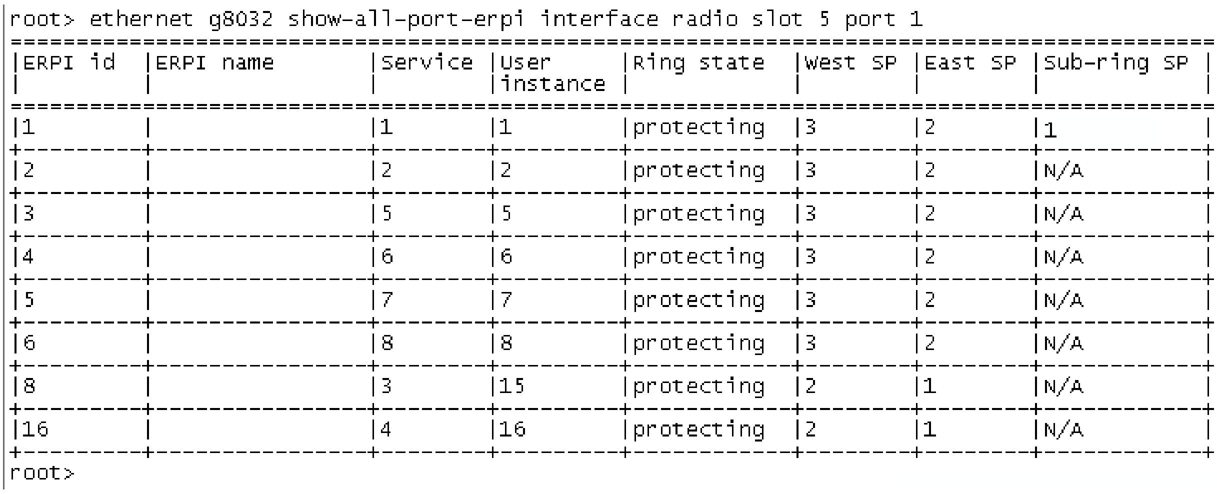
The following command displays all ERPIs with a service point on HSB protection group 2:

```
root> ethernet g8032 show-all-port-erpi group rp2
```

The following command displays all ERPIs with a service point on Multi-Carrier ABC group 1:

```
root> ethernet g8032 show-all-port-erpi group mc-abc1
```

The following is an example of this command's output.



```
root> ethernet g8032 show-all-port-erpi interface radio slot 5 port 1
===========================================================================================
|ERPI id  |ERPI name       |Service |User     |Ring state  |West SP |East SP |Sub-ring SP |
|         |                |        |instance |            |        |        |            |
===========================================================================================
|1        |                |1       |1        |protecting  |3       |2       |1           |
+---------+----------------+--------+---------+------------+--------+--------+------------+
|2        |                |2       |2        |protecting  |3       |2       |N/A         |
+---------+----------------+--------+---------+------------+--------+--------+------------+
|3        |                |5       |5        |protecting  |3       |2       |N/A         |
+---------+----------------+--------+---------+------------+--------+--------+------------+
|4        |                |6       |6        |protecting  |3       |2       |N/A         |
+---------+----------------+--------+---------+------------+--------+--------+------------+
|5        |                |7       |7        |protecting  |3       |2       |N/A         |
+---------+----------------+--------+---------+------------+--------+--------+------------+
|6        |                |8       |8        |protecting  |3       |2       |N/A         |
+---------+----------------+--------+---------+------------+--------+--------+------------+
|8        |                |3       |15       |protecting  |2       |1       |N/A         |
+---------+----------------+--------+---------+------------+--------+--------+------------+
|16       |                |4       |16       |protecting  |2       |1       |N/A         |
+---------+----------------+--------+---------+------------+--------+--------+------------+
root>
```

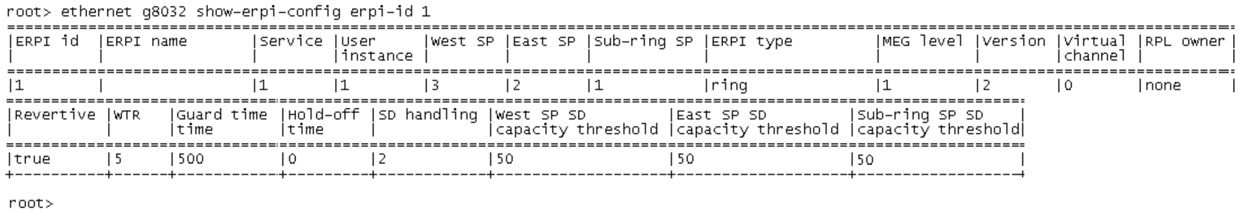
To display detailed information about a specific ERPI, enter the following command in root view:

```
root> ethernet g8032 show-erpi-config erpi-id <erpi-id>
```

The following command displays detailed output for ERPI 1:

```
root> ethernet g8032 show-erpi-config erpi-id 1
```

The following is an example `of this command's output.



```
root> ethernet g8032 show-erpi-config erpi-id 1
=========================================================================================================================================
|ERPI id  |ERPI name       |Service |User     |West SP |East SP |Sub-ring SP |ERPI type         |MEG level |Version |Virtual |RPL owner |
|         |                |        |instance |        |        |            |                  |          |        |channel |          |
=========================================================================================================================================
|1        |                |1       |1        |3       |2       |1           |ring              |1         |2       |0       |none      |
===============================================================================================================
|Revertive |WTR   |Guard time |Hold-off |SD handling |West SP SD        |East SP SD        |Sub-ring SP SD    |
|          |      |time       |time     |            |capacity threshold|capacity threshold|capacity threshold|
===============================================================================================================
|true      |5     |500        |0        |2           |50                |50                |50                |
+----------+------+-----------+---------+------------+------------------+------------------+------------------+

root>
```

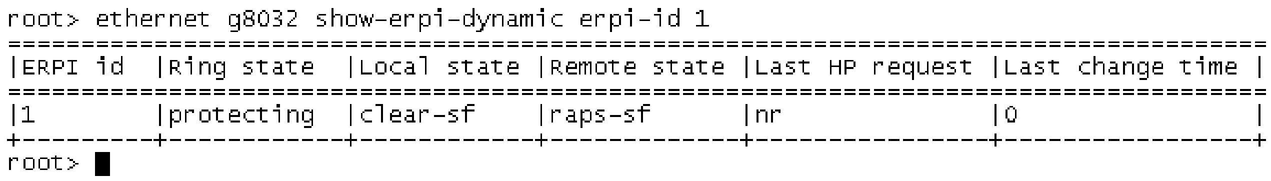
To display state information about a specific ERPI, enter the following command in root view:

```
root> ethernet g8032 show-erpi-dynamic erpi-id <erpi-id>
```

The following command displays detailed output for ERPI 1:

```
root> ethernet g8032 show-erpi-dynamic erpi-id 1
```

The following is an example of this command's output.



```
root> ethernet g8032 show-erpi-dynamic erpi-id 1
==================================================================================
|ERPI id  |Ring state  |Local state |Remote state |Last HP request |Last change time |
==================================================================================
|1        |protecting  |clear-sf    |raps-sf      |nr              |0                |
+---------+------------+------------+-------------+----------------+-----------------+
root> █
```

Table 239: G.8032 ERPI Display Command Input Parameters

Parameter	Input Type	Permitted Values	Description
interface	Variable	eth radio	Enter the type of interface: eth – Ethernet radio – Radio
slot	Number	Ethernet: 1 Radio: • PTP 850C and PTP 850E: 1 PTP 850S: 2	
port	Number	• Ethernet interface on PTP 850C: 1-4 • Ethernet interface on PTP 850E: 1-7 • Ethernet interface on PTP 850S: 1-3 • Radio interface on an PTP 850C: 1-2 Radio interface on an PTP 850E or PTP	The port number of the interface.
group	Variable	lag1 lag2 lag3 lag4 mc-abc1 mc-abc2 mc-abc3 mc-abc4	To enter interface view for a LAG group, enter the group (lag1 - lag4). To enter interface view for a Multi-Carrier ABC group, enter the group (mc-abc1 – mc-abc4) (PTP 850C only).
erpi-id	Number	1-64	The ID of the ERPI for which you want to perform or clear the switch, initiate convergence, or display information.

Table 240: G.8032 ERPI Display Command Output Parameters

Parameter	Description
ERPI ID	A unique ID that identifies the ERPI.
ERPI Name	A descriptive name for the ERPI.
Service	The ID of the Ethernet service to which the ERPI belongs.
User Instance	The MSTI to which the Ethernet service is mapped.

Parameter	Description
Ring State	Indicates the current ERPI state. Possible values are: Initializing Idle Pending Protecting FS (Forced Switch) MS (Manual Switch)
West SP	The interface to which the west ERPI service point belongs.
East SP	The interface to which the east ERPI service point belongs.
Sub-Ring SP	The interface to which the ERPI service point that connects the Ring to the Sub-Ring belongs.
ERPI Type	The ERPI type (Ring, Sub-Ring, or Ring with Sub-Ring).
MEG Level	The Maintenance Entity Group (MEG) level used for R-APS messages sent in the ERPI.
Version	The ERPI (G.8032) protocol version currently being used in the unit.
Virtual Channel	Reserved for future use.
RPL Owner	Indicates whether the ERPI is currently an RPL owner, and if it is, which ERPI port is the owner.
Revertive	Indicates whether the ERPI is currently in revertive mode.
WTR	The Wait to Restore (WTR) timer. This timer sets the minimum time (in minutes) the system waits after signal failure before entering revertive mode.
Guard Time	The minimum time (in msec) the system waits after recovery from a signal failure before accepting new R-APS messages. The purpose of this timer is to prevent unnecessary state changes that might be caused by outdated messages.
Hold-Off Time	The minimum time (in msec) the system waits before reacting to a signal failure.
SD Handling	Reserved for future use.
West SP SD Capacity Threshold	Reserved for future use.
East SP SD Capacity Threshold	Reserved for future use.
Sub-Ring SP SD Capacity Threshold	Reserved for future use.
Local State	The current local state input to the ERPI state machine.
Remote State	The last event received from the other end of the link.
Last HP Request	The last high priority request.
Last Change Time	The time of the last ring state transition.

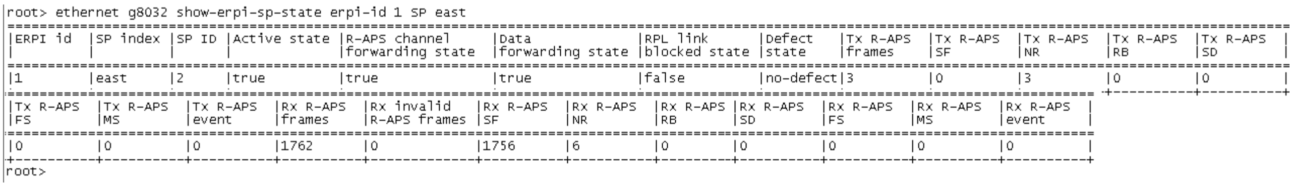
To display the state of a specific service point, enter the following command in root view:

```
root> ethernet g8032 show-erpi-sp-state erpi-id <erpi-id> SP
<SP>
```

The following command displays the current state of the East service point for ERPI 1:

```
root> ethernet g8032 show-erpi-sp-state erpi-id 1 SP east
```

The following is an example of this command's output.



```
root> ethernet g8032 show-erpi-sp-state erpi-id 1 SP east
===============================================================================================================================================================
|ERPI id  |SP index |SP ID |Active state |R-APS channel    |Data             |RPL link       |Defect   |Tx R-APS  |Tx R-APS  |Tx R-APS  |Tx R-APS  |Tx R-APS  |
|         |         |      |             |forwarding state |forwarding state |blocked state  |state    |frames    |SF        |NR        |RB        |SD        |
===============================================================================================================================================================
|1        |east     |2     |true         |true             |true             |false          |no-defect|3         |0         |3         |0         |0         |
========================================================================================================================================+----------+----------+
|Tx R-APS  |Tx R-APS  |Tx R-APS  |Rx R-APS  |Rx invalid  |Rx R-APS  |Rx R-APS  |Rx R-APS  |Rx R-APS  |Rx R-APS  |Rx R-APS  |Rx R-APS  |
|FS        |MS        |event     |frames    |R-APS frames|SF        |NR        |RB        |SD        |FS        |MS        |event     |
=======================================================================================================================================
|0         |0         |0         |1762      |0           |1756      |6         |0         |0         |0         |0         |0         |
+----------+----------+----------+----------+------------+----------+----------+----------+----------+----------+----------+----------+
root>
```

Table 241: G.8032 Service Point Display Command Output Parameters

Parameter	Description
ERPI ID	A unique ID that identifies the ERPI.
SP Index	Identifies the service point in the ERPI.
SP ID	The Service Point ID.
Active State	Indicates whether or not the service point is active for traffic forwarding.
R-APS Channel Forwarding State	Indicates whether the service point is forwarding R-APS messages.
Data Forwarding State	Indicates whether the service point is in unblocked (forwarding) state.
RPL Link Blocked State	Only relevant if the ERPI to which the service point belongs is the RPL owner. Indicates whether the service point is in blocked state.
Defect State	Indicates whether the service point is in Signal Fail (SF) or Signal Defect (SD) state. **Note:** Support for Signal Defect state is planned for future release.
TX R-APS Frames	The number of R-APS frames that have been transmitted via the service point.
TX R-APS SF	The number of R-APS Signal Fail (SF) frames that have been transmitted via the service point.
TX R-APS NR	The number of R-APS No Request (NR) frames that have been transmitted via the service point.
TX R-APS RB	The number of R-APS RPL Blocked (RB) frames that have been transmitted via the service point.
TX R-APS SD	The number of R-APS Signal Degrade (SD) frames that have been transmitted via the service point.

Parameter	Description
TX R-APS FS	The number of R-APS Forced Switch (FS) frames that have been transmitted via the service point.
TX R-APS MS	The number of R-APS Manual Switch (MS) frames that have been transmitted via the service point.
TX R-APS Event	Reserved for future use.
RX R-APS Frames	The number of R-APS frames that have been received by the service point.
RX Invalid R-APS Frames	The number of R-APS frames with an invalid format that have been received by the service point.
RX R-APS SF	The number of R-APS Signal Fail (SF) frames that have been received by the service point.
RX R-APS NR	The number of R-APS No Request (NR) frames that have been received by the service point.
TX R-APS RB	The number of R-APS RPL Blocked (RB) frames that have been transmitted by the service point.
TX R-APS SD	The number of R-APS Signal Degrade (SD) frames that have been transmitted by the service point.
TX R-APS FS	The number of R-APS Forced Switch (FS) frames that have been transmitted by the service point.
TX R-APS MS	The number of R-APS Manual Switch (MS) frames that have been transmitted by the service point.
TX R-APS Event	Reserved for future use.

Configuring MSTP (CLI)

This section includes:

- *Configuring the MSTP Bridge Parameters (CLI)*
- *Configuring the MSTP Port Parameters (CLI)*

Note: P2P services are not affected by MSTP, and continue to traverse ports that are blocked by MSTP.

MSTP cannot be configured on management ports, including management ports used for traffic (PTP 850S).

Configuring the MSTP Bridge Parameters (CLI)

This section includes:

- Enabling and Disabling MSTP (CLI)
- Defining the Number of MSTIs (CLI)
- Setting the BPDU Destination MAC Address (CLI)
- Freezing MSTP (CLI)
- Resetting the MSTP Stack (CLI)
- Handling Signal Degrade (SD) Failures (CLI)
- Setting the Configuration ID (CLI)
- Mapping Services to MSTIs (CLI)
- Setting the Bridge Level Spanning Tree Parameters (CLI)
- Setting and Viewing the Bridge Level MSTI Parameters (CLI)
- Viewing the MSTP Parameters (CLI)

Enabling and Disabling MSTP (CLI)

Enabling MSTP starts the protocol and sets all port states in all MSTP instances to Blocking. Convergence upon enabling the protocol generally takes less than two seconds.

Note: All mapping of Ethernet services to MSTP instances (MSTIs) should be performed *before* enabling MSTP, For instructions, see *Mapping Services to MSTIs (CLI)*.

To enable MSTP on the unit, enter the following command in root view:

```
root> ethernet mstp mstp-enable
```

Disabling MSTP stops the MSTP protocol from running and sets all ports in all MSTP instances to Forwarding state.

To disable MSTP on the unit, enter the following command in root view:

```
root> ethernet mstp mstp-disable
```

To display whether MSTP is currently enabled or disabled on the unit, enter the following command in root view:

```
root> ethernet mstp show-mstp-enabled
```

Defining the Number of MSTIs (CLI)

PTP 820C and PTP 820V can support from 1 to 16 Multiple Spanning Tree Instances (MSTIs) on a single unit. This does not include the Common and Internal Spanning Tree (CIST).

To specify the number of MSTIs, enter the following command in root view:

```
root> ethernet mstp set number-of-instances <MSTI>
```

To display the number of MSTIs on the unit, enter the following command in root view:

```
root> ethernet mstp show-number-of-instances
```

Table 242: Defining Number of MSTIs CLI Parameters

Parameter	Input Type	Permitted Values	Description
MSTI	Number	2-16	The number of MSTIs on the unit. This number does not include the Common and Internal Spanning Tree (CIST).

The following command sets the number of MSTIs to 14:

```
root> ethernet mstp set number-of-instances 14
```

Setting the BPDU Destination MAC Address (CLI)

To specify the destination MAC address for BPDUs generated in the unit, enter the following command in root view:

```
root> ethernet mstp set bpdu-destination-mac <bpdu-destination-
mac>
```

Table 243: BPDU Destination MAC Address CLI Parameters

Parameter	Input Type	Permitted Values	Description
bpdu-destination-mac	Variable	customer provider	`customer` – The destination MAC address of BPDUs is 0x0180-C200-0000. Provider BPDUs are either tunneled or discarded. `provider` – The destination MAC address of BPDUs is 0x0180-C200-0008. Customer BPDUs are either tunneled or discarded.

Freezing MSTP (CLI)

You can freeze MSTP in the unit. When MSTP is frozen, BPDUs are neither transmitted nor processed, and all port states are maintained as they were before MSTP was frozen.

To freeze MSTP, enter the following command in root view:

```
root> ethernet mstp mstp-freeze
```

To unfreeze MSTP, enter the following command in root view:

```
root> ethernet mstp mstp-defreeze
```

To display whether MSTP is or is not currently frozen in the unit, enter the following command in root view:

```
root> ethernet mstp show-mstp-frozen
```

Resetting the MSTP Stack (CLI)

To reset MSTP on the unit, enter the following command in root view:

```
root> ethernet mstp mstp-reset
```

19.2.1.1 Handling Signal Degrade (SD) Failures (CLI)

Signal Degrade failures (SD) can either be ignored or treated the same as SF, which means an SD failure triggers a topology change.

To determine how SD failures are treated, enter the following command in root view:

```
root> ethernet mstp set sd-handling <sd-handling>
```

Table 244: MSTP Signal Degrade Failure CLI Parameters

Parameter	Input Type	Permitted Values	Description
sd-handling	Variable	ignored same-as-SF	`ignored` – Signal Degrade (SD) failures are ignored in MSTP. `same-as-SF` – MSTP handles SD failures the same as Signal Failure, i.e., an SD failure triggers a topology change.

Setting the Configuration ID (CLI)

The configuration ID attributes include the Configuration Name and the Revision Level. These attributes are part of the Bridge Configuration Identifier.

To set the configuration ID attributes, enter the following command in root view:

```
root> ethernet mstp set configuration-name <configuration-name>
revision-level <revision-level>
```

To display the configuration ID attributes, enter the following command in root view:

```
root> ethernet mstp show-config-id
```

Table 245: MSTP Configuration ID CLI Parameters

Parameter	Input Type	Permitted Values	Description
configuration-name	Text String		The IEEE 802.1Q Configuration Name. The Configuration Name is part of the bridge configuration Identifier.
revision-level	Number	0-65535	The IEEE 802.1Q Revision Level. The Revision Level is part of the bridge configuration Identifier.

Mapping Services to MSTIs (CLI)

By default, all Ethernet services are assigned to MSTI 0 (CIST). You can map Ethernet services to other MSTIs.

Note: All mapping of Ethernet services to MSTP instances (MSTIs) should be performed *before* enabling MSTP.

To assign a service to another MSTI, enter the following command in root view:

```
root> ethernet generalcfg instance-to-service-mapping set
service sid <sid> instance-id <instance-id>
```

To assign a range of services to another MSTI, enter the following command in root view:

```
root> ethernet generalcfg instance-to-service-mapping set
service sid <sid> to <sid> instance-id <instance-id>
```

To display the service to MSTI mapping for a specific service, enter the following command in root view:

```
root> ethernet generalcfg instance-to-service-mapping show
service sid <sid>
```

To display the service to MSTI mapping for a range of services, enter the following command in root view:

```
root> ethernet generalcfg instance-to-service-mapping show
service sid <sid> to <sid>
```

Table 246: MSTP Service to MSTI Mapping CLI Parameters

Parameter	Input Type	Permitted Values	Description
sid	Number or Range	Any Ethernet service or range of services configured in the unit.	The service ID.
instance-id	Number	1-16, 4095	The MSTI to which you want to map the service.

The following command assigns Service 1 to MSTI 2:

```
root> ethernet generalcfg instance-to-service-mapping set
service sid 1 instance-id 2
```

The following command assigns Services 1 through 10 to MSTI 2:

```
root> ethernet generalcfg instance-to-service-mapping set
service sid 1 to 10 instance-id 2
```

The following command displays the service to MSTI mapping for services 1 through 1000:

```
root> ethernet generalcfg instance-to-service-mapping show
service sid 1 to 1000
```

Setting the Bridge Level Spanning Tree Parameters (CLI)

The bridge level spanning tree parameters determine most of the bridge MSTP parameters, including parameters that are applied to all bridges when this bridge is acting as the root.

To set the CIST bridge priority, enter the following command in root view:

```
root> ethernet mstp set cist-bridge-priority <cist-bridge-
priority>
```

To set the CIST hold time, enter the following command in root view:

```
root> ethernet mstp set cist-bridge-hold-time <cist-bridge-
hold-time>
```

To set the CIST maximum age, enter the following command in root view:

```
root> ethernet mstp set cist-bridge-max-age <cist-bridge-max-
age>
```

To set the CIST forward delay, enter the following command in root view:

```
root> ethernet mstp set cist-bridge-forward-delay <cist-bridge-
forward-delay>
```

To set the CIST Hello Time, enter the following command in root view:

```
root> ethernet mstp set cist-bridge-hello-time <cist-bridge-
hello-time>
```

To set the CIST maximum number of hops, enter the following command in root view:

```
root> ethernet mstp set cist-bridge-max-hops <cist-bridge-max-
hops>
```

Table 247: MSTP Bridge Level Spanning Tree CLI Parameters

Parameter	Input Type	Permitted Values	Description
cist-bridge-priority	Number	0-61440, in steps of 4096.	Enter a value as the writeable portion of the Bridge ID. This value constitutes the first two octets of the Bridge ID.
cist-bridge-hold-time	Number	10-100	Enter a value (in cs) as the interval length during which no more than two configuration bridge PDUs will be transmitted by this node.
cist-bridge-max-age	Number	600-4000	Enter a value (in cs) that all bridges will use, when this bridge is the root, as the maximum age of MSTP information learned from the network
cist-bridge-forward- delay	Number	400-3000	Enter a value (in cs) that all bridges will use, when this bridge is the root, as the speed at which ports change their spanning state when moving
cist-bridge-hello-time	Number	100-1000	Enter the value (in cs) that all bridges will use, when this bridge is the root, as the Hello Time. The Hello Time determines how often the switch
cist-bridge-max-hops	Number	6-40	Enter the value that all bridges will use, when this bridge is the root, as the maximum number of hops allowed for a BPDU within a region

Setting and Viewing the Bridge Level MSTI Parameters (CLI)

To set the bridge priority for an MSTI, enter the following command in root view:

```
root> ethernet mstp set instance <msti-id> msti-bridge-priority
<msti-bridge-priority>
```

To display the bridge parameters of an MSTI, enter the following command in root view:

```
root> ethernet mstp show-msti-attributes instance <msti-id>
```

Table 248: Bridge Level MSTI CLI Parameters

Parameter	Input Type	Permitted Values	Description
instance	Number	1-16	Enter the MSTI ID of the MSTI you want to configure.

Parameter	Input Type	Permitted Values	Description
msti-bridge-priority	Number	0-61440, in steps of 4096.	The MSTI writeable portion of the Bridge ID.
interface	Variable	eth radio pwe	Enter the type of interface: eth – Ethernet radio – Radio pwe – TDM
slot	Number	Ethernet: 1 Radio: • PTP 850C and PTP 850E: 1 PTP 850S: 2	
port	Number	• Ethernet interface on PTP 850C: 1-4 • Ethernet interface on PTP 850E: 1-7 • Ethernet interface on PTP 850S: 1-3 • Radio interface on an PTP 850C: 1-2 • Radio interface on an PTP 850E or PTP	The port number of the interface.
group	Variable	lag1 lag2 lag3 lag4 mc-abc1 mc-abc2 mc-abc3 mc-abc4	To enter interface view for a LAG group, enter the group (lag1 - lag4). To enter interface view for a Multi-Carrier ABC group, enter the group (mc-abc1 – mc-abc4) (PTP 850C only).

The following command sets the bridge priority for MSTI 15 to 28672:

```
root> ethernet mstp set instance 15 msti-bridge-priority 28672
```

The following command displays the bridge parameters of MSTI 10:

```
root> ethernet mstp show-msti-attributes instance 10
```

Viewing the MSTP Parameters (CLI)

To display the general MSTP parameters, enter the following command in root view:

```
root> ethernet mstp show-gen-attributes
```

Configuring the MSTP Port Parameters (CLI)

This section includes:

- Configuring and Viewing the CIST Port Parameters (CLI)
- Configuring and Viewing the MSTI Port Parameters (CLI)
- Viewing and Resetting Port BPDU Counters (CLI)

Configuring and Viewing the CIST Port Parameters (CLI)

To set the CIST port priority of a port, enter the following command in root view:

```
root> ethernet mstp set interface <interface> slot <slot> port
<port> cist-port-priority <cist-port-priority>
```

To set the CIST port priority of an interface group, enter the following command in root view:

```
root> ethernet mstp set group <group> cist-port-priority <cist-
port-priority>
```

To set the CIST path cost of a port, enter the following command in root view:

```
root> ethernet mstp set interface <interface> slot <slot> port
<port> cist-port-path-cost <cist-port-path-cost>
```

To set the CIST path cost of an interface group, enter the following command in root view:

```
root> ethernet mstp set group <group> cist-port-path-cost
<cist-port-path-cost>
```

To set a port's administrative edge port parameter for the CIST, enter the following command in root view:

```
root> ethernet mstp set interface <interface> slot <slot> port
<port> cist-port-edge-port <cist-port-edge-port>
```

To set an interface group's administrative edge port parameter for the CIST, enter the following command in root view:

```
root> ethernet mstp set group <group> cist-port-edge-port
<cist-port-edge-port>
```

To set a port's MAC Enabled parameter for the CIST, enter the following command in root view:

```
root> ethernet mstp set interface <interface> slot <slot> port
<port> cist-port-mac-enabled <cist-port-mac-enabled>
```

To set an interface group's MAC Enabled parameter for the CIST, enter the following command in root view:

```
root> ethernet mstp set group <group> cist-port-mac-enabled
<cist-port-mac-enabled
```

To display a port's CIST parameters, enter the following command in root view:

```
root> ethernet mstp show-cist-port-attributes interface
<interface> slot <slot> port <port>
```

To display an interface group's CIST parameters, enter the following command in root view:

```
root> ethernet mstp show-cist-port-attributes group <group>
```

Table 249: CIST Port CLI Parameters

Parameter	Input Type	Permitted Values	Description
interface	Variable	eth radio	Enter the type of interface: `eth` – Ethernet `radio` – Radio
slot	Number	Ethernet: 1 Radio: - PTP 850C and PTP 850E: 1 PTP 850S: 2	
port	Number	- Ethernet interface on PTP 850C: 1-4 - Ethernet interface on PTP 850E: 1-7 - Ethernet interface on PTP 850S: 1-3 - Radio interface on an PTP 850C: 1-2 - Radio interface on an PTP 850E or PTP 850S: 1	The port number of the interface.
group	Variable	lag1 lag2 lag3 lag4 mc-abc1 mc-abc2 mc-abc3 mc-abc4	To enter interface view for a LAG group, enter the group (lag1 - lag4). To enter interface view for a Multi-Carrier ABC group, enter the group (mc-abc1 – mc-abc4) (PTP 850C only).
cist-port-priority	Number	0-240, in multiples of 16.	The priority contained in the first octet of the
cist-port-path-cost	Number	1-200000000.	The configurable assigned value for the contribution of this port to the path cost of paths towards the spanning tree root. **Note:** Changing the value of this parameter is considered to be a
cist-port-edge-port	Variable	true false	`true` – The port is considered an edge port in the CIST. `false` – The port is

Parameter	Input Type	Permitted Values	Description
cist-port-mac-enabled	Variable	forceTrue forceFalse auto	forceTrue – The MAC is treated as if it is connected to a point-to-point LAN, regardless of any indications to the contrary that are generated by the MAC entity. forceFalse –The MAC is treated as if it is connected to a non-point-to-point LAN, regardless of any indications to the contrary that are generated by the MAC entity. auto – The MAC Enabled parameter is set to True if the MAC is connected to a point-to-point or full-duplex LAN. The MAC Enabled parameter is set to False if the MAC is connected to a non-point-to-point and half-duplex LAN.

The following command sets the CIST port priority for Ethernet port 3 to 192:

```
root> ethernet mstp set interface eth slot 1 port 3 cist-port-
priority 192
```

The following command sets the CIST port priority for HSB protection group 1 to 192:

```
root> ethernet mstp set group rp1 cist-port-priority 192
```

The following command sets the CIST path cost for Ethernet port 3 to 20,000:

```
root> ethernet mstp set interface eth slot 1 port 3 cist-path-
cost 20000
```

The following command sets the CIST path cost for LAG 1 to 20,000:

```
root> ethernet mstp set group lag1 cist-path-cost 20000
```

The following command sets radio interface 1 on an PTP 850C to be an Edge port in the CIST:

```
root> ethernet mstp set interface radio slot 1 port 1 cist-
port-admin-edge true
```

The following command displays the CIST parameters of LAG 1:

```
root> ethernet mstp show-cist-port-attributes group lag1
```

Configuring and Viewing the MSTI Port Parameters (CLI)

To set the port priority for an MSTI and port, enter the following command in root view:

```
root> ethernet mstp set instance <instance> interface
<interface> slot <slot> port <port> msti-port-priority <msti-
port-priority>
```

To set the port priority for an MSTI and an interface group, enter the following command in root view:

```
root> ethernet mstp set instance <instance> group <group> msti-
port-priority <msti-port-priority>
```

To set the path cost for a port in a specific MSTI, enter the following command in root view:

```
root> ethernet mstp set instance <instance> interface
<interface> slot <slot> port <port> msti-port-path-cost <msti-
port-path-cost>
```

To set the path cost for an interface group in a specific MSTI, enter the following command in root view:

```
root> ethernet mstp set instance <instance> group <group> msti-
port-path-cost <msti-port-path-cost>
```

To display the MSTI parameters for a specific MSTI and port, enter the following command in root view:

```
root> ethernet mstp show-msti-port-attributes instance
<instance> interface <interface> slot <slot> port <port>
```

To display the MSTI parameters for a specific MSTI and interface group, enter the following command in root view:

```
root> ethernet mstp show-msti-port-attributes instance
<instance> group <group>
```

Table 250: MSTI Port CLI Parameters

Parameter	Input Type	Permitted Values	Description
instance	Number	1-16	Enter the MSTI ID of the MSTI you want to configure.
interface	Variable	eth radio	Enter the type of interface: eth – Ethernet radio – Radio
slot	Number	Ethernet: 1 Radio: • PTP 850C and PTP 850E: 1 PTP 850S: 2	

Parameter	Input Type	Permitted Values	Description
port	Number	• Ethernet interface on PTP 850C: 1-4 • Ethernet interface on PTP 850E: 1-7 • Ethernet interface on PTP 850S: 1-3 • Radio interface on an PTP 850C: 1-2 • Radio interface on an PTP 850E or PTP	The port number of the interface.
group	Variable	lag1 lag2 lag3 lag4 mc-abc1 mc-abc2 mc-abc3 mc-abc4	To enter interface view for a LAG group, enter the group (lag1 - lag4). To enter interface view for a Multi-Carrier ABC group, enter the group (mc-abc1 – mc-abc4) (PTP 850C only).
msti-port-priority	Number	0-240, in multiples of 16.	The priority contained in the first octet of the two-octet Port ID.
msti-port-path-cost	Number	1-200000000.	The port's Path Cost parameter for the MSTI. **Note:** Changing the value of this parameter may cause re-initialization of the MSTI for which the parameter is changed. No other MSTI should be affected.

The following command sets the MSTI port priority for MSTI 14 on Ethernet port 2 to 192:

```
root> ethernet mstp set instance 14 interface eth slot 1 port 2
msti-port-priority 192
```

The following command sets the MSTI port priority for MSTI 14 on LAG 1 to 192:

```
root> ethernet mstp set instance 14 group lag1 msti-port-
priority 192
```

The following command sets the MSTI path cost for MSTI 12 on Ethernet port 3 to 20000:

```
root> ethernet mstp set instance 12 interface eth slot 1 port 3
msti-port-path-cost 20000
```

The following command sets the MSTI path cost for MSTI 12 on HSB protection group 1 to 20000:

```
root> ethernet mstp set instance 12 group rp1 msti-port-path-
cost 20000
```

The following command displays the MSTI parameters for MSTI 10 and radio interface 1:

```
root> ethernet mstp show-msti-port-attributes instance 10
interface radio slot 2 port 1
```

The following command displays the MSTI parameters for MSTI 10 and LAG 1:

```
root> ethernet mstp show-msti-port-attributes instance 10 group
lag1
```

Viewing and Resetting Port BPDU Counters (CLI)

To view the BPDU counters for a port, enter the following command in root view:

```
root> ethernet mstp show-port-counters interface <interface>
slot <slot> port <port>
```

To view the BPDU counters for an interface group, enter the following command in root view:

```
root> ethernet mstp show-port-counters group <group>
```

To reset the BPDU counters, enter the following command in root view:

```
root> ethernet mstp reset-counters
```

Table 251: Port BPDU Counters CLI Parameters

Parameter	Input Type	Permitted Values	Description
interface	Variable	eth radio	Enter the type of interface: `eth` – Ethernet `radio` – Radio
slot	Number	Ethernet: 1 Radio: • PTP 850C and PTP 850E: 1 PTP 850S: 2	
port	Number	• Ethernet interface on PTP 850C: 1-4 • Ethernet interface on PTP 850E: 1-7 • Ethernet interface on PTP 850S: 1-3 • Radio interface on an PTP 850C: 1-2 • Radio interface on an PTP 850E or PTP 850S:	The port number of the interface.

group	Variable	lag1 lag2 lag3 lag4 mc-abc1 mc-abc2 mc-abc3 mc-abc4	To enter interface view for a LAG group, enter the group (lag1 - lag4). To enter interface view for a Multi-Carrier ABC group, enter the group (mc-abc1 – mc-abc4) (PTP 850C only).

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

Note

For an overview of ETH-BN, see ETH-BN Overview.

You must first create an ETH-BN entity consisting of the Monitored Interface on the one hand, and the Control Interface on the other. You must then use separate commands to enable or disable bandwidth monitoring of the monitored interface and transmission of messages. You can also set various parameters related to the bandwidth sampling and the transmitted bandwidth messages.

To create an ETH-BN entity, enter the following command in root view:

```
root> ethernet ebn ebn-entity-create ebn-name <eb-name> monitored-
interface <monitored-interface> monitored-slot <monitored-slot>
monitored-port <monitored-port> control-interface <control-interface>
control-slot <control-slot> vlan <vlan>
```

To change the name of an ETH-BN entity, enter the following command in root view:

```
root> ethernet ebn ebn-name-set ebn-name <ebn-name> new-ebn-name <ebn-
name>
```

To set the Admin status of an ETH-BN entity, enter the following command in root view:

```
root> ethernet ebn ebn-admin-set ebn-name <ebn-name> admin <admin-state>
```

To set the Maintenance Level of messages sent by the ETH-BN entity, enter the following command in root view:

```
root> ethernet ebn ebn-mel-set ebn-name <ebn-name> mel <mel>
```

Note

If CFM MEPs are being used, the MEL must be set to a value greater than the MEG level of the MEP. Otherwise, the BNM frames will be dropped.

If CFM MEPs are not being used, the MEL for ETH-BN must be set to a value greater than 0. Otherwise, the BNM frames will be dropped.

To set the VLAN with which messages sent by the ETH-BN entity are transmitted, enter the following command in root view:

```
root> ethernet ebn ebn-vlan-set ebn-name <ebn-name> vlan <vlan>
```

To determine whether periodic BNM frames should be sent even when there is no bandwidth degradation in the monitored interface, enter the following command in root view:

```
root> ethernet ebn ebn-is-always-send ebn-name <string> is-always-send
<is-always-send>
```

To delete an ETH-BN entity, enter the following command in root view:

```
root> ethernet ebn ebn-entity-delete ebn-name <ebn-name>
```

To show a summary of all ETH-BN entities defined, enter the following command in root view:

```
root> ethernet ebn ebn-entities-summary-show
```

To show a summary of the configuration and status of a specific ABN entity, enter the following command in root view:

```
root> ethernet ebn ebn-entity-show ebn-name <ebn-name>
```

To set how often messages are transmitted when bandwidth is below the nominal value, enter the following command in root view:

```
root> ethernet ebn ebn-period-set ebn-name <ebn-name> period <period>
```

To set the holdoff time, enter the following command in root view. Holdoff time is the amount of time the system waits when bandwidth degradation occurs, before transmitting a message. If the bandwidth is below the nominal value when the holdoff period ends, the system starts transmitting messages:

```
root> ethernet ebn ebn-holdoff-set ebn-name <ebn-name> holdoff <holdoff-time>
```

To clear the messages counter, enter the following command in root view:

```
root> ethernet ebn ebn-entity-counter-reset ebn-name <ebn-name>
```

Table 206 ETH-BN Entity CLI Parameters

Parameter	Input Type	Permitted Values	Description
ebn-name	Text String		The name of the ABN entity.
monitored-interface	Variable	radio	This parameter is always set to radio.
monitored-slot	Number	1	
monitored-port	Number	1	
control-interface	Variable	eth	This parameter is always set to eth.
control-slot	Number	1	This parameter is always set to 1.
control-port	Number	1-7	The specific Ethernet interface to which messages are transmitted when bandwidth in the monitored interface degrades below the nominal value.

Parameter	Input Type	Permitted Values	Description
mel	Number	0-7	The CFM Maintenance Level of messages sent by an ETH-BN entity.
vlan	Variable	untag 1 - 4094, except 4092 (reserved for the default management service)	The VLAN on which messages are transmitted (optional). The CoS of the VLAN is automatically set to 7.
is-always-send	Variable	true false	Specifies whether periodic BNM frames are sent even when there is no bandwidth degradation in the monitored interface: • **true** – BNM frames are always sent, even when the bandwidth is at its nominal value. **false** – BNM frames are only sent when the current bandwidth is lower than the nominal bandwidth (default value).
admin-state	Variable	up down	Enter up to enable ETH-BN monitoring on the interface, or down to disable EBN monitoring on the interface.
period	Variable	4-one-second 5-ten-seconds 6-sixty-seconds	How often messages are transmitted when **is-always-send** is set to **true** or, if not, when bandwidth is below the nominal value: **4-one-second** – Message is sent every one second.

Parameter	Input Type	Permitted Values	Description
			5-ten-seconds – Message is sent every ten seconds. **6-sixty-seconds** – Message is sent every minute. The default value is ten seconds.
holdoff-time	Number	0-10	The amount of time (in seconds) the system waits when bandwidth degradation occurs, before transmitting a message. The default value is 10 seconds.

The following command creates an EBN entity with the following attributes:

- The name of the EBN entity is Test.
- The monitored radio interface is interface 1
- The Ethernet control interface is Ethernet port 1
- The MEL is set to 7.
- BNM frames are only sent when the current bandwidth is lower than the nominal bandwidth.
- When the current bandwidth is below the nominal value, BNM frames are sent every 60 seconds, after a holdoff time of 10 seconds.
- BNM frames are untagged

```
root>ethernet ebn ebn-entity-create ebn-name Test monitored-interface
radio monitored-slot 1 monitored-port 1 control-interface eth control-
slot 1 control-port 7 vlan untag

root>ethernet ebn ebn-admin-set ebn-name Test admin up

root>ethernet ebn ebn-mel-set ebn-name Test mel 7

root>ethernet ebn ebn-is-always-send ebn-name Test is-always-send false

root>ethernet ebn ebn-period-set ebn-name Test period 6-sixty-seconds

root>ethernet ebn ebn-holdoff-set ebn-name Test holdoff 10

root>
```

Configuring LLDP (CLI)

Link Layer Discovery Protocol (LLDP) is a vendor-neutral layer 2 protocol that can be used by a network element attached to a specific LAN segment to advertise its identity and capabilities and to receive identity and capacity information from physically adjacent layer 2 peers. LLDP is a part of the IEEE 802.1AB – 2005 standard that enables automatic network connectivity discovery by means of a port identity information exchange between each port and its peer. Each port periodically sends and also expects to receive frames called Link Layer Discovery Protocol Data Units (LLDPDU). LLDPDUs contain information in TLV format about port identity, such as MAC address and IP address.

LLDP is used to send notifications to the NMS, based on data of the local unit and data gathered from peer systems. These notifications enable the NMS to build an accurate network topology.

This section includes:

- Configuring the General LLDP Parameters (CLI)
- Displaying the General LLDP Parameters (CLI)
- Configuring LLDP Port Parameters (CLI)
- Displaying LLDP Port Parameters (CLI)
- Displaying LLDP Local System Parameters (CLI)
- Displaying the LLDP Remote System Parameters (CLI)
- Displaying LLDP Statistics (CLI)

Configuring the General LLDP Parameters (CLI)

This section explains how to define the general LLDP parameters for the unit. For instructions on defining port-specific parameters, see Configuring LLDP Port Parameters (CLI).

To define the Transmit Interval, which is the interval at which LLDP frames are transmitted, enter the following command in root view:

```
root> ethernet lldp tx-interval-set tx-interval <tx-interval>
```

The time-to-live (TTL) determines the length of time LLDP frames are retained by the receiving device. The TTL is determined by multiplying the Transmit Interval by the TTL Multiplier.

To define the TTL Multiplier, enter the following command in root view:

```
root> ethernet lldp tx-hold-multiplier-set hold-multiplier
<hold-multiplier>
```

To define the interval between transmission of LLDP notifications during normal transmission periods, enter the following command in root view:

```
root> ethernet lldp notif-interval-set notif-interval <notif-
interval>
```

Table 253: General LLDP CLI Parameters

Parameter	Input Type	Permitted Values	Description
tx-interval	Number	5-3600	The interval, in seconds, at which LLDP frames are transmitted. The default value is 30.
hold-multiplier	Number	2-10	The TTL Multiplier, which is multiplied by the Transmit Interval to determine the TTL, in seconds, of LLDP frames. The default value is 4.
notif-interval	Number	5-3600	The interval, in seconds, between transmission of LLDP notifications during normal transmission periods. The default value is 30.

The following commands set the Transmit Interval to 50 seconds with a TTL Multiplier of 5. This produces a TTL of 4 minutes and 10 seconds.

```
root> ethernet lldp tx-interval-set tx-interval 50
root> ethernet lldp tx-hold-multiplier-set hold-multiplier 50
```

The following command sets a Notification Interval of 20 seconds:

```
root> ethernet lldp notif-interval-set notif-interval 20
```

Displaying the General LLDP Parameters (CLI)

To display the general LLDP parameters, enter the following command in root view:

```
root> ethernet lldp configuration-scalers-show
```

The following information is displayed:

Message Tx Interval - The interval, in seconds, at which LLDP frames are transmitted, as defined by the `ethernet lldp tx-interval-set tx-interval` command. The default value is 30.

Message Tx Hold Multiplier - The TTL Multiplier, as defined by the `ethernet lldp tx-hold-multiplier-set hold-multiplier` command. The TTL Multiplier is multiplied by the Transmit Interval to determine the TTL, in seconds, of LLDP frames. The default value is 4.

Reinit Delay - The minimum time, in seconds, the system waits after the LLDP Admin status becomes Disabled until it will process a request to reinitialize LLDP. In this release, this parameter is set at 2.

Notification Interval - The interval, in seconds, between transmission of LLDP notifications during normal transmission periods, as defined by the `ethernet lldp notif-interval-set notif-interval` command. The default value is 30.

Tx Credit Max - The maximum number of consecutive LLDPDUs that can be transmitted at any one time. In this release, the Tx Credit Max is set at 5.

Message Fast Tx - The interval, in seconds, at which LLDP frames are transmitted during fast transmission periods, such as when the unit detects a new neighbor. In this release, this parameter is set at 1.

Message Fast Init - The initial value used to initialize the variable which determines the number of transmissions that are made during fast transmission periods. In this release, this parameter is set at 4.

Configuring LLDP Port Parameters (CLI)

This section explains how to enable LLDP per port, and determine how LLDP operates and which TLVs are sent for each port:

To define how the LLDP agent operates on a specific port, enter the following command in root view:

```
root> ethernet lldp agent-admin-set interface eth slot <slot>
port <port> agent-admin <agent-admin>
```

To enable or disable LLDP notifications to the NMS on a specific port, enter the following command in root view:

```
root> ethernet lldp agent-notif-enable interface eth slot
<slot> port <port> agent-notif-enable <agent-notif-enable>
```

Table 254: LLDP Port CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	1	The slot in which the card resides.
port	Number	- IP—50C: 1-4 - PTP 850E: 1-7 - PTP 850S: 1-3	The port for which you want to configure LLDP.
agent-admin	Variable	txOnly rxOnly txAndR x disabled	Defines how the LLDP protocol operates for this port: - txOnly - The LLDP agent transmits LLDP frames on this port but does not update information about its peer. - `rxOnly` - The LLDP agent receives but does not transmit LLDP frames on this port. - `txAndRx` - The LLDP agent transmits and receives LLDP frames on this port (default value). - `disabled` - The LLDP agent does not transmit or receive LLDP frames on this port.

agent-notif-enable	Variable	true false	- `true` - The agent sends a Topology Change trap to the NMS whenever the system information received from its peer changes. - `false` - Notifications to the NMS are disabled (default value).

The following commands configure Ethernet port 3 to transmit and receive LLDP frames and to send a Topology Change trap to the NMS whenever the system information of its peer changes:

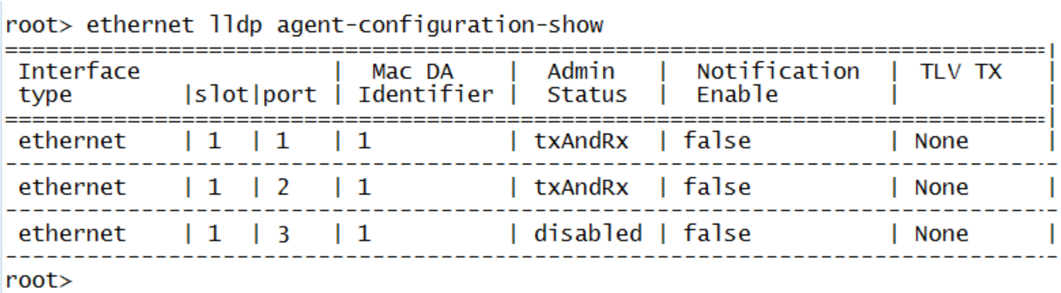
```
root> ethernet lldp agent-admin-set interface eth slot 1 port 3
agent-admin txAndRx

root> ethernet lldp agent-notif-enable interface eth slot 1
port 3 agent-notif-enable true
```

Displaying LLDP Port Parameters (CLI)

To display the LLDP agent configuration on all ports, enter the following command in root view:

```
root> ethernet lldp agent-configuration-show
```

The following is a sample output of the command:



```
root> ethernet lldp agent-configuration-show
=================================================================================|
 Interface                 |  Mac DA     |  Admin    |  Notification   |  TLV TX   |
 type         |slot|port   |  Identifier |  Status   |  Enable         |           |
=================================================================================|
 ethernet     | 1  | 1     | 1           | txAndRx   | false           | None      |
----------------------------------------------------------------------------------
 ethernet     | 1  | 2     | 1           | txAndRx   | false           | None      |
----------------------------------------------------------------------------------
 ethernet     | 1  | 3     | 1           | disabled  | false           | None      |
----------------------------------------------------------------------------------
root>
```

Displaying LLDP Local System Parameters (CLI)

This section includes:

- Displaying Local Unit Parameters (CLI)
- Displaying Local Port Parameters (CLI)
- Displaying Local Unit Management Information (CLI)
- Displaying Local Unit Management Information per Port (CLI)
- Displaying Unit’s Destination MAC Addresses (CLI)

Displaying Local Unit Parameters (CLI)

To display the local unit's unit parameters, as transmitted by the LLDP agents, enter the following command in root view:

```
root> ethernet lldp local-system-scalars-show
```

The following information is displayed:

- **local Chassis Id Subtype** - The type of encoding used to identify the local unit. In this release, this parameter is always set to 4 (MAC Address).
- **local Chassis Id** - The MAC Address of the local unit.
- **local System Name** - The system name included in TLVs transmitted by the LLDP agent. To define the system name, see *Configuring Unit Parameters (CLI)*.
- **local System Description** - The system description included in TLVs transmitted by the LLDP agent.
- **local System Cap Supported** - A bitmap value used to identify which system capabilities are supported on the local system, as included in TLVs transmitted by the LLDP agent. The bitmap is defined by the following parameters:
  - 0 - other
  - 1 - repeater
  - 2 - bridge
  - 3 - wlanAccessPoint
  - 4 - router
  - 5 - telephone
  - 6 - docsisCableDevice
  - 7 - stationOnly
  - 8 - cVLANComponent
  - 9 - sVLANComponent
  - 10 - twoPortMACRelay
- **local System Cap Enabled** - A bitmap value used to identify which system capabilities are enabled on the local system, as included in TLVs transmitted by the LLDP agent. The bitmap is defined by the following parameters:
  - 0 - other
  - 1 - repeater
  - 2 - bridge
  - 3 - wlanAccessPoint
  - 4 - router
  - 5 - telephone
  - 6 - docsisCableDevice
  - 7 - stationOnly
  - 8 - cVLANComponent
  - 9 - sVLANComponent
  - 10 - twoPortMACRelay

Displaying Local Port Parameters (CLI)

To display local port parameters, as transmitted by the LLDP agent, enter the following command in root view:

```
root> ethernet lldp local-port-show
```

The following information is displayed:

- **Interface type/slot/port** - The port type, slot number, and port number.
- **Port ID Subtype** - The type of encoding used to identify the port in LLDP transmissions. In this release, this parameter is always set to MAC Address.
- **Port ID** - The port's MAC address.
- **Description** - A text string that describes the port. In this release, this parameter is always set to ethPort.

Displaying Local Unit Management Information (CLI)

To display the local unit's management information, enter the following command in root view:

```
root> ethernet lldp local-mng-show
```

The following information is displayed:

- **Mng Addr SubType** - The format of the local unit's IP Address. In this release, only IPV4 is supported.
- **Management Address** - The local unit's IP address.
- **Mng Addr Length** - Reserved for future use.
- **Mng Addr IF SubType** - Reserved for future use.
- **Mng Addr IF** - Reserved for future use.
- **Mng Addr OID** - Reserved for future use.

Displaying Local Unit Management Information per Port (CLI)

To display the local unit's management information per port, enter the following command in root view:

```
root> ethernet lldp mng-addr-table-show
```

The following information is displayed:

- **Interface type/slot/port** - The port type, slot number, and port number.
- **Dest Mac Address** - Defines the MAC address associated with the port for purposes of LLDP transmissions.
- **Mng Address subType** - Defines the type of the management address identifier encoding used for the Management Address. In this release, only IpV4 is supported.
- **Management Address** - The unit's IP address.
- **Mng Address Tx Enable** - Indicates whether the unit's Management Address is transmitted with LLDPDUs. In this release, the Management Address is always sent.

Displaying Unit's Destination MAC Addresses (CLI)

To display the destination MAC address or range of MAC addresses associated with the unit, and their internal index, enter the following command in root view:

```
root> ethernet lldp mac-da-table-show
```

The following information is displayed:

- **LLDP DA Index** - The internal index associated with the unit's destination LLDP MAC address.
- **LLDP DA** - The unit's destination LLDP MAC address.

Displaying the LLDP Remote System Parameters (CLI)

This section includes:

- Displaying the LLDP Remote Unit Parameters (CLI)
- Displaying the LLDP Remote Management Data per Port (CLI)

Note: Remote information is not displayed for ports that belong to a LAG group.

Displaying the LLDP Remote Unit Parameters (CLI)

To display the peer's LLDP unit parameter information, starting from a specific time, enter the following command in root view. If no time is specified, all data is displayed.

```
root> ethernet lldp agent-remote-table-show agent-start-time
<agent-start-time> interface eth slot <slot> port <port>
```

Table 255: LLDP Remote Unit CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	1	The slot in which the card resides.
port	Number	• PTP 850S: 1-3 • PTP 850E: 1-7	The port for which you want to configure LLDP.
agent-start-time	Date	Use the format: dd-mm-yyyy,hh:mm:ss	The sys-up-time of the entry creation.

The following information is displayed:

- **Time Mark** – The time the entry was created.
- **Interface Type/Slot/Port** – The port for which you are displaying data about the peer.
- **Rem Dest Mac Address** – The peer LLDP agent's destination MAC Address.
- **Remote Index** – An arbitrary local integer value used by this agent to identify a particular connection instance, unique only for the indicated peer.
- **Remote Chassis ID subType** – The type of encoding used to identify the peer hardware unit.
- **Remote Chassis ID** – An octet string used to identify the peer hardware unit.
- **Rem Port ID subType** – The type of port identifier encoding used in the peer's

Port ID.

- **Rem Port ID** – An octet string used to identify the port component associated with the peer.
- **Rem Port Description** – A description of the peer's port.
- **Rem System Name** – The peer's system name.
- **Rem System Description** – The peer's system description.
- **Rem System Cap Supported** - The bitmap value used to identify which system capabilities are supported on the peer. The bitmap is defined by the following parameters:
    - 0 - other
    - 1 - repeater
    - 2 - bridge
    - 3 - wlanAccessPoint
    - 4 - router
    - 5 - telephone
    - 6 - docsisCableDevice
    - 7 - stationOnly
    - 8 - cVLANComponent
    - 9 - sVLANComponent
    - 10 - twoPortMACRelay
- **Rem System Cap Enabled** - The bitmap value used to identify which system capabilities are enabled on the peer. The bitmap is defined by the following parameters:
    - 0 - other
    - 1 - repeater
    - 2 - bridge
    - 3 - wlanAccessPoint
    - 4 - router
    - 5 - telephone
    - 6 - docsisCableDevice
    - 7 - stationOnly
    - 8 - cVLANComponent
    - 9 - sVLANComponent
    - 10 - twoPortMACRelay
- **Remote Changes** - Indicates whether there are changes in the peer's MIB, as determined by the variable **remoteChanges**. Possible values are:
    - **True** - Changes have taken place in the peer's MIB since the defined agent- start-time.
    - **False** - No changes have taken place in the peer's MIB since the defined agent-*start-time*.

Displaying the LLDP Remote Management Data per Port (CLI)

To display remote LLDP management data from a specific port, starting from a specific time, enter the following command in root view. If no time is specified, all data is displayed.

```
root> ethernet lldp agent-remote-mng-show agent-start-time
<agent-start-time> interface eth slot <slot> port <port>
```

Table 256: LLDP Remote Management Data Per Port CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	1	
port	Number	• PTP 850S: 1-3 • PTP 850E: 1-7	The port for which you want to configure LLDP.
agent-start-time	Date	Use the format: dd-mm-yyyy,hh:mm:ss	The sys-up-time of the entry creation.

The following information is displayed:

- **Time Mark** - The time the entry was created.
- **Interface Type/Slot/Port** - The port for which you are displaying data about the peer.
- **Rem Dest Mac Address** - The peer LLDP agent's destination MAC Address.
- **Remote Index** - An arbitrary local integer value used by this agent to identify a particular connection instance, unique only for the indicated peer.
- **Remote Mng Addr subType** - The type of management address identifier encoding used in the associated LLDP Agent Remote Management Address.
- **Remote Mng Address** - The octet string used to identify the management address component associated with the remote system. The purpose of this address is to contact the management entity.
- **Remote Mng IF subType** - The enumeration value that identifies the interface numbering method used for defining the interface number, associated with the remote system. Possible values are:
  - unknown(1)
  - ifIndex(2)
  - systemPortNumber(3)
- **Agent Rem OID** - The OID value used to identify the type of hardware component or protocol entity associated with the management address advertised by the remote system agent.

Displaying LLDP Statistics (CLI)

This section includes:

- Displaying Statistics Regarding Changes in Peer Unit (CLI)
- Displaying LLDP Transmission Statistics (CLI)

- Displaying LLDP Received Frames Statistics (CLI)

Displaying Statistics Regarding Changes in Peer Unit (CLI)

To display statistics about changes reported via LLDP by the remote unit, enter the following command in root view:

```
root> ethernet lldp statistics-scalars-show
```

The following information is displayed:

- **stats Rem Tables Last Change Time** - The time of the most recent change in the remote unit, as reported via LLDP.
- **stats Rem Tables Inserts** - The number of times the information from the remote system has changed.
- **stats Rem Tables Deletes** - The number of times the information from the remote system has been deleted.
- **stats Rem Tables Drops** - Reserved for future use.
- **stats Rem Tables Ageouts** - The number of times the information from the remote system has been deleted from the local unit's database because the information's TTL has expired. The `RX Ageouts` counter is similar to this counter, but is for specific ports rather than the entire unit.

Displaying LLDP Transmission Statistics (CLI)

To display statistics about LLDP transmissions and transmission errors, enter the following command in root view:

```
root> ethernet lldp statistics-port-tx-show
```

The following information is displayed:

- **LLDP TX Statistics Ifindex** - The index value used to identify the port in LLDP transmissions.
- **LLDP TX Statistics DA ID** - The LLDP MAC address associated with this entry.
- **LLDP TX Statistics Total Frames** - The number of LLDP frames transmitted by the LLDP agent on this port to the destination MAC address.
- **LLDP TX Statistics No. of Length Error** - The number of LLDPDU Length Errors recorded for this port and destination MAC address. If the set of TLVs that is selected in the LLDP local system MIB by network management would result in an LLDPDU that violates LLDPDU length restrictions, then the No. of Length Error statistic is incremented by 1, and an LLDPDU is sent containing the mandatory TLVs plus as many of the optional TLVs in the set as will fit in the remaining LLDPDU length.

Displaying LLDP Received Frames Statistics (CLI)

To display statistics about LLDP frames received by the unit, enter the following command in root view:

```
root> ethernet lldp statistics-port-rx-show
```

The following information is displayed:

- **RX Destination Port** - The index value used to identify the port in LLDP transmissions.

- **RX DA Index** - The index value used to identify the destination MAC address associated with this entry.
- **RX Total Discarded** - The number of LLDP frames received by the LLDP agent on this port, and then discarded for any reason. This counter can provide an indication that LLDP header formatting problems may exist with the local LLDP agent in the sending system or that LLDPDU validation problems may exist with the local LLDP agent in the receiving system.
- **RX Invalid Frames** - The number of invalid LLDP frames received by the LLDP agent on this port while the agent is enabled.
- **RX Valid Frames** - The number of valid LLDP frames received by the LLDP agent on this port.
- **RX Discarded TLVs** - The number of LLDP TLVs discarded for any reason by the LLDP agent on this port.
- **RX Unrecognized TLVs** - The number of LLDP TLVs received on the given port that are not recognized by LLDP agent.
- **RX Ageouts** - The number of age-outs that occurred on the port. An age-out is the number of times the complete set of information advertised by the remote system has been deleted from the unit's database because the information timeliness interval has expired. This counter is similar to the `LLDP No. of Ageouts` counter, except that it is per port rather than for the entire unit. This counter is set to zero during agent initialization. This counter is incremented only once when the complete set of information is invalidated (aged out) from all related tables on a particular port. Partial ageing is not allowed.

Chapter 23: Synchronization (CLI)

This section includes:

- Changing the ETSI/ANSI Mode (CLI)
- Configuring the Sync Source (CLI)
- Configuring the Outgoing Clock (CLI)
- Changing the Default Quality (CLI)
- Configuring the Revertive Timer (CLI)
- Configuring SSM Messages (CLI)
- Displaying Synchronization Status and Parameters (CLI)
- Configuring 1588 Transparent Clock (CLI)

Changing the ETSI/ANSI Mode (CLI)

By default, PTP 850 units are set to ETSI mode. No mode change is necessary to configure an MRMC script, even if an FCC (ANSI) script is used. However, to configure a sync source on which the sync source Quality parameter must be set according to ANSI specifications. You must change the ETSI/ANSI mode to ANSI before configuring the sync source.

To change the ETSI/ANSI mode, enter the following command in root view:

```
root> platform management set interfaces-standard <ansi|etsi>
```

The following command changes the ETSI/ANSI mode from the default value of ETSI to ANSI mode:

```
root> platform management set interfaces-standard ansi
```

To display the current ETSI/ANSI mode, enter the following command in root view:

```
root> platform management show interfaces-standard
```

Changing the ETSI/ANSI mode does *not* require unit reset.

Configuring the Sync Source (CLI)

Note

To configure a sync source on which the sync source Quality parameter must be set according to ANSI specifications, change the ETSI/ANSI mode to ANSI before configuring the sync source. See Changing the ETSI/ANSI Mode (CLI).

Frequency signals can be taken by the system from Ethernet and radio interfaces. The reference frequency may also be conveyed to external equipment through different interfaces.

Frequency is distributed by configuring the following parameters in each node:

System Synchronization Sources – These are the interfaces from which the frequency is taken and distributed to other interfaces. Up to 16 sources can be configured in each node. A revertive timer can be configured. For each interface, you must configure:

- **Priority (1-16)** – No two synchronization sources can have the same priority.
- **Quality** – The quality level applied to the selected synchronization source. This enables the system to select the source with the highest quality as the current synchronization source.

Each unit determines the current active clock reference source interface:

- The interface with the highest available quality is selected.
- From among interfaces with identical quality, the interface with the highest priority is selected.

When configuring the Sync source, the Sync mode must be set to its default setting of automatic. To display the current Sync mode, enter the following CLI command in root view:

```
root> platform sync mode show
```

If the Sync mode is set to pipe, you must set it to automatic by entering the following CLI command in root view:

```
root> platform sync mode set automatic
```

When configuring an Ethernet interface as a Sync source, the Media Type of the interface must be rj45 or sfp, *not* auto-type. To view and configure the Media Type of an Ethernet interface, see Configuring an Interface’s Media Type (CLI).

This section includes:

Configuring an Ethernet Interface as a Synchronization Source (CLI)

Configuring a Radio Interface as a Synchronization Source (CLI)

Configuring an Ethernet Interface as a Synchronization Source (CLI)

Note

In order to select an Ethernet interface, you must first specify the media type for this interface. See Configuring Ethernet Services (CLI).

To configure an Ethernet interface as a synchronization source, enter the following command in root view:

```
root> platform sync source add eth-interface slot <slot> port <port>
priority <priority> quality <quality>
```

To edit the parameters of an existing Ethernet interface synchronization source, enter the following command in root view:

```
root> platform sync source edit eth-interface slot <slot> port <port>
priority <priority> quality <quality>
```

To remove an Ethernet interface as a synchronization source, enter the following command in root view:

```
root> platform sync source remove eth-interface slot <slot> port <port>
```

Table 207 Sync Source Ethernet CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	1	
port	Number	1-7	The interface to be configured as a synchronization source.
priority	Number	1 – 16	The priority of this synchronization source relative to other synchronization sources configured in the unit.
quality	Variable	For ETSI systems: automatic prc ssu-a ssu-b g813.8262 For ANSI (FCC) systems: automatic prs stratum-2 transit-node stratum-3e stratum-3 smc unknown	The quality level applied to the selected synchronization source. This enables the system to select the source with the highest quality as the current synchronization source. If the quality is set to automatic, then the quality is determined by the received SSMs. If no valid SSM messages are received or in case of interface failure (such as LOS, LOC, LOF), the quality becomes "failure." SSM must be enabled on the remote interface in order for the interface to receive SSM messages. If the quality is configured to a fixed value, then the quality status becomes “failure” upon interface failure (such as LOS, LOC, LOF).

The following command configures Ethernet port 2 as a synchronization source with priority = 8, and quality = automatic:

```
root> platform sync source add eth-interface slot 1 port 2 priority 8
quality automatic
```

The following command changes the priority of this synchronization source to 6:

```
root> platform sync source edit eth-interface slot 1 port 2 priority 6
```

The following command removes this synchronization source:

```
root> platform sync source remove eth-interface slot 1 port 2
```

Configuring a Radio Interface as a Synchronization Source (CLI)

To configure a radio interface as a synchronization source, enter the following command in root view:

```
root> platform sync source add radio-interface slot <slot> port <port>
radio-channel <radio-channel> priority <priority> quality <quality>
```

To edit the parameters of an existing radio interface synchronization source, enter the following command in root view:

```
root> platform sync source edit radio-interface slot <slot> port <port>
radio-channel <radio-channel> priority <priority> quality <quality>
```

To remove a radio interface as a synchronization source, enter the following command in root view:

```
root> platform sync source remove radio-interface slot <slot> port <port>
radio-channel <radio-channel>
```

Table 208 Sync Source Radio CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	1	
port	Number	1	
radio-channel	Number	0	
priority	Number	1 – 16	The priority of this synchronization source relative to other synchronization sources configured in the unit.

Parameter	Input Type	Permitted Values	Description
quality	Variable	For ETSI systems: automatic prc ssu-a ssu-b g813.8262 For ANSI (FCC) systems: automatic prs stratum-2 transit-node stratum-3e stratum-3 smc unknown	The quality level applied to the selected synchronization source. This enables the system to select the source with the highest quality as the current synchronization source. If the quality is set to automatic, then the quality is determined by the received SSMs. If no valid SSM messages are received or in case of interface failure (such as LOS, LOC, LOF), the quality becomes "failure." SSM must be enabled on the remote interface in order for the interface to receive SSM messages.

The following command configures the radio interface as a synchronization source with priority = 16, and quality = automatic:

```
root> platform sync source add radio-interface slot 2 port 1 radio-
channel 0 priority 16 quality automatic
```

The following command changes the priority of this synchronization source to 14:

```
root> platform sync source edit radio-interface slot 2 port 1 radio-
channel 0 priority 14
```

The following command removes this synchronization source:

```
root> platform sync source remove radio-interface slot 2 port 1 radio-
channel 0
```

Configuring the Outgoing Clock (CLI)

For each interface, you can choose between using the system clock or the interface's internal clock as its synchronization source. By default, interfaces use the system clock.

When configuring the outgoing clock, the Sync mode must be set to its default setting of automatic. To display the current Sync mode, enter the following command in root view:

```
root> platform sync mode show
```

If the Sync mode is set to pipe, you must set it to automatic by entering the following command in root view:

```
root> platform sync mode set automatic
```

;

To set the interface clock for a radio interface, enter the following command in root view:

```
root> platform sync interface-clock set radio-interface slot 1 port 1
radio-channel <radio-channel> source <source>
```

To set the interface clock for an Ethernet interface, enter the following command in root view:

```
root> platform sync interface-clock set eth-interface slot <slot> port
<port> source <source>
```

Note

To configure the interface clock on an Ethernet interface, the Media Type of the interface must be rj45 or sfp, *not* auto-type. To view and configure the Media Type of an Ethernet interface, see Configuring Ethenet Interfaces (CLI).

Table 209 Outgoing Clock CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	1	
port	Number	ethernet: 1-7 radio: 1	The port number of the interface.
radio-channel	Number	0 – 84	The radio-channel configured for the synchronization source.
source	Variable	system-clock local-clock	system-clock – The interface uses the system clock as its synchronization source. local-clock – The interface uses its internal clock as its synchronization source.

The following command sets the clock source for the radio interface to its internal clock:

```
root> platform sync interface-clock set radio-interface slot 1 port 1
radio-channel 0 source local-clock
```

The following command sets the clock source for Eth7 to the system clock:

```
root> platform sync interface-clock set eth-interface slot 1 port 7
source system-clock
```

Changing the Default Quality (CLI)

Under certain circumstances in which an adequate clock signal is unavailable, an interface may go from locked state to holdover state. Normally, when an interface is in holdover state, it uses stored data to determine its outgoing clock. However, you can set the unit to apply a default quality of DNU (Do Not Use) to any interface in holdover state. To set the default quality to DNU, enter the following CLI command in root view:

```
root> platform sync default-quality set quality DNU
```

To set the default quality back to its default value, enter the following CLI command in root view:

```
root> platform sync default-quality set quality Default
```

To display the default quality, enter the following CLI command in root view:

```
root> platform sync default-quality show
```

Configuring the Revertive Timer (CLI)

You can configure a revertive timer for the unit. When the revertive timer is configured, the unit will not switch to another synchronization source unless that source has been stable for at least the number of seconds defined in the revertive timer. This helps to prevent a situation in which numerous switchovers occur when a synchronization source reports a higher quality for a brief time interval, followed by a degradation of the source's quality. By default, the revertive timer is set to 0, which means that it is disabled.

To configure the revertive timer, enter the following command in root view:

```
root> platform sync revertive-timer set rev_time <rev_time>
```

Table 210: Synchronization Revertive Timer CLI Parameters

Parameter	Input Type	Permitted Values	Description
rev_time	Number	1-1800	The revertive timer, in seconds.

The following command sets the revertive timer as 7 seconds:

```
root> platform sync revertive-timer set rev_time 7
```

To display the revertive timer, enter the following command in root view:

```
root> platform sync revertive-timer show
```

Configuring SSM Messages (CLI)

In order to provide topological resiliency for synchronization transfer, PTP 850E implements the passing of SSM messages over the Ethernet and radio interfaces. SSM timing in PTP 850E complies with ITU-T G.781.

In addition, the SSM mechanism provides reference source resiliency, since a network may have more than one source clock.

The following are the principles of operation:

At all times, each source interface has a “quality status” which is determined as follows:

- If quality is configured as fixed, then the quality status becomes “failure” upon interface failure (such as LOS, LOC, LOF).
- If quality is automatic, then the quality is determined by the received SSMs. If no valid SSM messages are received or in case of interface failure (such as LOS, LOC, LOF), the quality becomes "failure."

Each unit holds a parameter which indicates the quality of its reference clock. This is the quality of the current synchronization source interface.

The reference source quality is transmitted through SSM messages to all relevant radio interfaces.

In order to prevent loops, an SSM with quality “Do Not Use” is sent from the active source interface (both radio and Ethernet).

In order for an interface to transmit SSM messages, SSM must be enabled on the interface. By default, SSM is disabled on all interfaces.

When configuring SSM, the Sync mode must be set to its default setting of automatic. To display the current Sync mode, enter the following command in root view:

```
root> platform sync mode show
```

If the Sync mode is set to pipe, you must set it to automatic by entering the following command in root view:

```
root> platform sync mode set automatic
```

To enable SSM on a radio interface, enter the following command in root view:

```
root> platform sync ssm admin radio-interface slot <slot> port <port>
admin on
```

To disable SSM on a radio interface, enter the following command in root view:

```
root> platform sync ssm admin radio-interface slot <slot> port <port>
admin off
```

To enable SSM on an Ethernet interface, enter the following command in root view:

```
root> platform sync ssm admin eth-interface slot <slot> port <port> admin
on
```

To disable SSM on an Ethernet interface, enter the following command in root view:

```
root> platform sync ssm admin eth-interface slot <slot> port <port> admin
off
```

The following command enables SSM on radio interface 2:

```
root> platform sync ssm admin radio-interface slot 2 port 2 admin on
```

The following command enables SSM on Ethernet port 1:

```
root> platform sync ssm admin eth-interface slot 1 port 1 admin on
```

Displaying Synchronization Status and Parameters (CLI)

To display the synchronization sources configured in the system, enter the following command in root view:

```
root> platform sync source config show
```

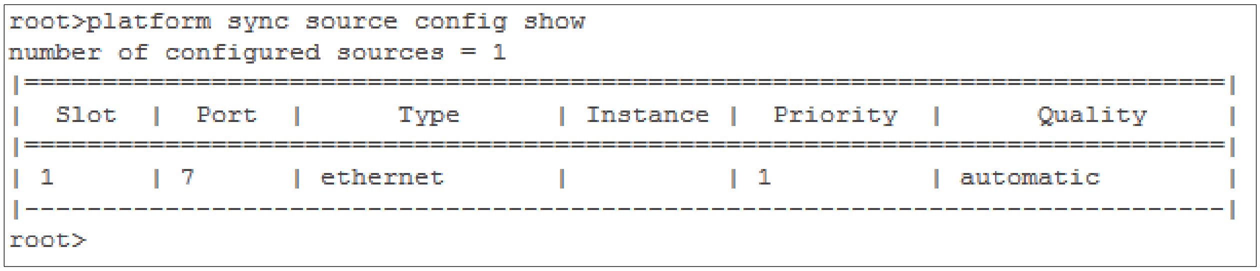
The following is a sample synchronization source display output:

```
number of configured sources = 4
|============================================================|
| Slot | Port | Type | Instance | Priority | Quality |
|============================================================|
| 1 | 7 | Ethernet | | 11 | automatic |
|------------------------------------------------------------|
| 1 | 1 |  Radio   | | 6 | automatic |
|------------------------------------------------------------|
```

To display the synchronization source status, enter the following command in root view:

```
root> platform sync source status show
```

The following is a sample synchronization source status display output:



```
root>platform sync source config show
number of configured sources = 1
|===========================================================================|
|   Slot   |  Port   |        Type        | Instance |  Priority  |      Quality      |
|===========================================================================|
| 1        | 7       | ethernet           |          | 1          | automatic         |
|---------------------------------------------------------------------------|
root>
```

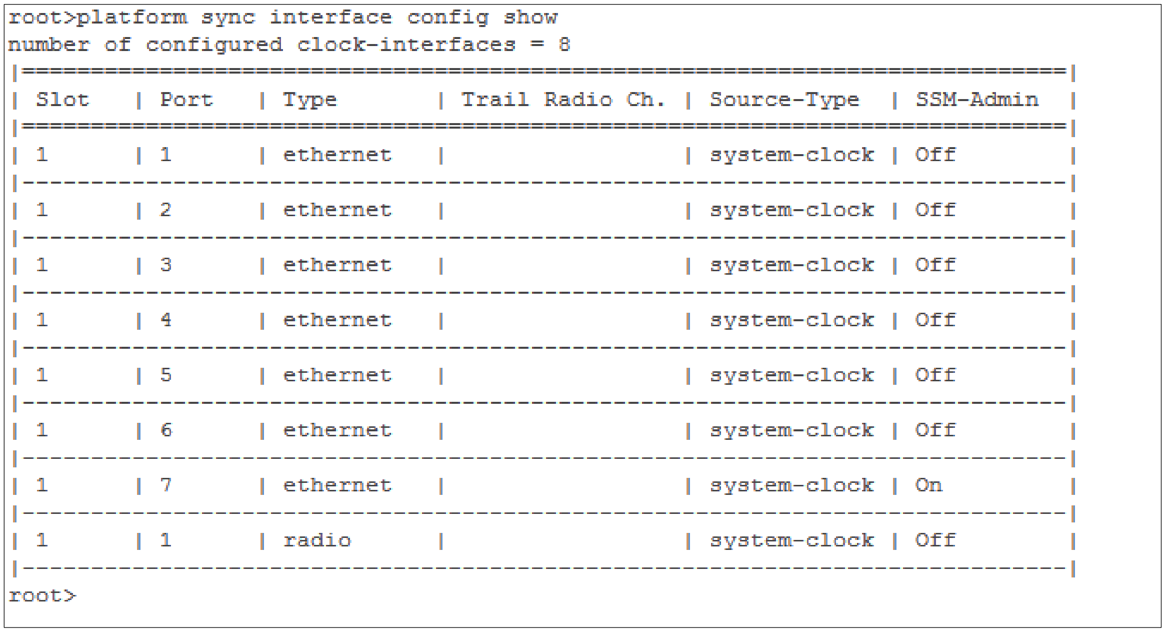
To display the current system reference clock quality, enter the following command in root view:

```
root> platform sync source show-reference-clock-quality
```

To display the current synchronization configuration of the unit's interfaces, enter the following command in root view:

```
root> platform sync interface config show
```

The following is a sample interface synchronization configuration display output:



```
root>platform sync interface config show
number of configured clock-interfaces = 8
|=============================================================================|
| Slot    | Port    | Type         | Trail Radio Ch. | Source-Type  | SSM-Admin  |
|=============================================================================|
| 1       | 1       | ethernet     |                 | system-clock | Off        |
|-----------------------------------------------------------------------------|
| 1       | 2       | ethernet     |                 | system-clock | Off        |
|-----------------------------------------------------------------------------|
| 1       | 3       | ethernet     |                 | system-clock | Off        |
|-----------------------------------------------------------------------------|
| 1       | 4       | ethernet     |                 | system-clock | Off        |
|-----------------------------------------------------------------------------|
| 1       | 5       | ethernet     |                 | system-clock | Off        |
|-----------------------------------------------------------------------------|
| 1       | 6       | ethernet     |                 | system-clock | Off        |
|-----------------------------------------------------------------------------|
| 1       | 7       | ethernet     |                 | system-clock | On         |
|-----------------------------------------------------------------------------|
| 1       | 1       | radio        |                 | system-clock | Off        |
|-----------------------------------------------------------------------------|
root>
```

To display the current system clock status, enter the following command in root view:

```
root> platform sync clu-state show
```

The following is a sample system clock status display output:

```
CLU is in Free-running mode
```

Configuring 1588 Transparent Clock (CLI)

PTP 850E uses 1588v2-compliant Transparent Clock to counter the effects of delay variation. Transparent Clock measures and adjusts for delay variation, enabling the PTP 850 to guarantee ultra-low PDV.

A Transparent Clock node resides between a master and a slave node, and updates the timestamps of PTP packets passing from the master to the slave to compensate for delay, enabling the terminating clock in the slave node to remove the delay accrued in the Transparent Clock node. The Transparent Clock node is itself neither a master nor a slave node, but rather, serves as a bridge between master and slave nodes.

Note that in release 11.1:

- 1588 TC is not supported when Master-Slave communication is using the IPv6 transport layer.
- 1588 TC cannot be used in Multiband configurations.

> Note
>
> Make sure to enable Transparent Clock on the remote side of the link before enabling it on the local side.

To configure Transparent Clock:

1 Add the port receiving synchronization from the customer side as a Sync source, with Sync Interface Priority 1. See *Configuring an Ethernet Interface as a Synchronization Source (CLI)*.

2 Add a radio interface as a Sync source, with lower priority than the port receiving synchronization from the customer side. See *Configuring a Radio Interface as a Synchronization Source (CLI)*.

3 On the remote side of the radio link, add the radio interface facing the local device as a Sync source, with Sync Interface Priority 1. See *Configuring a Radio Interface as a Synchronization Source (CLI)*.

4 Add the port receiving synchronization from the customer side as a Sync source, with Sync Interface Priority 1. See *Configuring an Ethernet Interface as a Synchronization Source (CLI)*.

5 Verify that the Sync Interface Quality Status of the first Sync source is not Failure. See ***Error! R eference source not found.***.

6 Enter the following command in root view to enable Transparent Clock:

```
root> platform sync ptp set admin enable
```

> Note
>
> To disable Transparent Clock, enter the following command in root view:

```
root> platform sync ptp set admin disable
```

> Note
>
> Disabling 1588 PTP can drastically affect time synchronization performance in the entire network.

7 Enter the following command in root view to assign the radio that will carry the PTP packets and determine the direction of the PTP packet flow.

```
root> platform sync ptp-tc set radio slot <slot> port <port> direction
<upstream|downstream>
```

The direction parameter must be set to different values on the two sides of the link, so that if you set the local side to `upstream`, you must set the remote side to `downstream`, and vice versa. Otherwise than that, it does not matter how you set this parameter.

To display the Transparent Clock settings, enter the following command in root view:

```
root> platform sync ptp-tc show status
```

The following commands enable Transparent Clock and configure the radio to send PTP packets upstream:

```
root> platform sync ptp-tc set admin enable
root> platform sync ptp-tc set radio slot 1 port 1 direction upstream
```

8 1588 packets should be mapped to CoS 7. By default, 1588 packets are *not* mapped to any CoS. To map 1588 packets to CoS 7, you must *disable* CoS preservation for 1588 packets. This must be performed via CLI, using the following command:

```
root> ethernet generalcfg ptp-tc cos-preserve set admin disable
```

9 To map 1588 packets to CoS 7, enter the following command:

```
root> ethernet generalcfg ptp-tc cos-preserve cos value 7
```

After you enter these commands, 1588 packets will automatically be mapped to CoS 7.

> Note
>
> If necessary, you can use the ethernet generalcfg ptp-tc cos-preserve cos value command to map a different CoS value (0-7) to 1588 packets, but it is recommended to map 1588 packets to CoS 7.

Configuring 1588 Boundary Clock (CLI)

Boundary Clock complies with ITU-T Telecom Profile G.8275.1. This enables PTP 850E, with Boundary Clock, to meet the rigorous synchronization requirements of 5G networks.

The Boundary Clock in PTP 850E supports up to 16 1588 slave clock devices.

The Boundary Clock terminates the PTP flow it receives on the slave port, recovers the time and phase, and regenerates the PTP flow on the master ports.

The Boundary Clock node selects the best synchronization source available in the domain and regenerates PTP towards the slave clocks. This reduces the processing load from grandmaster clocks and increases the scalability of the synchronization network, while rigorously maintaining timing accuracy.

The PTP 850E Boundary Clock mechanism requires the use of untagged Ethernet multicast PTP packets as specified in G.8275.1.

Note

Boundary Clock and Transparent Clock can be used together in the same PTP 850E node

Note that in release 11.1:

- 1588 BC can only be used in a chain or star topology. It cannot be used in a ring topology.
- 1588 BC is not supported when Master-Slave communication is using the IPv6 transport layer.

Enabling Boundary Clock (CLI)

Note

Before configuring Boundary Clock, you must configure Transparent

Clock. See Configuring 1588 Transparent Clock (CLI).

To enable Boundary Clock, enter the following command in root view to enable:

```
root> platform sync ptp set admin enable
```

You can configure up to 16 interfaces per unit to be part of the Boundary Clock node. These interfaces can be radio and Ethernet interfaces, but not TDM interfaces or groups (e.g., LAG or Multi-Carrier ABC groups).

For each interface, use the following commands to enable and define Boundary Clock.

To enable Boundary Clock on a port, enter the following command in root view:

```
root> platform sync ptp-bc interfaces set interface-type
<interface-type> slot 1 port <port> admin enable
```

To set the port's role in the Boundary Clock node, enter the following command in

root view:

```
root> platform sync ptp-bc interfaces set interface-type
<interface-type> slot <slot> port <port> master-only <master-
only>
```

Optionally, use the following command to set the Local Priority. The Local Priority value is taken into account when two identical announce messages are received by at least two different ports. In such a case, the Boundary Clock mechanism selects the slave port based on the best (lowest) Local Priority. The default value is 128.

```
root> platform sync ptp-bc interfaces set interface-type
<interface-type> slot <slot> port <port> local-priority <local-
priority>
```

Use the following command to set a MAC address for multicast re-transmission of PTP packets:

```
root> platform sync ptp-bc interfaces set interface-type
<interface-type> slot <slot> port <port> dest-mac <dest-mac>
```

Table 211 Boundary Clock Configuration CLI Parameters

Parameter	Input Type	Permitted Values	Description
interface-type	Variable	ethernet radio	
port	Number	ethernet: 1-7 radio: 1	The port number.
admin	Variable	enable disable	Enables or disables Boundary Clock on the port.
master-only	Variable	yes no	yes – The port can only be used as the master port, which means the port acts as a PTP synchronization source for other nodes. no – The port can be used as either a master port or the slave port. The slave port receives PTP synchronization input from an external grandmaster clock. The Best Master Clock Algorithm (BMCA) determines the port's role, based on its determination of which is the best available grandmaster clock. Only one slave port can exist in a single PTP 850E node at any one time.
local-priority	Number	1-255	
dest-mac	Variable	01-1B-19-00-00-00 01-80-C2-00-00-0E	01-1B-19-00-00-00 – General group address. An 802.1Q VLAN Bridge would forward the frame unchanged. 01-80-C2-00-00-0E – Individual LAN Scope group address. An 802.1Q VLAN Bridge would drop the frame.

The following commands set up a Boundary Clock node that includes Ethernet interfaces Eth3 and Eth7 and the radio carrier. The Ethernet interfaces can serve as master or slave; the slave role is allocated dynamically according to the interface receiving the best grandmaster announce message according to the BMCA. The radio interfaces can only serve in the master role, i.e., they distribute PTP synchronization but do not receive PTP synchronization from an external grandmaster.

```
root> platform sync ptp set admin enable


root> platform sync ptp-bc interfaces set interface-type
ethernet slot 1 port 3 admin enable
root> platform sync ptp-bc interfaces set interface-type
ethernet slot 1 port 3 master-only no


root> platform sync ptp-bc interfaces set interface-type
ethernet slot 1 port 7 admin enable
root> platform sync ptp-bc interfaces set interface-type
ethernet slot 1 port 7 master-only no


root> platform sync ptp-bc interfaces set interface-type radio
slot 1 port 1 admin enable
```

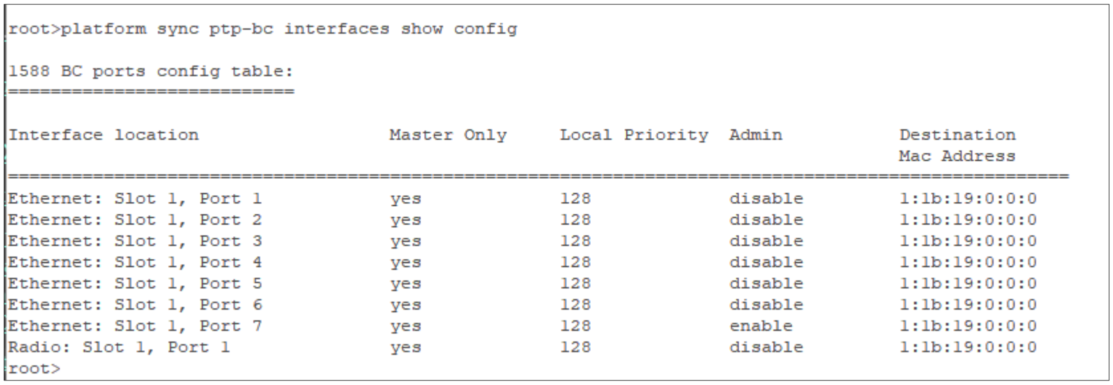
In addition, you must perform the following steps to properly configure the Boundary Clock node:

1. To map PTP packets into the Boundary Clock node, a service point must be created on each interface in the Boundary Clock node. This service point must be defined to gather untagged packets. See *Adding a Service Point (CLI)*.
2. Add a port receiving synchronization from the customer side as a Sync source, with Sync Interface Priority 1. See Configuring the Sync Source (CLI).
3. Add a radio interface as a Sync source, with lower priority than the port receiving synchronization from the customer side. See Configuring the Sync Source (CLI).
4. On the remote side of the radio link, add the radio interface facing the local device as a Sync source, with Sync Interface Priority 1. See Configuring the Sync Source (CLI).
5. On the remote side of the radio link, if there is an Ethernet port conveying synchronization, add this port as a Sync source, with lower priority than the radio interface. See Configuring the Sync Source (CLI).
6. Verify that the Sync Interface Quality Status of the first Sync source is not Failure. See Displaying Synchronization Status and Parameters (CLI).

Use the following command to display the current Boundary Clock configuration:

```
root> platform sync ptp-bc interfaces show config
```

Figure 330 1588 Boundary Clock – Current Configuration Sample Display (CLI)



```
root>platform sync ptp-bc interfaces show config

1588 BC ports config table:
===========================

Interface location                Master Only    Local Priority  Admin           Destination
                                                                                 Mac Address
=================================================================================================
Ethernet: Slot 1, Port 1          yes            128             disable         1:1b:19:0:0:0
Ethernet: Slot 1, Port 2          yes            128             disable         1:1b:19:0:0:0
Ethernet: Slot 1, Port 3          yes            128             disable         1:1b:19:0:0:0
Ethernet: Slot 1, Port 4          yes            128             disable         1:1b:19:0:0:0
Ethernet: Slot 1, Port 5          yes            128             disable         1:1b:19:0:0:0
Ethernet: Slot 1, Port 6          yes            128             disable         1:1b:19:0:0:0
Ethernet: Slot 1, Port 7          yes            128             enable          1:1b:19:0:0:0
Radio: Slot 1, Port 1             yes            128             disable         1:1b:19:0:0:0
root>
```

Displaying and Setting the Boundary Clock Default Parameters (CLI)

The following commands set the Boundary Clock default parameters.

The Priority 2 value is one of the factors used by the BMCA to determine the grandmaster. The PTP 850E's Boundary Clock node advertises this value when it is not locked on an external grandmaster. The default value is 128. The following command can be used to change the Boundary Clock node's Priority 2 value.

```
root> platform sync ptp-bc clock set priority2 <priority2>
```

The following command sets the Boundary Clock node's Domain Number. The default value is 24. The following command can be used to change the Boundary Clock node's Domain Number.

```
root> platform sync ptp-bc clock set domain-number <domain-
number>
```

The Local Priority value is taken into account when two identical announce messages are received by at least two different ports. In such a case, the Boundary Clock mechanism selects the slave port based on the best (lowest) Local Priority. The default value is 128. The following command can be used to change the Boundary Clock node's default Local Priority.

```
root> platform sync ptp-bc clock set local-priority <local-
priority>
```

You can select the maximum number of PTP clocks traversed from the grandmaster to the slave clock in the local PTP 850E Boundary Clock node. If the defined number is exceeded, packets from this grandmaster candidate are discarded and the grandmaster will not be eligible for use by the Boundary Clock node. The default value is 255. The following command can be used to change the Boundary Clock node's maximum number of PTP clocks traversed.

```
root> platform sync ptp-bc clock set max-steps-removed <max-
steps-removed>
```

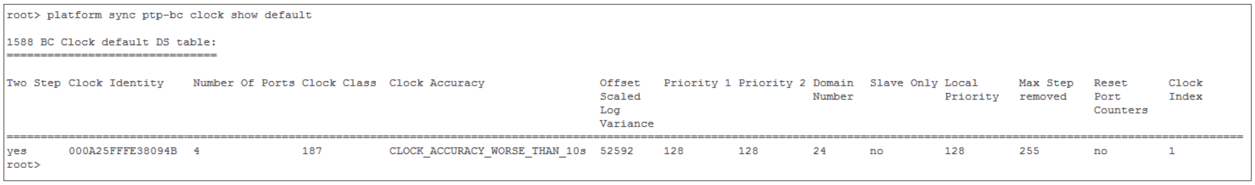
Table 212 Boundary Clock Default Settings – CLI Parameters

Parameter	Input Type	Permitted Values
priority2	Number	0-255
domain-number	Number	24-43
local-priority	Number	1-255
max-steps-removed	Number	1-255

Use the following command to display the Boundary Clock node's default parameters.

```
root> platform sync ptp-bc clock show default
```

Figure 331 1588 Boundary Clock – Default Parameters Sample Display (CLI)



```
root> platform sync ptp-bc clock show default

1588 BC Clock default DS table:
===============================

Two Step Clock Identity    Number Of Ports Clock Class  Clock Accuracy                 Offset   Priority 1 Priority 2 Domain  Slave Only Local      Max Step   Reset      Clock
                                                                                       Scaled                         Number             Priority   removed    Port       Index
                                                                                       Log                                                                     Counters
                                                                                       Variance
==================================================================================================================================================================================
yes      000A25FFFE38094B  4               187          CLOCK_ACCURACY_WORSE_THAN_10s  52592    128        128        24      no         128        255        no         1
root>
```

Table 213 Boundary Clock Default Parameters

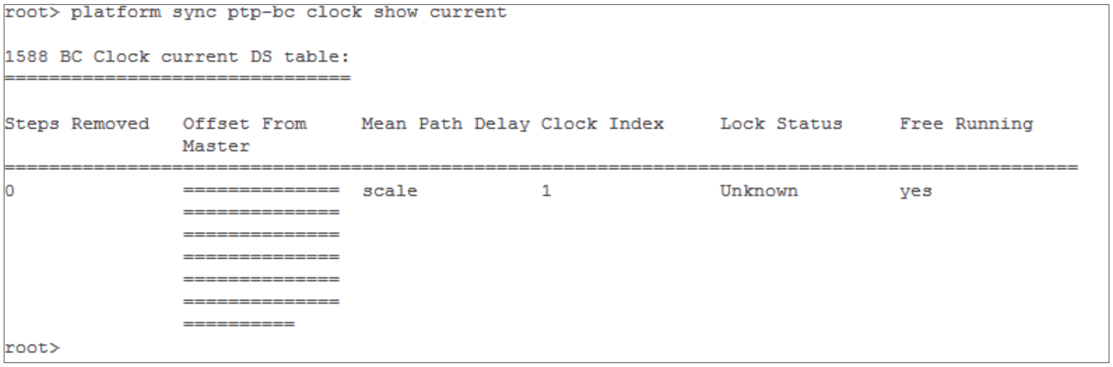
Parameter	Definition
Two Step (read only)	Indicates whether the Boundary Clock node is operating in two-step mode. In PTP 850E, this is always set to Yes.
Clock Identity (read only)	Identifies the system clock.
Number of Ports (read only)	Displays the number of ports on the unit on which Boundary Clock is enabled. The maximum is 16 per PTP 850E unit.
Clock Class (read only)	One of the elements of the clock quality, as defined in IEEE-1588.
Clock Accuracy (read only)	One of the elements of the clock quality, as defined in IEEE-1588.
Offset Scaled Log Variance (read only)	One of the elements of the clock quality, as defined in IEEE-1588.
Priority 1 (read only)	Always displays 128.
Priority 2	One of the factors used by the BMCA to determine the grandmaster. The PTP 850E’s Boundary Clock node advertises this value when it is not locked on an external grandmaster. The default value is 128 (user- configurable).
Domain Number	The default value is 24 (user-configurable).
Slave Only (read only)	Indicates whether the Boundary Clock node is operating in slave mode only. In PTP 850E, this is always set to no.
Max Step Removed	The maximum number of PTP clocks traversed from the grandmaster to the slave clock in the local PTP 850E Boundary Clock node. If the defined number is exceeded, packets from this grandmaster candidate are discarded and the grandmaster will not be eligible for use by the Boundary Clock node. The default value is 255 (user- configurable).
Reset Port Counters	In PTP 850E, this is always set to no.
Clock Index	In PTP 850E, this is always set to 1.

Displaying the Boundary Clock Advanced Parameters (CLI)

Use the following command to display the Boundary Clock node’s general sadvanced parameters.

```
root> platform sync ptp-bc clock show current
```

Figure 332 1588 Boundary Clock – Advanced (General) Parameters Sample Display (CLI)

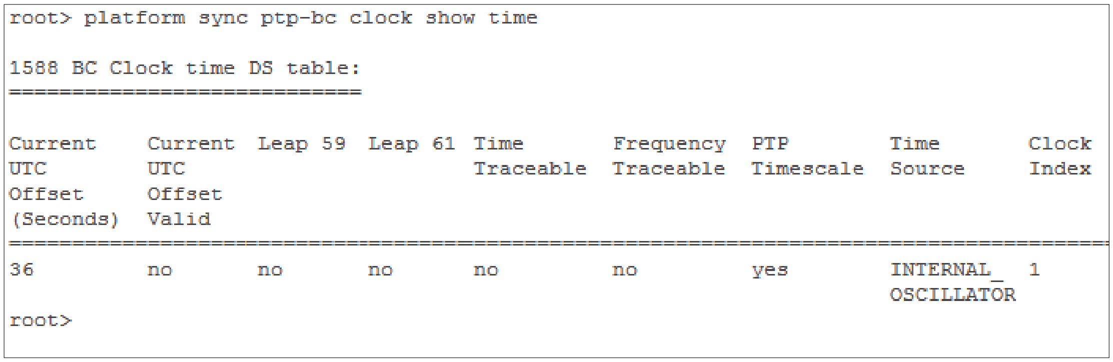


```
root> platform sync ptp-bc clock show current

1588 BC Clock current DS table:
===============================

Steps Removed   Offset From     Mean Path Delay Clock Index     Lock Status     Free Running
                Master
================================================================================================
0               ==============  scale           1               Unknown         yes
                ==============
                ==============
                ==============
                ==============
                ==============
                ==========
root>
```

Use the following command to display information about the Boundary Clock node's current time parameters.

```
root> platform sync ptp-bc clock show time
```

Figure 333 1588 Boundary Clock – Time Parameters Sample Display (CLI)



```
root> platform sync ptp-bc clock show time

1588 BC Clock time DS table:
============================

Current    Current  Leap 59  Leap 61  Time       Frequency  PTP        Time       Clock
UTC        UTC                        Traceable  Traceable  Timescale  Source     Index
Offset     Offset
(Seconds)  Valid
=========================================================================================
36         no       no       no       no         no         yes        INTERNAL_  1
                                                                       OSCILLATOR
root>
```

All of the advanced Boundary Clock parameters are read-only. Below table lists and describes the Boundary Clock advanced parameters.

Table 214 Boundary Clock Advanced Parameters (CLI)

Parameter	Definition
Steps Removed	The number of PTP clocks traversed from the grandmaster to the slave clock in the local PTP 850E Boundary Clock node. You can define a maximum number of steps in the Clock Default Parameters page. See *Displaying and Setting the Boundary Clock Default Parameters*.
Offset from Master (Nanoseconds)	The time difference between the master clock and the local slave clock (in ns).
Mean Path Delay (Nanoseconds)	The mean propagation time for the link between the master and the local slave (in ns).
Lock Status	Provides 1588 Boundary Clock stack lock status information.
Free Running	APR stack manual freerun state.

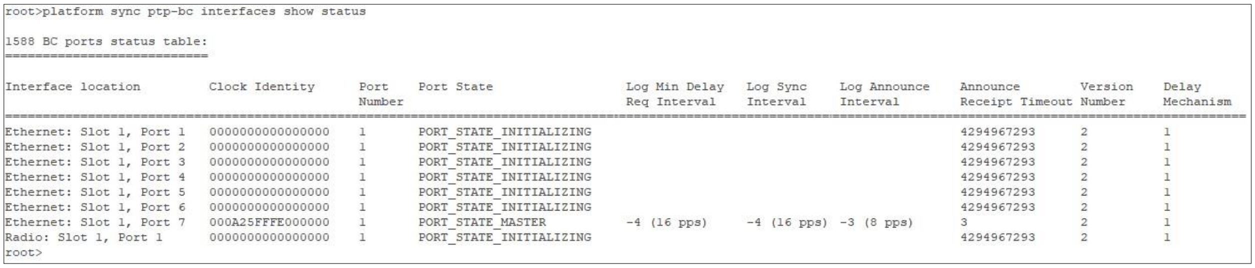
Master Clock Identity	The clock identity of the current master clock.
Master Port Number	The clock identity of the current master port.
Grandmaster Identity	The clock identity of the current grandmaster.
Grandmaster Clock Class	The clock class of the current grandmaster. The clock class is one of the elements of the clock quality, as defined in IEEE-1588.
Grandmaster Clock Accuracy	The clock accuracy of the current grandmaster. The clock accuracy is one of the elements of the clock quality, as defined in IEEE-1588.
Grandmaster Offset Scaled Log Variance	The offset scaled log variance of the current grandmaster. The offset scaled log variance is one of the elements of the clock quality, as defined in IEEE-1588.
Grandmaster Priority 1	The Priority 1 value of the current grandmaster.
Grandmaster Priority 2	The Priority 2 value of the current grandmaster.
Current UTC Offset (Seconds)	The current UTC offset value (in seconds).
Current UTC Offset Valid	Indicates whether the current UTC offset value is valid.
Leap 59	Indicates that the last minute of the current UTC day contains 59 seconds.
Leap 61	Indicates that the last minute of the current UTC day contains 61 seconds.
Time Traceable	Traceability to the primary time reference.
Frequency Traceable	Traceability to the primary frequency reference.
PTP Timescale	Indicates whether the clock time scale of the grandmaster clock is PTP.
Time Source	The source of the time used by the grandmaster clock.

Displaying the Boundary Clock Port Parameters (CLI)

Use the following command to display the Boundary Clock port parameters.

```
root> root> platform sync ptp-bc interfaces show status
```

Figure 334 1588 Boundary Clock Port Parameters (CLI)



```
root>platform sync ptp-bc interfaces show status

1588 BC ports status table:
===========================

Interface location         Clock Identity      Port    Port State                 Log Min Delay   Log Sync    Log Announce    Announce        Version    Delay
                                               Number                             Req Interval    Interval    Interval        Receipt Timeout Number     Mechanism
===================================================================================================================================================================
Ethernet: Slot 1, Port 1   0000000000000000    1       PORT_STATE_INITIALIZING                                                4294967293      2          1
Ethernet: Slot 1, Port 2   0000000000000000    1       PORT_STATE_INITIALIZING                                                4294967293      2          1
Ethernet: Slot 1, Port 3   0000000000000000    1       PORT_STATE_INITIALIZING                                                4294967293      2          1
Ethernet: Slot 1, Port 4   0000000000000000    1       PORT_STATE_INITIALIZING                                                4294967293      2          1
Ethernet: Slot 1, Port 5   0000000000000000    1       PORT_STATE_INITIALIZING                                                4294967293      2          1
Ethernet: Slot 1, Port 6   0000000000000000    1       PORT_STATE_INITIALIZING                                                4294967293      2          1
Ethernet: Slot 1, Port 7   000A25FFFE000000    1       PORT_STATE_MASTER          -4 (16 pps)     -4 (16 pps) -3 (8 pps)      3               2          1
Radio: Slot 1, Port 1      0000000000000000    1       PORT_STATE_INITIALIZING                                                4294967293      2          1
root>
```

Table 215 Boundary Clock Port Parameters (CLI)

Parameter	Definition
Clock Identity	The PTP 850E unit's clock identity. The same value is used for every port that belongs to the Boundary Clock node.
Port Number	Displays the number of the port according to the activation sequence of every port.
Port State	Indicates whether the port is currently acting as Master (distributing PTP to other nodes) or Slave (receiving PTP from a grandmaster).
Log Min Delay Req Interval	The minimum allowed interval between Delay Request messages.
Log Sync Interval	Interval between sync messages.
Log Announce Interval	The interval between Announce messages.
Announce Receipt Timeout	The maximum allowed number of intervals without receiving any Announce messages.
Version Number	Always displays 2.
Delay Mechanism	Always displays 1.

Displaying the Boundary Clock Port Statistics (CLI)

Use the following command to display the Boundary Clock statistics.

```
root> platform sync ptp-bc interfaces show statistics
interface-type <interface-type> slot 1 port <port> clear-on-
read <yes|no>
```

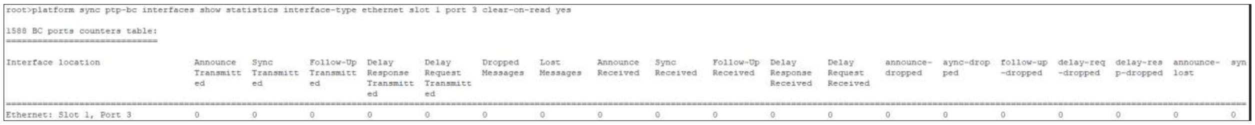
Table 216 Boundary Clock Configuration CLI Parameters

Parameter	Input Type	Permitted Values	Description
interface-type	Variable	ethernet radio	
port	Number	ethernet: 1-7 radio: 1	The port number.
clear-on-read	Boolean	yes no	If yes is selected, the interface statistics are cleared after the command is executed.

The following command displays statistics for Eth3, and clears the statistics after displaying them.

```
root> platform sync ptp-bc interfaces show statistics
interface-type ethernet slot 2 port 1 clear-on-read yes
```

Figure 335 1588 Boundary Clock Statistics (CLI)



```
root>platform sync ptp-bc interfaces show statistics interface-type ethernet slot 1 port 3 clear-on-read yes

1588 BC ports counters table:
=============================

Interface location               Announce  Sync      Follow-Up Delay     Delay     Dropped   Lost      Announce  Sync      Follow-Up Delay     Delay     announce- aync-drop follow-up delay-req delay-res announce- syn
                                 Transmitt Transmitt Transmitt Response  Request   Messages  Messages  Received  Received  Received  Response  Request   dropped   ped       -dropped  -dropped  p-dropped lost
                                 ed        ed        ed        Transmitt Transmitt                                                   Received  Received
                                                               ed        ed
===========================================================================================================================================================================================================================
Ethernet: Slot 1, Port 3         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0
```

Table 217 Boundary Clock Port Statistics (CLI)

Parameter	Definition
Announce Transmitted	The number of Announce messages that have been transmitted from the port.
Sync Transmitted	The number of Sync messages that have been transmitted from the port.
Follow-Up Transmitted	The number of Follow-Up messages that have been transmitted from the port.
Delay Response Transmitted	The number of Delay Response messages that have been transmitted from the port.
Delay Request Transmitted	The number of Delay Request messages that have been transmitted from the port.
Dropped Messages	The number of dropped messages.
Lost Messages	The number of lost messages.

Parameter	Definition
Announce Received	The number of Announce messages that have been received by the port.
Sync Received	The number of Sync messages that have been received by the port.
Follow-Up Received	The number of Follow-Up messages that have been received by the port.
Delay Response Received	The number of Delay Response messages that have been received by the port.
Delay Request Received	The number of Delay Request messages that have been received by the port.

Disabling Boundary Clock (CLI)

Use the following command to disable each Boundary Clock interface in the node. It is important to disable Boundary Clock on the interfaces *before* disabling

1588 PTP.

```
root> platform sync ptp-bc interfaces set interface-type
<interface-type> slot 1 port <port> admin disable
```

After disabling the Boundary Clock interfaces, enter the following command in root view:

```
root> platform sync ptp set admin disable
```

Note

Disabling 1588 PTP disables both Transparent Clock and Boundary Clock, and can drastically affect time synchronization performance in the entire network.

Chapter 24: Access Management and Security (CLI)

This section includes:

- Configuring the General Access Control Parameters (CLI)
- Configuring the Password Security Parameters (CLI)
- Configuring Users (CLI)
- Configuring X.509 CSR Certificates (CLI)
- Configuring HTTPS Cipher Hardening (CLI)
- Blocking Telnet Access (CLI)
- Uploading the Security Log (CLI)
- Uploading the Configuration Log (CLI)
- Enabling NETCONF (CLI)

Related Topics:

- Logging On (CLI)

Configuring the General Access Control Parameters (CLI)

To avoid unauthorized login to the system, the following parameters should be set:

Inactivity Timeout

Blocking access due to login failures

Blocking unused accounts

This section includes:

Configuring the Inactivity Timeout Period (CLI)

Configuring Blocking Upon Login Failure (CLI)

Configuring Blocking of Unused Accounts (CLI)

Configuring the Inactivity Timeout Period (CLI)

A system management session automatically times out after a defined period (in minutes) with no user activity. To configure the session timeout period, enter the following command in root view:

```
root> platform security protocols-control session inactivity-timeout set
<inactivity-timeout>
```

To display the currently configured session timeout period, enter the following command in root view:

```
root> platform security protocols-control session inactivity-timeout show
```

Table 218 Inactivity Timeout Period CLI Parameters

Parameter	Input Type	Permitted Values	Description
inactivity-timeout	Number	1 - 60	The session inactivity timeout period (in minutes).

The following command sets the session inactivity timeout period to 30 minutes:

```
root> platform security protocols-control session inactivity-timeout set
30
```

Configuring Blocking Upon Login Failure (CLI)

Upon a configurable number of failed login attempts, the system blocks the user from logging in for a configurable number of minutes.

To configure the number of failed login attempts that will temporarily block the user from logging into the system, enter the following command in root view:

```
root> platform security access-control block-failure-login attempt set
<attempt>
```

To define the period (in minutes) for which a user is blocked after the configured number of failed login attempts, enter the following command in root view:

```
root> platform security access-control block-failure-login period set
<period>
```

To display the current failed login attempt blocking parameters, enter the following command in root view:

```
root> platform security access-control block-failure-login show
```

Table 219 Blocking Upon Login Failure CLI Parameters

Parameter	Input Type	Permitted Values	Description
attempt	Number	1 - 10	If a user attempts to login to the system with incorrect credentials this number of times consecutively, the user will temporarily be prevented from logging into the system for the time period defined by the platform security access-control block-failure-login period set command.
period	Number	1 - 60	The duration of time, in minutes, that a user is prevented from logging into the system after the defined number of failed login attempts.

The following commands configure a blocking period of 45 minutes for users that perform 5 consecutive failed login attempts:

```
root> platform security access-control block-failure-login attempt set 5
root> platform security access-control block-failure-login period set 45
```

Configuring Blocking of Unused Accounts (CLI)

You can configure a number of days after which a user is prevented from logging into the system if the user has not logged in for the configured number of days. You can also manually block a specific user.

To configure the blocking of unused accounts period, enter the following command in root view:

```
root> platform security access-control block-unused-account period set
<period>
```

Once the user is blocked, you can use the following command to unblock the user:

```
root> platform security access-control user-account block user-name
<user-name> block no
```

To manually block a specific user, enter the following command in root view:

```
root> platform security access-control user-account block user-name
<user-name> block yes
```

To display the currently configured blocking of unused account period, enter the following command in root view:

```
root> platform security access-control block-unused-account show
```

Table 220 Blocking Unused Accounts CLI Parameters

Parameter	Input Type	Permitted Values	Description
period	Number	0, 30 - 90	The number of days after which a user is prevented from logging into the system if the user has not logged in for the configured number of days. If you enter 0, this feature is disabled.
user-name	Text String	Any valid user name.	The name of the user being blocked or unblocked.

The following command configures the system to block any user that does not log into the system for 50 days:

```
root> platform security access-control block-unused-account period set 50
```

The following commands block, then unblock, a user with the user name John_Smith:

```
root> platform security access-control user-account block user-name
John_Smith block yes

root> platform security access-control user-account block user-name
John_Smith block no
```

Configuring the Password Security Parameters (CLI)

You can configure enhanced security requirements for user passwords.

This section includes:

Configuring Password Aging (CLI)

Configuring Password Strength Enforcement (CLI)

Forcing Password Change Upon First Login (CLI)

Displaying the System Password Settings (CLI)

Configuring Password Aging (CLI)

Passwords remain valid from the first time the user logs into the system for the number of days (20-90) set by this command. If you set this parameter to 0, password aging is disabled, and passwords remain valid indefinitely.

To configure password aging, enter the following command in root view:

```
root> platform security access-control password aging set <password
aging>
```

Table 221 Password Aging CLI Parameters

Parameter	Input Type	Permitted Values	Description
password aging	Number	0, 20 - 90	The number of days that user passwords will remain valid from the first time the user logs into the system.

Example

The following command sets the password aging time to 60 days:

```
root> platform security access-control password aging set 60
```

Configuring Password Strength Enforcement (CLI)

To set password strength enforcement, enter the following command in root view:

```
root> platform security access-control password enforce-strength set
<enforce-strength>
```

Table 222 Password Strength Enforcement CLI Parameters

Parameter	Input Type	Permitted Values	Description
password aging	Number	0, 20 - 90	The number of days that user passwords will remain valid from the first time the user logs into the system.
enforce-strength	Boolean	Yes no	When yes is selected: Password length must be at least eight characters. Password must include characters of at least three of the following character types: lower case letters, upper case letters, digits, and special characters. For purposes of meeting this requirement, upper case letters at the beginning of the password and digits at the end of the password are not counted. The last five password you used cannot be reused.

Example

The following command enables password strength enforcement:

```
root> platform security access-control password enforce-strength set yes
```

Forcing Password Change Upon First Login (CLI)

To determine whether the system requires users to change their password the first time they log into the system, enter the following command in root view.

```
root> platform security access-control password first-login set <first-login>
```

To require users to change their password the first time they log in, enter the following command in root view:

```
root> platform security access-control password first-login set yes
```

Table 223 Force Password Change on First Time Login CLI Parameters

Parameter	Input Type	Permitted Values	Description
first-login	Boolean	Yes no	When yes is selected, the system requires users to change their password the first time they log in.

Displaying the System Password Settings (CLI)

Use the following command to display the system password settings:

```
root> platform security access-control password show-all
```

Configuring Users (CLI)

This section includes:

User Configuration Overview (CLI)

Configuring User Profiles (CLI)

Configuring User Accounts (CLI)

Related topics:

Logging On (CLI)

User Configuration Overview (CLI)

User configuration is based on the Role-Based Access Control (RBAC) model. According to the RBAC model, permissions to perform certain operations are assigned to specific roles. Users are assigned to particular roles, and through those role assignments acquire the permissions to perform particular system functions.

In the PTP 850 GUI, these roles are called user profiles. Up to 50 user profiles can be configured. Each profile contains a set of privilege levels per functionality group, and defines the management protocols (access channels) that can be used to access the system by users to whom the user profile is assigned.

The system parameters are divided into the following functional groups:

Security

Management

Radio

TDM

Ethernet

Synchronization

A user profile defines the permitted access level per functionality group. For each functionality group, the access level is defined separately for read and write operations. The following access levels can be assigned:

None – No access to this functional group.

Normal – The user has access to parameters that require basic knowledge about the functional group.

Advanced – The user has access to parameters that require advanced knowledge about the functional group, as well as parameters that have a significant impact on the system as a whole, such as restoring the configuration to factory default settings.

Configuring User Profiles (CLI)

User profiles enable you to define system access levels. Each user must be assigned a user profile. Each user profile contains a detailed set of read and write permission levels per functionality group.

The system includes a number of pre-defined user profiles. You can edit these profiles, and add user profiles. Together, the system supports up to 50 user profiles.

To create a new user profile with default settings, enter the following command:

```
root> platform security access-control profile add name <profile-name>
```

To edit the settings of a user profile, enter the following command:

```
root> platform security access-control profile edit group name <profile-
name> group <group> write-lvl <write-lvl> read-lvl <read-lvl>
```

Table 224 User Profile CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile--name	Text String	Up to 49 characters	The name of the user profile.
group	Variable	security management radio ethernet sync	The functionality group for which you are defining access levels.
write-lvl	Variable	none normal advanced	The read level for the functionality group.
read-lvl	Variable	none normal advanced	The read level for the functionality group.

Example

The following commands create a user profile called “operator” and give users to whom this profile is assigned normal write privileges for all system functionality and advanced read privileges for all functionality except security features.

```
root> platform security access-control profile add name operator

root> platform security access-control profile edit group name operator
group security write-lvl normal read-lvl normal group management write-
lvl normal read-lvl advanced group radio write-lvl normal read-
lvl advanced group ethernet write-lvl normal read-lvl advanced group sync
write-lvl normal read-lvl advanced
```

Limiting Access Protocols for a User Profile (CLI)

The user profile can limit the access channels that users with the user profile can use to access the system. By default, a user profile includes all access channels.

Use the following command to limit the protocols users with this user profile can use to access the system.

```
root> platform security access-control profile edit mng-channel name
<profile-name> channel-type <channel-type> allowed <allowed>
```

Table 225 User Profile Access Protocols CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile--name	Text String	Up to 49 characters	The name of the user profile.
profile-name	Text String	Up to 49 characters	The name of the user profile.
channel-type	Variable	Serial Web NMS Telnet SSH	The access channel type allowed or disallowed by the command for users with this user profile.
allowed	Boolean	yes no	yes – Users with this user profile can access the access channel type defined in the preceding parameter. no - Users with this user profile cannot access the access channel type defined in the preceding parameter.

Example

The following command prevents users with the user profile "operator" from accessing the system via NMS:

```
root> platform security access-control profile edit mng-channel name
operator channel-type NMS allowed no
```

Configuring User Accounts (CLI)

You can configure up to 2,000 users. Each user has a user name, password, and user profile. The user profile defines a set of read and write permission levels per functionality group (see Configuring User Profiles (CLI)).

To create a new user account, enter the following command:

```
root> platform security access-control user-account add user-name <user-name> profile-name <profile-name> expired-date <expired-date>
```

When you create a new user account, the system will prompt you to enter a default password. If Enforce Password Strength is activated (refer to Configuring Password Strength Enforcement (CLI)), the password must meet the following criteria:

Password length must be at least eight characters.

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

The last five password you used cannot be reused.

To block or unblock a user account, enter the following command:

```
root> platform security access-control user-account block user-name <user-name> block <block>
```

To change a user account's expiration date, enter the following command:

```
root> platform security access-control user-account edit expired-date user-name <user-name> expired-date <expired-date>
```

To change a user account's profile, enter the following command:

```
root> platform security access-control user-account edit profile-name user-name <user-name> profile-name <profile name>
```

To delete a user account, enter the following command:

```
root> platform security access-control user-account delete user-name <user-name>
```

To display all user accounts configured on the unit and their settings, including whether the user is currently logged in and the time of the user's last logout, enter the following command:

```
root> platform security access-control user-account show
```

To display the settings of a specific user account, enter the following command:

```
root> platform security access-control user-account show user-name <user-name>
```

Table 226 User Accounts CLI Parameters

Parameter	Input Type	Permitted Values	Description
user-name	Text String	Up to 32 characters	The name of the user profile.
profile name	Text String	Up to 49 characters	The name of the User Profile you want to assign to the user. The User Profile defines the user’s access permissions per functionality group.

Parameter	Input Type	Permitted Values	Description
expired-date	Date	Use the format: YYYY-MM-DD	Optional. The date on which the user account will expire. On this date, the user automatically becomes inactive.
block	Variable	yes no	yes - blocks the account. no - unblocks the account.

Example

The following command creates a user account named Tom_Jones, with user profile “operator”. This user’s account expires on February 1, 2014.

```
root> platform security access-control user-account add user-name
Tom_Jones profile-name operator expired-date 2014-02-01
```

Configuring RADIUS (CLI)

This section includes:

- RADIUS Overview (CLI)
- Activating RADIUS Authentication (CLI)
- Configuring the RADIUS Server Attributes (CLI)

> Note
>
> For instructions on configuring a RADIUS server, see Configuring a RADIUS Server.

RADIUS Overview (CLI)

The RADIUS protocol provides centralized user management services. PTP 850E supports RADIUS server and provides a RADIUS client for authentication and authorization. When RADIUS is enabled, a user attempting to log into the system from any access channels (CLI, WEB, NMS) is not authenticated locally. Instead, the user's credentials are sent to a centralized standard RADIUS server which indicates to the PTP 850E whether the user is known, and which privilege is to be given to the user.

You can define up to two Radius servers. If you define two, one serves as the primary server and the other as the secondary server.

Activating RADIUS Authentication (CLI)

To enable or disable Radius access control, enter the following command:

```
root> platform security radius-admin set <admin>
```

Table 227 Activate RADIUS CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin	Variable	enable disable	Enables or disables Radius access control.

Configuring the RADIUS Server Attributes (CLI)

To configure Radius server attributes, enter the following command:

```
root> platform security radius-server-communication-ipv4 set
server-id <server-id> ip-address <ip-address> port <radius-
port> retries <retries> timeout <timeout> secret <shared-
secret>
```

Table 228 Configure RADIUS Server CLI Parameters

Parameter	Input Type	Permitted Values	Description
server-id	Number	1 2	1 - The primary Radius server 2 - The secondary Radius server.
ip-address	Dotted decimal format	Any valid IP address	The IP address of the Radius server.
radius-port	Number	0-65535	The port ID of the RADIUS server.
retries	Number	3-30	The number of times the device will try to communicate with the RADIUS server before declaring the server to be unreachable.
timeout	Number	1-10	The timeout (in seconds) that the agent will wait in each communication with the selected RADIUS server before retrying if no response is received.
shared- secret	String	Between 22- 128 characters	The shared secret of the RADIUS server.

The following command configures Radius server attributes for the primary Radius server:

```
root> platform security radius-server-communication-ipv4 set
server-id 1 ip-address 192.168.1.99 port 1812 retries 5 timeout
10 secret U8glp3KJ6FKGksdgase4IQ9FMm
```

Displaying Remote Access Users

You can view remote access user connectivity and permissions information for all RADIUS or users currently connected. To do so, enter the following command in root view:

```
root> platform security remote-access show
```

The following user information is displayed, for each currently connected remote access user:

- **User Name** – The user name
- **Access Channels** – The permitted access channels.
- **Number of Active Sessions** – The number of currently open sessions.
- **Security Func Group Read level** – The Read access level in the Security functional group: None, Regular or Advanced.
- **Security Func Group Write level** – The Write access level in the Security functional group: None, Regular or Advanced.
- **Management Func Group Read level** – The Read access level in the Management functional group: None, Regular or Advanced.
- **Management Func Group Write level** – The Write access level in the Management functional group: None, Regular or Advanced.
- **Radio Func Group Read level** – The Read access level in the Radio functional group: None, Regular or Advanced.
- **Radio Func Group Write level** – The Write access level in the Radio functional group: None, Regular or Advanced.
- **TDM Func Group Read level** – The Read access level in the TDM functional group: None, Regular or Advanced.
- **TDM Func Group Write level** – The Write access level in the TDM functional group: None, Regular or Advanced.
- **Eth Func Group Read level** – The Read access level in the Eth functional group: None, Regular or Advanced.
- **Eth Func Group Write level** – The Write access level in the Eth functional group: None, Regular or Advanced.
- **Sync Func Group Read level** – The Read access level in the Sync functional group: None, Regular or Advanced.
- **Sync Func Group Write level** – The Write access level in the Sync functional group: None, Regular or Advanced.

Configuring X.509 CSR Certificates (CLI)

The web interface protocol for accessing PTP 850 can be configured to HTTP (default) or HTTPS. It cannot be set to both at the same time.

Before setting the protocol to HTTPS, you must:

1 Create and upload a CSR file. See Generating a Certificate Signing Request (CSR) File (CLI).

2 Download the certificate to the PTP 850 and install the certificate. See Downloading a Certificate (CLI).

3 Enable HTTPS. See Enabling HTTPS (CLI).

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

> **Note**
>
> For these operations, SFTP must be used.

This section includes:

Generating a Certificate Signing Request (CSR) File (CLI)

Downloading a Certificate (CLI)

Enabling HTTPS (CLI)

Generating a Certificate Signing Request (CSR) File (CLI)

Generating a Certificate Signing Request (CSR) File (CLI)

To set the CSR parameters, enter the following command in root view:

```
root> platform security csr-set-parameters common-name <common-name>
country <country> state <state> locality <locality> organization
<organization> org-unit <org-unit> email <email> file-format <file-
format>
```

To display the currently-configured CSR parameters, enter the following command in root view:

```
root> platform security csr-show-parameters
```

If the IP address family is configured to be IPv4, enter the following command in root view to configure the SFTP server parameters for the CSR file upload:

```
root> platform security csr-set-server-parameters server-ipv4 <server-
ipv4> server-path <server-path> filename <filename> server-username
<username> server-password <password>
```

If the IP address family is configured to be IPv6, enter the following command in root view to configure the SFTP server parameters for the CSR file upload:

```
root> platform security csr-set-server-parameters server-ipv6 <server-
ipv6> server-path <server-path> filename <filename> server-username
<username> server-password <password>
```

To display the currently-configured SFTP parameters for CSR upload, enter the following command in root view:

```
root> platform security csr-show-server-parameters
```

To generate and upload a CSR, enter the following command in root view:

```
root> platform security csr-generate-and-upload
```

To display the status of a pending CSR generation and upload operation, enter the following command in root view:

```
root> platform security csr-generate-and-upload-show-status
```

Table 229 CSR Generation and Upload CLI Parameters

Parameter	Input Type	Permitted Values	Description
common name	String		The fully–qualified domain name for your web server. You must enter the exact domain name.
country	String		The two-letter ISO abbreviation for your country (e.g., US)
state	String		The state, province, or region in which the organization is located. Do not abbreviate.
locality	String		The city in which the organization is legally located.
organization	String		The exact legal name of your organization. Do not abbreviate.
org-unit	String		The division of the organization that handles the certificate.
email	String		An e-mail address that can be used to contact your organization.
file-format	Variable	PEM DER	The file format of the CSR. In this version, only PEM is supported.
server-ipv4	Dotted decimal format.	Any valid IPv4 IP address.	The IPv4 address of the PC or laptop you are using as the SFTP server.
server-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The IPv6 address of the PC or laptop you are using as the SFTP server.

Parameter	Input Type	Permitted Values	Description
server-path	Text String		The directory path to which you are uploading the CSR. Enter the path relative to the SFTP user's home directory, not the absolute path.If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
filename	Text String		The name you want to give the CSR.
username	Text String		The user name for the SFTP session.
password	Text String		The password for the SFTP session. To configure the SFTP settings without a password, simply omit this parameter.

Downloading a Certificate (CLI)

If the IP address family is configured to be IPv4, enter the following command in root view to configure the SFTP server parameters for downloading a certificate:

```
root> platform security certificate-set-download-parameters server-ipv4
<server-ipv4> server-path <server-path> filename <filename> server-
username <username> server-password <password>
```

If the IP address family is configured to be IPv6, enter the following command in root view to configure the SFTP server parameters for downloading a certificate:

```
root> platform security certificate-set-download-parameters server-ipv6 <
server-ipv6> server-path <server-path> filename <filename> server-
username <username> server-password <password>
```

To display the currently-configured SFTP parameters for downloading a certificate, enter the following command in root view:

```
root> platform security certificate-show-download-parameters
```

To download a certificate, enter the following command in root view:

```
root> platform security certificate-download
```

To display the status of a pending certificate download, enter the following command in root view:

```
root> platform security certificate-download-show-status
```

To install a certificate, enter the following command in root view:

```
root> platform security certificate-install
```

Table 230 Certificate Download and Install CLI Parameters

Parameter	Input Type	Permitted Values	Description
server-ipv4	Dotted decimal format.	Any valid IPv4 IP address.	The IPv4 address of the PC or laptop you are using as the SFTP server.
server-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The IPv6 address of the PC or laptop you are using as the SFTP server.
server-path	Text String		The directory path from which you are downloading the certificate. Enter the path relative to the SFTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
filename	Text String		The certificate’s file name in the SFTP server.
username	Text String		The user name for the SFTP session.
password	Text String		The password for the SFTP session. To configure the SFTP settings without a password, simply omit this parameter.

Enabling HTTPS (CLI)

By default, HTTP is used by PTP 850 as its web interface protocol.

To change the protocol to HTTPS, enter the following command in root view:

```
root> platform security url-protocol-set url-protocol https
```

Note

Make sure you have installed a valid certificate in the PTP 850 before changing the web interface protocol to HTTPS. Failure to do this may prevent users from accessing the Web EMS.

To change the protocol back to HTTP, enter the following command in root view:

```
root> platform security url-protocol-set url-protocol http
```

To display which protocol is currently enabled, enter the following command in root view:

```
root> platform security url-protocol-show
```

Configuring HTTPS Cipher Hardening (CLI)

You can configure the PTP 850E to operate in HTTPS strong mode. In HTTPS strong mode, SSLv3, TLSv1.0, and TLSv1.1 are disabled completely and only certain ciphers are supported in TLSv1.2.

For a list of supported HTTPS ciphers, including an indication of which ciphers are supported in HTTPS strong mode, refer to *Annex B – Supported Ciphers for Secured Communication Protocols* in the Release Notes for the System release version you are using.

To set HTTPS strong mode, enter the following command:

```
root> platform security https-ciphers-hardening-level-set level strong
```

To set HTTPS normal mode, enter the following command:

```
root> platform security https-ciphers-hardening-level-set level normal
```

Note: The default HTTP cipher mode is normal.

To display the current HTTPS cipher mode, enter the following command:

```
root> platform security https-ciphers-hardening-level-show
```

Downloading and Installing an RSA Key (CLI)

PTP 850 devices support RSA keys for communication using HTTPS and SSH protocol. The PTP 850 device comes with randomly generated default private and public RSA keys. However, you can replace the private key with a customer-defined private key. The corresponding RSA public key will be generated based on this private key. The file must be in PEM format. Supported RSA private key sizes are 2048, 4096, and 8192.

The following is an example of a valid RSA private key file:

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC+7jRmt27yF4xDh
5Pc8w4ikvXUu32BI0eOyELmeUBnEeIHbCOXD3upi8+ZnH51Q+8hzgoSqXgEYFgZMo
F/sXCrO2yf62UJ5ohj3zadhx/7585zoGwHtYz1S62hsa4+cdAl/i1Vbc6CoUBh5642XYj
e+Q+q1XJtObed884eaQcXUFLIBipYKvVx2kuelymansE91WJU+UjFlc3aiQG8qsSgW5
Ar6wet0pXkP2Vdemo//QAXXjcTqqMBuizrIhIcvi+OKYFI9kSh21ZqSgjvK3cfAssCJBIY5
d6t6bVkX9p2gjo/lPnErjAv7W6IZoemotb5KAeSHeR1sYTw17/xIpM7AgMBAAECggE
AAwIiLKQMOq4kh/UXD/OPAIPDXyp1jjaTw8dBm811OG5wttzXGrxJ+OIFX5Rn79Db
HnbayCiJL8tMe2dx5yhY+hA247roX3ua0w57cuPxnp21izc+S0fC7H/TTM1jpRCbATp
aruTRMIitinZshJGA73Lsod3v36GEXxm/6dHnz/drCs2F4NdHWpjMAAG/1CiBwut8jN
kJUwa78Ivk3JF+XRoZ0txN2mIybQxxzjuNXqZbNO6H3Ua2u1iYyD+McfgOWCCUfSns
tGRhFg0OsQuqj6d74qKVQWaukEH91SVZHEoqX6DgpKy4INZBxORZmITNmadwNh
w5O7rvFxZ205u4gQKBgQDT5bXvc0Ok+Ypm2xnIbu2GFjxNYwYhR3TvHPy14NIO5Q
9I/uDqwrSL1igzaIr6EbZyLu8cDXa4aybrzCyBfPeG89Qq+a6J3JR/RwJndLyjV4h5CT8Z
y4O/wjgTrP3Rhq7LAbWgLjSarafLgruHTcnOifhkK7MK7Fr+xi2IJfOKQQKBgQDmq1eY
NzIMPIATESIsfbkcL49jSsu70kYg0g5IoI6+bVPo9K7mopICtWC/fwdNIUAfO+vr/231Y
UfSo7YNEDNNRoT/NwvqqtAYxZaIUdIQxhMywF9jjYBBuq6+f/7+dwDfNBtMb2q7hc
eTdk6yZ8/MehCkvSwOBmP+Iq0FwTmmewKBgQCIxmj31G1ve+rTXUZmkKIy7OJwiL
AbCRRqnXr3r9Om43151i2QfJNTc1AwKVzTI1ftLNrUT5Q541qnzyxigaoFYmzy0jPCI1
d128/9sE6EW87hImLDg3ynYQMOIaDRc1T8bXHyxzNQb9t+U+DykeD4POifNbD1Ms
Rd3h1xDn/iAQKBgHmKpukJkCNgYgjp7g3AYR084izLaHZa4aDBjc0v4QQtzxzccJwN5
SmQMJ42bL6wecz7YeBEAshcrd+La42Oj7mUAtgHRTwtLOEgm6TQmANGmy8OtjRa
hs4bc5/ICZNDWS5C4m9v9aIBYFuO5wCSOqffWY20L9Zj/6RR+HEj0yCpAoGAHwrbR
qPVZtZptFuNsCq130dtmqI7HFQAIqrc5DwP7YSsznE6biHfLUw891xu0vmevALrCaoe
OMaidugohgiorSJO4qk7I3XN3pUJhPYqbhtdCVnBI2Fm9pr3V/SHGvrI1NW92cXObe
Q2UEBiKPOyQKfOBIbac707u0HqaTu+/ts=
-----END PRIVATE KEY-----
```

You can download and install a private RSA key via HTTP, HTTPS, or SFTP. It is strongly recommended not to use HTTP to download RSA key files.

> Note
>
> To download an RSA key file using HTTP or HTTPS, you must use the Web EMS. See Downloading an RSA Key via HTTP or HTTPS.

To display the current RSA public key, enter the following command in root view:

```
root> platform security rsa-show-installed-public-key
```

If the IP address family is configured to be IPv4, enter the following command in root view to configure the SFTP server parameters for downloading the RSA key:

```
root> platform security rsa-set-download-parameters server-ipv4
<server-ipv4> server-path <server-path> filename <filename>
server-username <username> server-password <password>
```

If the IP address family is configured to be IPv6, enter the following command in root view to configure the SFTP server parameters for downloading the RSA key:

```
root> platform security rsa-set-download-parameters server-ipv6
<server-ipv6> server-path <server-path> filename <filename>
server-username <username> server-password <password>
```

To download an RSA key, enter the following command in root view:

```
root> platform security rsa-download
```

To install the RSA key, enter the following command in root view:

```
root> platform security rsa-install
```

Table 231 RSA Key Download and Install CLI Parameters

Parameter	Input Type	Permitted Values	Description
server-ipv4	Dotted decimal format.	Any valid IPv4 IP address.	The IPv4 address of the PC or laptop you are using as the SFTP server.
server-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The IPv6 address of the PC or laptop you are using as the SFTP server.
server-path	Text String		The directory path from which you are downloading the RSA key. Enter the path relative to the SFTP user's home directory, not the absolute path. If the location is the home directory, it should be populated with "". If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be populated with "".
filename	Text String		The RSA key file’s name in the SFTP server.
username	Text String		The user name for the SFTP session.
password	Text String		The password for the SFTP session. To configure the SFTP settings without a password, populate this parameter with “”..

Blocking Telnet Access (CLI)

You can block telnet access to the unit. By default, telnet access is not blocked.

To block telnet access, enter the following command:

```
root> platform security protocols-control telnet admin set disable
```

To unblock telnet access, enter the following command:

```
root> platform security protocols-control telnet admin set enable
```

To display whether telnet is currently allowed (enable) or blocked (disable), enter the following command:

```
root> platform security protocols-control telnet show
```

Note

When you block telnet, any current telnet sessions are immediately disconnected.

Uploading the Security Log (CLI)

The security log is an internal system file which records all changes performed to any security feature, as well as all security related events.

In order to read the security log, you must upload the log to an FTP or SFTP server. PTP 850 works with any standard FTP or SFTP server. For details, see Installing and Configuring an FTP or SFTP Server.

Before uploading the security log, you must install and configure the FTP server on the laptop or PC from which you are performing the download. See Installing and Configuring an FTP or SFTP Server.

To set the FTP parameters for security log upload, enter the following command in root view:

```
root> platform security file-transfer set server-path <server-path> file-
name <file-name> ip-address <ip-address> protocol <protocol> username
<username> password <password>
```

To display the FTP channel parameters for uploading the security log, enter the following command in root view:

```
root> platform security file-transfer show configuration
```

To upload the security log to your FTP server, enter the following command in root view:

```
root> platform security file-transfer operation set upload-security-log
```

To display the progress of a current security log upload operation, enter the following command in root view:

```
root> platform security file-transfer show operation
```

To display the result of the most recent current security log upload operation, enter the following command in root view:

```
root> platform security file-transfer show status
```

Table 232 Security Log CLI Parameters

Parameter	Input Type	Permitted Values	Description
server-path	Text String		The directory path to which you are uploading the security log. Enter the path relative to the FTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".

Parameter	Input Type	Permitted Values	Description
file-name	Text String		The name you want to give the file you are uploading.
ip-address	Dotted decimal format.	Any valid IP address.	The IP address of the FTP server.
protocol	Variable	ftp sftp	
username	Text String		The user name for the FTP or SFTP session.
password	Text String		The password for the FTP or SFTP session. To configure the FTP settings without a password, simply omit this parameter.

Example

The following commands configure an FTP channel for security log upload to IP address 192.168.1.80, in the directory “current”, with file name “security_log_Oct8.zip”, user name “anonymous”, and password “12345”, and initiate the upload:

```
root> platform security file-transfer set server-path \current file-name
security_log_Oct8.zip ip-address 192.168.1.80 protocol ftp username
anonymous password 12345

root> platform security file-transfer operation set upload-security-log
```

Uploading the Configuration Log (CLI)

The configuration log lists actions performed by users to configure the system. This file is mostly used for security, to identify suspicious user actions. It can also be used for troubleshooting.

In order to upload the configuration log, you must install an FTP or SFTP server on the laptop or PC from which you are performing the upload. PTP 850 works with any standard FTP or SFTP server. For details, see Installing and Configuring an FTP or SFTP Server.

To set the FTP or SFTP parameters for configuration log export, enter the following command in root view:

```
root> platform security configuration-log-upload-params set path <path>
file-name <file-name> ip-address <ip-address> protocol <protocol>
username <username> password <password>
```

To display the FTP or SFTP parameters for configuration log export, enter the following command in root view:

```
root> platform security configuration-log-upload-params show
```

To export the configuration log, enter the following command in root view:

```
root> platform security configuration-log upload
```

To display the status of a configuration log export operation, enter the following command in root view

```
root> platform security configuration-log-upload-status show
```

Table 233 Configuration Log CLI Parameters

Parameter	Input Type	Permitted Values	Description
path	Text String		The directory path to which you are exporting the configuration log. Enter the path relative to the FTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".

Parameter	Input Type	Permitted Values	Description
file-name	Text String		The name you want to give the file you are exporting. **Note:** You must add the suffix .zip to the file name. Otherwise, the file import may fail. You can export the file using any name, then add the suffix .zip manually. For example: UnitInfo.zip If the Unit Information file is exported several times consecutively, the file itself will not be replaced. Instead, the filename will be updated by time stamp. For example: UnitInfo.zip.11-05-14 03-31-04
ip-address	Dotted decimal format.	Any valid IP address.	The IP address of the PC or laptop you are using as the FTP or SFTP server.
protocol	Variable	ftp sftp	The file transfer protocol.
username	Text String		The user name for the FTP or SFTP session.
password	Text String		The password for the FTP or SFTP session. To configure the FTP or SFTP settings without a password, simply omit this parameter.

Note

The path and fie name, together, cannot be more than:

If the IP address family is configured to be IPv4: 236 characters
If the IP address family is configured to be IPv6: 220 characters

Examples

The following commands configure an FTP channel for configuration log export to IP address 192.168.1.99, in the directory “current”, with file name “cfg_log”, user name “anonymous”, and password “12345.”

```
root> platform security configuration-log-upload-params set path \file-
name cfg_log ip-address 192.168.1.99 protocol ftp username anonymous
password 12345

root> platform unit-info channel set protocol frp
```

The following command exports the configuration log to the external server location:

```
root> platform security configuration-log upload
```

Enabling NETCONF (CLI)

PTP 850E devices support SDN, with NETCONF/YANG capabilities. This enables PTP 850E devices to be managed via SDN using Cambium's SDN controller, SDN Master.

In order for the device to be managed via SDN, you must enable NETCONF on the device. By default, NETCONF is disabled.

To enable NETCONF, enter the following command in root view:

```
root>platform security protocols-control netconf admin set enable
```

To disable NETCONF, enter the following command in root view:

```
root>platform security protocols-control netconf admin set disable
```

To display the current NETCONF configuration on the device, enter the following command in root view:

```
root>platform security protocols-control netconf show-all
```

Terminating all Active Sessions (CLI)

You can terminate all active sessions of all users by entering the following command in root view:

```
root> platform security access-control disconnect all
```

This command terminates sessions using any channel type:

- Serial
- Web
- NMS
- Telnet
- SSH

Chapter 25: Alarm Management and Troubleshooting (CLI)

This section includes:

Viewing Current Alarms (CLI)

To display all alarms currently raised on the unit, enter the following command in root view:

```
root> platform status current-alarm show module unit
```

To display the most severe alarm currently raised in the unit, enter the following command in root view:

```
root> platform status current-alarm show most-severe-alarm module unit
```

Viewing the Event Log (CLI)

The Event Log displays a list of current and historical events and information about each event.

To display the event log, enter the following command in root view:

```
root> platform status event-log show module unit
```

To clear the event log, enter the following command in root view:

```
root> platform status event-log clear module unit
```

Editing Alarm Text and Severity (CLI)

You can view a list of alarm types, edit the severity level assigned to individual alarm types, and add additional descriptive text to individual alarm types.

This section includes:

Displaying Alarm Information (CLI)

To display a list of all alarm types and their severity levels and descriptions, enter the following command in root view:

```
root> platform status alarm-management show alarm-id all
```

Editing an Alarm Type (CLI)

To edit an alarm type's severity level, enter the following command in root view:

```
root> platform status alarm-management set alarm-id <alarm-id> severity-
level <severity-level>
```

To add descriptive information to an alarm type, enter the following command in root view:

```
root> platform status alarm-management set alarm-id <alarm-id>
additional-text <additional-text>
```

Table 234 Editing Alarm Text and Severity CLI Parameters

Parameter	Input Type	Permitted Values	Description
alarm-id	Number	All valid alarm type IDs, depending on system configuration	Enter the unique Alarm ID that identifies the alarm type.
severity-level	Variable	indeterminate critical major minor warning	The severity of the alarm, as displayed to users.
additional-text	Text String	255 characters	An additional text description of the alarm type.

Example

The following command changes the severity level of alarm type 401 (Ethernet Loss of Carrier) to minor:

```
root> platform status alarm-management set alarm-id 401 severity-level
minor
```

Setting Alarms to their Default Values (CLI)

To restore an alarm type's severity level and description to their default values, enter the following command in root view:

```
root> platform status alarm-management set alarm-id <alarm-id> restore
default
```

To restore the severity levels and descriptions of all alarm types to their default values, enter the following command in root view:

```
root> platform status alarm-management set all default
```

Table 235 Restoring Alarms to Default CLI Parameters

Parameter	Input Type	Permitted Values	Description
alarm-id	Number	All valid alarm type IDs, depending on system configuration	Enter the unique Alarm ID that identifies the alarm type.

Example

The following command restores alarm type 401 (Ethernet Loss of Carrier) to its default severity level:

```
root> platform status alarm-management set alarm-id 401 restore default
```

Configuring a Timeout for Trap Generation (CLI)

You can configure a wait time of up to 120 seconds after an alarm is cleared in the system before the alarm is actually reported as being cleared. This prevents traps flooding the NMS in the event that some external condition causes the alarm to be raised and cleared continuously.

This means that when the alarm is cleared, the alarm continues to be displayed and no clear alarm trap is sent until the timeout period is finished.

The timeout for trap generation can be configured via CLI. By default, the timeout is 10 seconds.

Note

If the unit is upgraded from an earlier version to System Release 10.0 or higher, the timeout retains its previous value until it is changed. That means if it was never configured, it retains its previous default value of 0. If the unit is set to its factory default configuration, the timeout is set to 10 seconds.

To configure the timeout (in seconds) for trap generation, enter the following command in root view:

```
root> platform status alarm-management alarm-stabilization-set time <0-120>
```

To disable the timeout for trap generation, enter the following command in root view:

```
root> platform status alarm-management alarm-stabilization-set time 0
```

To display the current trap generation timeout, enter the following command in root view:

```
root> platform status alarm-management alarm-stabilization-show
```

The following command sets a trap generation timeout of 60 seconds:

```
root> platform status alarm-management alarm-stabilization-set time 60
```

Disabling Alarms and Events (CLI)

You can choose to disable selected alarms and events. Any alarm or event can be disabled, so that no indication of the alarm is displayed, and no traps are sent for the alarm.

If you disable an alarm that is currently raised, the alarm is treated as if it has been cleared. If an alarm that has been disabled is enabled while it is in a raised state, the alarm is treated as if it has just been raised when it is enabled.

If a timeout for trap generation is configured, and a disabled alarm is enabled while the alarm is raised, the timeout count begins to run when the alarm is enabled. If an alarm is disabled while raised, the timeout count begins to run upon disabling the alarm, and an alarm cleared trap is sent when the timeout expires.

To disable an alarm or event, enter the following command in root view:

```
root> platform status alarm-management set alarm-id <alarm ID> admin disable
```

To enable an alarm or event, enter the following command in root view:

```
root> platform status alarm-management set alarm-id <alarm ID> admin enable
```

To display a list of all disabled alarms and events, and their attributes, enter the following command in root view:

```
root> platform status alarm-management show all admin disable attributes
```

To display a list of all enabled alarms and events and their attributes, enter the following command in root view:

```
root> platform status alarm-management show all admin enable attributes
```

To enable all alarms and events, enter the following command in root view:

```
root> platform status alarm-management set all admin default
```

The alarm status commands `platform status alarm-management show alarm-id all` and `platform status alarm-management show alarm-id <alarm-id> attributes` display alarms, even if they are disabled. The Alarm Admin column in the output displays whether the alarm or event is enabled or disabled.

Configuring Voltage Alarm Thresholds and Displaying Voltage PMs (CLI)

You can configure undervoltage and overvoltage alarm thresholds.

The default thresholds for PTP 850E are:

Undervoltage Raise Threshold: 36V

Undervoltage Clear Threshold: 38V

Overvoltage Raise Threshold: 60V

Overvoltage Clear Threshold: 58V

These thresholds determine when the following alarms are raised and cleared:

Alarm #32000: Under voltage

Alarm #32001: Over voltage

To display the current thresholds, enter the following command in root view.

```
root> platform management voltage thresholds show
```

To change the threshold for raising an undervoltage alarm, enter the following command in root view:

```
root> platform management undervoltage set raise-threshold <0-100>
```

To change the threshold for clearing an undervoltage alarm, enter the following command in root view:

```
root> platform management undervoltage set clear-threshold <0-100>
```

To change the threshold for raising an overvoltage alarm, enter the following command in root view:

```
root> platform management overvoltage set raise-threshold <0-100>
```

To change the threshold for clearing an overvoltage alarm, enter the following command in root view:

```
root> platform management overvoltage set clear-threshold <0-100>
```

You can display voltage PMs that indicate, per 15-minute and 24-hour periods:

The number of seconds the unit was in an undervoltage state during the measured period.

The number of seconds the unit was in an overvoltage state during the measured period.

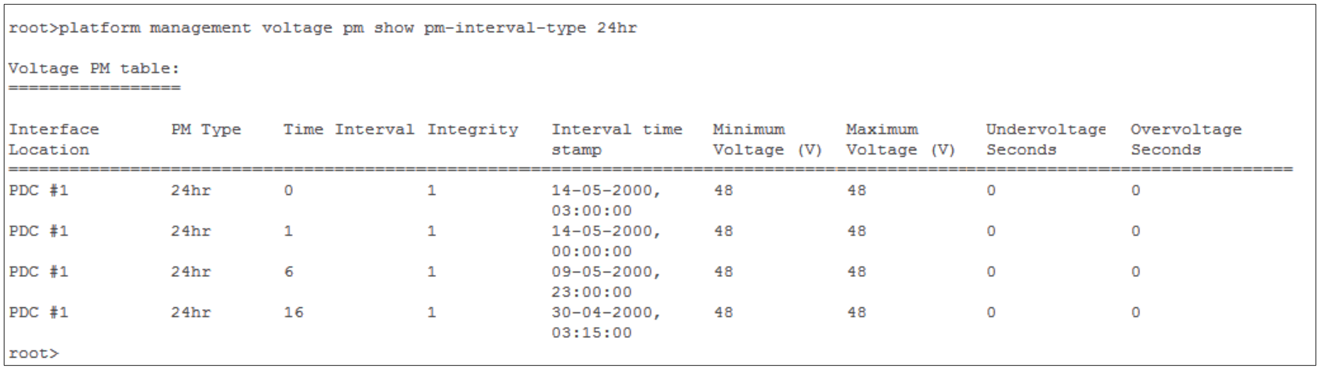
The lowest voltage during the measured period.

The highest voltage during the measured period.

To display voltage PMs, enter the following command in root view:

```
root> platform management voltage pm show pm-interval-type
<all|15min|24hr>
```

For example:



```
root>platform management voltage pm show pm-interval-type 24hr

Voltage PM table:
=================

Interface       PM Type    Time Interval Integrity    Interval time  Minimum      Maximum      Undervoltage  Overvoltage
Location                                              stamp          Voltage (V)  Voltage (V)  Seconds       Seconds
===============================================================================================================================
PDC #1          24hr       0             1            14-05-2000,    48           48           0             0
                                                      03:00:00
PDC #1          24hr       1             1            14-05-2000,    48           48           0             0
                                                      00:00:00
PDC #1          24hr       6             1            09-05-2000,    48           48           0             0
                                                      23:00:00
PDC #1          24hr       16            1            30-04-2000,    48           48           0             0
                                                      03:15:00
root>
```

The Integrity column indicates whether the PM is valid:

0 indicates a valid entry.

1 indicates an invalid entry. This can be caused by a power surge or power failure that occurred during the interval.

Uploading Unit Info (CLI)

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

Note

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

In order to export a unit information file, you must install an FTP or SFTP server on the laptop or PC from which you are performing the upload. PTP 850 works with any standard FTP or SFTP server. For details, see Installing and Configuring an FTP or SFTP Server.

To set the FTP or SFTP parameters for unit information file export, enter one of the following commands in root view. If the IP protocol selected in platform management ip set ip-address-family is IPv4, enter the destination IPv4 address. If the selected IP protocol is IPv6, enter the destination IPv6 address.

```
root> platform unit-info channel server set ip-address <server-ipv4>
directory <directory> filename <filename> username <username> password
<password>

root> platform unit-info channel server-ipv6 set ip-address <server-ipv6>
directory <directory> filename <filename> username <username> password
<password>
```

To set the protocol for unit information file export, enter the following command in root view.

```
root> platform unit-info channel set protocol <protocol>
```

To display the FTP or SFTP parameters for unit information file export, enter one of the following commands in root view:

```
root> platform unit-info-file channel show

root> platform unit-info-file channel-ipv6 show
```

To create a unit information file based on the current state of the system, enter the following command in root view:

```
root> platform unit-info-file create
```

To export the unit information file you just created, enter the following command in root view:

```
root> platform unit-info-file export
```

To display the status of a unit information file export operation, enter the following command in root view

```
root> platform unit-info-file status show
```

Table 236 Uploading Unit Info CLI Parameters

Parameter	Input Type	Permitted Values	Description
server-ipv4	Dotted decimal format.	Any valid IPv4 address.	The IPv4 address of the PC or laptop you are using as the FTP or SFTP server.
server-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The IPv6 address of the PC or laptop you are using as the FTP or SFTP server.
directory	Text String		The directory path to which you are exporting the unit information file. Enter the path relative to the FTP or SFTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "//".
filename	Text String		The name you want to give the file you are exporting. **Note:** You must add the suffix .zip to the file name. Otherwise, the file import may fail. You can export the file using any name, then add the suffix .zip manually.
username	Text String		The user name for the FTP or SFTP session.
password	Text String		The password for the FTP or SFTP session. To configure the FTP or SFTP settings without a password, simply omit this parameter.
protocol	Variable	ftp sftp	The file transfer protocol.

The following commands configure an FTP or SFTP channel for configuration log export to IP address 192.168.1.99, in the directory “current”, with file name “cfg_log”, user name “anonymous”, and password “12345.”

```
root> platform security configuration-log-upload-params set path \\ file-
name cfg_log ip-address 192.168.1.99 protocol ftp username anonymous
password 12345
root> platform unit-info channel set protocol ftp
```

The following commands create a unit information file and export the file to the external server location:

```
root> platform unit-info-file create
root> platform unit-info-file export
```

Example

The following commands configures an FTP channel for unit information file export to IP address 192.168.1.99, in the directory “current”, with file name “version_8_backup.zip”, user name “anonymous”, and password “12345.”

```
root> platform unit-info channel server set ip-address 192.168.1.99
directory \current filename version_8_backup.zip username anonymous
password 12345

root> platform unit-info channel set protocol ftp
```

The following commands create a unit information file and export the file to the external server location:

```
root> platform unit-info-file create

root> platform unit-info-file export
```

Activating the Radio Logger (CLI)

The Radio Logger, when it is activated, gathers technical data about the radio and its operation. By default, the Radio Logger is inactive. It should only be activated by technical support personnel, or by the customer upon request of Customer Support team. Data gathered by the Radio Logger is added to the Unit Info file, which can be exported from the unit and sent to Customer Support upon their request. See ***Error! Reference source not found.***.

> **Note:** In order to conserve CPU resources, do not activate the Radio Logger unless it is necessary for unit diagnostic purposes, and do not leave it active longer than necessary.

To activate the Radio Logger, enter the following command in root view:

```
root> logger start logger-type radio logger-duration <1-1440> slot1 1
port1 1 slot2 2 port2 2
```

The `logger-duration` parameter is set in minutes. The following command activates the logger for 40 minutes:

```
root> logger start logger-type radio logger-duration 40 slot1 2 port1 1
```

To display whether the Radio Logger is currently active, enter the following command in root view:

```
root> logger get status logger-type radio
```

For example, the following display indicates the Radio Logger has been set on both carriers for 20 minutes, and that the Logger is set to run for an additional 1191 seconds:

```
root> logger get status logger-type radio
Logger status:
Logger duration(in minutes): 20
Logger time left(in seconds): 1191
Active instances list:
Slot 1 Port 1
root>
```

To stop the Radio Logger manually, enter the following command in root view:

```
root> logger stop logger-type radio
```

To delete all data that has been saved by the Radio Logger, enter the following command in root view:

```
root> logger delete logger files<logger-type>.
```

Important Note: Whenever you activate the Radio Logger, any previous Radio Logger results are deleted.

Performing Diagnostics (CLI)

This section includes:

Performing Radio Loopback (CLI)

Performing Ethernet Loopback (CLI)

Performing Radio Loopback (CLI)

You can perform loopback on a radio.

To set the timeout for a radio loopback, enter the following command:

```
radio[x/x]> radio loopbacks-timeout set duration <duration>
```

To display the radio loopback timeout, enter the following command:

```
radio[x/x]>radio loopbacks-timeout show
```

To activate an RF loopback, enter the following command:

```
radio[x/x]>rf loopback-rf set admin <admin>
```

Table 237 Radio Loopback CLI Parameters

Parameter	Input Type	Permitted Values	Description
duration	Number	0 – 1440	The timeout, in minutes, for automatic termination of a loopback. A value of 0 indicates that there is no timeout.
admin	Variable	on off	Set on to initiate an RF loopback.

Examples

The following commands initiate an RF loopback on radio carrier 1 with a timeout of two minutes:

```
radio[2/1]> radio loopbacks-timeout set duration 2
radio[2/1]>rf loopback-rf set admin on
```

Performing Ethernet Loopback (CLI)

Ethernet loopbacks can be performed on any logical Ethernet interface except a LAG. When Ethernet loopback is enabled on an interface, the system loops back all packets ingressing the interface. This enables loopbacks to be performed over the link from other points in the network.

To configure loopback on an Ethernet interface, go to interface view for the interface and enter the following command:

```
eth type eth[x/x]> loopback admin <loopback-admin-state>
```

To configure the loopback duration time, go to interface view for the interface and enter the following command:

```
eth type eth[x/x]> loopback set duration <loopback-duration>
```

You can select whether to swap DA and SA MAC addresses during the loopback. Swapping addresses prevents Ethernet loops from occurring. It is recommended to enable MAC address swapping if LLDP is enabled.

To configure MAC address swapping, go to interface view for the interface and enter the following command:

```
eth type eth[x/x]> loopback swap-mac-address admin <MAC_swap-admin-state>
```

To view loopback status, go to interface view for the interface and enter the following command:

```
eth type eth[x/x]> loopback status show
```

Table 238 Ethernet Loopback CLI Parameters

Parameter	Input Type	Permitted Values	Description
loopback-admin-state	Variable	enable disable	Enter **enable** to enable Ethernet loopback on the interface, or **disable** to disable Ethernet loopback on the interface.
loopback-duration	Number	1 - 900	The loopback duration time, in seconds.
MAC_swap-admin-state	Variable	enable disable	Enter **enable** to enable MAC address swapping, or **disable** to disable MAC address swapping.

Examples

The following command enables Ethernet loopback on Ethernet interface 2.

```
eth type eth [1/2]> loopback admin enable
```

The following command sets the loopback duration time to 900 seconds.

```
eth type eth [1/2]> loopback set duration 900
```

The following command enables MAC address swapping during the loopback.

```
eth type eth [1/2]> loopback swap-mac-address admin enable
```

The following command displays Ethernet port loopback status.

```
eth type eth [1/2]> loopback status show
```

Configuring Service OAM (SOAM) Fault Management (FM) (CLI)

This section includes:

SOAM Overview (CLI)

The Y.1731 standard and the MEF-30 specifications define Service OAM (SOAM). SOAM is concerned with detecting, isolating, and reporting connectivity faults spanning networks comprising multiple LANs, including LANs other than IEEE 802.3 media.

Y.1731 Ethernet FM (Fault Management) consists of three protocols that operate together to aid in fault management:

Continuity check

Link trace

Loopback

Note

Link trace is planned for future release.

PTP 850 utilizes these protocols to maintain smooth system operation and non-stop data flow.

The following are the basic building blocks of FM:

MD (Maintenance Domain) – An MD defines the management space on a network, typically owned and operated by a single entity, for which connectivity faults are managed via SOAM.

MA/MEG (Maintenance Association/Maintenance Entity Group) – An MA/MEG contains a set of MEPs or MIPs.

MEP (MEG End Points) – Each MEP is located on a service point of an Ethernet service at the boundary of the MEG. By exchanging CCMs (Continuity Check Messages), local and remote MEPs have the ability to detect the network status, discover the MAC address of the remote unit/port where the peer MEP is defined, and identify network failures.

MIP –(MEG Intermediate Points) – Similar to MEPs, but located inside the MEG and can only respond to, not initiate, CCM messages.

CCM (Continuity Check Message) – MEPs in the network exchange CCMs with their peers at defined intervals. This enables each MEP to detect loss of connectivity or failure in the remote MEP.

Configuring MDs (CLI)

In the current release, you can define one MD, with an **MD Format** of **None**.

To add an MD, enter the following command in root view:

```
root> ethernet soam md create md-id <md-id> md-format none md-name <md-
name> md-level <md-level>
```

Note

Support for MDs with the MD format Character String is planned for future release. In this release, the software enables you to configure such MDs, but they have no functionality.

The following command creates MD 5, named TR-988 with maintenance level 5.

```
root> ethernet soam md create md-id 5 md-format none md-name TR-988 md-
level 5
```

To delete an MD, enter the following command in root view. Before deleting an MD, you must delete any MA/MEG associated with the MD.

```
root> ethernet soam md delete md-id <md-id>
```

To display a list of MDs and their attributes, enter the following command in root view:

```
root> ethernet soam md show
```

Table 239 Maintenance Domain CLI Parameters

Parameter	Input Type	Permitted Values	Description
md-id	Number	1-4294967295	
md-name	String	Up to 43 alphanumeric characters.	An identifier for the MD. The MD Name should be unique over the domain.

Parameter	Input Type	Permitted Values	Description
md-level	Number	0-7	The maintenance level of the MD. The maintenance level ensures that the CFM frames for each domain do not interfere with each other. Where domains are nested, the encompassing domain must have a higher level than the domain it encloses. The maintenance level is carried in all CFM frames that relate to that domain. The maintenance level must be the same on both sides of the link. **Note:** In the current release, the maintenance level is not relevant to the SOAM functionality.

Configuring MA/MEGs (CLI)

You can configure up to 1280 MEGs per network element. MEGs are classified as Fast MEGs or Slow MEGs according to the CCM interval (see Table 240):

Fast MEGs have a CCM interval of 1 second.

Slow MEGs have a CCM interval of 10 seconds, 1 minute, or 10 minutes.

You can configure up to 64 MEP pairs per network element.

To add an MA/MEG, enter the following command in root view:

```
root> ethernet soam meg create meg-id <meg-id> meg-fmt charString meg-
name <meg-name> meg-level <meg-level> service-id <0-4095>
```

Note

In the current release, charString is the only available MEG name format.

The following command creates MEG ID 1, named FR-10, with MEG level 4, assigned to Ethernet service 20.

```
root> ethernet soam meg create meg-id 1 meg-fmt charString meg-name FR-10
meg-level 4 service-id 20
```

To set the interval at which CCM messages are sent within the MEG, enter the following command in root view:

```
root> ethernet soam meg ccm-interval set meg-id <meg-id> ccm <ccm>
```

The following command sets an interval of one second between CCM messages for MEG 1.

```
root> ethernet soam meg ccm-interval set meg-id 1 ccm interval1s
```

To determine whether MIPs are created on the MEG, enter the following command in root view:

```
root> ethernet soam meg mip set meg-id <meg-id> mhf <1-
4|defMHFnone|defMHFdefault|defMHFexplicit|defMHFdefer>
```

The following command creates MIPs on any service point in the MEG:

```
root> ethernet soam meg mip set meg-id 1 mhf defMHFdefault
```

To delete a MEG, enter the following command in root view:

```
root> ethernet soam meg delete <meg-id> ccm <ccm>
```

Note

To can only delete a MEG if no MEPs or MIPs are attached to the MEP.

To display a list of all MEGs configured on the unit, enter the following command in root view:

```
root> ethernet soam meg show
```

To display MEG attributes, including the number of MEPS, local MEPS, and MIPs attached to the MEG, enter the following command in root view:

```
root> ethernet soam meg attributes show meg-id <meg-id>
```

Table 240 SOAM MEG CLI Configuration Parameters

Parameter	Input Type	Permitted Values	Description
meg-id	Number	1-4294967295	Enter an ID for the MEG.
meg-name	String	Up to 44 alphanumeric characters	A name to identify the MEG.

Parameter	Input Type	Permitted Values	Description
meg-level	Number	0-7	The MEG level must be the same for MEGs on both sides of the link. Higher levels take priority over lower levels. If MEGs are nested, the OAM flow of each MEG must be clearly identifiable and separable from the OAM flows of the other MEGs. In cases where the OAM flows are not distinguishable by the Ethernet layer encapsulation itself, the MEG level in the OAM frame distinguishes between the OAM flows of nested MEGs. Eight MEG levels are available to accommodate different network deployment scenarios. When customer, provider, and operator data path flows are not distinguishable based on means of the Ethernet layer encapsulations, the eight MEG levels can be shared among them to distinguish between OAM frames belonging to nested MEGs of customers, providers and operators. The default MEG level assignment among customer, provider, and operator roles is: The customer role is assigned MEG levels 6 and 7 The provider role is assigned MEG levels 3 through 5 The operator role is assigned MEG levels: 0 through 2 The default MEG level assignment can be changed via a mutual agreement among customer, provider, and/or operator roles. The number of MEG levels used depends on the number of nested MEs for which the OAM flows are not distinguishable based on the Ethernet layer encapsulation.
service-id	Number	0-4095	Assign the MEG to an Ethernet service. You must define the service before you configure the MEG.

Parameter	Input Type	Permitted Values	Description
ccm	Variable	interval1s interval10s interval1min interval10min	interval1s – One second (default) interval10s – 10 seconds interval1min – One minute interval10min – 10 minutes It takes a MEP 3.5 times the CCM interval to determine a change in the status of its peer MEP. For example, if the CCM interval is 1 second, a MEP will detect failure of the peer 3.5 seconds after it receives the first CCM failure message. If the CCM interval is 10 minutes, the MEP will detect failure of the peer 35 minutes after it receives the first CCM failure message.
mhf	Variable	defMHFnone defMHFdefault defMHFexplicit defMHFdefer	Determines whether MIPs are created on the MEG. Options are: defMHFnone – No MIPs are created. defMHFdefault – MIPs are created on any service point in the MEG. defMHFexplicit – MIPs are created on the service points of the MEG when a lower-level MEP exists on the service point. This option is usually used when the operator’s domain is encompassed by another domain. defMHFdefer – No MIPs are created.

Configuring MEPs (CLI)

Each MEP is attached to a service point in an Ethernet service. The service and service point must be configured before you configure the MEP. See Configuring Ethernet Services (CLI).

Each MEP inherits the same VLAN, C-VLAN, or S-VLAN configuration as the service point on which it resides. See Configuring Service Points (CLI).

In order to set the VLAN used by CCM/LBM/LTM if the service point is defined ambiguously (for example PIPE, Bundle-C, Bundle-S, or All-to-One), the service point’s C-VLAN/S-VLAN parameter should not be set to N.A.

To configure a MEP, you must:

1 Add MEPs to the relevant MA/MEG. In this stage, you add both local and remote MEPs. The only thing you define at this point is the MEP ID. See Adding Local and Remote MEPs (CLI).

2 Configure the local MEPs. At this point, you determine which MEPs are local MEPs. The system automatically defines the other MEPs you configured in the previous step as remote MEPs. See Configuring the Local MEPs (CLI).

3 Enable the Local MEPs. See Enabling Local MEPs (CLI).

Adding Local and Remote MEPs (CLI)

To add a MEP, enter the following command in root view:

```
root> ethernet soam meg mep add meg-id <meg-id> mep-id <mep-id>
```

The following command adds MEP 25 on MEG 2.

```
root> ethernet soam meg mep add meg-id 2 mep-id 25
```

To remove a MEP, enter the following command in root view:

```
root> ethernet soam meg mep remove meg-id <meg-id> mep-id <mep-id>
```

The following command removes MEP 25 from MEG 2.

```
root> ethernet soam meg mep remove meg-id 2 mep-id 25
```

To display a list of all MEPs that belong to a specific MEG, enter the following command in root view:

```
root> ethernet soam meg mep show meg-id <meg-id>
```

Configuring the Local MEPs (CLI)

Once you have added local and remote MEPs, you must configure the MEPs and determine which are the local MEPs.

To make a defined MEP a local MEP, you must assign the MEP to a service point on the Ethernet service on which the MEG resides.

To assign a MEP to a service point, enter the following command in root view:

```
root> ethernet soam mep create meg-id <meg-id> mep-id <mep-id> sp-id <sp-
id> mep-dir <mep-dir>
```

The following command assigns MEP 35 on MEG 2 to Service Point 3 on the service on which MEG 2 resides.

```
root> ethernet soam mep create meg-id 2 mep-id 35 sp-id 3 mep-dir down
```

To change a MEP from a local to a remote MEP, enter the following command in root view:

```
root> ethernet soam mep delete meg-id <meg-id> mep-id <mep-id>
```

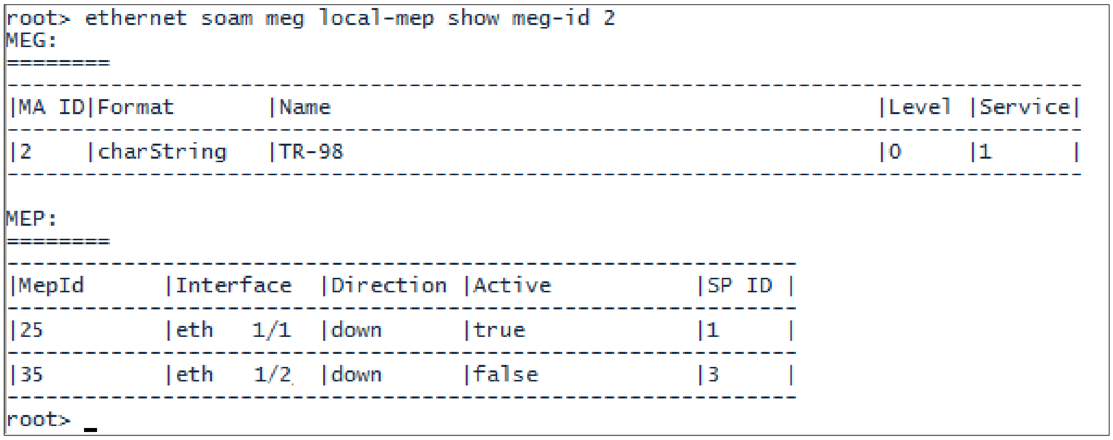
The following command changes MEP 35 from a local to a remote MEP.

```
root> ethernet soam mep delete meg-id 2 mep-id 35
```

To display a list of local MEPs for a specific MEG, enter the following command in root view:

```
root> ethernet soam meg local-mep show meg-id <meg-id>
```

For example:



```
root> ethernet soam meg local-mep show meg-id 2
MEG:
========
------------------------------------------------------------------------------------------------------
|MA ID|Format       |Name                                                  |Level |Service|
------------------------------------------------------------------------------------------------------
|2    |charString   |TR-98                                                 |0     |1      |
------------------------------------------------------------------------------------------------------

MEP:
========
------------------------------------------------------------------------------
|MepId       |Interface   |Direction |Active            |SP ID |
------------------------------------------------------------------------------
|25          |eth   1/1   |down      |true              |1     |
------------------------------------------------------------------------------
|35          |eth   1/2   |down      |false             |3     |
------------------------------------------------------------------------------
root> _
```

Enabling Local MEPs (CLI)

Once you have added a MEP and defined it as a local MEP, you must enable the MEP by setting the MEP to Active, enabling CCM messages from the MEP, and assigning a CCM-LTM priority to the MEP.

To set a MEP to Active, enter the following command in root view:

```
root> ethernet soam mep active set meg-id <meg-id> mep-id <mep-id> mep-
active <mep-active>
```

The following command sets MEP 35 on MEG 2 to Active.

```
root> ethernet soam mep active set meg-id 2 mep-id 35 mep-active true
```

To enable or disable the sending of CCM messages on a MEP, enter the following command in root view:

```
root> ethernet soam mep ccm-enable set meg-id <meg-id> mep-id <mep-id>
enabled <ccm-enabled>
```

The following command assigns enables CCM messages for MEP 35 on MEG 2.

```
root> ethernet soam mep ccm-enable set meg-id 2 mep-id 35 enabled true
```

To set a MEP's CCM-LTM priority, enter the following command in root view:

```
root> ethernet soam mep ccm-ltm-prio set meg-id <meg-id> mep-id <mep-id>
ccm-ltm-priority <ccm-ltm-priority>
```

The following command sets the CCM-LTM priority of MEP 35 in MEG 2 to 5.

```
root> ethernet soam mep ccm-ltm-prio set meg-id 2 mep-id 35 ccm-ltm-
priority 5
```

Table 241 MEP CLI Configuration Parameters

Parameter	Input Type	Permitted Values	Description
meg-id	Number	1-4294967295	Enter an ID for the MEG.
mep-id	Number	1-8191	A name to identify the MEG.
sp-id	Number	0-32	The Service Point ID of the service point to which you want to assign the MEP.

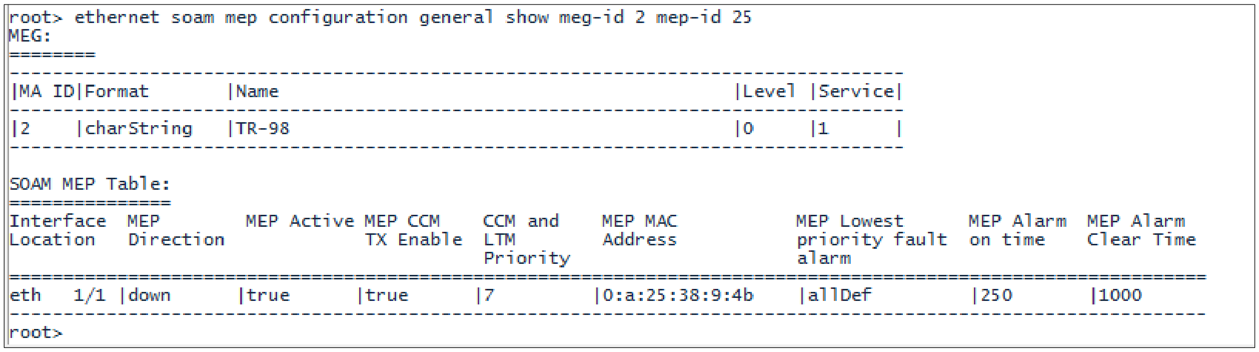
Parameter	Input Type	Permitted Values	Description
mep-dir	Variable	up down	The MEP direction.
ccm-enabled	Variable	true false	true – CCM messages are enabled on the MEP. false – CCM messages are disabled on the MEP.
ccm-ltm-priority	Number	0-7	The p-bit included in CCMs sent by this MEP.
mep-active	Variable	true false	true – The MEP is Active. false – The MEP is Inactive.

Displaying MEP and Remote MEP Attributes (CLI)

To display the attributes of a specific MEP, enter the following command in root view:

```
root> ethernet soam mep configuration general show meg-id <meg-id <meg-id> mep-id <mep-id>
```

For example:

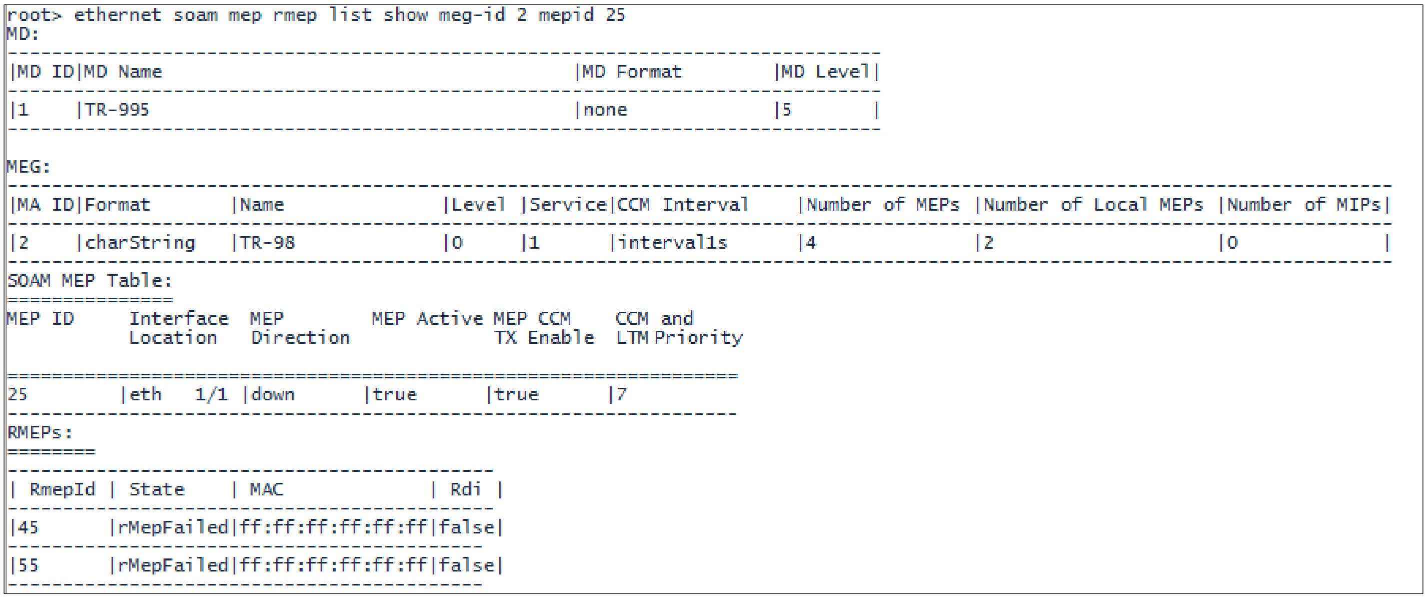


```
root> ethernet soam mep configuration general show meg-id 2 mep-id 25
MEG:
========
-----------------------------------------------------------------------------------
|MA ID|Format       |Name                                          |Level |Service|
-----------------------------------------------------------------------------------
|2    |charString   |TR-98                                         |0     |1      |
-----------------------------------------------------------------------------------

SOAM MEP Table:
===============
Interface  MEP        MEP Active MEP CCM    CCM and    MEP MAC           MEP Lowest      MEP Alarm  MEP Alarm
Location   Direction             TX Enable  LTM        Address           priority fault  on time    Clear Time
                                            Priority                     alarm
===============================================================================================================
eth   1/1 |down      |true      |true      |7        |0:a:25:38:9:4b    |allDef         |250       |1000
---------------------------------------------------------------------------------------------------------------
root>
```

To display a list of remote MEPs (RMEPs) and their parameters per MEG and local MEP, enter the following command in root view:

```
root> ethernet soam mep rmep list show meg-id <meg-id <meg-id> mep-id <mep-id>
```

For example:

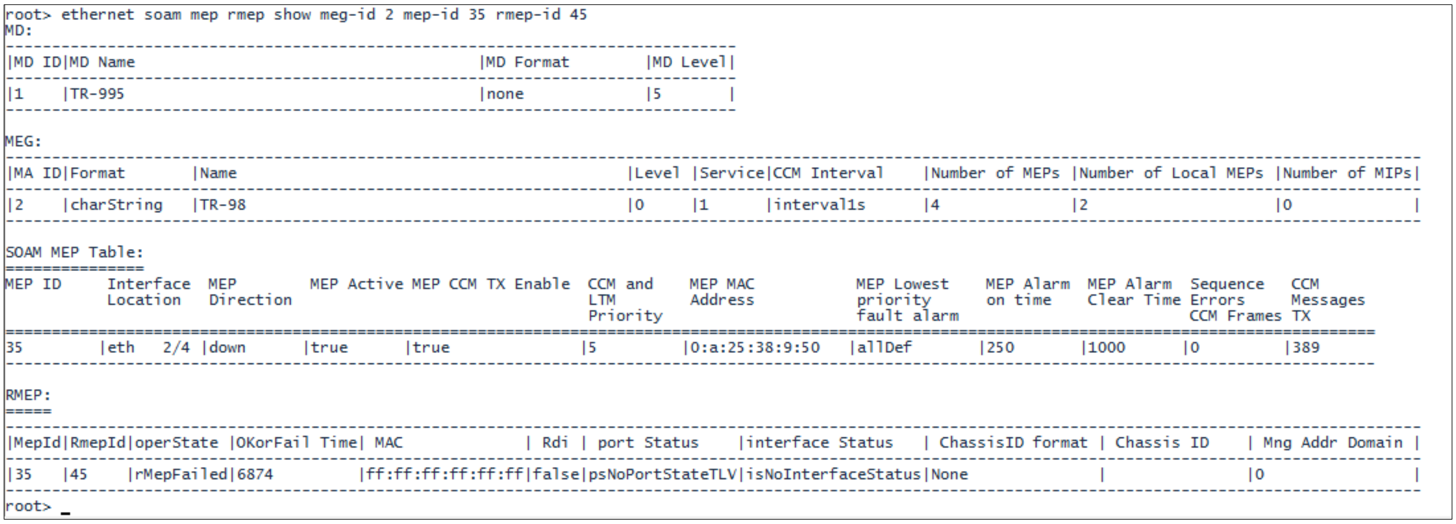


```
root> ethernet soam mep rmep list show meg-id 2 mepid 25
MD:
--------------------------------------------------------------------------------
|MD ID|MD Name                                       |MD Format        |MD Level|
--------------------------------------------------------------------------------
|1    |TR-995                                        |none             |5       |
--------------------------------------------------------------------------------

MEG:
-----------------------------------------------------------------------------------------------------------------------------------
|MA ID|Format       |Name                |Level  |Service|CCM Interval    |Number of MEPs |Number of Local MEPs |Number of MIPs|
-----------------------------------------------------------------------------------------------------------------------------------
|2    |charString   |TR-98               |0      |1      |interval1s      |4              |2                    |0             |
-----------------------------------------------------------------------------------------------------------------------------------
SOAM MEP Table:
===============
MEP ID      Interface  MEP         MEP Active MEP CCM    CCM and
            Location   Direction              TX Enable  LTM Priority

===================================================================
25          |eth   1/1 |down       |true       |true       |7
-------------------------------------------------------------------
RMEPs:
========
---------------------------------------------
| RmepId | State     | MAC               | Rdi |
---------------------------------------------
|45      |rMepFailed|ff:ff:ff:ff:ff:ff|false|
---------------------------------------------
|55      |rMepFailed|ff:ff:ff:ff:ff:ff|false|
---------------------------------------------
```

To display a list of remote MEPs (RMEPs) and their parameters per MEG and local MEP, enter the following command in root view:

```
root> ethernet soam mep rmep show meg-id meg-id < meg-id <meg-id> mep-id
<mep-id> rmep-id <rmep-id>
```

For example:



```
root> ethernet soam mep rmep show meg-id 2 mep-id 35 rmep-id 45
MD:
--------------------------------------------------------------------------------
|MD ID|MD Name                                       |MD Format        |MD Level|
--------------------------------------------------------------------------------
|1    |TR-995                                        |none             |5       |
--------------------------------------------------------------------------------

MEG:
----------------------------------------------------------------------------------------------------------------------------------------------------
|MA ID|Format       |Name                                             |Level  |Service|CCM Interval    |Number of MEPs |Number of Local MEPs |Number of MIPs|
----------------------------------------------------------------------------------------------------------------------------------------------------
|2    |charString   |TR-98                                            |0      |1      |interval1s      |4              |2                    |0             |
----------------------------------------------------------------------------------------------------------------------------------------------------

SOAM MEP Table:
===============
MEP ID      Interface  MEP         MEP Active MEP CCM TX Enable  CCM and     MEP MAC              MEP Lowest     MEP Alarm    MEP Alarm    Sequence    CCM
            Location   Direction                                 LTM         Address              priority       on time      Clear Time  Errors      Messages
                                                                 Priority                         fault alarm                             CCM Frames  TX
=============================================================================================================================================
35          |eth   2/4 |down       |true       |true              |5          |0:a:25:38:9:50     |allDef        |250         |1000        |0           |389
---------------------------------------------------------------------------------------------------------------------------------------------

RMEP:
=====
----------------------------------------------------------------------------------------------------------------------------------------------------
|MepId|RmepId|operState |OKorFail Time| MAC              | Rdi | port Status     |interface Status    | ChassisID format | Chassis ID     | Mng Addr Domain |
----------------------------------------------------------------------------------------------------------------------------------------------------
|35   |45    |rMepFailed|6874         |ff:ff:ff:ff:ff:ff|false|psNoPortStateTLV|isNoInterfaceStatus|None              |                |0                |
----------------------------------------------------------------------------------------------------------------------------------------------------
root> _
```

Table 242 MEP and Remote MEP Status Parameters (CLI)

Parameter	Description
MD Parameters	
MD ID	The MD ID.
MD Name	The MD name (44 characters).
MD Format	The MD format (None).

Parameter	Description
MD Level	The maintenance level of the MD (0-7).
MEG Parameters	
MA ID	The MA/MEG ID.
Format	charString in the current release.
Name	The MA/MEG name (43 characters).
Level	The MEG Level (0-7).
Service	The Service ID of the Ethernet service to which the MEG belongs.
CCM Interval	The interval at which CCM messages are sent within the MEG.
Number of MEPs	The number of MEPs that belong to the MEG.
Number of Local MEPs	The number of local MEPs that belong to the MEG.
Number of MIPs	The number of MIPs that belong to the MEG.
SOAM MEP Table Parameters	
MEP ID	The MEP ID.
Interface Location	The interface on which the service point associated with the MEP is located.
MEP Direction	Up or Down.
MEP Active	Indicates whether the MEP is enabled (true) or disabled (false).
MEP CCM TX Enable	Indicates whether the MEP is configured to send CCMs (true or false).
CCM and LTM Priority	The p-bit included in CCMs sent by the MEP (0-7).
MEP MAC Address	The MAC address of the service point associated with the MEP.
MEP Lowest priority fault alarm	The lowest defect priority that can trigger alarm generation. Defects with a lower priority will not trigger alarms.
MEP Alarm on time	The amount of time that defects must be present before an alarm is generated, in msec intervals (250-1000).
MEP Alarm Clear Time	The amount of time that defects must be absent before an alarm is cleared, msec intervals (250-1000).
Sequence errors CCM Frames	The number of out-of-sequence CCM messages received.
CCM Messages TX	The number of transmitted CCM messages.
RMEP Parameters	

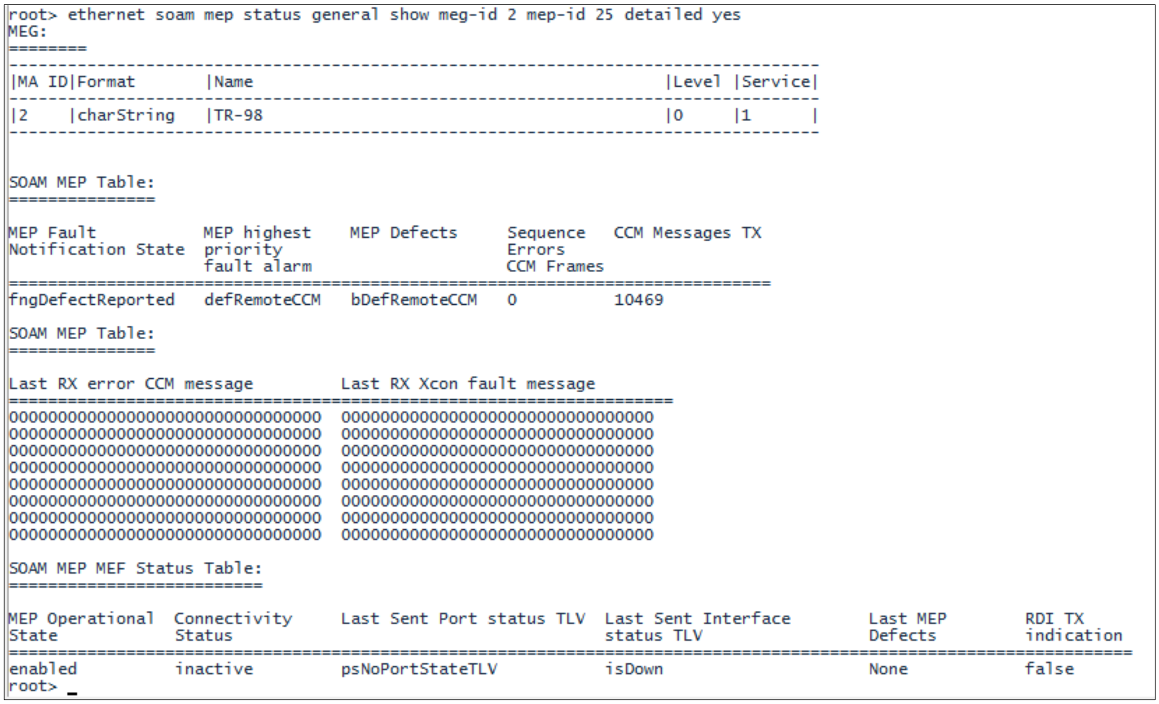
Parameter	Description
MepId	The MEP ID of the local MEP paired with the remote MEP.
Rmep Id	The remote MEP ID.
operState	The operational state of the remote MEP.
OKorFail Time	The timestamp marked by the remote MEP indicating the most recent CCM OK or failure it recorded. If none, this field indicates the amount of time, in msec intervals, since SOAM was activated.
MAC	The MAC Address of the interface on which the remote MEP is located.
Rdi	Displays the state of the RDI (Remote Defect Indicator) bit in the most recent CCM received by the remote MEP: **True** – RDI was received in the last CCM. **False** – No RDI was received in the last CCM.
Port Status	The Port Status TLV in the most recent CCM received from the remote MEP. Reserved for future use.
Interface Status	The Interface Status TLV in the most recent CCM received from the remote MEP. Indicates the operational status of the interface (Up or Down).
Chassis ID Format	Displays the address format of the remote chassis (in the current release, MAC Address).
Chassis ID	Displays the MAC Address of the remote chassis.
Mng Addr Domain	Displays the BASE MAC address of the remote unit (the unit on which the remote MEP resides).,

Displaying Detailed MEP Error Information (CLI)

To display the entire frame of the last CCM error message and the last CCM cross-connect error message received by a specific local MEP, along with other detailed information, enter the following command in root view:

```
root> ethernet soam mep status general show meg-id <meg-id> mep-id <mep-id> detailed yes
```

For example:



```
root> ethernet soam mep status general show meg-id 2 mep-id 25 detailed yes
MEG:
========
-----------------------------------------------------------------------------------
|MA ID|Format       |Name                                          |Level |Service|
-----------------------------------------------------------------------------------
|2    |charString   |TR-98                                         |0     |1       |
-----------------------------------------------------------------------------------


SOAM MEP Table:
===============

MEP Fault           MEP highest    MEP Defects     Sequence   CCM Messages TX
Notification State  priority                       Errors
                    fault alarm                    CCM Frames
==============================================================================
fngDefectReported   defRemoteCCM   bDefRemoteCCM   0          10469

SOAM MEP Table:
===============

Last RX error CCM message         Last RX Xcon fault message
====================================================================
00000000000000000000000000000000  00000000000000000000000000000000
00000000000000000000000000000000  00000000000000000000000000000000
00000000000000000000000000000000  00000000000000000000000000000000
00000000000000000000000000000000  00000000000000000000000000000000
00000000000000000000000000000000  00000000000000000000000000000000
00000000000000000000000000000000  00000000000000000000000000000000
00000000000000000000000000000000  00000000000000000000000000000000
00000000000000000000000000000000  00000000000000000000000000000000

SOAM MEP MEF Status Table:
==========================

MEP Operational  Connectivity     Last Sent Port status TLV  Last Sent Interface        Last MEP        RDI TX
State            Status                                      status TLV                 Defects         indication
===================================================================================================================
enabled          inactive         psNoPortStateTLV           isDown                     None            false
root> _
```

To display the same information without the last RX error CCM and fault messages, enter the following command in root view:

```
root> ethernet soam mep status general show meg-id <meg-id> mep-id <mep-id> detailed no
```

The **Last RX error CCM message** field displays the frame of the last CCM that contains an error received by the MEP.

The **Last RX Xcon fault message** field displays the frame of the last CCM that contains a cross-connect error received by the MEP.

Note

A cross-connect error occurs when a CCM is received from a remote MEP that has not been defined locally.

Performing Loopback (CLI)

To set the interval between loopback message transmissions in a loopback session, enter the following command in root view:

```
root> ethernet soam loopback interval set meg-id <meg-id> mep-id <mep-id> interval <0-60000>
```

For example, the following command sets the loopback interval for MEP 25 on MEG 1 to 5 seconds:

```
root> ethernet soam loopback interval set meg-id 1 mep-id 25 interval 5000
```

To set the loopback message frame size and data pattern, enter the following command in root view:

```
root> ethernet soam loopback data set meg-id <meg-id> mep-id <mep-id>
size <size> pattern <pattern>
```

For example, the following command sets the loopback frame size to 128 and the pattern to zero for MEP 25 on MEG 1 to 5 seconds:

```
root> ethernet soam loopback data set meg-id 1 mep-id 25 size 128 pattern
zeroPattern
```

To set the loopback priority bit size and drop-enable parameters, enter the following command in root view:

```
root> ethernet soam loopback prio set meg-id <meg-id> mep-id <mep-id>
prio <priority> drop <drop>
```

For example, the following command sets a priority bit size of 5 and enables frame dropping for MEP 25 on MEG 1 to 5 seconds:

```
root> ethernet soam loopback prio set meg-id 1 mep-id 25 prio 5 drop true
```

To set the loopback destination by MAC address, set the number of loopback messages to transmit and the interval between messages, and initiate the loopback, enter the following command in root view:

```
root> ethernet soam loopback send meg-id <meg-id> mep-id <mep-id> dest-
mac-addr <dest-mac-addr> tx-num <tx-num> tx-interval <interval>
```

For example, the following command initiates a loopback session with the interface having MAC address 00:0A:25:38:09:4B. The session is configured to send 100 loopback messages at six-second intervals.

```
root> ethernet soam loopback send meg-id 1 mep-id 25 dest-mac-addr
00:0A:25:38:09:4B tx-num 100 tx-interval 6000
```

To set the loopback destination by MEP ID, set the number of loopback messages to transmit and the interval between messages, and initiate the loopback, enter the following command in root view:

```
root> ethernet soam loopback send meg-id <meg-id> mep-id <mep-id> dest-
mep-id <dest-mac-addr> tx-num <tx-num> tx-interval <interval>
```

For example, the following command initiates a loopback session with the interface having MAC address 00:0A:25:38:09:4B. The session is configured to send 100 loopback messages at six-second intervals.

```
root> ethernet soam loopback send meg-id 1 mep-id 25 dest-mac-addr
00:0A:25:38:09:4B tx-num 100 tx-interval 6000
```

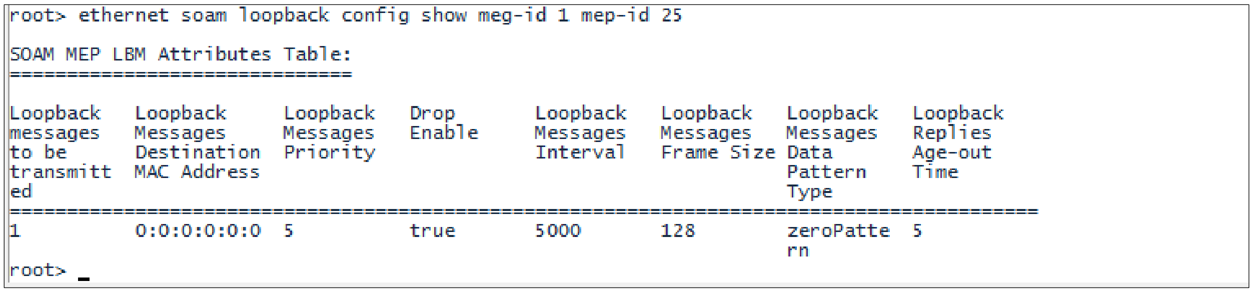
Note

If you initiate the loopback via MEP ID, the loopback will only be activated if CCMs have already been received from the MEP. For this reason, it is recommended to initiate loopback via MAC address.

To display the loopback attributes of a MEP, enter the following command in root view:

```
root> ethernet soam loopback config show meg-id <meg-id> mep-id <mep-id>
```

For example:



```
root> ethernet soam loopback config show meg-id 1 mep-id 25

SOAM MEP LBM Attributes Table:
==============================

Loopback   Loopback     Loopback   Drop       Loopback   Loopback   Loopback   Loopback
messages   Messages     Messages   Enable     Messages   Messages   Messages   Replies
to be      Destination  Priority              Interval   Frame Size Data       Age-out
transmitt  MAC Address                                              Pattern    Time
ed                                                                  Type
==========================================================================================
1          0:0:0:0:0:0  5          true       5000       128        zeroPatte  5
                                                                    rn
root> _
```

To stop a loopback that is already in progress, enter the following command in root view:

```
root> ethernet soam loopback stop meg-id <meg-id> mep-id <mep-id>
```

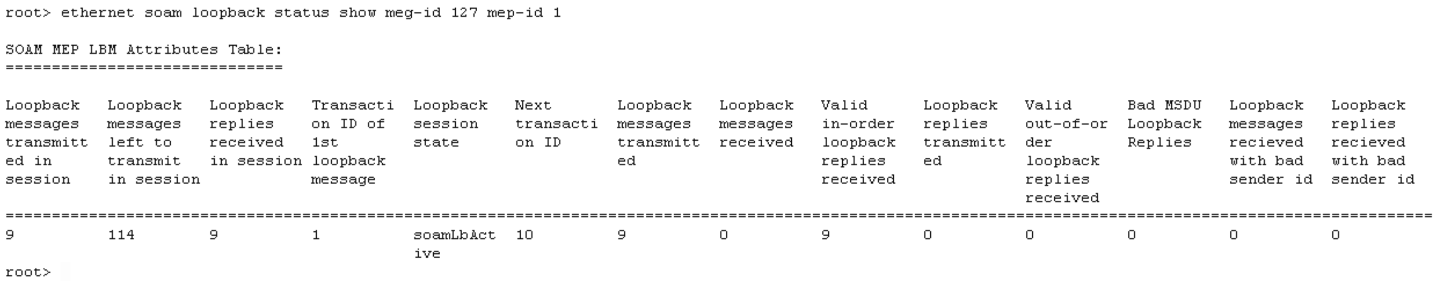
Table 243 Loopback CLI Parameters

Parameter	Input Type	Permitted Values	Description
meg-id	Number	1-4294967295	The MEG ID of the MEG on which the loopback is being configured or run.
mep-id	Number	1-8191	The MEP ID of the MEP on which the loopback is being configured or run.
interval	Number	0-60000	The interval (in ms) between each loopback message. Note that the granularity for this parameter is 100 ms. If you enter a number that is not in multiples of 100, the value will be rounded off to the next higher multiple of 100. Also, the lowest interval is 1000 ms (1 second). If you enter a smaller value, it will be rounded up to 1000 ms.
size	Number	64-1518	The frame size for the loopback messages. Note that for tagged frames, the frame size will be slightly larger than the selected frame size.
pattern	Variable	zeroPattern onesPattern	The type of data pattern to be sent in an OAM PDU Data TLV.
priority	Number	0-7	The priority bit for tagged frames.
drop	Boolean	true false	**true** – Frame dropping is enabled. **false** – Frame dropping is disabled.
dest-mac-addr	Six groups of two hexadecimal digits		The MAC address of the interface to which you want to send the loopback. If you are not sure what the interface's MAC address is, you can get it from the Interface Manager by entering the `platform if-manager show interfaces` command in root view.

Parameter	Input Type	Permitted Values	Description
dest-mep-id	Number	1-8191	The MEP ID of the interface to which you want to send the loopback.
tx-num	Number	0-1024	The number of loopback messages to transmit. If you enter 0, loopback will not be performed.

```
To display loopback results, enter the following command in root
view:root> ethernet soam loopback status show meg-id <meg-id> mep-id
<mep-id>
```

The following is a sample output for this command on MEG ID 127, MEP ID 1.



```
root> ethernet soam loopback status show meg-id 127 mep-id 1

SOAM MEP LBM Attributes Table:
==============================

Loopback   Loopback   Loopback   Transacti  Loopback   Next       Loopback   Loopback   Valid      Loopback   Valid      Bad MSDU   Loopback   Loopback
messages   messages   replies    on ID of   session    transacti  messages   messages   in-order   replies    out-of-or  Loopback   messages   replies
transmitt  left to    received   1st        state      on ID      transmitt  received   loopback   transmitt  der        Replies    recieved   recieved
ed in      transmit   in session loopback                         ed                    replies    ed         loopback              with bad   with bad
session    in session            message                                                received              replies               sender id  sender id
                                                                                                              received
==========================================================================================================================================================
9          114        9          1          soamLbAct  10         9          0          9          0          0          0          0          0
                                            ive
root>
```

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

CW mode enables you to transmit a single or dual frequency tones, for debugging purposes.

To work in CW mode, enter the following command:

```
radio[x/x] modem tx-source set admin enable
```

Once you are in CW mode, you can choose to transmit in a single tone or two tones.

To transmit in a single tone, enter the following command in radio view:

```
radio[x/x] modem tx-source set mode one-tone freq-shift <freq-shift>
```

To transmit two tones, enter the following command in radio view:

```
radio[x/x] modem tx-source set mode two-tone freq-shift <freq-shift>
freq-shift2 <freq-shift>
```

To exit CW mode, enter the following command:

```
radio[x/x] modem tx-source set admin disable
```

Table 244 CW Mode CLI Parameters

Parameter	Input Type	Permitted Values	Description
freq-shift	Number	0-7000	Enter the frequency you want to transmit, in KHz.

The following commands set a single-tone transmit frequency of 5050 KHz on radio interface 1, then exit CW mode and return the interface to normal operation:

```
root> radio slot 2 port 1
radio[2/1] modem tx-source set admin enable
radio[2/1] radio[x/x] modem tx-source set mode one-tone freq-shift 5050
radio[2/1] modem tx-source set admin disable
```

Chapter 26: Maintenance

This section includes:

- Troubleshooting Tips
- Temperature Ranges
- PTP 850C Interface Pin-outs and LEDS
- PTP 850E Interface Pin-outs and LEDS
- PTP 850S Interface Pin-outs and LEDS
- PoE Injector Pin-outs and LEDs – Standard PoE
- PoE Injector Pin-outs and LEDs – Passive PoE

Troubleshooting Tips

Platform

- If during or right after a software upgrade the message *Your session has expired, please login again* appears and you cannot log in, it is recommended to refresh the Web EMS page (F5) after completion of the upgrade. If pressing F5 does not help, clear the browser's cache by pressing Ctrl+Shift+Delete.

XPIC

- For XPIC links, if one of the polarizations has significantly reduced performance, check to make sure the antenna's rectangular interface was replaced with a circular adaptor.[17]
- For XPIC links, the RSL should be similar for both polarizations. The XPI value should be similar for both polarizations; the difference should not be more than 2 dB.[17]

[17] Only relevant for PTP 850C and PTP 850E.

Unit Protection

- When switchover takes place, a series of GARP packets are sent identifying the MAC address of the new management interface. This enables the management device to immediately re-establish the management connection. By default, three GARP packets are sent:
  - The first GARP packet is sent immediately upon switchover.
  - The second GARP packet is sent 500 ms after switchover.
  - The third GARP packet is sent one second after switchover.

  The number of GARP packets is user-configurable. If you experience a delay in re-establishing management, you can increase the number of GARP packets that are sent upon switchover. The number of packets can be changed to any value from 0 (disabling the feature) to 10. Packets are sent at intervals of 500 ms.

  Use the following CLI command to change the number of GARP packets to be sent upon switchover:

```
root>platform management protection debug set garp <0-10>
```

  Use the following CLI command to show the current configuration of this parameter:

```
root>platform management protection debug show garp
```

Temperature Ranges

The following are the permissible unit temperature ranges for PTP 850E.

- **-33°C to 55°** – Temperature range for continuous operating temperature with high reliability.
- **-45°C to 60°C** – Temperature range for exceptional temperatures, tested successfully, with limited margins.

  An extreme temperature alarm (32002) is raised if the unit's internal temperature goes above 90°C or below -40°C. The alarm is cleared when the temperature goes above 87°C or below -37°C.

To display the current unit temperature, see Configuring Unit Parameters.

The permissible IDU humidity range is 5%RH to 100%RH

Troubleshooting Tips

For XPIC links, if one of the polarizations has significantly reduced performance, check to make sure the antenna's rectangular interface was replaced with a circular adaptor.

For XPIC links, the RSL should be similar for both polarizations. The XPI value should be similar for both polarizations; the difference should not be more than 2 dB.

If during or right after a software upgrade the message *Your session has expired, please login again* appears and you cannot log in, it is recommended to refresh the Web EMS page (F5) after completion of the upgrade. If pressing F5 does not help, clear the browser's cache by pressing Ctrl+Shift+Delete.

PTP 850C Interface Pin-outs and LEDS

PTP 850C Interfaces

For traffic, the PTP 850C has an RJ-45 interface and two optical SFP/SFP+ cages. The PTP 850C also has an SFP cage for Dualband configurations.[18]

The PTP 850C also has an RJ-45 management port.

For power, the PTP 850C has a DC power interface (-48V) (P1). The PTP 850C can also be powered via PoE using the RJ-45 traffic port.

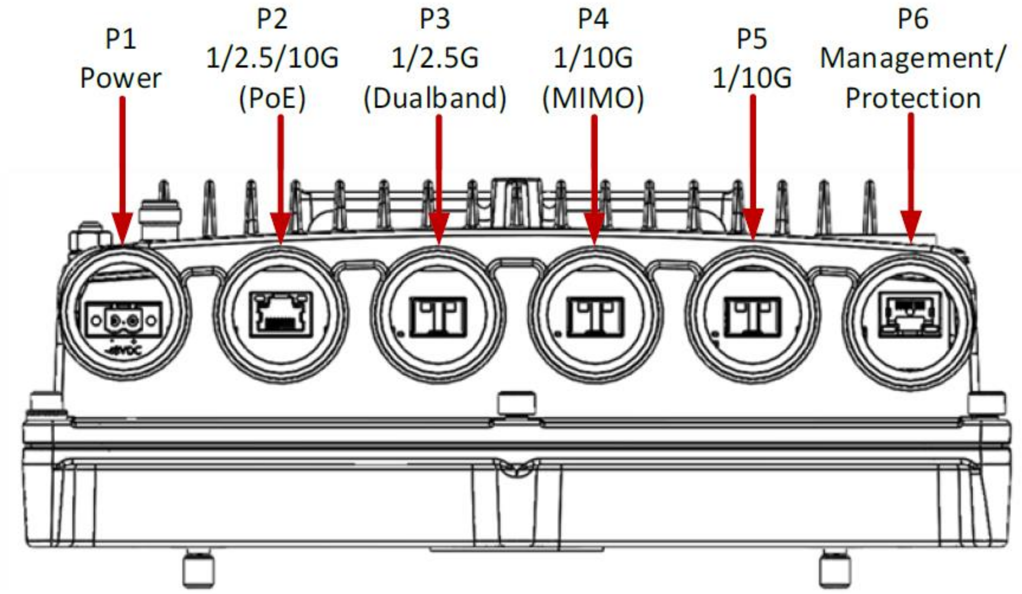


Figure 452: PTP 850C Interfaces

- Port 1 – Power Interface (-48V)
- Port 2 (Eth 1):

  □ RJ-45: 1000BASE-T, 2.5GBASE-T, 10GBASE-T

  □ PoE
- Port 3 (Eth 2):

  □ SFP cage which supports SFP standard □ Electric: 1000BASE-T, 2.5GBASE-T □ Optical: 1000BASE-X, 2.5GBASE-X

  □ Optical: 1/2.5GE Dualband

Note: Dualband is planned for future release.

In System release 11.3, only 2.5G is supported for traffic.

[18] Dualband is planned for future release.

- Port 4 (Eth 3):
  - SFP cage which supports SFP+ standard
  - Electric: 1000BASE-T, 10GBASE-T
  - Optical: 1000BASE-X, 10GBASE-X
  - Optical: Cambium Networks proprietary MIMO interface, if this port serves as an extension port for data sharing. By default, the port is a traffic port unless a MIMO group has been created
- Port 5 (Eth 4):
  - SFP cage which supports SFP+ standard
  - Electric: 1000BASE-T, 10GBASE-T
  - Optical: 1000BASE-X, 10GBASE-X

Note: In System relase 11.3, only 10G is supported.

- Port 6:
  - RJ-45: 100BASE-T
  - Management and Protection port (no traffic)
- 2 RF Interfaces: Standard interface per frequency band
- RSL interface: BNC connector
- Source sharing: TNC connector
- Grounding screw

PTP 850C Interface Pin-outs

P2 (Eth 1) – PoE GbE Electrical Interface (RJ-45)

Table 295: PTP 850C P2 PoE Electric Interface - RJ-45/ Pinouts

Pin no.	Description
1	BI_DA+ (Bi-directional pair +A)
2	BI_DA- (Bi-directional pair -A)
3	BI_DB+ (Bi-directional pair +B)
4	BI_DC+ (Bi-directional pair +C)
5	BI_DC- (Bi-directional pair -C)
6	BI_DB- (Bi-directional pair -B)
7	BI_DD+ (Bi-directional pair +D)
8	BI_DD- (Bi-directional pair -D)

23.3.2.1 P3 (Eth 2) GbE Optical Interface (SFP)

P3 is an SFP cage that supports the SFP standard. This port is used exclusively for Dualband configurations.

P4 (Eth 3) 10G Optical Interface (SFP+)

P4 is an SFP cage that supports the SFP and SFP+ standards.

P5 (Eth 4) 10G Optical Interface (SFP+)

P5 is an SFP cage that supports the SFP and SFP+ standards.

P6 –Management Electrical Interface (RJ-45)

Table 296: PTP 850C MGT Interface - RJ-45/ Pinouts

Pin no.	Description
1	BI_DA+ (Bi-directional pair +A)
2	BI_DA- (Bi-directional pair -A)
3	BI_DB+ (Bi-directional pair +B)
4	BI_DC+ (Bi-directional pair +C)
5	BI_DC- (Bi-directional pair -C)
6	BI_DB- (Bi-directional pair -B)
7	BI_DD+ (Bi-directional pair +D)
8	BI_DD- (Bi-directional pair -D)

Table 297: GbE Port Pin-Outs

RSL Interface

PTP 850E uses a two-pin connection to measure the RSL level using standard voltmeter test leads:

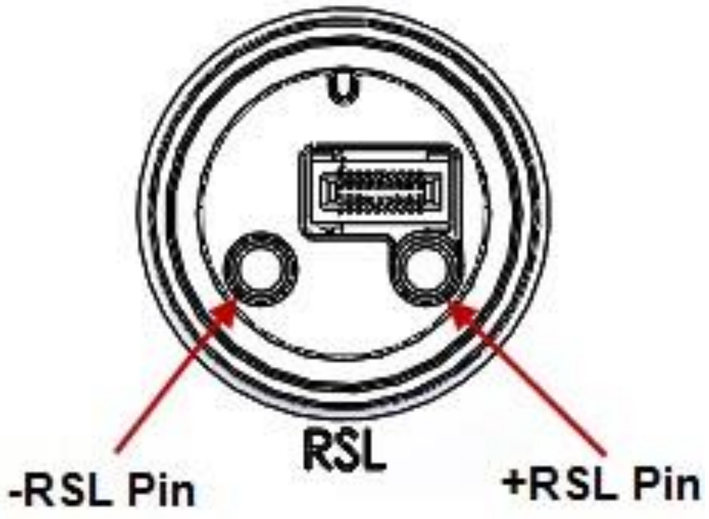


Figure 453: RSL Pins

PTP 850C LEDs

PTP 850C provides the following LEDs to indicate the status of the unit's interfaces, and the unit as a whole:

- P2 (Eth 1) – PoE GbE Electrical Interface (RJ-45) LEDs
- P3 (Eth 2) GbE Optical Interface (SFP) LEDs
- P4 (Eth 3) 10G Optical Interface (SFP+)
- P5 (Eth 4) 10G Optical Interface (SFP+)
- Status LED

P2 (Eth 1) – PoE GbE Electrical Interface (RJ-45) LEDs

Eth 1 is an RJ-45 traffic and PoE interface with two green LEDs, one on either side of the interface. Both LEDs indicate the interface's Admin and cable connection status:

Note: Only the right LED shows Blinking Green to indicate when there is traffic on the interface.

The left LED indicates the link status In the current release, this LED is Green when Admin is Enabled.

The right LED indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

- **Off** – Admin is Disabled *or* no cable is connected to the interface.
- **Green** – Admin is Enabled and a cable is connected to the interface.
- **Blinking Green** – Admin is Enabled and a cable is connected to the interface, *and* there is traffic on the interface.

P3 (Eth 2) GbE Optical Interface (SFP) LEDs

P3 is an SFP cage that supports the SFP standard. This port is used exclusively for Dualband configurations.

Note: Dualband is planned for future release.

There is one Green LED to the left of the interface. The LED indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

- **Off** – Admin is Disabled *or* no cable is connected to the interface.
- **Green** – Admin is Enabled and a cable is connected to the interface.
- **Blinking Green** – Admin is Enabled and a cable is connected to the interface, *and* there is traffic on the interface.

Note: The LED does not indicate traffic on the interface (Blinking Green) in 2.5G mode.

P4 (Eth 3) 10G Optical Interface (SFP+)

P4 is an SFP cage that supports the SFP and SFP+ standards.

There is one Green LED to the left of the interface. The LED indicates the interface's Admin and cable connection status:

- **Off** – Admin is Disabled *or* no cable is connected to the interface.
- **Green** – Admin is Enabled and a cable is connected to the interface.

P5 (Eth 4) 10G Optical Interface (SFP+)

P5 is an SFP cage that supports the SFP and SFP+ standards.

There is one Green LED to the left of the interface. The LED indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

- **Off** – Admin is Disabled *or* no cable is connected to the interface.
- **Green** – Admin is Enabled and a cable is connected to the interface.
- **Blinking Green** – Admin is Enabled and a cable is connected to the interface, *and* there is traffic on the interface.

Management/Protection GbE Electrical Interface (RJ-45) LEDs

P6 is an RJ-45 management interface. There are two LEDs next to the MGT interface, a Green LED to the left of the interface and an Orange LED to the right of the interface.

The Green LED indicates the interface's status as a management port:

- **Off** – Admin is Disabled.
- **Green** – Admin is Enabled.
- **Blinking Green** – Admin is Enabled and management traffic is passing through the interface (TX, RX, or both).

If the port is being used for protection, the Orange LED indicates the status of the mate unit:

- **Off** – The interface is not operational (Down).
- **Green** – The interface is operational (Up).
- **Blinking Green** – The interface is operational, *and* there is traffic on the interface (TX, RX, or both).

Note: Unit protection is planned for future release.

Status LED

The Status LED is located on the front of the PTP 850C unit, above the RSL interface. It indicates the overall status of the unit:

- **Off** – The power is off.
- **Red** – The unit is in init stage.
- **Blinking Red** – The unit has a Major or Critical alarm.
- **Green** – The unit is Up, all enabled radios are Up, and there are no Major or Critical alarms. In unit protection configurations, Green indicates that the unit is the Active unit.
- **Blinking Green** – The unit is Up, all enabled radios are Up, and there are no Major or Critical alarms. In unit protection configurations,

Blinking Green indicates that the unit is the Standby unit.

Note: Unit protection for PTP 850C is planned for future release.

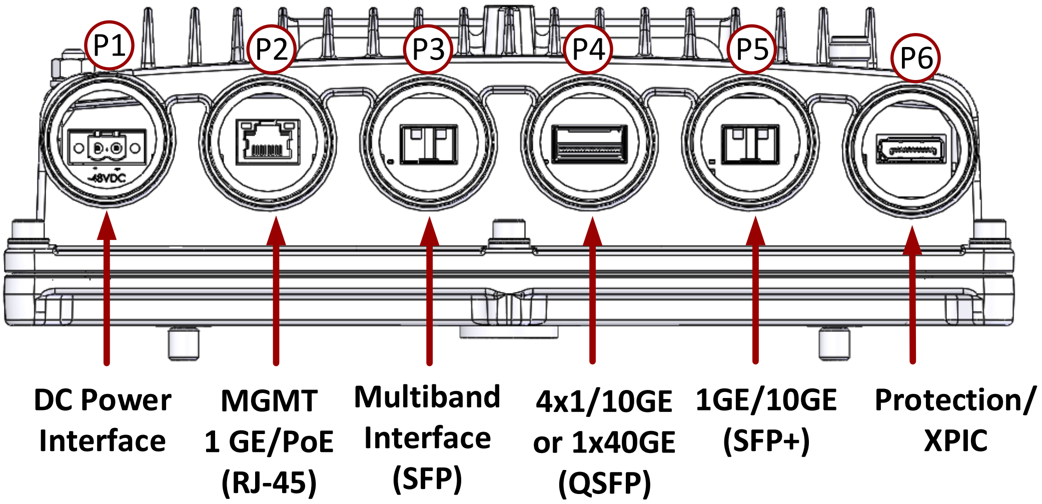
PTP 850E Connector Pin-outs

The PTP 850E has an optical SFP cage, an optical SFP/SFP+ cage, and a QSFP cage for traffic and one RJ-45 port for management and PoE.

For power, the PTP 850E has a DC power interface (-48V) (P1). Optionally, when used in all-outdoor configurations, the PTP 850E can also receive PoE power from a Cambium-approved PoE injector via P2, an RJ-45 port that is also used for management.

Power redundancy can be achieved by using both a DC power input and a passive PoE injector simultaneously. The PTP 850E monitors both power feeds and uses the best power source at any given moment.

Figure 336 PTP 850E Interfaces



Port 1 – Power Interface (-48V)

Port 2 (MNG 1/Eth 1):

- Electric: 10/100/1000Base-T RJ-45
- Management port (no traffic)
- PoE

Port 3 (Eth 2):

- SFP cage which supports SFP standard
- 1/2.5GE MultiBand port (user-configurable)

Port 4 (Eth 3, Eth 4, Eth 5, Eth 6):

- QSFP cage which supports QSFP standard
- 4x1G/10G or 1x40GE Eth traffic (user configurable)
- Option for SFP+ (1x10GE) with adaptor

Port 5 (Eth 7):

- SFP cage which supports SFP+ standard
- 10GE Eth traffic

Port 6:

- External Connection – Reserved for future use.

Antenna Port – Cambium proprietary flange (flange compliant with UG385/U)

RSL interface – DVM interface to enable voltage measurement for RSL indication. The RSL measurement is performed using standard DVM testing probes. To access the RSL interface, the user must remove the port’s cover and insert the DVM plugs into the sockets, according to the polarization markings.

Grounding screw

P2 (Eth 1) – MGT/PoE GbE Electrical Interface (RJ-45)

Table 245: PTP 850E MGT Interface - RJ-45/ Pinouts

Pin no.	Description
1	BI_DA+ (Bi-directional pair +A)
2	BI_DA- (Bi-directional pair -A)
3	BI_DB+ (Bi-directional pair +B)
4	BI_DC+ (Bi-directional pair +C)
5	BI_DC- (Bi-directional pair -C)
6	BI_DB- (Bi-directional pair -B)
7	BI_DD+ (Bi-directional pair +D)
8	BI_DD- (Bi-directional pair -D)

P3 (Eth 2) GbE Optical Interface (SFP)

P3 is an SFP cage that supports the SFP standard. This port is used exclusively for Multiband configurations.

P4 (Eth 3, Eth 4, Eth 5, Eth 6) 40 GbE Optical Interface (QSFP)

P4 (QSFP) is a QSFP cage which supports the QSFP standard. With a QSFP to SFP adaptor, it also supports the SFP and SFP+ standards.

In release 11.1, Port 4 supports 4x1/10Gbps configurations. With a QSFP-to-SFP adaptor, Port 4 also supports 1x1/10Gbps configurations.

P5 (Eth 7) 10G Optical Interface (SFP+)

Eth1 is an SFP cage that supports the SFP+ standard. Eth 7 is supported for 10G Ethernet traffic only.

Protection/XPIC Port

This port is reserved for future use.

RSL Interface

PTP 850E uses a two-pin connection to measure the RSL level using standard voltmeter test leads:

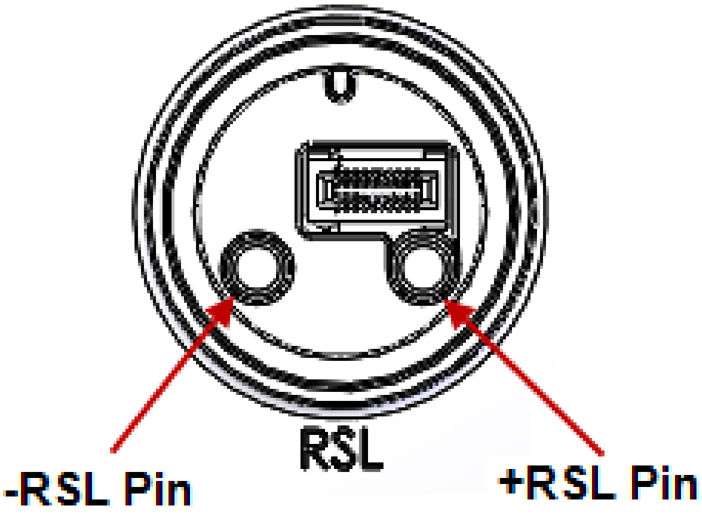


Figure 337: RSL Pins

PTP 850E LEDs

The PTP 850E provides the following LEDs to indicate the status of the unit's interfaces, and the unit as a whole:

- P2 MGT/PoE GbE Electrical Interface (RJ-45) LEDs
- P4/Eth3-6 40G Optical Interface (QSFP) LED
- P5/Eth7 1/10G Optical Interface (SFP+) LEDs
- Status LED
- Protection LED

P2 MGT/PoE GbE Electrical Interface (RJ-45) LEDs

There are two LEDs next to the MGT interface, a Green LED to the left of the interface and an Orange LED to the right of the interface.

The Orange LED indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

Off - Admin is Disabled *or* no cable is connected to the interface.

Green - Admin is Enabled and a cable is connected to the interface.

Blinking Green - Admin is Enabled and a cable is connected to the interface, *and* there is traffic on the interface.

The Green LED is not functional in this release.

P4/Eth3-6 40G Optical Interface (QSFP) LEDs

P4 (QSFP) is a QSFP cage which supports the QSFP standard. With a QSFP-to-SFP adaptor, it also supports the SFP and SFP+ standards.

In System release 11.1, Port 4 supports 4x1/10Gbps configurations. These are configured as Eth 3, Eth4, Eth5, and Eth6. With a QSFP-to-SFP adaptor, it also supports 1x1/10Gbps configurations (Eth3).

There is one Green LED to the left of the interface. This LED indicates the status of the interface:

- **Off** – Admin is Disabled for all of the interfaces connected to P4 (Eth3, Eth4, Eth5, and Eth6), or no cable is connected to the interface.
- **Green** – Admin is Enabled for at least one of the interfaces connected to P4 and a cable is connected to the interface.

P5/Eth7 1/10G Optical Interface (SFP+) LEDs

Eth1 is an SFP cage that supports regular SFP and SFP+.

There is one Green LED to the left of the interface. The LED is for Eth7 and indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

Off - Admin is Disabled *or* no cable is connected to the interface.

Green - Admin is Enabled and a cable is connected to the interface.

Blinking Green - Admin is Enabled and a cable is connected to the interface, *and* there is traffic on the interface.

Note

The LED does not indicate traffic on the interface (Blinking Green) in 10G mode.

Status LED

The Status LED indicates the status of the main board:

Off – The power is off.

Red – The unit is initializing.

Red Blinking - The power is on, and one or more major or critical alarms are raised.

Green - The power is on, the unit is up, the radio is up, and no major or critical alarms are raised.

Protection LED

Reserved for future use.

PTP 850S Interface Pin-outs

Port 1 – MGT/PoE GbE Electrical Interface (RJ-45)

Table 299: PTP 850S MGT Interface - RJ-45/ Pinouts

Pin no.	Description
1	BI_DA+ (Bi-directional pair +A)
2	BI_DA- (Bi-directional pair -A)
3	BI_DB+ (Bi-directional pair +B)
4	BI_DC+ (Bi-directional pair +C)
5	BI_DC- (Bi-directional pair -C)
6	BI_DB- (Bi-directional pair -B)
7	BI_DD+ (Bi-directional pair +D)
8	BI_DD- (Bi-directional pair -D)

Port 2 – Eth2/Eth3 GbE Optical Interface (SFP/CSFP)

Eth2/Eth3 is an SFP cage that supports regular and CSFP standards.

Port 3 – Eth1 10G Optical Interface (SFP+)

Eth1 is an SFP cage that supports the SFP+ standard. Eth1 can be configured by the user for 1G or 10G Ethernet traffic.

EXT – Extension Port

This port is reserved for future use.

Power Adaptor

For configurations in which power is not provided via PoE, a special adaptor (PTP 820_Mini_Power_Adaptor) is available that enables users to connect a two-wire power connector to the PoE port. This adaptor is located inside of the gland. In such configurations, only one electrical GbE interface is available (MGT).

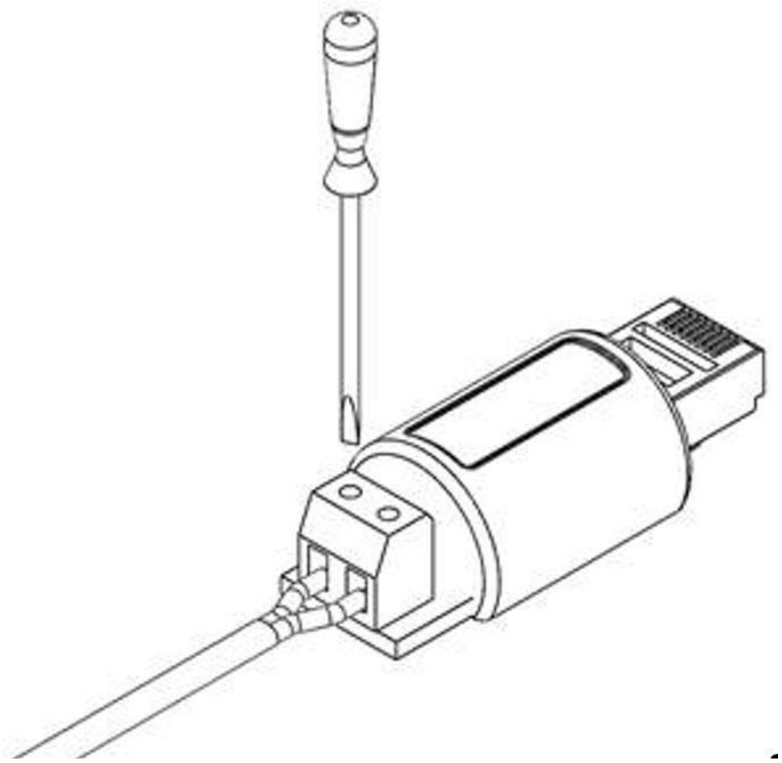


Figure 459: Two-Wire to PoE Port Power Adaptor

RSL Interface

PTP 850S uses a two-pin connection to measure the RSL level using standard voltmeter test leads:

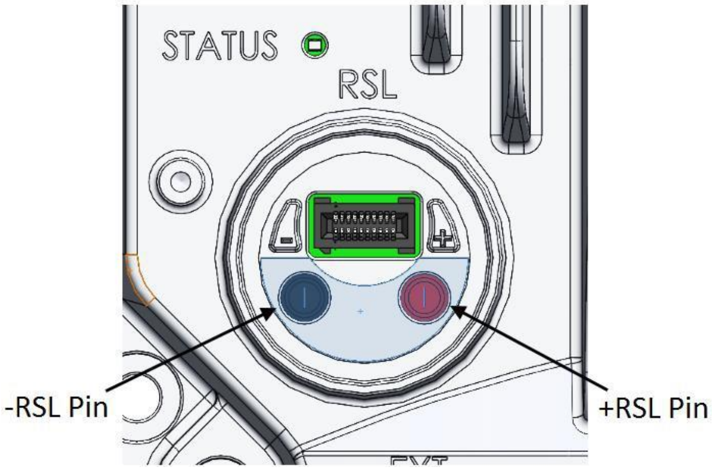


Figure 460: RSL Pins

PTP 850S LEDs

PTP 850S provides the following LEDs to indicate the status of the unit's interfaces, and the unit as a whole:

- Eth1 10G Optical Interface (SFP+) LEDs
- Eth2/Eth3 GbE Optical Interface (SFP/CSFP) LEDs
- MGT GbE Electrical Interface (RJ-45) LEDs
- Radio LED
- Status LED

Eth1 10G Optical Interface (SFP+) LEDs

Eth1 is an SFP cage that supports regular SFP and SFP+.

There is one Green LED to the left of the interface. The LED is for Eth1 and indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

- **Off** - Admin is Disabled *or* no cable is connected to the interface.
- **Green** - Admin is Enabled and a cable is connected to the interface.
- **Blinking Green** - Admin is Enabled and a cable is connected to the interface, *and* there is traffic on the interface.

Note: The LED does not indicate traffic on the interface (Blinking Green) in 10G mode.

Eth2/Eth3 GbE Optical Interface (SFP/CSFP) LEDs

Eth2/Eth3 is an SFP cage that supports regular and CSFP standards.

- When Eth2/Eth3 is used with a regular SFP, it provides Ethernet port 2.
- When Eth2/Eth3 is used with CSFP, it provides two Ethernet ports: Ethernet port 2 and Ethernet port 3.

Note: The Web EMS displays Ethernet port 3 even if a regular SFP is used, and there is no Ethernet port 3. You must avoid configuring Ethernet port 3 in this case.

There are two LEDS to the left of the interface. The LED to the left or the upper LED is for Eth2. When CSFP is used, the LED to the right or the lower LED is for Eth3; otherwise, it is inactive.

Each LED indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

- **Off** - Admin is Disabled *or* no cable is connected to the interface.
- **Green** - Admin is Enabled and a cable is connected to the interface.
- **Blinking Green** - Admin is Enabled and a cable is connected to the interface, *and* there is traffic on the interface.

MGT GbE Electrical Interface (RJ-45) LEDs

There are two LEDs next to the MGT interface, a Green LED to the left of the interface and an Orange LED to the right of the interface.

The Orange LED indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

- **Off** - Admin is Disabled *or* no cable is connected to the interface.
- **Green** - Admin is Enabled and a cable is connected to the interface.
- **Blinking Green** - Admin is Enabled and a cable is connected to the interface, *and* there is traffic on the interface.

The Green LED is not functional in this release.

Radio LED

The Radio LED indicates the status of the radio link:

- **Off** – The radio is off; the carrier is Admin = Disabled in the Interface Manager.
- **Green** - The power is on, and the carrier is operational (up).
- **Orange** – A signal degrade condition exists on the carrier.
- **Red** - A loss of frame (LOF) or excessive BER condition exists on the carrier.

Status LED

The Status LED indicates the status of the main board:

- **Off** – The power is off.
- **Green** - The power is on, and no alarms are raised on the motherboard.
- **Orange** - The power is on, and one or more minor alarms or warnings are raised on the motherboard.
- **Red** - The power is on, and one or more major or critical alarms are raised on the motherboard.

Protection LED

Reserved for future use.

PoE Injector Pin-outs and LEDs – Standard PoE

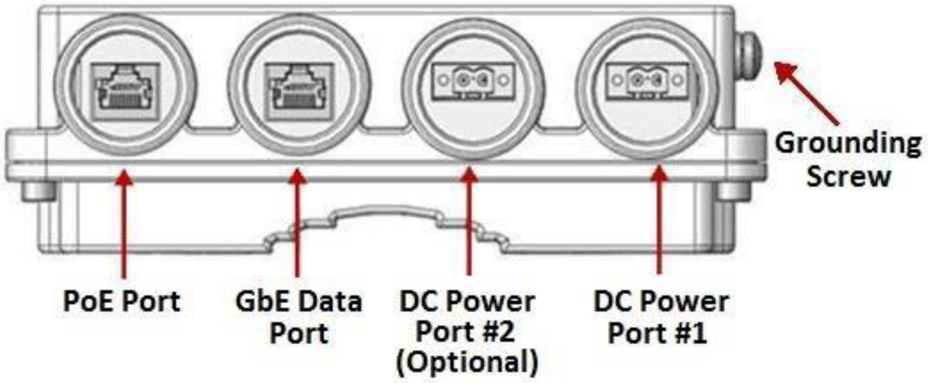


Figure 461: PoE Injector Connectors

PoE Injector Pin-outs and LEDs – Standard PoE

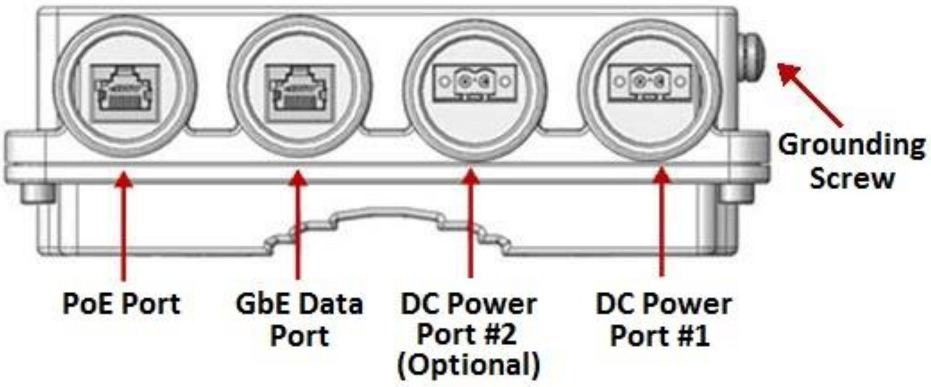


Figure 338: PoE Injector Connectors

PoE Injector Pin-outs and LEDs – Standard PoE

This section applies to the standard PoE Injector units with the following marketing models:

PoE_Inj_AO_2DC_24V_48V

PoE_Inj_AO

PoE Port

Table 246: PoE Injector PoE Port - RJ-45 Pinouts

Pin no.	Description
1	BI_DA+ (Bi-directional pair +A)
2	BI_DA- (Bi-directional pair -A)
3	BI_DB+ (Bi-directional pair +B)
4	BI_DC+ (Bi-directional pair +C)
5	BI_DC- (Bi-directional pair -C)
6	BI_DB- (Bi-directional pair -B)
7	BI_DD+ (Bi-directional pair +D)
8	BI_DD- (Bi-directional pair -D)

Data Port

Table 247: PoE Injector RJ-45 Data Port Supporting 10/100/1000Base-T

Pin no.	Description
1	BI_DA+ (Bi-directional pair +A)
2	BI_DA- (Bi-directional pair -A)
3	BI_DB+ (Bi-directional pair +B)
4	BI_DC+ (Bi-directional pair +C)
5	BI_DC- (Bi-directional pair -C)
6	BI_DB- (Bi-directional pair -B)
7	BI_DD+ (Bi-directional pair +D)
8	BI_DD- (Bi-directional pair -D)

DC

One or two DC ports, depending on the PoE Injector model:

Two models of the PoE Injector are available:

PoE_Inj_AO_2DC_24V_48V – Includes two DC power ports with power input ranges of ±(18-60)V each.

PoE_Inj_AO – Includes one DC power port (DC Power Port #1), with a power input range of ±(40-60)V.

These ports are UL-60950 compliant, with a 2-pin connector.

PoE Injector LEDs – Standard PoE

PWR1 (Bi-color LED)

- **Green** – Power available on PWR1 DC input
- **Off** – No power is available on PWR1 DC input.

PWR2 (Bi-color LED)

- **Green** – Power available on PWR2 DC input,
- **Off** – No power is available on PWR2 DC input.

PoE (Tri -color LED)

- **Orange** – No load is detected
- **Green** – Providing in-line power
- **Blinking Red** – Invalid/over-load
- **Off** – no power to the injector unit.

Radio LED

The Radio LED indicates the status of the radio link:

Off – The radio is off.

Green - The power is on, and all carriers are operational (up).

Orange - A signal degrade condition exists in at least one carrier.

Red - A loss of frame (LOF) or excessive BER condition exists in at least one carrier.

PoE Injector Pin-outs and LEDs – Passive PoE

This section applies the passive PoE used with power redundancy. The marketing model of this PoE is: *AC_POE_STD_PWR_INDOOR*

PoE Injector Pin-outs and LEDs – Passive PoE

RJ-45 output pinout: 3,4,5,6 (+) and 1,2,7,8 (-)

AC Input Specifications

AC Input Voltage Rating:	100VAC to 240VAC
AC Input Voltage Range:	90VAC to 264VAC
AC Input Current:	2.5A (rms) Max 90 VAC at Full Load 1.2A (rms) Max 240VAC at Full Load
AC Input Frequency:	47Hz to 63Hz
ACInput Inrush Current:	50A Max @115VAC at Full Load 75A Max @230VAC at Full Load

DC Output Specifications

DC Output Voltage:	+57-54VDC (+56V Nominal)
Output Power:	90W Maximum

PoE Injector LEDs – Passive PoE

Blue Solid: Power Good/Power Out

Chapter 27: Alarms List

The following table lists all alarms used in the PTP 850 products.

Table 302: Alarms

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
10	radio-digital-loopback	Alarm	Equipment	Framer digital loopback	Warning	User enabled framer digital loopback.	Disable framer digital loopback.
11	ntp-local	Alarm	Communications	NTP locked on local clock	Warning	The configured and enabled NTP servers are all unreachable or providing insufficient quality.	Configure or enable another NTP server, one that is reachable with sufficient quality.
15	ntp-locked	Event	Communications	NTP locked on server	Indeterminate		
28	main-board-warm-reset	Event		Unit warm reset.	Indeterminate		
29	main-board-cold-reset	Event		Unit reset.	Warning		
30	main-board-poe-low-voltage-alarm	Alarm		POE input voltage is too low	Warning		
31		Event		Change Remote request was sent	Major		
32		Event		Protection switchover due to remote request	Major		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
33	protection-mimo-misconfiguration-alarm	Alarm			Major	Unit Redundancy and MIMO 4x4 cannot operate simultaneously.	
100	lag-degraded	Alarm	Equipment	LAG is not fully functional - LAG Degraded.	Major		
101	lag-down	Alarm	Equipment	LAG operational state is down	Critical		
102	ethernet-loopback-active-alarm	Alarm	Equipment	Loopback is active	Major	Ethernet loopback is active.	Wait till loopback timeout expires or disable loopback.
103	port-mirroring-is-active	Alarm	Equipment	Slot X port XX is mirrored to slot Y port YY	Minor	Mirroring is enabled by user configuration.	Disable mirroring.
120	port-speed-mismatch-alarm	Alarm	Equipment	Port speed mismatch	Major	System reset is required after the port speed was changed.	Change the port speed to its previous value, OR Reset the system.
150	auto-state-propagation-interface-down-alarm	Alarm	Communications	Auto-state-propagation is triggered	Major	Failure of the radio interface which is monitored for automatic state propagation causes automatic shutdown of the controlled interface.	Check adjacent radio interface for failure conditions that caused automatic state propagation.
200	protection-communication-down-alarm	Alarm	Equipment	Protection communication is down	Major	Mate unit is absent/failure. Protection cable is disconnected. Unit failure.	Check existence of mate unit. Check protection cable connection between units. Reset mate unit. Replace mate unit.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
201	protection-lockout-alarm	Alarm	Equipment	Protection in Lockout State	Major		
202	protection-switch-command	Event	Equipment	Protection switchover due to local failure	Major		
203	protection-mate-not-present-alarm	Alarm	Equipment	Mate does not exist	Major	Mate does not exist or cable unplugged.	
204	protection-hsb-insufficient-alarm	Alarm	Equipment	HSB insufficient configuration	Critical	External Protection configured both with HSB.	Remove External Protection and HSB configuration.
205	protection-revertive-primary-insufficient-alarm	Alarm	Equipment	Protection revertive mode - insufficient configuration	warning	Identical configuration for the revertive-primary parameter.	Ensure one (and only one) unit is configured as the primary unit.
307	tdm-link-up	Event	Equipment	TDM interface is up	Warning		
308	tdm-link-down	Event	Equipment	TDM interface is down	Warning		
401	TrafficPhyLocAlarm	Alarm	Equipment	Loss of Carrier	Major	Cable disconnected. Defective cable.	Check connection of cable Replace cable.
407	ethernet-link-up	Event	Equipment	Ethernet interface is up	Warning		
408	ethernet-link-down	Event	Equipment	Ethernet interface is down	Warning		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
601	radio-excessive-ber	Alarm	Communications	Radio excessive BER	Major	Fade in the link. Defective IF cable. Fault in RFU. Fault in RMC (Radio Modem Card).	Check link performance. Check IF cable and replace if required. Replace RFU. Replace RMC (Radio Modem Card).
602	remote-link-id-mismatch	Alarm	Equipment	Link ID mismatch	Major	Link ID is not the same at both sides of link	Configure same Link ID for both sides of link
603	radio-lof	Alarm	Communications	Radio loss of frame	Critical	Fade in the link. Defective IF cable. Fault in RFU. Fault in RMC (Radio Modem Card). Different radio scripts at both ends of the link.	Check link performance. Check IF cable and replace if required. Replace RFU. Replace RMC (Radio Modem Card). Make sure same script is loaded at both ends of the link.
604	radio-signal-degrade	Alarm	Communications	Radio signal degrade	Minor	Fade in the link. Defective IF cable. Fault in RFU. Fault in RMC (Radio Modem Card).	Check link performance. Check IF cable and replace if required. Replace RFU. Replace RMC (Radio Modem Card).
605	radio-link-up	Event	Equipment	Radio interface is up	Warning		
606	radio-link-down	Event	Equipment	Radio interface is down	Warning		
607	rfu-frequency-scanner-in-process	Alarm	Equipment	Frequency scanner in progress	Warning	The frequency scanner activated.	Stop the frequency scanner process.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
801	corrupted-file-card- failure	Alarm	Equipment	Corrupted inventory file	Major	The inventory file is corrupted	Reset the card. Reset the system. Replace the card.
802	file-not-found	Alarm	Equipment	Inventory file not found	Warning	The inventory file is missing	Reset the system. Reinstall the software.
803	sfp-rx-power-level-low	Alarm	Equipment	SFP port RX power level is below the rx power level low threshold	Warning	Remote SFP port Tx laser power is too low. Fiber length is too long or fiber type doesn't fit the installed SFP.	Verify remote SFP Tx laser power is within range. Check fiber type and length fit the installed SFP. If not, replace it with an appropriate one.
804	sfp-rx-power-level-high	Alarm	Equipment	SFP port RX power level is above the rx power level high threshold	Warning	Remote SFP Tx power is too high.	Add attenuator on Rx side.
805	sfp-tx-power-level-low	Alarm	Equipment	SFP port TX power level is below the tx power level low threshold	Warning	SFP transmit laser power is too low	Check laser Bias current. If it is too low, replace SFP.
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	

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
901	demo-license-alarm	Alarm	Equipment	Demo mode is active	Warning	Demo mode has been activated by the user	Disable demo mode
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-violation-alarm	Alarm	Equipment	Activation key violation	Critical	The current configuration does not match the activation-key-enabled feature set. 48 hours after an "activation-key-violation" alarm is raised, sanction mode is activated in which all alarms except the activation key violation alarm are cleared and no new alarms are raised.	Get the list of features' configurations that are violated via the "activation key information report". Install a new activation key that allows the use of all required features.
908	demo-license-about-to-expire-alarm	Alarm	Equipment	Demo mode is about to expire	Major	Demo mode allowed period is about to end within 10 days	Disable demo mode and install a new valid activation key.
910	license-signature-failed-alarm	Alarm	Equipment	Activation key signature failure	Major	Activation key validation has failed due to invalid product serial number	Replace the IDU

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
911	license-violation-runtime-counter-expired	Event	Equipment	Activation key violation sanction is enforced	Major		
913	license-bad-xml-file-alarm	Alarm	Equipment	Activation key components are missing or corrupted	Major	Essential internal activation key components are missing or corrupted.	Reinstall software
1002	radio-protection-configuration-mismatch	Alarm	Equipment	Radio protection configuration mismatch	Major	The configuration between the radio protection members is not aligned	Apply a copy-to-mate command to copy the configuration from the required radio to the other one
1006	radio-protection-switchover-event	Event	Equipment	Radio protection switchover - reason	Warning	Protection decision machine initiated switchover due to local failure or user command	Check the system for local failures
1007	radio-protection-no-mate	Alarm	Equipment	Radio protection no mate	Major	Radio protection function is missing radio module, module defected or disabled	Add radio module. Replace a defective existing radio module. Make sure all radio interfaces are enabled.
1008	radio-protection-remote-switch-request	Event	Equipment	Remote switchover request was sent - reason	Warning		
1009	radio-protection-lockout	Alarm	Equipment	Radio protection lockout command is on	Major	The user has issued a lockout command	Clear the lockout command
1010	ethernet-protection-switchover	Event	Equipment	Ethernet Interface Group protection switchover	Warning	LOC event on an Ethernet interface. Protection group member was disabled or pulled out of the shelf.	Check the system for local failures. Check external equipment.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1011	interface-protection-lockout	Alarm	Equipment	Interface protection lockout is on	Major	The user has issued a lockout command	Clear the lockout command
1012	interface-protection-no-mate	Alarm	Equipment	Interface protection no mate: mate interface is missing or disabled	Major	Interface protection function is missing interface module, module defected or disabled.	Add interface module. Replace a defective existing interface module. Make sure all interface interfaces are enabled.
1102	software-installation-status	Event	Processing	Software installation status:	Warning		
1105	software-new-version-installed	Event	Processing	New version installed	Warning	A software version has been installed but system has not been reset.	
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
1150	backup-started	Event	Processing	Configuration file backup generation started	Warning	User command	

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
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	
1153	restore-succeeded	Event	Processing	Configuration successfully restored from file backup	Warning	Configuration restore finished successfully	
1154	restore-failure	Event	Processing	Failure in configuration restoring from backup file	Warning	System failed in attempt to restore configuration from backup file	Configuration file system type mismatch Invalid or corrupted configuration file
1155	restore-canceled	Event	Processing	Configuration restore operation cancelled	Warning	Restore operation cancelled because of user command or execution of another configuration management operation	Try again
1156	file-transfer-issued	Event	Processing	User issued command for transfer of configuration file	Warning	User command	
1157	file-transfer-succeeded	Event	Processing	Configuration file transfer successful	Warning	Configuration file transfer successful	
1158	file-transfer-failure	Event	Processing	Configuration file transfer failure	Warning	Communications failure. File not found in server	Mark sure protocol details are properly configured. Make sure file exists.
1159	file-transfer-in-progress	Event	Processing	Configuration file transfer in progress	Warning	File transfer started	

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
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	Syntax Error. Error returned by system during runtime	Verify script in the relevant line, and run again. Note that script may assume pre-existing configuration.
1166	unit-info-file-transfer-status-changed	Event	Processing	Unit info file transfer status:	Warning		
1167	unit-info-file-creation-status-changed	Event	Processing	Unit info file creation status:	Warning		
1169	restore-started	Event	Processing	Configuration restore operation started	Warning	Restore operation started because of user command	
1201	file-missed	Alarm	Equipment	Modem firmware file not found	Critical	Modem file is missing	Download software package. Reset the system.
1202	load-failed	Alarm	Equipment	Modem firmware was not loaded successfully	Critical	Modem firmware file is corrupted. System failure.	Download software package. Reset the system.
1203	modem-wd-reset	Event	Equipment	Modem watch-dog reset event	Warning		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1301	fpga-file-currupt-alarm	Alarm	Equipment	Radio MRMC script LUT file is corrupted	Critical	Damaged radio MRMC script LUT file	Download the specific radio MRMC script LUT file
1302	fpga-file-not-found-alarm	Alarm	Equipment	Radio MRMC script LUT file is not found	Critical	Missing radio MRMC script LUT file	Download the specific radio MRMC script LUT file
1304	modem-script-file-corrupt-alarm	Alarm	Equipment	Radio MRMC script modem file is corrupted	Critical	Damaged radio MRMC script modem file	Download the specific radio MRMC script modem file
1305	modem-script-file-not-found-alarm	Alarm	Equipment	Radio MRMC script modem file is not found	Critical	Missing radio MRMC script modem file	Download the specific radio MRMC script modem file
1308	rfu-file-corrupt-alarm	Alarm	Equipment	Radio MRMC file is corrupted	Critical	Damaged Radio MRMC script LUT file	Download the specific radio MRMC RFU file
1309	rfu-file-not-found-alarm	Alarm	Equipment	Radio MRMC RFU file is not found	Major	Missing radio MRMC RFU file	Download the specific radio MRMC RFU file
1312	script-loading-failed	Alarm	Equipment	Radio errrror! MRMC script loading failed	Major	Damaged hardware module	Replace the radio hardware module
1313	mrmc-profile-below-thresh1	Alarm	Equipment	MRMC RX profile below threshold 1	Major		
1314	mrmc-profile-below-thresh2	Alarm	Equipment	MRMC RX profile below threshold 2	Critical		
1401	incompatible-rfu-tx-calibration	Alarm	Equipment	Incompatible RFU TX calibration	Major	RFU calibration tables require SW upgrade	Upgrade IDU SW
1501	remote-communication-failure	Alarm	Equipment	Remote communication failure	Critical	Fade in the link	Check the link performance
1601	if-loopback	Alarm	Equipment	IF loopback	Warning	User enabled IF loopback	Disable IF loopback

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1602	lock-detect	Alarm	Equipment	IF synthesizer is unlocked.	Critical	Extreme temperature condition. HW failure.	Check installation. Reset the RMC (Radio Modem Card) module. Replace the RMC (Radio Modem Card).
1610	rsl-degradation-threshold-out-of-range	Alarm	Equipment	Radio Receive Signal Level is below the configured threshold	Warning	RSL is very low due to: Weather conditions, obstruction in antenna line of sight, antennae alignment. Configured threshold needs to be adjusted.2.	Check for obstruction in link path. Check the antennae alignment and link planning. Recalculate the Path Loss and set the threshold accordingly. Check link settings - Tx Power and Tx Frequency. Hardware problem.
1651	atpc-override	Alarm	Communications	ATPC overridden: Tx level has been equal to the Max Tx level for a longer time than allowed	Warning	Actual transmitted signal level has been at its maximum value for longer than allowed. This is probably caused by a configuration error or link planning error.	Correct the transmission levels. The alarm will be cleared only upon manual clearing.
1697	radio-unit-extreme-temperature	Alarm	Equipment	Radio unit extreme temperature	Warning	Installation conditions. Defective RFU.	Check installation conditions. Verify operation as per product's specs. Replace RFU.
1698	radio-unit-low-voltage	Alarm	Equipment	Radio unit input voltage is too low	Warning	Power supply output too low. Power cable to RFU.	Check Power supply. Replace cable.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1699	radio-unit-high-voltage	Alarm	Equipment	Radio unit input voltage is too high	Warning	Power Supply output too high.	Check power supply.
1700	fw-download-failure	Alarm	Communications	Radio unit not aligned to IDU	Critical	FW alignment interrupted, power disruption, ODU cable malfunction. Damaged ODU.	Reinitiate FW download by disable/enable the corresponding port. Replace RFU.
1701	cable-open	Alarm	Equipment	Cable open	Major	Cable is not connected to the IDU's radio interface or the RFU.	Check IF cable and connectors. Verify that the N-Type connector inner pin is not spliced. Replace RMC (Radio Modem Card). Replace RFU.
1702	cable-short	Alarm	Equipment	Cable short	Major	Physical short at the IF cable	Check IF cable and connectors. Verify that the N-Type connector inner pin is not spliced. Replace RMC (Radio Modem Card). Replace RFU.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1703	communication-failure	Alarm	Equipment	RFU communication failure	Warning	Defective IF cable. IF cable not connected properly. Defective RMC (Radio Modem Card). Defective RFU. RFU software download in progress.	Check IF cable and connectors. Verify that N-Type connector inner pin is not spliced. Replace RMC (Radio Modem Card). Replace RFU. For a high power RF Unit: Check BMA connector on OCB Check BMA connector on RFU.
1704	delay-calibration-failure-1	Alarm	Equipment	RFU delay calibration failure 1	Warning	Defective RFU	Reset the RMC (Radio Modem Card) / RFU. Replace RFU.
1705	delay-calibration-failure-2	Alarm	Equipment	RFU delay calibration failure 2	Warning	Calibration cannot be completed due to notch detection	Enter delay calibration value manually.
1706	extreme-temp-cond	Alarm	Equipment	RFU extreme temperature	Warning	Installation conditions. Defective RFU.	Check installation conditions. Verify operation as per product's specs. Replace RFU.
1707	radio-unit-abc-incompatible-rfu	Alarm	Equipment	RFU is incompatible with ABC configuration	Warning	The RFU type does not support the type of Multi-Carrier ABC the user has configured.	Replace the RFU with an RFU type that supports the configured Multi-Carrier ABC type.

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	Check if problem repeats and if errors/alarms reported. 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	IF cable connection. Defective RFU. Defective RMC (Radio Modem Card).	Check IF cable connectors. Verify that N-Type connector inner pin is not spliced. Replace RMC (Radio Modem Card). Replace RFU.
1712	no-signal-from-rfu	Alarm	Equipment	Low IF signal from RFU	Warning	Low RX IF signal (140 MHz) from RFU.	Check IF cable and connectors. Verify that N-Type connector inner pin is not spliced. Replace RMC (Radio Modem Card). Replace RFU.
1713	pa-extreme-temp-cond	Alarm	Equipment	RFU PA extreme temperature	Warning	Installation conditions. Defective RFU.	Check installation conditions. Replace RFU.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1714	power-failure-12v	Alarm	Equipment	RFU power failure (12v)	Major	Defective IF cable/connector. Defective RFU. Defective IDU.	Replace IF cable/connector. Replace RFU. Replace IDU.
1715	power-failure-1point5	Alarm	Equipment	RFU power failure (1.5v)	Major	Defective IF cable/connector. Defective RFU. Defective IDU.	Replace IF cable/connector. Replace RFU. Replace IDU.
1716	power-failure-24v	Alarm	Equipment	RFU power failure (24v)	Major	Defective IF cable/connector. Defective RFU. Defective IDU.	Replace IF cable/connector. Replace RFU. Replace IDU.
1717	power-failure-6v	Alarm	Equipment	RFU power failure (6v pro)	Major	Defective IF cable/connector. Defective RFU. Defective IDU.	Replace IF cable/connector. Replace RFU. Replace IDU.
1718	power-failure-6v-sw	Alarm	Equipment	RFU power failure (6v SW)	Major	Defective IF cable/connector. Defective RFU. Defective IDU.	Replace IF cable/connector. Replace RFU. Replace IDU.
1719	power-failure-minus-5v	Alarm	Equipment	RFU power failure (-5v)	Major	Defective IF cable/connector. Defective RFU. Defective IDU.	Replace IF cable/connector. Replace RFU. Replace IDU.
1720	power-failure-vd	Alarm	Equipment	RFU power failure (Vd)	Major	Defective IF cable/connector. Defective RFU. Defective IDU.	Replace IF cable/connector. Replace RFU. Replace IDU.
1721	reset-occurred	Event	Equipment	RFU reset	Major		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1722	rfu-loopback-active	Alarm	Equipment	RFU loopback is active	Major	User has activated RFU loopback.	Disable RFU 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.	Replace RFU.
1727	rx-level-out-of-range	Alarm	Equipment	RFU RX level out of range	Warning	RSL is very low, link is down.	Check antenna alignment & link planning. Check link settings (TX power, TX frequency). Check antenna connections. Replace local/remote RFU.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1728	rx-level-path1-out-of-range	Alarm	Equipment	RFU RX level path1 out of range	Warning	Improper installation. Fading event. Defective RFU.	Check that the fault is not due to rain/multi-path fading or lack of LOS. Check link settings (TX power, TX frequency). Check antenna alignment. Check antenna connections. Replace local/remote RFU.
1729	rx-level-path2-out-of-range	Alarm	Equipment	RFU RX level path2 out of range	Warning	Improper installation. Fading event. Defective RFU.	Check that the fault is not due to rain/multi-path fading or lack of LOS. Check link settings (TX power, TX frequency). Check antenna alignment. Check antenna connections. Replace local/remote RFU.
1730	radio-unit-communication-failure	Alarm	Equipment	Radio unit communication failure	Critical	Defective RFU cable. RFU cable not connected properly. Defective RIC (Radio Interface Card). Defective RFU. RFU initialization in progress. RFU powered off.	Check RFU power supply. Check RFU cable and connectors. Replace RIC (Radio Interface Card). Replace RFU.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1731	power-supply-radio-unit-cable-open	Alarm	Equipment	Power supply cable open	Major	Power is enabled but consumption is lower than threshold.	Check ETH cable and connectors. Verify RFU is connected. If RFU connected with optical cable, disable power interface.
1732	power-supply-radio-unit-cable-short	Alarm	Equipment	Power supply cable short	Major	Power is enabled but consumption reached the threshold. Physical short at the ETH cable.	Check ETH cable and connectors. Replace RIC (Radio Interface Card) Replace RFU. If RFU connected with optical cable, disable power interface.
1733	synthesizer-unlocked	Alarm	Equipment	RFU synthesizer unlocked	Major	At least one of the RFU synthesizers is unlocked	Replace RFU. In XPIC mode, replace mate RFU as well.
1734	tx-level-out-of-range	Alarm	Equipment	RFU TX level out of range	Minor	Defective RFU (the RFU cannot transmit the requested TX power)	Replace RFU. Intermediate solution - reduce TX power.
1735	tx-mute	Alarm	Equipment	RFU TX Mute	Warning	RFU Transmitter muted by user	Unmute the RFU transmitter
1736	unknown-rfu-type	Alarm	Equipment	IDU SW does not support this type of RFU	Major	IDC SW does not support the RFU	Upgrade IDC SW
1737	card-extracted-from-slot	Event	Equipment	Card was extracted from slot	Warning	Card was extracted from slot	NA
1738	card-failure	Alarm	Equipment	Card is in Failure state	Major	Card is down as a result of card failure	Reset Card. Check if slot was disabled.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
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.	Reset Card. Download software package. Try to insert another Card.
1741	card-inserted-to-slot	Event	Equipment	Card was inserted to slot	Warning	Card was inserted to slot	NA
1742	card-intermediate-channel-failure	Alarm	Equipment	Card is in interconnection failure state	Major	Card is down as a result of card interconnection failure	Reset Card. Check if the slot was disabled.
1743	card-missing	Alarm	Equipment	Expected Card is missing in slot	Major	Card is missing. Expected Card Type configured on empty slot.	Insert Expected Card. Clear Expected Card Type.
1744	card-not-supported-for-slot	Alarm	Equipment	This Card type is not supported in this slot	Major	The card is not on the Allowed Card Types list for this slot.	Reset. Insert Card belongs to Allowed Card Types list.
1745	card-state-is-down	Event	Equipment	Card operational state is Down	Indeterminate	Card state was change to Down state	NA
1746	card-state-is-up	Event	Equipment	Card operational state is Up	Indeterminate	Card state was change to Up state	NA
1747	card-state-is-up-with-alarms	Event	Equipment	Card operational state is Up with Alarms	Indeterminate	Card state was change to Up state but with Alarms indication	NA
1748	card-unexpected	Alarm	Equipment	Unexpected Card Type in slot	Minor	Expected card type is different than the actual card type	Insert Expected Card. Change Expected Card Type.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
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-insertion-event	Event	Equipment	FAN Card was inserted to slot	Warning	FAN Card was inserted to slot	
1755	fan-card-missing	Alarm	Equipment	FAN Card is missing in slot	Critical	FAN Card is missing. Slot enabled when empty.	Insert FAN Card. Disable slot.
1757	fan-failure	Alarm	Equipment	FAN Card is in Failure state	Major	FAN Card is in Failure state	Change FAN Card
1758	pdc-card-extraction-event	Event	Equipment	Power Supply was extracted from slot	Warning	Power Supply was extracted from slot	
1759	pdc-card-insertion-event	Event	Equipment	Power Supply was inserted to slot	Warning	Power Supply was inserted to slot.	
1760	pdc-card-missing	Alarm	Equipment	Power Supply is missing in slot	Major	Power Supply is missing. Slot enabled when empty.	Insert Power Supply. Disable slot.
1761	pdc-over-voltage	Alarm	Equipment	Over voltage	Major	System Power Voltage higher than allowed.	NA
1762	pdc-under-voltage	Alarm	Equipment	Under voltage	Major	System Power Voltage Lower than allowed.	NA
1763	TCC-fpga-fw-not-found	Alarm	Equipment	The Main board firmware is not found	Warning		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1764	TCC-fw-load-fail	Alarm	Equipment	Download Main Board firmware has failed	Major	Firmware download was unsuccessful.	Reset board. Download software package. Try to insert another board.
1765	tcc-powerup-reset-event	Event	Equipment	Main Board was reset	Warning		
1766	upload-software-failed	Event	Equipment	RFU installation failure	Warning	Unsupported RFU type. IDU-RFU communications problem. RFU failure.	Make sure RFU is supported by SW version. Check IDU-RFU cable. Replace RFU.
1767	upload-software-started	Event	Equipment	RFU installation in progress	Warning	User command	
1768	upload-software-succeeded-event	Event	Equipment	RFU installation successfully completed	Warning	User command	
1770	cable-lof-rfu	Event	Equipment	Unit performing power-up.	Major		
1771	cable-error-rfu	Alarm	Equipment	RFU cable error.	Major	Errors in signal from IDU to XCVR.	Check the IF cable and connectors. Verify that the N-Type/TNC connector inner pin is not spliced. Replace RMC. Replace XCVR.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1772	xpic-data-los	Alarm	Equipment	Radio XPIC sync loss	Major	Signaling between RMCs (Radio Modem Cards) for XPIC functionality has failed	Check that the RMCs are in allowed slots. Populate the RMCs in different allowed location in the chassis. Replace RMC/s. Replace chassis.
1773	early-warning	Alarm	Communications	Radio early warning.	Warning	The estimated radio BER (Bit Error Rate) is above 10E-12.	Check link performance. Check IF cable, and replace if required. Replace XCVR. Replace RMC.
1774	sw-download-incompatible-rfu	Alarm	Equipment	RFU software download cannot be initiated.	Critical	The hardware of the XCVR is OK, but is it running with METRO radio application.	Upgrade the XCVR software application via XPAND-IP and then reinitiate software download..
1775	hw-incompatible-rfu	Alarm	Equipment	RFU software download is not possible.	Critical	Wrong type of XCVR, the XCVR hardware is METRO.	Replace the XCVR
1776	pll-rmc	Alarm	Equipment	RMC hardware failure.	Major	RMC hardware failure of the clock distributor.	Replace the RMC.
1777	rfu-mute-with-timeout	Event	Equipment	RFU TX Mute with timeout	Warning	RFU Transmitter muted by user.	Unmute the RFU transmitter or wait for expiration of the timeout.
1778	rfu-power-decreased-due-to-pa-temp	Alarm	Equipment	RFU power decreased due to PA temperature	Major	Defective RFU (the RFU cannot transmit the requested TX power).	Replace RFU. Intermediate solution - reduce TX power.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
1780	mrmc-running-script-deleted	Event	Equipment	MRMC running script is deleted	Warning	New installed software package does not include the running MRMC radio script	Make sure the required software package include the running MRMC radio script. Download and install the correct software package.
1781	mrmc-running-script-updated	Event	Equipment	MRMC running script is updated	Warning	New installed software package does has an updated version of the running MRMC radio script	Reset the radio carrier to reacquire the new updated MRMC radio script
1782	radio-2_5gbps-mismatch-configuration	Alarm	Equipment	2.5Gbps mismatch configuration	Warning	The card cannot function outside of an ABC group in 2.5Gbps mode.	Add the card to an ABC group, or change the Slot Section to 1Gbps.
1783	remote-fault-indication	Alarm	Communication	Radio remote fault indication (RFI)	Minor		
1790	np-hw-failure	Alarm	Equipment	Hardware failure	Critical	An internal hardware failure has been detected by the system.	Replace the card or unit reporting the hardware failure.
1794	interface-not-functional-until-reset	Alarm	equipment	Interface is not operational until chassis reset	Warning	Changes were made to platform due to user configuration	Reset chassis
1800	t3-loc-alarm	Alarm	Equipment	T3 sync interface Loss of Carrier	Major	Cable disconnected. Defective cable.	Check connection of the cable. Replace the cable.
1975	radio-fan-failure	Alarm	Equipment	RFU fan failure	Major	RFU fan is disconnected. RFU fan HW failure. RFU fan jammed.	Check fan cable connection to the RFU. Check/replace the fan. Clear/clean the fan.
2001	pwe3-pwc-s-card-reset	Alarm	Equipment	TDM-LIC has rebooted and is not in service now	Major	Recent TDM-LIC card reset; System malfunction.	Wait for card to reboot. Reset the TDM-LIC card.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2002	pwe3-pwc-s-config-mismatch	Alarm	Equipment	TDM-LIC configuration mismatch	Major	Recent warm reset of TDM-LIC; System malfunction.	Power cycle the TDM-LIC.
2003	pwe3-pwc-s-front-panel-clock-los	Alarm	Equipment	Loss of Signal (LOS) on TDM-LIC's front panel clock port	Major	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2004	pwe3-pwc-s-host-pw-lic-comm-disrupt	Alarm	Equipment	Communication with TDM-LIC is disrupted in Host-Card direction	Minor	System malfunction	Reset the TDM-LIC.
2005	pwe3-pwc-s-hw-failure	Alarm	Equipment	TDM-LIC hardware failure	Major	System malfunction	Reset the TDM-LIC.
2006	pwe3-pwc-s-pw-lic-host-comm-disrupt	Alarm	Equipment	No communication with TDM-LIC	Major	System malfunction	Reset the TDM-LIC.
2007	pwe3-pws-s-jitter-buffer-overrun	Alarm	Equipment	Jitter-buffer-overrun alarm on TDM service	Major	Something wrong on TDM service synchronization	Check TDM service configuration
2008	pwe3-pws-s-late-frame	Alarm	Equipment	Late-frame alarm on TDM service	Warning	Something wrong on TDM service	Check TDM service configuration
2009	pwe3-pws-s-loss-of-frames	Alarm	Equipment	Loss-of-frames alarm on TDM service	Major	Failure along the network path of TDM service	Check network or configuration for errors in the network transport side of the service
2010	pwe3-pws-s-malformed-frames	Alarm	Equipment	Malformed-frames alarm on TDM service	Major	Payload size does not correspond to the defined value. Mismatch in PT value in RTP header (if used)	Check TDM service configuration

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2011	pwe3-pws-s-misconnection	Alarm	Equipment	Misconnection alarm on TDM service	Major	Stray packets with wrong RTP configurations are received and dropped.	Check TDM service configuration
2012	pwe3-tdm-port-s-ais	Alarm	Equipment	Alarm Indication Signal (AIS) on TDM-LIC TDM port	Major	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment.
2013	pwe3-tdm-port-s-lof	Alarm	Equipment	Loss Of Frame (LOF) on TDM-LIC TDM port	Major	Line is not properly connected. External equipment is faulty.	
2014	pwe3-tdm-port-s-lomf	Alarm	Equipment	Loss Of Multi-Frame (LOMF) on TDM-LIC TDM port	Major	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment.
2015	pwe3-tdm-port-s-loopback-alarm	Alarm	Equipment	Loopback on TDM-LIC TDM port	Warning	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment.
2016	pwe3-tdm-port-s-los	Alarm	Equipment	Loss Of Signal (LOS) on TDM-LIC TDM port	Major	Line is not properly connected. Cable is faulty. External equipment is faulty. Defective TDM-LIC.	Reconnect line. Check line cables. Check external equipment.
2017	pwe3-tdm-port-s-rai	Alarm	Equipment	Remote Alarm Indication (RAI) on TDM-LIC TDM port	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2018	pwe3-tdm-port-s-unexpected-signal-alarm	Alarm	Equipment	E1/DS1 Unexpected signal on TDM-LIC TDM port	Warning	Port is disabled. Line is connected to a disabled port.	Enable relevant port. Disconnect cable from relevant port.
2021	pwe3-pwc-s-ssm-rx-changed	Event	Equipment	SSM received pattern change was discovered	Warning		No action is required.
2022	pwe3-stm1oc3-s-excessive-ber-alarm	Alarm	Equipment	Excessive BER on TDM-LIC STM1/OC3 port	Major	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2023	pwe3-stm1oc3-s-lof-alarm	Alarm	Equipment	Loss Of Frame (LOF) on TDM-LIC STM1/OC3 port	Major	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2024	pwe3-stm1oc3-s-loopback-alarm	Alarm	Equipment	Loopback on TDM-LIC STM1/OC3 port	Warning	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2025	pwe3-stm1oc3-s-los-alarm	Alarm	Equipment	Loss Of Signal (LOS) on TDM-LIC STM1/OC3 port	Critical	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2026	pwe3-stm1oc3-s-mute-override-alarm	Alarm	Equipment	SFP is muted on TDM-LIC STM1/OC3 port	Warning		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2027	pwe3-stm1oc3-s-sfp-absent-alarm	Alarm	Equipment	SFP absent in TDM-LIC STM1/OC3 port	Critical	SFP is not properly installed. SFP is faulty.	Install SFP properly. Replace the card.
2028	pwe3-stm1oc3-s-sfp-failure-alarm	Alarm	Equipment	SFP failure on TDM-LIC STM1/OC3 port	Critical	SFP is not properly installed. SFP is faulty.	Install SFP properly. Replace the card.
2029	pwe3-stm1oc3-s-sfp-tx-fail-alarm	Alarm	Equipment	SFP transmit failure on TDM-LIC STM1/OC3 port	Critical	SFP is not properly installed. SFP is faulty.	Install SFP properly. Replace the card.
2030	pwe3-stm1oc3-s-signal-degrade-alarm	Alarm	Equipment	Signal Degrade on TDM-LIC STM1/OC3 port	Minor	Line is not properly connected. SFP is not properly installed. SFP is faulty. External equipment is faulty	Install SFP properly. Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2031	pwe3-stm1oc3-s-slm-alarm	Alarm	Equipment	J0 Trace Identifier Mismatch on TDM-LIC STM1/OC3 port	Minor	J0 misconfiguration. Line is not properly connected. SFP is not properly installed. External equipment is faulty.	Make sure expected and received J0 match. Install SFP properly. Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2032	pwe3-stm1oc3-s-ssm-rx-changed	Event	Equipment	SSM pattern received on TDM-LIC STM1/OC3 port changed	Warning		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2033	pwe3-vc12vt15-s-ais-alarm	Alarm	Equipment	Alarm Indication Signal (AIS) on TDM-LIC VC12/VT1.5	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2034	pwe3-vc12vt15-s-excessive-ber-alarm	Alarm	Equipment	Excessive BER on TDM-LIC VC12/VT1.5	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2035	pwe3-vc12vt15-s-loopback-alarm	Alarm	Equipment	Loopback on TDM-LIC VC12/VT1.5	Warning	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2036	pwe3-vc12vt15-s-rcv-plm-alarm	Alarm	Equipment	Payload Mismatch Path (PLM) received on TDM-LIC VC12/VT1.5	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2037	pwe3-vc12vt15-s-rcv-rdi-alarm	Alarm	Equipment	Remote Defect Indication (RDI) received on TDM-LIC VC12/VT1.5	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2038	pwe3-vc12vt15-s-rcv-slm-alarm	Alarm	Equipment	Signal Label Mismatch (SLM) received on TDM-LIC VC12/VT1.5	Minor	J2 misconfiguration. Line is not properly connected. External equipment is faulty.	Make sure expected and receive J2 match. Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2039	pwe3-vc12vt15-s-signal-degrade-alarm	Alarm	Equipment	Signal Degrade on TDM-LIC VC12/VT1.5	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2040	pwe3-vc12vt15-s-unequipped-alarm	Alarm	Equipment	Unequipped on TDM-LIC VC12/VT1.5	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2041	pwe3-card-group-s-config-mismatch	Alarm	Equipment	TDM-LIC card protection configuration mismatch	Major	The configuration between the TDM-LIC card protection members is not aligned	Apply a copy-to-mate command to copy the configuration from the required TDM-LIC to the other one
2042	pwe3-card-group-s-lockout	Alarm	Equipment	TDM-LIC card protection group lockout command is on	Minor	The user has issued a lockout command	Clear the lockout command
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

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2044	pwe3-card-group-s-protection-switch-evt	Event	Equipment	TDM-LIC card protection switch over, priority	Warning	LOS alarm on a STM1 interface of the TDM-LIC card protection group member; A TDM-LIC card protection group member was disabled or pulled out of the shelf	Check line cables. Check external equipment.
2045	pwe3-vc12vt15-s-lop-alarm	Alarm	Equipment	Loss Of Pointer (LOP) received on TDM-LIC VC12/VT1.5	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment. Power cycle the TDM-LIC.
2046	pwe3-tunnel-groups-s-protection-switch	Event	Equipment	Path protection switch on TDM service	Minor	Failure along service primary path. User command.	Check errors along primary path Check local service configuration.
2047	pwe3-tunnel-groups-s-revertive-switch	Event	Equipment	Path protection revertive switch on TDM service	Minor	Primary path has been operational for the duration of the defined WTR time	-
2100	STM-1-OC-3-IN-LOS	Alarm	Equipment	Loss of Signal on Line Interface (LOS) on STM-1/OC-3 port.	Critical	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment.
2101	STM-1-OC-3-IN-LOF	Alarm	Equipment	Loss of Frame on Line Interface (LOF) on STM-1/OC-3 port.	Major	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2102	STM-1-OC-3-IN-MSAIS	Alarm	Equipment	Alarm Indication Signal on Line Interface (MS-AIS/AIS-L) received.	Minor	Line is not properly connected. External equipment is faulty.	Reconnect line. Check line cables. Check external equipment.
2103	STM-1-OC-3-IN-MSRDI	Alarm	Equipment	Remote Defect Indication on Line Interface (MS-RDI/RDI-L) received.	Minor	External equipment is faulty.	Check external equipment.
2104	STM-1-OC-3-RX-LOS	Alarm	Equipment	Loss of STM-1/OC-3 Frame on Radio Interface.	Major	All channels in Multi Carrier ABC group are down. Incorrect configuration on remote side.	Check link performance. Check radio alarms for channel. Check configuration.
2105	STM-1-OC-3-RX-MSAIS	Alarm	Equipment	MS-AIS/AIS-L on Radio Interface detected.	Minor	Remote STM-1/OC-3 signal is missing (LOS/LOF/MS-AIS/AIS-L on remote STM-1/OC-3 interface). STM-1/OC-3 Channel removed due to reduced radio capacity on remote side.	Check remote equipment.
2106	STM-1-OC-3-RX-RDI	Alarm	Equipment	MS-RDI/RDI-L on Radio Interface detected.	Minor	External equipment is faulty.	Check remote equipment.
2107	STM-1-OC-3-LOOPBACK	Alarm	Equipment	STM-1/OC-3 Loopback	Warning	Looping.	Remove looping.
2108	STM-1/OC-3-CHANNEL-1-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	Reduced capacity. Fading	Check link performance. Check radio alarms for channel.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2109	STM-1-OC-3-PBRS-INSERTION	Alarm	Equipment	PRBS insertion.	Warning	PRBS insertion on STM-1/OC-3 card.	Remove PRBS insertion.
2110	STM-1-OC-3-SFP-NOT-DETECTED	Alarm	Equipment	SFP absent in STM-1/OC-3 port.	Critical	SFP is not properly installed. SFP is faulty.	Install SFP properly. Replace the card.
2111	STM-1-OC-3-SFP-TX-FAILURE	Alarm	Equipment	SFP Transmit Failure on STM-1/OC-3 port.	Critical	SFP is faulty.	Replace SFP or insert SFP if it is not inserted correctly. Replace the card.
2112	STM-1-OC-3-SFP-TX-MUTED	Alarm	Equipment	SFP is muted on STM-1/OC-3 port.	Warning	SFP is muted by configuration.	Remove muting.
2113	STM-1/OC-3-CHANNEL-2-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	Reduced capacity. Fading.	Check link performance. Check radio alarms for channel.
2114	STM-1/OC-3-CHANNEL-3-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	Reduced capacity. Fading.	Check link performance. Check radio alarms for channel.
2115	STM-1/OC-3-CHANNEL-4-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	Reduced capacity. Fading.	Check link performance. Check radio alarms for channel.
2116	STM-1/OC-3-CHANNEL-5-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	Reduced capacity. Fading.	Check link performance. Check radio alarms for channel.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2117	STM-1/OC-3-CHANNEL-6-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	Reduced capacity. Fading.	Check link performance. Check radio alarms for channel.
2118	STM-1/OC-3-CHANNEL-7-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	Reduced capacity. Fading.	Check link performance. Check radio alarms for channel.
2119	STM-1/OC-3-CHANNEL-8-REMOVED	Alarm	Equipment	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	Reduced capacity. Fading.	Check link performance. Check radio alarms for channel.
2120	STM1-OC3-GROUP-ACTIVITY-CHANGED	Event	Equipment	STM-1/OC-3 Group protection switchover	Warning	LOS alarm on an STM-1/OC-3 interface. STM1-OC3 Group protection group member was disabled or pulled out of the shelf.	Check line cables. Check external equipment.
2200	MC-ABC-Local-LOF	Alarm	Communications	Multi Carrier ABC LOF.	Critical	All channels in Multi Carrier ABC group are down.	Check link performance on all radio channels in Multi Carrier ABC group. Check radio alarms for channels in Multi Carrier ABC group. Check configuration of Multi Carrier ABC group.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2201	MC-ABC-local-cap-below	Alarm		Multi Carrier ABC bandwidth is below the threshold	Major	One of the radio channels in the Multi Carrier ABC group has a lower capacity than expected Minimum bandwidth threshold configuration is wrong	Check link performance on all radio channels in Multi Carrier ABC group Check radio alarms for channels in Multi Carrier ABC group Check configuration of Multi Carrier ABC group Minimum bandwidth threshold
2203	MC-ABC-Lvds-Error-Sl2	Alarm	Equipment	LVDS RX Error Slot 1.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.
2204	MC-ABC-Lvds-Error-Sl3	Alarm	Equipment	LVDS RX Error Slot 3.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.
2205	MC-ABC-Lvds-Error-Sl4	Alarm	Equipment	LVDS RX Error Slot 4.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.
2206	MC-ABC-Lvds-Error-Sl5	Alarm	Equipment	LVDS RX Error Slot 5.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.
2207	MC-ABC-Lvds-Error-Sl6	Alarm	Equipment	LVDS RX Error Slot 6.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.
2208	MC-ABC-Lvds-Error-Sl7	Alarm	Equipment	LVDS RX Error Slot 7.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2209	MC-ABC-Lvds-Error-Sl8	Alarm	Equipment	LVDS RX Error Slot 8.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.
2210	MC-ABC-Lvds-Error-Sl9	Alarm	Equipment	LVDS RX Error Slot 9.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.
2211	MC-ABC-Lvds-Error-Sl10	Alarm	Equipment	LVDS RX Error Slot 10.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.
2212	MC-ABC-Lvds-Error-Sl12	Alarm	Equipment	LVDS RX Error Slot 12.	Major	Hardware failure between RMC and TCC cards.	Replace RMC. Replace TCC. Replace chassis.
2213	MC-ABC-robustness-member-disabled	Alarm	Equipment	MC-ABC member has been disabled due to robustness reason	Major	The corresponding MC-ABC member has been temporarily disabled within the group. It was caused by consecutive RFU HW failures	Verify the proper functioning and connectivity of the cable and RF unit.
2219	MC-ABC-Ch-Id-Mismatch-Ch1	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch1.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.
2220	MC-ABC-Ch-Id-Mismatch-Ch2	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch2.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.
2221	MC-ABC-Ch-Id-Mismatch-Ch3	Alarm	Equipment	Multi Carrier ABC Channel Id Mismatch Ch3.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.
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.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
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.
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 Manual Disabled Ch6.	Warning	Admin state for channel is down.	Enable admin state for channel.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
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	Check link performance on all channels in Enhanced Multi Carrier ABC group. Check alarms for channels in Enhanced Multi Carrier ABC group. Check configuration of Enhanced Multi Carrier ABC group.
2300	protection-configuration-mismatc	Alarm	Equipment	Protection configuration mismatch!	Major	The configuration between the protected devices is not aligned.	Apply copy-to-mate command to copy the configuration from the required device to the other one.
2301	protection-copytomate-started	Event	Processing	Copy to mate started	Indeterminate	The copy-to-mate command has just begun!	This is a notification
2302	protection-copytomate-completed	Event	Processing	Copy to mate completed	Indeterminate	The copy-to-mate command was completed.	This is a notification
2400	cpri-optical-rx-los	Alarm	Equipment	Loss of CPRI optical signal - based on RX level lower than a predefined threshold	Critical	No SFP is connected. Issue with the Fiber link.	Check Fiber connection

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
2401	cpri-los	Alarm	Equipment	CPRI LOS caused by at least 16 8B/10B violation events in a whole hyperframe	Major	Input signal is not in a CPRI format. CPRI format is different than the configured one. Errors in the CPRI link that feeds the system.	1. Check CPRI format. 2. Check CPRI link/cable.
2402	cpri-clock-unit-unlock	Alarm	Equipment	CPRI clock unit is not locked	Warning	The recovered clock of the CPRI module is not locked.	Check the clock source of the CPRI module.
3000	chassis-reset-event	Event	Equipment	Chassis was reset	Warning	User issued a command to reset the chassis.	Wait until the reset cycle is ended and the system is up and running.
3001	10gbps-mode-front-panel-ports-unavailable	Alarm	Equipment	Reset chassis to activate front panel Ethernet ports	Warning	Front panel Ethernet ports cannot work when slot 12 is configured in 10Gbps mode.	Reset chassis.
3002	slot-mode-front-panel-ports-not-functional	Alarm	Equipment	Front panel Ethernet port cannot function in current configured capacity mode	Warning	Front panel Ethernet port cannot work in a mode other than 1Gbps.	Configure the relevant capacity mode to 1 Gbps mode.
3003	abc-mode-not-functional	Alarm	Equipment	Multi Carrier ABC group is not functional in current configured capacity mode	Warning	Multi Carrier ABC group does not support the configured capacity mode.	Configure the relevant capacity mode to 1 Gbps mode.
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.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
4001	slotsection-2_5gbps-compatibility	Alarm	Equipment	Card cannot function in 2.5Gbps mode.	Warning	The user set an expected card that does not support 2.5Gbps.	Change the Slot Section to 1Gbps.
4002	slot-slotsection-10gbps-card-not-functional	Alarm	Equipment	Card is not functional until chassis is reset	Warning	Slot is not in 10Gbps mode.	Reset chassis.
5000	failure-login-event	Event	Equipment	User blocked due to consecutive failure login	Indeterminate	User blocked due to consecutive failure login	The user should wait few minutes until it account will be unblock
5001	g8032-protection-switching-alarm	Alarm	Processing	ERPI is either in protection state or forced protection state	Minor	Either link failure happened in the ring or force/manual command is active.	Fix the broken link in the ring or release the force/manual command.
5002	g8032-failure-of-protocol-pm-alarm	Alarm	Processing	More than a single RPL is configured in a ring	Warning	User configuration	Reconfigure the RPL
5003	lldp-topology-change	Event	Processing	LLDP topology change	Warning	New neighbor	None
5004	security-log-upload-started-event	Event	Equipment	Security log upload started	Indeterminate	Security log upload started	
5005	security-log-upload-failed-event	Event	Equipment	Security log upload failed	Indeterminate	Security log upload failed	
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	

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
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		
5013	sync-T0-quality-change-event	Event	Equipment	System sync reference T0 quality has changed	Major		
5014	sync-pipe-invalid-interface-clock-source	Alarm	Equipment	The pipe interface clock-source in signal-interface table is not system-clock	Major		
5015	sync-pipe-missing-edge	Alarm	Equipment	The pipe is missing an edge interface	Major	Regenerator contains less than 2 interfaces	Accomplish configuration by assigning second interface
5016	sync-pipe-interface-op-state-down	Alarm	Equipment	Pipe interface operational state is down	Major	At least one of Regenerator Interfaces status is down	Checking regenerator Admin status
5017	sync-pipe-invalid-pipe	Alarm	Equipment	Pipe is invalid	Major	Interfaces has Configuration or Operation fails	Configuration not accomplished
5018	sync-1588-tc-not-operational	Alarm	Equipment	1588TC is not operational	Major	System Failure	Reboot the unit
5020	sync-T3-remote-loopback	Alarm	Equipment	T3 interface at loopback mode	Warning		
5021	sync-T4-analog-loopback	Alarm	Equipment	T4 interface at loopback mode	Warning		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5030	soam-connectivity-failure	Alarm	Processing	A connectivity failure in MA/MEG	Minor	Wrong link configurations.	Check the link in the traffic path
5031	soam-def-error-failure	Alarm	Processing	Error CCM received	Major	Invalid CCMs has been received	Check the link in the traffic path
5032	soam-def-mac-failure	Alarm	Processing	Remote mep MAC status not up	Minor	Remote MEP's associated MAC is reporting an error status	Check remote MEP's MAC status
5033	soam-def-rdi-failure	Alarm	Processing	Mep Rdi received	Minor	Remote Defect indication has been received from remote MEP	Check the SOAM configurations
5034	soam-remote-ccm-failure	Alarm	Processing	Remote mep CCMs are not received	Major	The MEP is not receiving CCMs from at least one of the remote MEPs	Check that all remote MEPs are configured or enabled
5035	soam-def-xcon-failure	Alarm	Processing	Cross Connect CCM received	Major	CCM from another MAID or lower MEG level have been received	Check MA/MEG and MEP configurations
5036	ptp-stream-state-change	Event	Processing	1588-BC port state changed	Warning		
5037	ptp-bmca-update	Event	Processing	1588-BC BMCA has been updated.	Warning		
5038	ptp-output-squelch	Event	Processing	1588-BC outputs are squelched.	Warning		
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		

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5041	ptp-leap-seconds-flag-change	Event	Processing	1588-BC one of the leap seconds flags have changed.	Warning		
5042	ptp-message-interval-change	Event	Processing	1588-BC message interval change detected.	Warning		
5043	ptp-message-rate-announce	Alarm	Processing	1588-BC announce message rate is below expected.	Major	Misconfiguration of the peer system.	Check the configuration of the peer system.
5044	ptp-message-rate-sync	Alarm	Processing	1588-BC sync message rate is below expected.	Major	Misconfiguration of the peer system.	Check the configuration of the peer system.
5045	ptp-message-rate-delay-req	Alarm	Processing	1588-BC delay request message rate is below expected.	Major	Misconfiguration of the peer system.	Check the configuration of the peer system.
5046	ptp-no-syncE	Alarm	Processing	1588-BC performance is degraded due to loss of system clock reference.	Critical	Loss of system clock reference.	Restore the system clock synchronization to a PRC-traceable source.
5047	soam-csf-rdi-alarm	Alarm	Processing	Auto-state-propagation indication received	Major	Remote system triggered auto-state-propagation	Resolve the problem on the .remote system.
5048	lacp-port-out-of-sync-alarm	Alarm	processing	LACP port out of collecting-distributing	Major	LACP port was not selected by the aggregator or partner is out of sync	Resolve the problem on the remote system
5100	mkey-mismatch	Alarm	Equipment	Master key mismatch cross over the link	Critical	Master Key was not set correctly.	Verify the Master Key.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
5101	mkey-no-exist	Alarm	Equipment	No Master Key set, default value used	Warning	Crypto module has been enabled, but no Master Key has been loaded.	Set the Master Key.
5102	general-encryption-failure	Alarm	Equipment	Payload Encryption failure	Critical	Radio LOF on Tx/Rx direction. The session key does not match across the link. The AES admin setting does not match across the link.	Validate the MSE on both sides of the link. Validate the session key on both sides of the link. Validate the AES admin setting on both sides of the link.
5104	kep-initiated	Event	Equipment	Key Exchange Protocol in progress, Traffic has been blocked	Indeterminate		
5105	kep-remote-initiated	Event	Equipment	Key Exchange Protocol initiated by remote side	Indeterminate		
5107	bypass-self-test-alarm	Alarm	Equipment	FIPS Bypass Self-Test failed	Critical	Disk failure	
5108	post-fail-alarm	Alarm	Equipment	Power On Self-Test Failed	Critical	System failure	Reboot the unit.
5109	main-board-non-fips-alarm	Alarm	Equipment	Main Board is not FIPS certified	Critical	Main Board used is not FIPS certified	Use a FIPS-certified TCC.
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

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
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
30007	Clock-source-sharing-failure-event	Event	Equipment	Clock source sharing failure	Critical	Faulty coaxial cable between master and slave RFUs. Hardware failure in Master RFU. Hardware failure in Slave RFU.	Try re-initiation of MIMO. If still fails: Replace faulty coaxial cable and reset Master RFU. Replace faulty RFU.
31000	Insufficient-conditions-for-MIMO-alarm	Alarm	Equipment	Insufficient conditions for MIMO	Critical	Insufficient conditions for MIMO. Hardware failure.	Make sure all cables between master and slave are connected (MIMO 4x4 only). Replace faulty units and check that cables are plugged.
31003	Unsuitable-hardware-for-MIMO-alarm	Alarm	Communications	Unsuitable hardware for MIMO	Critical	Unsuitable hardware for MIMO operation requirements. Dual carrier RFUs (MIMO 2x2 and 4x4). RFUs with MIMO bus interface (MIMO 4x4). Clock source sharing capability (MIMO 4x4).	Make sure both RFUs are compatible for MIMO operation.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
31004	Unsuitable-software-configuration-for-MIMO-alarm	Alarm	Communications	Unsuitable software configuration for MIMO	Critical	Not all MIMO carriers are set to same radio script or script is not compatible for MIMO. Radio TX and RX frequency is not identical on all MIMO carriers. XPIC or Multi radio or ATPC features are enabled.	Load same MIMO compatible radio script to all MIMO carriers. Set same TX and RX frequency on all MIMO carriers. Disable XPIC, Multi radio and ATPC on all MIMO carriers.
31005	Clock-source-sharing-failure-alarm	Alarm	Equipment	Clock source sharing cable unplugged	Critical	Faulty coaxial cable between master and slave RFUs Mate does not exist	Replace faulty coaxial cable and reset Master RFU. Replace faulty RFU.
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)

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
31104	AMCC-Invalid-ACM-Configuration-alarm	Alarm	Communications	Invalid ACM configuration	Critical	AMCC member have been set to fixed profile	Set AMCC member to adaptive ACM profiles
31105	AMCC-Mimo-not-supported-alarm	Alarm	Equipment	MIMO insufficient condition – configuration is not supported	Critical	MIMO script is not enabled on any radio member. Different TX/RX frequency. ATPC enabled. XPIC enabled. ACM mode (adaptive/Fixed) is not the same. Unit Redundancy enabled. Platform not supported.	Align MIMO script on all radio members. Align same frequency on all radio members. Disable ATPC. Disable XPIC. Align ACM mode. Disable Unit Redundancy. Replace unit.
31106	AMCC-Master-failure-alarm	Alarm	Equipment	MIMO insufficient condition – Master unit failure.	Critical	Master unit failure.	Verify Master unit power. Replace hardware.
31107	AMCC-Slave-failure-alarm	Alarm	Equipment	MIMO insufficient condition – Slave unit failure.	Critical	Slave unit failure.	Verify Slave unit power. Replace hardware.
31108	AMCC-Data-Sharing-cable-disconnected-alarm	Alarm	Equipment	MIMO insufficient condition – Data sharing cable failure.	Critical	Data sharing cable failure.	Verify Data sharing cable connected. Replace Data sharing cable.
31109	AMCC-Prot-port-cable-disconnected-alarm	Alarm	Equipment	MIMO insufficient condition – Mate communication cable failure.	Critical	Mate communication cable failure.	Verify Mate communication cable connected. Replace Mate communication cable.

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
31110	AMCC-Source-Sharing-cable-disconnected-alarm	Alarm	Equipment	MIMO insufficient condition – Source sharing cable failure.	Critical	Source sharing cable failure.	Verify Source sharing cable connected. Replace Source sharing cable.
31111	AMCC-Master-Slave-config-mismatch-alarm	Alarm	Equipment	MIMO insufficient condition - Master/Slave configuration mismatch	Critical	Master/Slave configuration mismatch due to: Different TX/RX frequency. Different MIMO script ID. Different ACM mode (adaptive/Fixed).	Align Master/Slave configuration.
31112	AMCC-Remote-failure-alarm	Alarm	Equipment	MIMO insufficient condition – Remote failure	Critical	MIMO remote failure.	Handle MIMO remote failure.
31115	AMCC-Data-Sharing-failure-alarm	alarm	Radio	AMCC insufficient condition - Units alignment failure.	Critical	Units alignment failure.	Verify Source sharing cable connected. Replace Source sharing cable. Verify Data sharing cable connected. Replace Data sharing cable. Verify using correct SFPs.
31118	AMCC-XPIC-not-supported-alarm	alarm	Radio	XPIC configuration is not supported	Critical	XPIC MRMC script is not configured Different TX/RX frequency. ACM mode (adaptive/fixed) is not configured the same.	Set XPIC MRMC script Align same frequency on all radio members. Align same ACM mode.
31119	AMCC-XPIC-remote-failure-alarm	alarm	Radio	XPIC configuration failure in remote	Warning	XPIC remote failure	Handle XPIC remote failure

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
31120	AMCC-XPIC-mate-communication-failure-alarm	Alarm	Communications	XPIC communication with mate unit is interrupted	Warning	The mate unit is unreachable. In FIPS mode, possible mismatch between the IPSec pre-shared keys configured on the two units.	Check the cable between the two units. In FIPS mode, make sure that the same IPSec pre-shared key is configured on the two units.
31121	AMCC-Radio-unit-failure-alarm	Alarm	Communications	AMCC insufficient condition - Radio unit failure.	Critical	Radio Unit failure.	Verify radio unit power. Replace HW.
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.	
32003	unit-mgr-unit-reset-event	Event	Management	Unit was reset.	Warning	User issued a command to reset the unit	Wait until the reset cycle is ended and the system is up and running
32004	unit-mgr-power-up-event	Event	Equipment	Unit Performed Power up	Warning		
33001	anti-theft-enabled-event	Event	Management	Anti-Theft Procedures have been enabled	Indeterminate		
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

Alarm ID	Name	Type	Group	Description	Severity	Probable Cause	Corrective Action
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

Glossary

Term	Definition
A	
ABC	Adaptive Bandwidth Control
ABN	Adaptive Bandwidth Notification
AC	Alternating Current
ACAP	Adjacent Channel Alternate Polarization
ACCP	Adjacent Channel Co-Polarization
ACM	Adaptive Coded Modulation
ACR	Adaptive Clock Recovery
AES	Advanced Encryption Standard
AFR	Advanced Frequency Reuse
AGC	Automatic Gain Control
AIS	Alarm Indicating Signal
ALC	Automatic Level Control
AMCC	Advanced Multi-Carrier Configuration
ANSI	American National Standards Institute
ASIC	Application Specified Integrated Circuit
ATPC	Automatic Transmit Power Control
AUX	Auxiliary Unit
B	
BB	Baseband
BBS	Baseband Switching
BER	Bit Error Rate
BLSR	Bidirectional Line Switch Ring
BPDU	Bridge Protocol Data Units
BWA	Broadband Wireless Access
C	
CBS	Committed Burst Size
CCDP	Co-Channel Dual Polarization

Term	Definition
CCITT	Comité Consultatif International de Télégraph et des Télécommunications (ITU)
CET	Carrier-Ethernet Transport
CFM	Connectivity Fault Management
CIR	Committed Information Rate
CLI	Command Line Interface
Clk	Clock
CODEC	Coder/Decoder
CoS	Class of Service
D	
DA	Destination Address
DC	Direct Current
DCB	Diversity Circulator Block
DCC	Data Communication Channel
DXC	Digital Cross Connect
DSCP	Differentiated Services Code Point
E	
EBS	Excess Burst Size
EIR	Excess Information Rate
EMC	Electromagnetic Compatibility
EOW	Engineering Order Wire
EPROM	Erasable Programmable Read Only Memory
ESD	Electrostatic Discharge
ESE	Electrical SFP Electrical
ESP	Electrical SFP SFP+ 10G
ESS	Electrical SFP SFP
ETSI	European Telecommunications Standards Institute
F	
FCC	Federal Communications Commission
FCS	Frame Check Sequence

Term	Definition
FTP	File Transfer Protocol
G	
GbE	Gigabit Ethernet
GFP	Generic Framing Procedure (Procedure for mapping of Ethernet traffic over a transport network)
GND	Ground
GRE	Generic Routing Encapsulation
GTP	GPRS Tunneling Protocol
H	
HBER	High Bit Error Rate
HDLC	High-level Data Link Control
HF	High Frequency (3-30 MHz)
HSB	Hot-Standby
HTTP	Hypertext Transfer Protocol
HTTPS	Secured Hypertext Transfer Protocol
I	
IDC	Indoor Controller
IF	Intermediate Frequency
IFC	IF Combining
ISO	International Organization for Standardization
ITU	International Telecom. Union
ITU-R	International Telecom. Union (former CCIR)
ITU-T	International Telecom. Union (former CCITT)
IVM	Inventory Module
L	
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LAN	Local Area Network
LBER	Low Bit Error Rate
LCAS	Link Capacity Adjustment Scheme

Term	Definition
LED	Light Emitting Diode
LIU	Line Interface Unit
LLDP	Link Layer Discovery Protocol
LLF	Link Loss Forwarding
LMS	License Management System
LO	Local Oscillator
LOC	Loss of Carrier
LOF	Loss of Frame
LOS	Loss of Signal
LSI	Large Scale Integration
LTE	Long-Term Evolution
M	
MAID	Maintenance Association Identifier
MPLS	Multi Protocol Label Switching
MSP	Multiplex Section Protection
MUX	Multiplexer
N	
NE	Network Element
NMS	Network Management System
NTP	Network Time Protocol
O	
OAM	Operation Administration & Maintenance (Protocols)
OCB	Outdoor Circulator Box
OHC	OverHead Connections
OMT	Orthogonal Mode Transducer
OOF	Out of Frame
OPEX	Operational Expenditure
P	
PBB-TE	Provider Backbone Bridge Traffic Engineering
PBS	Peak Burst Rate

Term	Definition
PC	Personal Computer
PCB	Printed Circuit Board
PDV	Packed Delay Variation
PIR	Peak Information Rate
PLL	Phase Locked Loop
PM	Performance Monitoring
PN	Provider Network
PROM	Programmable Read Only Memory
PSN	Packet Switched Network
PTP	Precision Timing Protocol
PWR	Power
Q	
QoE	Quality of Experience
QoS	Quality of Service
R	
RBAC	Role Based Access Control
RCVR	Receiver
RDI	Reverse Defect Indication
RF	Radio Frequency
RIP	Routing Information Protocol
RMON	Ethernet Statistics
RPS	Radio Protection Switching
RSL	Received Signal Level
RSSI	Received Signal Strength Indicator
RSTP	Rapid Spanning Tree Protocol
S	
SAP	Service Access Point
SDH	Synchronous Digital Hierarchy
SDWRR	Shaped Deficit Weighted Round Robin
SETS	Synchronous Equipment Timing Source

Term	Definition
SFTP	Secure FTP
SLA	Service Level Agreements
SNCP	Simple Network Connection Protection
SNMP	Simple Network Management Protocol
SNP	Service Network Point
SNR	Signal to Noise Ratio
SNTP	Simple Network Time Protocol
SOH	Section OverHead (ETSI)
SONET	Synchronous Optical NETwork
SP	Service Point
SSH	Secured Shell (Protocol)
SSM	Synchronization Status Message
STP	Spanning Tree Protocol
SyncE	Synchronous Ethernet
SVCE	Service Channel Equipment
T	
TC	Traffic Class
TIM	Trace Identifier Mismatch
TOH	Transport OverHead (ANSI)
TOS	Type Of Service
V	
VC	Virtual Container
VCO	Voltage Controlled Oscillator
VCXO	Voltage Controlled crystal Oscillator
VLSI	Very Large Scale of Integration
W	
WAN	Wide Area Network
Web EMS	Web-Based Element Management System
WFQ	Weighted Fair Queue
WG	Waveguide

Term	Definition
WRED	Weighted Random Early Detection
WRR	Weighted Round Robin
X	
XCVR	Transceiver (Transmitter/Receiver)
XMTR	Transmitter
XO	Crystal Oscillator
XPD	Cross Polar Differentiation
XPI	Cross Polariztion Isolation
XPIC	Cross Polarization Interference Cancellation