



USER GUIDE

PTP 820C/820S

System Release 10.0



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

About This User Guide	1
Contacting Cambium Networks	2
Purpose	3
Cross references	3
Feedback	3
Problems and warranty	4
Reporting problems	4
Repair and service	4
Hardware warranty	4
Security advice	5
Warnings, cautions, and notes	6
Warnings	6
Cautions	6
Notes	6
Caring for the environment	7
In EU countries	7
In non-EU countries	7
Chapter 1: Introduction.....	1-1
System Overview	1-2
Configuration Tips.....	1-2
PTP 820C	1-3
PTP 820S	1-3
PoE Injector Overview.....	1-3
PTP 820 Assured Platform	1-3
The Web-Based Element Management System.....	1-5
Reference Guide to Web EMS Menu Structure	1-13
Chapter 2: Getting Started.....	2-1
Assigning IP Addresses in the Network.....	2-2
Establishing a Connection	2-3
PC Setup.....	2-4
Logging on.....	2-6
Logging in Without Knowing the IP Address	2-6
Changing Your Password.....	2-8
Performing Quick Platform Setup.....	2-10
Mate Management Access (IP Forwarding).....	2-14
Configuring In-Band Management.....	2-15
Changing the Management IP Address	2-16

Configuring the Activation Key	2-18
Activation Key Overview	2-18
Viewing the Activation Key Status Parameters	2-19
Entering the Activation Key.....	2-20
To activate a demo activation key:	2-20
Displaying a List of Activation-Key-Enabled Features	2-21
Setting the Time and Date (Optional)	2-22
Enabling the Interfaces (Interface Manager)	2-25
Configuring the Radio Parameters	2-27
Enabling Link ID Mismatch Security.....	2-29
Configuring the Radio (MRMC) Script(s)	2-31
Radio Profiles.....	2-36
Enabling ACM with Adaptive Transmit Power.....	2-37
Operating in FIPS Mode	2-39
Requirements for FIPS Compliance.....	2-39
Enabling FIPS Mode.....	2-39
Configuring Grouping (Optional)	2-41
Creating Service(s) for Traffic	2-42
Chapter 3: Configuration Guide	3-1
System Configurations.....	3-2
Configuring a Link Using the Quick Configuration Wizard	3-3
Configuring a 1+0 Link Using the Quick Configuration Wizard	3-4
Configuring a 1+0 (Repeater) Link Using the Quick Configuration Wizard	3-8
Configuring a 2+0 Multi-Carrier ABC Link Using the Quick Configuration Wizard	3-12
Configuring Multi-Carrier ABC.....	3-19
Multi-Carrier ABC Overview.....	3-19
Configuring a Multi-Carrier ABC Group.....	3-19
Configuring the Multi-Carrier ABC Minimum Bandwidth Override Option.....	3-22
Adding and Removing Group Members.....	3-23
Deleting a Multi-Carrier ABC Group.....	3-24
Configuring Link Aggregation (LAG) and LACP	3-25
LAG Overview.....	3-25
Configuring a LAG Group.....	3-26
Enabling and Disabling LAG Group Shutdown in Case of Degradation Event	3-29
Configuring Enhanced LAG Distribution.....	3-30
Deleting a LAG Group.....	3-32
Displaying LACP Parameters and Statistics.....	3-32
Configuring XPIC.....	3-39
XPIC Overview	3-39
Configuring the Radio Carriers	3-39
Creating an XPIC Group.....	3-40
Performing Antenna Alignment for XPIC.....	3-40
Configuring Unit Protection with HSB Radio Protection (External Protection)	3-42

Unit Protection Overview	3-42
Configuring Ethernet Interface Protection	3-43
Configuring HSB Radio Protection	3-44
Configuring 2+2 HSB Protection on a PTP 820C Unit	3-47
Viewing the Configuration of the Standby unit.....	3-47
Editing Standby Unit Settings.....	3-48
Viewing Link and Protection Status and Activity	3-48
Manually Switching to the Standby Unit.....	3-49
Disabling Automatic Switchover to the Standby Unit.....	3-50
Disabling Unit Protection.....	3-50
Configuring 1 + 1 HSB with Space Diversity	3-50
Configuring MIMO and Space Diversity	3-54
MIMO and Space Diversity Overview	3-54
Configuring a MIMO Link	3-55
Creating a MIMO or Space Diversity Group	3-56
Enabling/Disabling a MIMO or Space Diversity Group	3-57
Setting the Role of a MIMO or Space Diversity Group.....	3-58
Resetting MIMO.....	3-59
Viewing MMI and XPI Levels	3-60
Deleting a MIMO or Space Diversity Group	3-61
Configuring Advanced Frequency Reuse (AFR)	3-62
AFR Overview	3-62
Initial Link Configuration and Alignment for AFR	3-63
Software Configuration for AFR	3-63
Deleting an AFR Group	3-67
Operating a PTP 820C in Single Radio Carrier Mode	3-69
Chapter 4: Unit Management.....	4-1
Defining the IP Protocol Version for Initiating Communications.....	4-2
Configuring the Remote Unit's IP Address.....	4-3
Changing the Subnet of the Remote IP Address.....	4-5
Configuration SNMP	4-7
Configuring Trap Managers.....	4-11
Installing and Configuring an FTP or SFTP Server	4-14
Configuring the Internal Ports for FTP or SFTP.....	4-17
Upgrading the Software	4-18
Viewing Current Software Versions	4-18
Software Upgrade Overview.....	4-19
Downloading and Installing Software.....	4-20
Downloading Software Via HTTP or HTTPS.....	4-20
Downloading Software Via FTP or SFTP.....	4-21
Installing Software	4-24
Configuring a Timed Installation	4-26
Backing Up and Restoring Configurations	4-27

Configuration Management Overview	4-27
Viewing Current Backup Files	4-27
Setting the Configuration Management Parameters	4-29
Exporting a Configuration File	4-31
Importing a Configuration File	4-31
Deleting a Configuration File	4-32
Backing Up the Current Configuration	4-32
Restoring a Saved Configuration	4-32
Editing CLI Scripts	4-33
Setting the Unit to the Factory Default Configuration	4-34
Performing a Hard (Cold) Reset	4-35
Configuring Unit Parameters	4-36
Configuring NTP	4-38
Displaying Unit Inventory	4-40
Chapter 5: Radio Configuration	5-1
Viewing the Radio Status and Settings	5-2
Configuring the Remote Radio Parameters	5-5
Configuring ATPC and ATPC Override Timer	5-8
Configuring Header De-Duplication and Frame Cut-Through	5-11
Viewing Header De-Duplication and Frame Cut-Through Counters	5-13
Configuring AES-256 Payload Encryption	5-17
Configuring and Viewing Radio PMs and Statistics	5-21
Configuring BER Thresholds and Displaying Current BER	5-21
Displaying MPMC Status	5-23
Displaying MPMC PMs	5-24
Displaying and Clearing Defective Block Counters	5-25
Displaying Signal Level PMs and Configuring Signal Level PM Thresholds	5-28
Displaying Modem BER (Aggregate) PMs	5-30
Displaying MSE PMs and Configuring MSE PM Thresholds	5-32
Displaying XPI PMs and Configuring XPI PM Threshold	5-34
Displaying Traffic PMs	5-36
Chapter 6: Ethernet Services and Interfaces	6-1
Configuring Ethernet Service(s)	6-2
Ethernet Services Overview	6-2
General Guidelines for Provisioning Ethernet Services	6-3
The Ethernet Services Page	6-3
Adding an Ethernet Service	6-4
Editing a Service	6-6
Deleting a Service	6-6
Enabling, Disabling, or Deleting Multiple Services	6-7
Viewing Service Details	6-7
Configuring Service Points	6-7
Setting the MRU Size and the S-VLAN Ethertype	6-21

Configuring Ethernet Interfaces.....	6-22
Configuring Automatic State Propagation and Link Loss Forwarding	6-25
Viewing Ethernet PMs and Statistics	6-28
RMON Statistics	6-28
Egress CoS Statistics	6-29
Port TX Statistics	6-31
Port RX Statistics.....	6-34
Chapter 7: Quality of Service (QoS)	7-1
QoS Overview	7-2
Configuring Classification	7-4
Classification Overview	7-4
Configuring Ingress Path Classification on a Logical Interface.....	7-5
Modifying the C-VLAN 802.1Q UP and CFI Bit Classification Table	7-7
Modifying the S-VLAN 802.1 UP and DEI Bit Classification Table.....	7-9
Modifying the DSCP Classification Table.....	7-10
Modifying the MPLS EXP Bit Classification Table	7-11
Configuring Policers (Rate Metering).....	7-13
Policer (Rate Metering) Overview	7-13
Configuring Policer Profiles	7-13
Assigning Policers to Interfaces.....	7-16
Configuring the Ingress and Egress Byte Compensation.....	7-20
Configuring Marking.....	7-21
Marking Overview	7-21
Enabling Marking	7-21
Modifying the 802.1Q Marking Table	7-22
Modifying the 802.1AD Marking Table.....	7-23
Configuring WRED	7-25
WRED Overview	7-25
Configuring WRED Profiles	7-25
Assigning WRED Profiles to Queues	7-28
Configuring Egress Shaping	7-29
Egress Shaping Overview	7-29
Configuring Queue Shaper Profiles.....	7-29
Configuring Service Bundle Shaper Profiles	7-31
Assigning a Queue Shaper Profile to a Queue.....	7-33
Assigning a Service Bundle Shaper Profile to a Service Bundle	7-35
Configuring Scheduling.....	7-38
Scheduling Overview.....	7-38
Configuring Priority Profiles.....	7-38
Configuring WFQ Profiles.....	7-42
Assigning a Priority Profile to an Interface	7-44
Assigning a WFQ Profile to an Interface	7-44
Chapter 8: Ethernet Protocols	8-1

Configuring Adaptive Bandwidth Notification (ABN)	8-2
Adaptive Bandwidth Notification Overview	8-2
Adding an ABN entity	8-2
Editing an ABN Entity	8-4
Deleting an ABN Entity	8-4
Viewing the Statistics for an ABN Entity	8-4
Configuring LLDP	8-6
LLDP Overview	8-6
Displaying Peer Status	8-6
Configuring the General LLDP Parameters	8-7
Configuring the LLDP Port Parameters	8-9
Displaying the Unit's Management Parameters	8-12
Displaying Peer Unit's Management Parameters	8-15
Displaying the Local Unit's Parameters	8-17
Displaying LLDP Statistics	8-22
Chapter 9: Synchronization	9-1
Configuring the SyncE Regenerator	9-2
Configuring the Sync Source	9-4
Viewing the Sync Source Status	9-5
Adding a Sync Source	9-6
Editing a Sync Source	9-7
Deleting a Sync Source	9-7
Configuring the Outgoing Clock and SSM Messages	9-8
Configuring 1588 Transparent Clock	9-10
Chapter 10: Access Management and Security	10-1
Configuring the General Access Control Parameters	10-2
Configuring the Password Security Parameters	10-4
Configuring the Session Timeout	10-5
Configuring Users	10-6
User Configuration Overview	10-6
Configuring User Profiles	10-7
Configuring Users	10-9
Configuring RADIUS	10-12
RADIUS Overview	10-12
Activating RADIUS Authentication	10-12
Configuring the RADIUS Server Attributes	10-13
Viewing RADIUS User Permissions and Connectivity	10-14
Configuring a RADIUS Server	10-16
Configuring X.509 CSR Certificates and HTTPS	10-36
Generating a Certificate Signing Request (CSR) File	10-36
Downloading a Certificate	10-38
Blocking Telnet Access	10-40
Uploading the Security Log	10-42

Uploading the Configuration Log	10-44
Chapter 11: Alarm Management and Troubleshooting	11-1
Viewing Current Alarms	11-2
Viewing Alarm Statistics	11-4
Viewing the Event Log	11-5
Editing Alarm Text and Severity	11-6
Displaying Alarm Information	11-6
Viewing the Probable Cause and Corrective Actions for an Alarm Type	11-7
Editing an Alarm Type	11-7
Setting Alarms to their Default Values	11-9
Uploading Unit Info	11-10
Performing Diagnostics	11-12
Performing Radio Loopback	11-12
Performing Ethernet Loopback	11-13
Configuring Service OAM (SOAM) Fault Management (FM)	11-14
Chapter 12: Web EMS Utilities	12-1
Restarting the HTTP Server	12-2
Calculating an ifIndex	12-2
Displaying, Searching, and Saving a list of MIB Entities	12-4
Chapter 13: Getting Started (CLI)	13-1
General (CLI)	13-3
Establishing a Connection (CLI)	13-3
PC Setup (CLI)	13-3
Logging On (CLI)	13-4
General CLI Commands	13-5
Changing Your Password (CLI)	13-6
Mate Management Access (IP Forwarding) (CLI)	13-7
Configuring In-Band Management (CLI)	13-9
Changing the Management IP Address (CLI)	13-10
Configuring the Activation Key (CLI)	13-12
Activation Key Overview (CLI)	13-12
Viewing the Activation Key Status Parameters (CLI)	13-12
Entering the Activation Key (CLI)	13-13
Activating a Demo Activation Key (CLI)	13-13
Displaying a List of Activation-Key-Enabled Features (CLI)	13-13
Setting the Time and Date (Optional) (CLI)	13-14
Setting the Daylight Savings Time (CLI)	13-15
Enabling the Interfaces (CLI)	13-16
Configuring the Radio Parameters (CLI)	13-18
Entering Radio View (CLI)	13-18
Muting and Unmuting a Radio (CLI)	13-18
Configuring the Transmit (TX) Level (CLI)	13-19
Configuring the Transmit (TX) Frequency (CLI)	13-19

Configuring the Radio (MRMC) Script(s) (CLI)	13-21
Displaying Available MRMC Scripts (CLI)	13-21
Assigning an MRMC Script to a Radio Carrier (CLI)	13-22
Enabling ACM with Adaptive Transmit Power (CLI)	13-24
Configuring the RSL Threshold Alarm (CLI)	13-25
Operating in FIPS Mode (CLI).....	13-26
Requirements for FIPS Compliance (CLI).....	13-26
Enabling FIPS Mode (CLI)	13-26
Configuring Grouping (Optional) (CLI).....	13-27
Creating Service(s) for Traffic (CLI)	13-28
Chapter 14: Configuration Guide (CLI).....	14-1
System Configurations (CLI)	14-2
Configuring Multi-Carrier ABC (CLI)	14-3
Multi-Carrier ABC Overview (CLI)	14-4
Configuring a Multi-Carrier ABC Group (CLI)	14-4
Configuring the Multi-Carrier ABC Minimum Bandwidth Override Option (CLI).....	14-5
Removing Members from a Multi-Carrier ABC Group (CLI)	14-6
Deleting a Multi-Carrier ABC Group (CLI)	14-7
Configuring Link Aggregation (LAG) and LACP (Optional) (CLI)	14-9
LAG Overview (CLI).....	14-9
Configuring a LAG Group (CLI)	14-10
Configuring LACP (CLI)	14-10
Viewing LAG Details (CLI)	14-11
Editing and Deleting a LAG Group (CLI)	14-11
Enabling and Disabling the LAG Group Shutdown in Case of Degradation Event Option (CLI).....	14-14
Configuring Enhanced LAG Distribution (CLI).....	14-14
Displaying LACP Parameters and Statistics (CLI)	14-15
Configuring XPIC (CLI).....	14-20
XPIC Overview (CLI)	14-20
Configuring the Radio Carriers for XPIC (CLI)	14-20
Creating an XPIC Group (CLI).....	14-21
Performing Antenna Alignment for XPIC (CLI).....	14-21
Configuring Unit Protection with HSB Radio Protection (External Protection) (CLI)	14-23
Unit Protection Overview (CLI)	14-23
Configuring Ethernet Interface Protection (CLI)	14-23
Configuring HSB Radio Protection (CLI)	14-24
Configuring 2+2 HSB Protection on a PTP 820C Unit (CLI)	14-26
Viewing the Configuration of the Standby unit (CLI).....	14-26
Editing Standby Unit Settings (CLI).....	14-26
Viewing Link and Protection Status and Activity (CLI)	14-27
Manually Switching to the Standby Unit (CLI)	14-27
Disabling Automatic Switchover to the Standby Unit (CLI)	14-28

Disabling Unit Protection (CLI).....	14-28
Configuring 1+1 HSB with Space Diversity (CLI).....	14-28
Configuring MIMO and Space Diversity (CLI)	14-30
MIMO and Space Diversity Overview (CLI).....	14-30
Configuring a MIMO Link (CLI)	14-31
Creating a MIMO or Space Diversity Group (CLI)	14-32
Enabling/Disabling a MIMO or Space Diversity Group (CLI)	14-32
Setting the Role of a MIMO or Space Diversity Group (CLI)	14-33
Resetting MIMO (CLI).....	14-33
Viewing MMI and XPI Levels (CLI).....	14-33
Deleting a MIMO or Space Diversity Group (CLI)	14-36
Configuring Advanced Frequency Reuse (AFR) (CLI)	14-37
Initial Link Configuration and Alignment for AFR (CLI)	14-37
Software Configuration for AFR (CLI).....	14-37
Deleting an AFR Group (CLI)	14-38
Operating a PTP 820C in Single Radio Carrier Mode (CLI).....	14-40
Chapter 15: Unit Management (CLI)	15-1
Defining the IP Protocol Version for Initiating Communications (CLI).....	15-2
Configuring the Remote Unit's IP Address (CLI)	15-3
Configuring the Remote Radio's IP Address in IPv4 format (CLI)	15-3
Configuring the Remote Radio's IP Address in IPv6 format (CLI)	15-4
Configuring SNMP (CLI)	15-5
Configuring Basic SNMP Settings (CLI)	15-5
Configuring SNMPv3 (CLI)	15-6
Displaying the SNMP Settings (CLI)	15-7
Configuring Trap Managers (CLI)	15-8
Configuring the Internal Ports for FTP or SFTP (CLI)	15-11
Upgrading the Software (CLI)	15-12
Software Upgrade Overview (CLI).....	15-12
Viewing Current Software Versions (CLI)	15-13
Configuring a Software Download (CLI)	15-13
Downloading a Software Package (CLI)	15-14
Installing and Upgrading Software (CLI).....	15-15
Backing Up and Restoring Configurations (CLI).....	15-17
Configuration Management Overview (CLI)	15-17
Setting the Configuration Management Parameters (CLI)	15-18
Backing up and Exporting a Configuration File (CLI)	15-19
Importing and Restoring a Configuration File (CLI)	15-20
Editing CLI Scripts (CLI)	15-21
Setting the Unit to the Factory Default Configuration (CLI)	15-22
Performing a Hard (Cold) Reset (CLI)	15-23
Configuring Unit Parameters (CLI)	15-24
Configuring NTP (CLI).....	15-26

Displaying Unit Inventory (CLI)	15-26
Chapter 16: Radio Configuration (CLI)	16-1
Viewing and Configuring the Remote Radio Parameters (CLI)	16-2
Displaying Communication Status with the Remote Radio (CLI)	16-2
Displaying the Remote Radio's Link ID (CLI)	16-2
Muting and Unmuting the Remote Radio (CLI)	16-2
Displaying the Remote Radio's RX Level (CLI)	16-3
Configuring the Remote Radio's TX Level (CLI)	16-3
Configuring Remote ATPC (CLI)	16-3
Configuring ATPC and ATPC Override Timer (CLI)	16-5
Configuring Header De-Duplication (CLI)	16-8
Displaying Header De-Duplication Information (CLI)	16-9
Configuring Frame Cut-Through (CLI)	16-11
Displaying Frame Cut-Through Information (CLI)	16-11
Configuring AES-256 Payload Encryption (CLI)	16-13
Configuring and Viewing Radio PMs and Statistics (CLI)	16-17
Displaying General Modem Status and Defective Block PMs (CLI)	16-17
Displaying Excessive BER (Aggregate) PMs (CLI)	16-18
Displaying BER Level and Configuring BER Parameters (CLI)	16-19
Configuring RSL Thresholds (CLI)	16-20
Configuring TSL Thresholds (CLI)	16-20
Displaying RSL and TSL Levels (CLI)	16-21
Configuring the Signal Level Threshold (CLI)	16-22
Configuring the MSE Thresholds and Displaying the MSE PMs (CLI)	16-23
Configuring the XPI Thresholds and Displaying the XPI PMs (CLI)	16-25
Displaying ACM PMs (CLI)	16-28
Chapter 17: Ethernet Services and Interfaces (CLI)	17-1
Configuring Ethernet Services (CLI)	17-2
Ethernet Services Overview (CLI)	17-2
General Guidelines for Provisioning Ethernet Services (CLI)	17-3
Defining Services (CLI)	17-4
Configuring Service Points (CLI)	17-9
Appendix A: Configuring C-VLAN CoS Preservation (CLI)	17-22
Appendix B: Configuring C-VLAN Preservation (CLI)	17-23
Appendix C: Configuring S-VLAN CoS Preservation (CLI)	17-24
Defining the MAC Address Forwarding Table for a Service (CLI)	17-29
Setting the MRU Size and the S-VLAN Ethertype (CLI)	17-34
Configuring the S-VLAN Ethertype (CLI)	17-34
Configuring the C-VLAN Ethertype (CLI)	17-35
Configuring the MRU (CLI)	17-35
Configuring Ethernet Interfaces (CLI)	17-35
Entering Interface View (CLI)	17-36
Displaying the Operational State of the Interfaces in the Unit (CLI)	17-38

Viewing Interface Attributes (CLI)	17-38
Configuring an Interface's Media Type (CLI)	17-38
Configuring an Interface's Speed and Duplex State (CLI)	17-39
Configuring an Interface's Auto Negotiation State (CLI)	17-40
Configuring an Interface's IFG (CLI)	17-40
Configuring an Interface's Preamble (CLI)	17-41
Adding a Description for the Interface (CLI)	17-41
Displaying Interface Statistics (RMON) (CLI)	17-42
Configuring Automatic State Propagation and Link Loss Forwarding (CLI)	17-43
Viewing Ethernet PMs and Statistics (CLI)	17-49
Displaying RMON Statistics (CLI)	17-49
Configuring Ethernet Port PMs and PM Thresholds (CLI)	17-50
Displaying Ethernet Port PMs (CLI)	17-50
Clearing Ethernet Port PMs (CLI)	17-54
Chapter 18: Quality of Service (QoS) (CLI)	18-1
Configuring Classification (CLI)	18-2
Classification Overview (CLI)	18-2
Configuring Ingress Path Classification on a Logical Interface (CLI)	18-2
Configuring VLAN Classification and Override (CLI)	18-3
Configuring 802.1p Classification (CLI)	18-5
Configuring DSCP Classification (CLI)	18-8
Configuring MPLS Classification (CLI)	18-12
Configuring a Default CoS (CLI)	18-14
Configuring Ingress Path Classification on a Service Point (CLI)	18-15
Configuring Ingress Path Classification on a Service (CLI)	18-15
Configuring Policers (Rate Metering) (CLI)	18-16
Overview of Rate Metering (Policing) (CLI)	18-16
Configuring Rate Meter (Policer) Profiles (CLI)	18-16
Displaying Rate Meter Profiles (CLI)	18-18
Deleting a Rate Meter Profile (CLI)	18-18
Attaching a Rate Meter (Policer) to an Interface (CLI)	18-19
Configuring the Line Compensation Value for a Rate Meter (Policer) (CLI)	18-24
Displaying Rate Meter Statistics for an Interface (CLI)	18-24
Configuring Marking (CLI)	18-26
Marking Overview (CLI)	18-26
Configuring Marking Mode on a Service Point (CLI)	18-26
Marking Table for C-VLAN UP Bits (CLI)	18-28
Marking Table for S-VLAN UP Bits (CLI)	18-29
Configuring WRED (CLI)	18-31
WRED Overview (CLI)	18-31
Configuring WRED Profiles (CLI)	18-31
Assigning a WRED Profile to a Queue (CLI)	18-33
Configuring Shapers (CLI)	18-35

Overview of Egress Shaping (CLI)	18-35
Configuring Service Bundle Shapers (CLI)	18-38
Configuring Egress Line Compensation for Shaping (CLI)	18-41
Configuring Scheduling (CLI)	18-42
Overview of Egress Scheduling (CLI)	18-42
Configuring Queue Priority (CLI)	18-42
Configuring Interface Priority Profiles (CLI)	18-43
Attaching a Priority Profile to an Interface (CLI)	18-46
Configuring Weighted Fair Queuing (WFQ) (CLI)	18-47
Displaying Egress Statistics (CLI)	18-51
Displaying Queue-Level PMs (CLI)	18-51
Displaying Service Bundle-Level PMs (CLI)	18-52
Chapter 19: Ethernet Protocols (CLI)	19-1
Configuring Adaptive Bandwidth Notification (ABN) (CLI)	19-2
Adaptive Bandwidth Notification Overview (CLI)	19-2
Configuring an ABN Entity (CLI)	19-2
Configuring LLDP (CLI)	19-7
Configuring the General LLDP Parameters (CLI)	19-7
Displaying the General LLDP Parameters (CLI)	19-8
Configuring LLDP Port Parameters (CLI)	19-9
Displaying LLDP Port Parameters (CLI)	19-10
Displaying LLDP Local System Parameters (CLI)	19-11
Displaying the LLDP Remote System Parameters (CLI)	19-13
Displaying LLDP Statistics (CLI)	19-16
Chapter 20: Synchronization (CLI)	20-1
Configuring SyncE Regenerator (CLI)	20-2
Changing the ETSI/ANSI Mode (CLI)	20-4
Configuring the Sync Source (CLI)	20-5
Configuring an Ethernet Interface as a Synchronization Source (CLI)	20-6
Configuring a Radio Interface as a Synchronization Source (CLI)	20-8
Clearing All Sync Sources (CLI)	20-9
Configuring the Outgoing Clock (CLI)	20-10
Configuring SSM Messages (CLI)	20-12
Configuring the Revertive Timer (CLI)	20-14
Displaying Synchronization Status and Parameters (CLI)	20-15
Configuring 1588 Transparent Clock (CLI)	20-17
Chapter 21: Access Management and Security (CLI)	21-1
Configuring the General Access Control Parameters (CLI)	21-3
Configuring the Inactivity Timeout Period (CLI)	21-3
Configuring Blocking Upon Login Failure (CLI)	21-3
Configuring Blocking of Unused Accounts (CLI)	21-4
Configuring the Password Security Parameters (CLI)	21-6
Configuring Password Aging (CLI)	21-6

Configuring Password Strength Enforcement (CLI).....	21-6
Forcing Password Change Upon First Login (CLI)	21-7
Displaying the System Password Settings (CLI)	21-8
Configuring Users (CLI)	21-9
User Configuration Overview (CLI).....	21-9
Configuring User Profiles (CLI)	21-10
Configuring User Accounts (CLI)	21-11
Configuring RADIUS (CLI)	21-14
RADIUS Overview (CLI)	21-14
Activating RADIUS Authentication (CLI)	21-14
Configuring the RADIUS Server Attributes (CLI).....	21-14
Viewing RADIUS Access Control and Server Attributes (CLI).....	21-15
Viewing RADIUS User Permissions and Connectivity (CLI)	21-15
Configuring X.509 CSR Certificates and HTTPS (CLI)	21-17
Generating a Certificate Signing Request (CSR) File (CLI)	21-17
Downloading a Certificate (CLI)	21-19
Enabling HTTPS (CLI).....	21-20
Blocking Telnet Access (CLI)	21-22
Uploading the Security Log (CLI)	21-23
Uploading the Configuration Log (CLI)	21-25
Chapter 22: Alarm Management and Troubleshooting (CLI)	22-1
Viewing Current Alarms (CLI)	22-2
Viewing the Event Log (CLI)	22-3
Editing Alarm Text and Severity (CLI).....	22-4
Displaying Alarm Information (CLI).....	22-4
Editing an Alarm Type (CLI)	22-4
Setting Alarms to their Default Values (CLI)	22-5
Configuring a Timeout for Trap Generation (CLI)	22-6
Uploading Unit Info (CLI).....	22-7
Performing Diagnostics (CLI)	22-10
Performing Radio Loopback (CLI).....	22-10
Performing Ethernet Loopback (CLI)	22-10
Configuring Service OAM (SOAM) Fault Management (FM) (CLI)	22-12
SOAM Overview (CLI)	22-12
Configuring MDs (CLI)	22-13
Configuring MA/MEGs (CLI)	22-14
Configuring MEPs (CLI).....	22-17
Displaying MEP and Remote MEP Attributes (CLI)	22-20
Displaying Detailed MEP Error Information (CLI).....	22-23
Performing Loopback (CLI).....	22-24
Working in CW Mode (Single or Dual Tone) (CLI)	22-28
Chapter 23: Maintenance	23-1
Temperature Ranges	23-2

Troubleshooting Tips	23-2
PTP 820C Connector Pin-outs	23-3
Eth1/PoE - GbE Electrical+PoE/Optical	23-3
Eth2 - GbE Electrical/Optical	23-4
MIMO Port	23-4
MGT/PROT - Management (FE-Standard) and Protection (FE-Non-Standard)	23-5
DC	23-5
RSL Interface	23-6
Source Sharing	23-6
PTP 820C LEDs	23-7
Electrical GbE Interface (RJ-45) LEDs	23-7
Optical GbE Interface (SFP) LEDs	23-7
Management FE Interface (RJ-45) LEDs	23-7
Status LED	23-8
Protection LED	23-8
PTP 820S Connector Pin-outs	23-9
Eth1/PoE - GbE Electrical+PoE/Optical	23-9
Eth2 - GbE Electrical/Optical	23-10
Eth3 - GbE Electrical/Optical	23-10
MGT/PROT - Management (FE-Standard) and Protection (FE-Non-Standard)	23-11
DC	23-11
RSL Interface	23-11
PTP 820S LEDs	23-12
Electrical GbE Interface (RJ-45) LEDs	23-12
Optical GbE Interface (SFP) LEDs	23-12
Management FE Interface (RJ-45) LEDs	23-13
Radio LED	23-13
Status LED	23-13
Protection LED	23-13
PoE Injector Pin-outs	23-14
PoE Port	23-14
Data Port	23-14
DC	23-15
PoE Injector LEDs	23-15
Radio LED	23-15
Chapter 24: Alarms List	24-16
Glossary	I

List of Figures

Figure 1	Main Web EMS Page	1-6
Figure 2	Displaying a Representation of the Front Panel	1-6
Figure 3	Main Web EMS Page with Representation of Front Panel	1-7
Figure 4	Displaying a Representation of the Front Panel	1-8
Figure 5	Main Web EMS Page with Representation of Front Panel – PTP 820C and PTP820S.....	1-8
Figure 6	Main Web EMS Page with Active and Standby Tabs	1-9
Figure 7	Related Pages Drop-Down List.....	1-9
Figure 8	Unit Summary Page	1-10
Figure 9	Unit Summary Page – Customizing Columns	1-10
Figure 10	Radio Summary Page	1-11
Figure 11	Radio Summary Page- Customizing Columns	1-12
Figure 12	Internet Protocol Properties Window	2-5
Figure 13	Login Page	2-6
Figure 14	Change User Password Page	2-8
Figure 15	Quick Configuration – Platform Setup Page	2-10
Figure 16	Quick Configuration– Platform Setup Summary Page	2-13
Figure 17	Local Networking Configuration Page.....	2-16
Figure 18	Activation Key Configuration Page.....	2-19
Figure 19	Activation Key Overview Page	2-21
Figure 20	Time Services Page	2-23
Figure 21	Interface Manager Page	2-25
Figure 22	Interface Manager – Edit Page	2-26
Figure 23	Multiple Selection Operation Section (Interface Manager Page)	2-26
Figure 24	Radio Parameters Page PTP 820C.....	2-27
Figure 25	Radio Parameters Page Per Carrier – PTP 820C	2-28
Figure 26	MRMC Symmetrical Scripts Page (ETSI)	2-31
Figure 27	MRMC Symmetrical Scripts Page (PTP 820C) (ETSI)	2-32
Figure 28	MRMC Symmetrical Scripts Page (PTP 820C) (FCC)	2-32
Figure 29	MRMC Symmetrical Scripts Page (Configuration) – PTP 820C.....	2-33
Figure 30	MRMC Symmetrical Scripts Page – Configuration – Adaptive Mode (PTP 820C)	2-34
Figure 31	Radio Parameters Page Per Carrier – PTP 820C	2-38
Figure 32	Security General Configuration Page.....	2-40
Figure 33	1+0 Quick Configuration Wizard – Page 1	3-4
Figure 34	1+0 Quick Configuration Wizard – Page 2.....	3-4
Figure 35	1+0 Quick Configuration Wizard – Page 3.....	3-6
Figure 36	1+0 Quick Configuration Wizard – Page 4.....	3-7
Figure 37	1+0 Quick Configuration Wizard – Page 5 (Summary Page)	3-8
Figure 38	1+0 Repeater Quick Configuration Wizard – Page 1.....	3-8
Figure 39	1+0 Repeater Quick Configuration Wizard – Page 2.....	3-9
Figure 40	1+0 Repeater Quick Configuration Wizard – Page 3.....	3-10
Figure 41	1+0 Repeater Quick Configuration Wizard – Page 4.....	3-10

Figure 42	1+0 Repeater Quick Configuration Wizard – Page 5.....	3-11
Figure 43	1+0 Repeater Quick Configuration Wizard – Page 6.....	3-12
Figure 44	2 + 0 Multi Carrier ABC Quick Configuration Wizard – Page 1	3-13
Figure 45	2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio #2 Selection Page	3-14
Figure 46	2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio XPIC Configuration Page.....	3-14
Figure 47	2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio Parameters Configuration Page	3-15
Figure 48	2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio Parameters Configuration Page (XPIC)	3-15
Figure 49	2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio MRMC Script Configuration Page	3-16
Figure 50	2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio MRMC Script Configuration Page - XPIC	3-16
Figure 51	2 + 0 Multi Carrier ABC Quick Configuration Wizard – Management Configuration Page.....	3-17
Figure 52	2 + 0 Multi Carrier ABC Quick Configuration Wizard –Summary Page	3-18
Figure 53	Multi-Carrier ABC Group Page (Empty)	3-20
Figure 54	Create ABC Group Wizard – First Page	3-20
Figure 55	Create ABC Group Wizard – Second Page	3-21
Figure 56	Create ABC Group Wizard – Finish Page.....	3-21
Figure 57	Multi-Carrier ABC Group – Edit Group Page.....	3-23
Figure 58	Multi Carrier ABC Group - Add/Remove Members Page	3-24
Figure 59	Create LAG Group – Page 1	3-27
Figure 60	Create LAG Group – Page 2.....	3-27
Figure 61	Create LAG Group – Final Page.....	3-28
Figure 62	Link Aggregation - Edit Page.....	3-28
Figure 63	Link Aggregation - Edit Page.....	3-31
Figure 64	LACP Aggregation Page	3-32
Figure 65	LACP Port Staus Page	3-34
Figure 66	LACP Port Status – View Page.....	3-34
Figure 67	LACP Port Statistics Page	3-36
Figure 68	LACP Port Debug Page	3-37
Figure 69	XPIC Configuration Page	3-40
Figure 70	Logical Interfaces – Edit Page.....	3-44
Figure 71	Unit Redundancy Page	3-45
Figure 72	Unit Redundancy Page when Redundancy Enabled	3-46
Figure 73	Interface Manager Page – Both Radio Carriers Enabled.....	3-47
Figure 74	Standby Tab of Radio Parameters Page	3-48
Figure 75	Unit Redundancy Page	3-49
Figure 76	MIMO Page.	3-51
Figure 77	Create Space Diversity Group- Page 1.	3-51
Figure 78	Create Space Diversity Group- Selection Summary	3-52
Figure 79	MIMO page – populated	3-52
Figure 80	MIMO – Edit Page (Space Diversity Group)	3-53

Figure 81 Create MIMO Group – Page 1.....	3-56
Figure 82 Create MIMO Group – Page 2.....	3-57
Figure 83 MIMO - Edit Page.....	3-58
Figure 84 MIMO - Edit Page.....	3-59
Figure 85 MIMO - Edit Page.....	3-60
Figure 86 MIMO - Edit Members Page	3-61
Figure 87 AFR 1+0 Deployment	3-62
Figure 88 AFR 1+0 Configuration.....	3-63
Figure 89 Advanced Multi Carrier Configuration Page (Empty)	3-64
Figure 90 AMCC Group – Select Group Parameters Page.....	3-64
Figure 91 AMCC Group – Select Group Parameters Page (Hub Site)	3-65
Figure 92 AMCC Group – Select Group Parameters Page (Tail Site)	3-66
Figure 93 AMCC Group – Selection Summary Page.....	3-67
Figure 94 Advanced Multi Carrier Configuration Page (Populated)	3-68
Figure 95 AMCC Group – Edit Page	3-68
Figure 96 Local Networking Configuration Page	4-2
Figure 97 Remote Networking Configuration Page – PTP 820C	4-3
Figure 98 Remote Networking Configuration Page – PTP 820S	4-4
Figure 99 Remote IP Configuration Page Per Carrier – PTP 820C.....	4-5
Figure 100 SNMP Parameters Page.....	4-7
Figure 101 V3 Users Page.....	4-8
Figure 102 V3 Users - Add Page	4-10
Figure 103 Trap Managers Page.....	4-11
Figure 104 Trap Managers - Edit Page	4-12
Figure 105 FileZilla Server User Configuration	4-15
Figure 106 FileZilla Server Shared Folder Setup.....	4-16
Figure 107 FTP Port Page.....	4-17
Figure 108 Versions Page	4-18
Figure 109 Download & Install Page – HTTP/ HTTPS Download – No File Selected	4-20
Figure 110 Download & Install page – HTTP/ HTTPS Download – File Selected.....	4-21
Figure 111 Download & Install Page - FTP.....	4-22
Figure 112 FTP Parameters Page	4-23
Figure 113 Install parameters Page.	4-26
Figure 114 Install parameters page- Software Management Timer.....	4-26
Figure 115 Backup Files Page.....	4-28
Figure 116 Configuration Management Page.....	4-29
Figure 117 FTP Parameters Page	4-29
Figure 118 Set to Factory Default Page	4-34
Figure 119 Reset Page.....	4-35
Figure 120 Unit Parameters Page	4-36
Figure 121 NTP Configuration Page	4-38
Figure 122 Inventory Page.....	4-40
Figure 123 Radio Parameters Page – PTP 820C.....	5-2

Figure 124 Radio Parameters Page Per Carrier – PTP 820C	5-3
Figure 125 Remote Radio Parameters Page – PTP 820C	5-5
Figure 126 Remote Radio Parameters Page – PTP 820S	5-5
Figure 127: Remote Radio Parameters Page Per Carrier – PTP 820C	5-6
Figure 128 ATPC Page – PTP 820C.....	5-9
Figure 129 ATPC – Edit Page per Carrier – PTP 820C.....	5-9
Figure 130 Radio Ethernet Interface Configuration Page – PTP 820C	5-11
Figure 131 Radio Ethernet Interface Configuration – Edit Page Per Carrier – PTP 820C	5-12
Figure 132 Radio Ethernet Interface Counters Page – PTP 820C	5-13
Figure 133 Radio Ethernet Interface Counters Page – PTP 820S	5-14
Figure 134 Radio Ethernet Interface Counters Page Per Carrier – PTP 820C	5-15
Figure 135 Payload Encryption Page.....	5-18
Figure 136 Payload Encryption – Edit Page	5-18
Figure 137 Payload Encryption – Edit Page with Master Key Displayed.....	5-19
Figure 138 Radio BER Thresholds Page	5-22
Figure 139 Radio BER Thresholds – Edit Page	5-22
Figure 140 MRMC Status Page	5-23
Figure 141 MRMC PM Report Page	5-24
Figure 142 Counters Page – PTP 820C.....	5-26
Figure 143 Counters Page – PTP 820S.....	5-26
Figure 144 Counters Page Per Carrier – PTP 820C	5-27
Figure 145 Signal Level PM Report Page.....	5-28
Figure 146 Signal Level Thresholds Configuration - Edit Page	5-29
Figure 147 Aggregate PM Report Page.....	5-30
Figure 148 MSE PM Report Page.....	5-32
Figure 149 Modem MSE Thresholds Configuration – Edit Page.....	5-33
Figure 150 XPI PM Report Page	5-34
Figure 151 XPI Thresholds Configuration – Edit Page	5-35
Figure 152 Capacity PM Report Page	5-36
Figure 153 Utilization PM Report Page.....	5-38
Figure 154 Ethernet Radio Capacity and Throughput Threshold Page.....	5-39
Figure 155 Frame Error PM Report Page	5-41
Figure 156 Ethernet Radio Utilization Threshold Page	5-41
Figure 157 Ethernet Services Page	6-3
Figure 158 Ethernet Services - Add page.....	6-5
Figure 159 Multiple Selection Operation Section (Ethernet Services)	6-7
Figure 160 Ethernet Service Points Page	6-9
Figure 161 Ethernet Service Points Page – Ingress Attributes	6-12
Figure 162 Ethernet Service Points Page – Egress Attributes	6-13
Figure 163 Ethernet Service Points - Add Page.....	6-16
Figure 164 Attached VLAN List Page.....	6-18
Figure 165 Attached VLAN List - Add Page	6-19
Figure 166 Ethernet General Configuration Page	6-21

Figure 167 Physical Interfaces Page	6-22
Figure 168 Physical Interfaces - Edit Page	6-23
Figure 169 Automatic State Propagation Page.....	6-26
Figure 170 Automatic State Propagation - Add Page	6-26
Figure 171 RMON Page.....	6-28
Figure 172 RMON Page – Hiding and Displaying Columns.....	6-29
Figure 173 Egress Cos Statistics Page.....	6-30
Figure 174 Egress CoS Statistics – Edit Page.....	6-31
Figure 175 Ethernet Port TX PM Report Page	6-32
Figure 176 Ethernet PM Port Admin Page	6-33
Figure 177 Ethernet Port Tx Threshold Page	6-34
Figure 178: Ethernet Port RX PM Report Page	6-35
Figure 179 Ethernet PM Port Admin Page	6-36
Figure 180 Ethernet Port Rx Threshold Page.....	6-36
Figure 181 QoS Block Diagram	7-2
Figure 182 Logical Interfaces Page	7-5
Figure 183 Logical Interfaces - Edit Page	7-6
Figure 184 802.1Q Classification Page	7-8
Figure 185 802.1Q Classification - Edit Page.....	7-8
Figure 186 802.1AD Classification Page.....	7-9
Figure 187 802.1Q Classification - Edit Page.....	7-9
Figure 188 DSCP Classification Page.....	7-10
Figure 189 DSCP Classification - Edit Page.....	7-10
Figure 190 MPLS Classification Page	7-11
Figure 191 MPLS Classification - Edit Page	7-12
Figure 192 Policer Profile Page	7-14
Figure 193 Policer Profile - Add Page	7-14
Figure 194 Logical Interfaces – Policers Page – Unicast Policer (Default).....	7-16
Figure 195 Logical Interfaces – Policers Page – Multicast Policer	7-17
Figure 196 Logical Interfaces – Policers Page – Broadcast Policer	7-18
Figure 197 Logical Interfaces – Policers Page – Ethertype Policer.....	7-19
Figure 198 802.1Q Marking Page	7-22
Figure 199 802.1Q Marking - Edit Page	7-22
Figure 200 802.1AD Marking Page.....	7-23
Figure 201 802.1AD Marking - Edit Page.....	7-24
Figure 202 WRED Profile Page	7-26
Figure 203 WRED Profile - Add Page.....	7-26
Figure 204 Logical Interfaces – WRED Page	7-28
Figure 205: Logical Interfaces – WRED - Edit Page	7-28
Figure 206 Queue Shaper Profile Page	7-30
Figure 207 Queue Shaper Profile – Add Page	7-30
Figure 208 Service Bundle Shaper Profile Page.....	7-32
Figure 209 Service Bundle Shaper Profile – Add Page	7-32

Figure 210	Logical Interfaces – Shaper – Egress Queue Shaper	7-34
Figure 211	Logical Interfaces – Egress Queue Shaper Configuration – Add Page.....	7-34
Figure 212	Logical Interfaces – Shaper – Egress Service Bundle Shaper	7-36
Figure 213	Logical Interfaces – Egress Service Bundle Shaper Configuration – Add Page	7-37
Figure 214	Scheduler Priority Profile Page	7-39
Figure 215	Scheduler Priority Profile – Add Page	7-40
Figure 216	Scheduler WFQ Profile Page	7-42
Figure 217	Scheduler WFQ Profile – Add Page	7-43
Figure 218	Logical Interfaces – Scheduler – Egress Port Scheduling Priority	7-44
Figure 219	Logical Interfaces – Scheduler – Egress Port Scheduling WFQ	7-45
Figure 220	ABN (Adaptive Bandwidth Notification) Page	8-2
Figure 221	ABN Configuration and Status – Add Page	8-3
Figure 222	ABN Configuration and Status - Statistics Page.....	8-5
Figure 223	LLDP Remote System Management Page	8-7
Figure 224	LLDP Configuration Parameters Page	8-8
Figure 225	LLDP Port Configuration Page.....	8-10
Figure 226	LLDP Port Configuration - Edit Page.....	8-10
Figure 227	LLDP Destination Address Table Page	8-13
Figure 228	LLDP Management TLV Configuration Page	8-14
Figure 229	LLDP Remote System Management Page	8-15
Figure 230	LLDP Remote System Table Page	8-16
Figure 231	LLDP Local System Parameters Page.....	8-17
Figure 232	LLDP Local System Port Page	8-19
Figure 233	LLDP Local System Management Page	8-20
Figure 234	LLDP Local System Management – View Page	8-21
Figure 235	LLDP Statistic Page	8-22
Figure 236	LLDP Port TX Statistic Page.....	8-23
Figure 237	LLDP Port RX Statistic Page	8-24
Figure 238	SyncE Regenerator Page	9-2
Figure 239	Pipe Configurations - Add Page.....	9-3
Figure 240	Sync Source Page	9-5
Figure 241	Sync Source – Add Page.....	9-6
Figure 242	Outgoing Clock Page.....	9-9
Figure 243	Outgoing Clock – Edit Page	9-9
Figure 244	1588-TC Page	9-10
Figure 245	1588 Transparent Clock Page	9-11
Figure 246	1588-TC – Edit Page.....	9-11
Figure 247	Access Control General Configuration Page	10-2
Figure 248	Access Control User Accounts - Edit Page.....	10-3
Figure 249	Access Control Password Management Page	10-4
Figure 250	Protocols Control Page	10-5
Figure 251	Access Control User Profiles Page	10-7
Figure 252	Access Control User Profiles - Add Page	10-8

Figure 253	Access Control User Accounts Page	10-9
Figure 254	Access Control User Accounts - Add Page	10-10
Figure 255	Radius Configuration Page	10-13
Figure 256	Radius Configuration – Edit Page	10-14
Figure 257	Radius Users Page	10-15
Figure 258	Radius Users Page – Expanded.....	10-15
Figure 259	Server Manager – Creating User Groups.....	10-17
Figure 260	Server Manager – Creating Users.....	10-18
Figure 261	Server Manager – Creating a RADIUS Client.....	10-19
Figure 262	Create Network Policy – Specify Name and Connection Type	10-21
Figure 263	Create Network Policy – Select Condition.....	10-22
Figure 264	Create Network Policy – User Group added to Policy’s Conditions	10-23
Figure 265	Create Network Policy – Specifying Access Permission.....	10-24
Figure 266	Create Network Policy – Configuring Authentication Methods	10-25
Figure 267	Create Network Policy – Insecure Authentication Method Query	10-25
Figure 268	Create Network Policy – Configuring Constraints	10-26
Figure 269	Create Network Policy – Configuring Settings	10-27
Figure 270	Create Network Policy – Adding Vendor Specific Attributes	10-28
Figure 271	Create Network Policy – Selecting to Add Attribute Information	10-29
Figure 272	Create Network Policy – Specifying the Vendor.....	10-29
Figure 273	Create Network Policy – Configuring Vendor-Specific Attribute Information	10-30
Figure 274	Create Network Policy – Example of Vendor-Specific Attribute Configuration.....	10-31
Figure 275	Create Network Policy – Stopping/Starting NPS Services	10-32
Figure 276	Security Certificate Request Page.....	10-37
Figure 277	FTP Parameters Page (Security Certificate Request)	10-38
Figure 278	Security Certification Download and Install Page	10-39
Figure 279	FTP Parameters Page (Security Certification Download & Install)	10-39
Figure 280	Protocols Control Page	10-40
Figure 281	Security Log Upload Page	10-42
Figure 282	FTP Parameters Page (Security Log Upload).....	10-43
Figure 283	Configuration Log Upload Page.....	10-44
Figure 284	Configuration Log Upload Page.....	10-45
Figure 285	Current Alarms Page.....	11-2
Figure 286	Current Alarms - View Page	11-2
Figure 287	Alarm Statistics Page	11-4
Figure 288	Event Log	11-5
Figure 289	Alarm Configuration Page	11-6
Figure 290	Alarm Configuration Page – Expanded	11-7
Figure 291	Alarm Configuration - Edit Page	11-9
Figure 292	Unit Info Page	11-10
Figure 293	Radio Loopbacks Page.....	11-12
Figure 294	Radio Loopbacks – Edit Page	11-13
Figure 295	Logical Interfaces – Loopback Page.....	11-14

Figure 296	SOAM MD Page.....	11-16
Figure 297	SOAM MD Page.....	11-16
Figure 298	SOAM MA/MEG Page	11-17
Figure 299	SOAM MA/MEG – Add Page	11-18
Figure 300	MEP List Page	11-21
Figure 301	Add MEP Page	11-22
Figure 302	SOAM MEP Page	11-22
Figure 303	Add SOAM MEP Wizard – Page 1	11-22
Figure 304	Add SOAM MEP Wizard – Page 2	11-23
Figure 305	Add SOAM MEP Wizard –Summary Page	11-24
Figure 306	SOAM MEP - Edit Page	11-26
Figure 307	SOAM MEP DB Table.....	11-27
Figure 308	MEP Last Invalid CCMS Page	11-28
Figure 309	SOAM MEP Loopback Page	11-30
Figure 310	Restart HTTP Page.....	12-2
Figure 311	ifIndex Calculator Page	12-3
Figure 312	MIB Reference Table Page.....	12-4
Figure 313	PTP 820C Interfaces.....	23-3
Figure 314	PTP 820C DC Port Connector.....	23-5
Figure 315	PTP 820S Interfaces.....	23-9
Figure 316	PTP 820S DC Connector.....	23-11
Figure 317:	PoE Injector Connectors	23-14

List of Tables

Table 1	PTP 820 Web EMS Menu Hierarchy	1-13
Table 2	Cables for Direct CPU Connection.....	2-6
Table 3	PTP 820 Web EMS Menu Hierarchy	2-19
Table 4	Activation Key-Enabled-Features Table Parameters	2-21
Table 5	Time Services Parameters	2-23
Table 6	MRMC Symmetrical Scripts Page Parameters.....	2-35
Table 7	Available Radio Profiles	2-36
Table 8	System Configurations.....	3-2
Table 9	LACP Aggregation Status Parameters	3-33
Table 10	LACP Port Status Parameters	3-35
Table 11	LACP Port Statistics	3-36
Table 12	LACP Port Debug Statistics	3-37
Table 13	SNMP V3 Authentication Parameters	4-10
Table 14	Trap Manager Parameters	4-12
Table 15	Versions Page Columns	4-18
Table 16	Download & Install Status Parameters	4-25
Table 17	Backup Files Page Columns.....	4-28
Table 18	Unit Parameters	4-36
Table 19	NTP Status Parameters	4-38
Table 20	Radio Status Parameters.....	5-4
Table 21	Remote Radio Parameters	5-6
Table 22:	Radio Ethernet Interface Counters Fields	5-15
Table 23	MRMC Status Parameters.....	5-24
Table 24	MRMC PMs.....	5-25
Table 25	Signal Level PMs.....	5-28
Table 26	Signal Level Thresholds.....	5-30
Table 27	Modem BER (Aggregate) PMs.....	5-31
Table 28	Modem MSE PMs	5-32
Table 29	XPI PMs.....	5-35
Table 30	Capacity/Throughput PMs	5-37
Table 31	Utilization PMs	5-39
Table 32	Frame Error Rate PMs	5-42
Table 33	Ethernet Services Page Parameters	6-4
Table 34	General Service Point Attributes	6-9
Table 35	Attached Interface Types	6-11
Table 36	Service Point Ingress Attributes	6-12
Table 37	Service Point Egress Attributes	6-13
Table 38	VLAN Classification Parameters.....	6-19
Table 39	Physical Interface Status Parameters	6-23
Table 40	Ethernet TX Port PMs	6-32
Table 41	Ethernet RX Port PMs.....	6-35

Table 42 Logical Interface Classification Parameters	7-6
Table 43 Policer Profile Parameters.....	7-15
Table 44 ABN Status Parameters.....	8-4
Table 45 ABN Entity Statistics Parameters	8-5
Table 46 LLDP Remote System Management Parameters.....	8-7
Table 47 LLDP Read-Only Configuration Parameters	8-8
Table 48 LLDP Configurable Configuration Parameters	8-9
Table 49 LLDP Port Configuration Status Parameters	8-12
Table 50 LLDP Management TLV Parameters	8-14
Table 51 LLDP Remote System Management Parameters.....	8-15
Table 52 LLDP Remote System Table Parameters	8-16
Table 53 LLDP Local System Parameters.....	8-17
Table 54 LLDP Local System Port Parameters	8-20
Table 55 LLDP Local System Management Parameters.....	8-21
Table 56 LLDP Statistics.....	8-22
Table 57 LLDP Port TX Statistics.....	8-24
Table 58 LLDP Port RX Statistics	8-25
Table 59 Sync Source Parameters.....	9-5
Table 60 Alarm Information	11-3
Table 61 Event Log Information.....	11-5
Table 62 Alarm Configuration Page Parameters	11-6
Table 63 SOAM MA/MEG Configuration Parameters	11-18
Table 64 SOAM MA/MEG Status Parameters.....	11-20
Table 65 SOAM MEP Parameters	11-24
Table 66 SOAM MEP DB Table Parameters.....	11-27
Table 67 MIMO Protection Cables.	13-7
Table 68 IP Address (IPv4) CLI Parameters	13-10
Table 69 IP Address (IPv6) CLI Parameters	13-11
Table 70 Local Time Configuration CLI Parameters.....	13-14
Table 71: Daylight Savings Time CLI Parameters	13-15
Table 72 Interface Configuration CLI Parameters	13-16
Table 73 Entering Radio View CLI Parameters	13-18
Table 74 Radio Mute/Unmute CLI Parameters	13-19
Table 75 Radio Transmit (TX) Level CLI Parameters	13-19
Table 76 Radio Transmit (TX) Frequency CLI Parameters.....	13-20
Table 77 MRMC Script CLI Parameters	13-21
Table 78 MRMC Script Assignment to Radio Carrier CLI Parameters.....	13-23
Table 79 System Configurations (CLI).....	14-2
Table 80 LAG Group CLI Parameters.....	14-12
Table 81 LACP Aggregation Status Parameters (CLI)	14-16
Table 82 LACP Port Status Parameters (CLI)	14-17
Table 83 LACP Port Statistics (CLI)	14-19
Table 84 MMI and XPI Levels CLI Parameters	14-35

Table 85 Remote Unit IP Address (IPv4) CLI Parameters	15-3
Table 86 Remote Unit IP Address (IPv6) CLI Parameters	15-4
Table 87 Basic SNMP CLI Parameters	15-5
Table 88 SNMPv3 CLI Parameters	15-6
Table 89 Trap Managers CLI Parameters	15-8
Table 90 Software Download CLI Parameters	15-13
Table 91 Configuration Management CLI Parameters	15-18
Table 92 Configuration Backup and Restore CLI Parameters	15-20
Table 93 Configuration Import and Restore CLI Parameters	15-20
Table 94 Unit Parameters CLI Parameters	15-24
Table 95 NTP CLI Parameters	15-26
Table 96 Remote Radio Mute/Unmute CLI Parameters	16-2
Table 97 Remote Radio TX Level CLI Parameters	16-3
Table 98 Remote Radio ATPC CLI Parameters	16-4
Table 99 Radio ATPC CLI Parameters	16-6
Table 100 Header De-Duplication CLI Parameters	16-9
Table 101 Aggregate PMs (CLI)	16-18
Table 102 Excessive BER CLI Parameters	16-20
Table 103 RSL Thresholds CLI Parameters	16-20
Table 104 TSL Thresholds CLI Parameters	16-21
Table 105 RSL and TSL PMs (CLI)	16-22
Table 106 Signal Level Threshold CLI Parameters	16-23
Table 107 MSE CLI Parameters	16-23
Table 108 MSE PMs (CLI)	16-25
Table 109 XPI Threshold CLI Parameters	16-25
Table 110 XPI PMs (CLI)	16-27
Table 111 ACM PMs (CLI)	16-29
Table 112 Adding Ethernet Service CLI Parameters	17-4
Table 113 Entering Ethernet Service View CLI Parameters	17-5
Table 114 Displaying Ethernet Service Details CLI Parameters	17-6
Table 115 Ethernet Service Operational State CLI Parameters	17-7
Table 116 Ethernet Service CoS Mode CLI Parameters	17-7
Table 117 Ethernet Service EVC CLI Parameters	17-8
Table 118 Deleting Ethernet Service CLI Parameters	17-9
Table 119 Service Points per Service Type	17-10
Table 120 Service Point Types per Interface	17-10
Table 121 Legal Service Point – Interface Type Combinations per Interface – SAP and SNP	17-12
Table 122 Legal Service Point – Interface Type Combinations per Interface – Pipe and MNG	17-13
Table 123 Add Service Point CLI Parameters	17-15
Table 124 Enable/Disable Broadcast Frames CLI Parameters	17-19
Table 125 Service Point CoS Preservation CLI Parameters	17-20
Table 126 Service Point Enable/Disable Flooding CLI Parameters	17-21
Table 127 C-VLAN CoS Preservation Mode CLI Parameters	17-22

Table 128	C-VLAN Preservation CLI Parameters	17-23
Table 129	S-VLAN CoS Preservation CLI Parameters	17-25
Table 130	Service Bundle CLI Parameters	17-26
Table 131	VLAN Bundle to Service Point CLI Parameters	17-27
Table 132	Display Service Point Attributes CLI Parameters	17-27
Table 133	Delete Service Point Attributes CLI Parameters	17-29
Table 134	MAC Address Forwarding Table Maximum Size CLI Parameters	17-30
Table 135	MAC Address Forwarding Table Aging Time CLI Parameters	17-30
Table 136	Adding Static Address to MAC Address Forwarding Table CLI Parameters	17-31
Table 137	Enabling MAC Address Learning CLI Parameters	17-32
Table 138	Configure S-VLAN Ethertype CLI Parameters	17-34
Table 139	Configure MRU CLI Parameters	17-35
Table 140	Entering Interface View CLI Parameters	17-36
Table 141	Interface Media Type CLI Parameters	17-39
Table 142	Interface Speed and Duplex State CLI Parameters	17-39
Table 143	Interface Auto Negotiation State CLI Parameters	17-40
Table 144	Interface IFG CLI Parameters	17-40
Table 145	Interface Preamble CLI Parameters	17-41
Table 146	Interface Description CLI Parameters	17-41
Table 147	Interface Statistics (RMON) CLI Parameters	17-42
Table 148:	Automatic State Propagation to an Ethernet Port CLI Parameters	17-45
Table 149	RMON Statistics CLI Parameters	17-49
Table 150	Port PM Thresholds CLI Parameters	17-50
Table 151	Ethernet Port PMs	17-52
Table 152	VLAN Classification and Override CLI Parameters	18-3
Table 153	802.1p Trust Mode CLI Parameters	18-5
Table 154	C-VLAN 802.1 UP and CFI Bit Classification Table Default Values	18-6
Table 155	C-VLAN 802.1 UP and CFI Bit Classification Table CLI Parameters	18-7
Table 156	S-VLAN 802.1 UP and DEI Bit Classification Table Default Values	18-7
Table 157	S-VLAN 802.1 UP and DEI Bit Classification Table CLI Parameters	18-8
Table 158	Trust Mode for DSCP CLI Parameters	18-10
Table 159	DSCP Classification Table Default Values	18-10
Table 160	Modify DSCP Classification Table CLI Parameters	18-12
Table 161	Trust Mode for MPLS CLI Parameters	18-13
Table 162	MPLS EXP Bit Classification Table Default Values	18-13
Table 163	MPLS EXP Bit Classification Table Modification CLI Parameters	18-14
Table 164	Default CoS CLI Parameters	18-14
Table 165	Rate Meter Profile CLI Parameters	18-17
Table 166	Assigning Rate Meter for Unicast Traffic CLI Parameters	18-20
Table 167	Assigning Rate Meter for Multicast Traffic CLI Parameters	18-21
Table 168	Assigning Rate Meter for Broadcast Traffic CLI Parameters	18-22
Table 169	Assigning Rate Meter per Ethertype CLI Parameters	18-23
Table 170	Assigning Line Compensation Value for Rate Meter CLI Parameters	18-24

Table 171	Displaying Rate Meter Statistics CLI Parameters.....	18-25
Table 172	Marking Mode on Service Point CLI Parameters	18-27
Table 173	Marking Table for C-VLAN UP Bits.....	18-28
Table 174	802.1q CoS and Color to UP and CFI Bit Mapping Table CLI Parameters	18-29
Table 175	802.1ad UP Marking Table (S-VLAN)	18-29
Table 176	802.1ad UP Marking Table (S-VLAN) CLI Parameters	18-30
Table 177	WRED Profile CLI Parameters	18-32
Table 178	Assigning WRED Profile to Queue CLI Parameters	18-34
Table 179	Queue Shaper Profiles CLI Parameters	18-36
Table 180	Attaching Shaper Profile to Queue CLI Parameters	18-37
Table 181	Service Bundle Shaper Profiles CLI Parameters	18-39
Table 182	Attaching Shaper Profile to Service Bundle CLI Parameters	18-40
Table 183	Egress Line Compensation for Shaping CLI Parameters	18-41
Table 184	Interface Priority Profile Example.....	18-43
Table 185	Interface Priority Profile CLI Parameters	18-44
Table 186	Interface Priority Sample Profile Parameters	18-45
Table 187	Attaching Priority Profile to Interface CLI Parameters.....	18-46
Table 188	WFQ Profile Example	18-47
Table 189	WFQ Profile CLI Parameters	18-48
Table 190	WFQ Sample Profile Parameters.....	18-49
Table 191	Attaching WFQ Profile to Interface CLI Parameters.....	18-50
Table 192	Egress Queue Level PMs CLI Parameters.....	18-51
Table 193	Egress Service Bundle Level PMs CLI Parameters	18-53
Table 194	ABN Entity CLI Parameters	19-3
Table 195	General LLDP CLI Parameters.....	19-8
Table 196	LLDP Port CLI Parameters	19-9
Table 197	LLDP Remote Unit CLI Parameters.....	19-14
Table 198	LLDP Remote Management Data Per Port CLI Parameters	19-15
Table 199	SyncE Regenerator CLI Parameters	20-2
Table 200	Sync Source Ethernet CLI Parameters	20-7
Table 201	Sync Source Radio CLI Parameters.....	20-8
Table 202	Outgoing Clock CLI Parameters.....	20-10
Table 203	Synchronization Revertive Timer CLI Parameters	20-14
Table 204	1588 Transparent Clock CLI Parameters	20-18
Table 205	Inactivity Timeout Period CLI Parameters	21-3
Table 206	Blocking Upon Login Failure CLI Parameters	21-4
Table 207	Blocking Unused Accounts CLI Parameters	21-5
Table 208	Password Aging CLI Parameters	21-6
Table 209	Password Strength Enforcement CLI Parameters	21-7
Table 210	Force Password Change on First Time Login CLI Parameters	21-7
Table 211	User Profile CLI Parameters.....	21-10
Table 212	User Profile Access Protocols CLI Parameters	21-11
Table 213	User Accounts CLI Parameters	21-12

Table 214	Activate RADIUS CLI Parameters	21-14
Table 215	Configure RADIUS Server CLI Parameters	21-15
Table 216	CSR Generation and Upload CLI Parameters	21-18
Table 217	Certificate Download and Install CLI Parameters	21-20
Table 218	Security Log CLI Parameters	21-23
Table 219	Configuration Log CLI Parameters	21-25
Table 220	Editing Alarm Text and Severity CLI Parameters	22-4
Table 221	Restoring Alarms to Default CLI Parameters	22-5
Table 222	Uploading Unit Info CLI Parameters	22-8
Table 223	Radio Loopback CLI Parameters.....	22-10
Table 224	Ethernet Loopback CLI Parameters	22-11
Table 225	Maintenance Domain CLI Parameters	22-13
Table 226	SOAM MEG CLI Configuration Parameters.....	22-15
Table 227	MEP CLI Configuration Parameters.....	22-19
Table 228	MEP and Remote MEP Status Parameters (CLI)	22-21
Table 229	Loopback CLI Parameters	22-26
Table 230	CW Mode CLI Parameters	22-28
Table 231:	PTP 820C Eth1/PoE Interface- RJ-45/SFP Pinouts	23-3
Table 232	PTP 820C Eth2 Interface - RJ-45/SFP Pinouts	23-4
Table 233	PTP 820C MIMO Port - RJ-45/SFP pinouts.....	23-4
Table 234	PTP 820C MGT/PROT Interface - RJ-45 Pinouts	23-5
Table 235	PTP 820S Eth1/PoE Interface- RJ-45/SFP Pinouts	23-9
Table 236	PTP 820S Eth2 Interface - RJ-45/SFP Pinouts.....	23-10
Table 237	PTP 820S Eth3/EXP Interface - RJ-45/SFP Pinouts.....	23-10
Table 238	PTP 820S MGT/PROT Interface - RJ-45 Pinouts	23-11
Table 239	PoE Injector PoE Port - RJ-45 Pinouts	23-14
Table 240	PoE Injector RJ-45 Data Port Supporting 10/100/1000Base-T	23-14

About This User Guide

This document explains how to configure and operate a PTP 820C/820S system. This document applies to software version 10.0

The PTP 820 system is a modular system with a wide variety of configuration options. Not all configurations are described in this manual.

This guide covers the following sections of PTP 820C/PTP 820S:

- Introduction
- Web EMS configuration
- CLI Configuration
- Maintenance
- Appendices

This guide contains the following Chapters:

- [Chapter 1: Introduction](#)
- [Chapter 2: Getting Started](#)
- [Chapter 3: Configuration Guide](#)
- [Chapter 4: Unit Management](#)
- [Chapter 5: Radio Configuration](#)
- [Chapter 6: Ethernet Services and Interfaces](#)
- [Chapter 7: Quality of Service \(QoS\)](#)
- [Chapter 8: Ethernet Protocols](#)
- [Chapter 9: Synchronization](#)
- [Chapter 10: Access Management and Security](#)
- [Chapter 11: Alarm Management and Troubleshooting](#)
- [Chapter 12: Web EMS Utilities](#)
- [Chapter 13: Getting Started \(CLI\)](#)
- [Chapter 14: Configuration Guide \(CLI\)](#)
- [Chapter 15: Unit Management \(CLI\)](#)
- [Chapter 16: Radio Configuration \(CLI\)](#)
- [Chapter 17: Ethernet Services and Interfaces \(CLI\)](#)
- [Chapter 18: Quality of Service \(QoS\) \(CLI\)](#)
- [Chapter 19: Ethernet Protocols \(CLI\)](#)
- [Chapter 20: Synchronization \(CLI\)](#)
- [Chapter 21: Access Management and Security \(CLI\)](#)

- [Chapter 22: Alarm Management and Troubleshooting \(CLI\)](#)
- [Chapter 23: Maintenance](#)
- [Chapter 24: Alarms List](#)

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, Global Headquarters 3800 Golf Road, Suite 360 Rolling Meadows, IL 60008 USA

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:

- [System Overview](#)
- [Configuration tips](#)
- [The Web-Based Element Management System](#)
- [Reference Guide to Web EMS Menu Structure](#)

This user manual provides instructions for configuring and operating the following systems:

- [Configuration Tips](#)
- [PTP 820C](#)
- [PTP 820S](#)

Each of these systems can be used with a PoE ([PoE Injector Overview](#)).

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.

System Overview

Configuration Tips

This section describes common issues and how to avoid them.

Ethernet Port configuration

- The Ethernet ports of a PTP 820C and PTP 820S 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.
- For instructions on configuring in-band management on the PTP 820, see [Configuring in-Band Management](#).

Link Aggregation

- If you are configuring LAG with an external switch, the switch must support LAG. For instructions on configuring LAG, see [Configuring Link Aggregation \(LAG\) and LACP](#).

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 820 hardware type with the same part number as the unit from which they were originally saved. For example, a PTP 820C configuration file can only be restored to a PTP 820C with the same part number as the unit from which it was saved.

PTP 820C

PTP 820C represents a new generation of radio technology, capable of high bit rates and longer reach, and suitable for more diverse deployment scenarios. PTP 820C is a dual-core, compact, all-outdoor backhaul Ethernet product that combines radio, baseband, and Carrier Ethernet functionality in a single, durable box for outdoor installations.

PTP 820C offers the convenience of an easy installation procedure, and full compatibility with RFU-C antennas. It is designed for use in network configurations which require high capacity solutions. PTP 820C covers the entire licensed frequency spectrum (6-38 GHz) and offers a wide capacity range, including Header De-Duplication.

PTP 820S

PTP 820S is an all-outdoor solution for backhaul sites. It provides high-performance, internetworking operating system, and supports all common features of the PTP 820 platform in a compact, environmentally friendly architecture.

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 820C or PTP 820S unit. 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.

PTP 820 Assured Platform

Cambium's PTP 820 Assured platform enhances network reliability and security, ensuring that mission-critical networks maintain availability, and protecting the confidentiality and integrity of their users' data.

The PTP 820 Assured platform is compliant with FIPS 140-2, including:

- Compliance with FIPS 140-2 specifications for cryptography module.
- FIPS 140-2 Level 2 physical security.
- AES-256 encryption (FIPS 197) over radio links.

The PTP 820 Assured platform also provides:

- Secured communication and protocols for management interface.
- Centralized user authentication management via RADIUS.
- Advanced identity management and password policy enforcement.
- Security events log.

- Secure product architecture and development.

The following products are included in the PTP 820 Assured platform:

- PTP 820C Assured
- PTP 820S Assured

**Note**

System release 10.0 cannot be used in PTP 820 Assured platforms. For PTP 820 Assured, use system release 8.3.

The Web-Based Element Management System

This section includes:

- [Introduction to the Web EMS](#)
- [Web EMS Page Layout](#)
- [Unit Summary Page](#)
- [Radio Summary Page](#)

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 820 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.


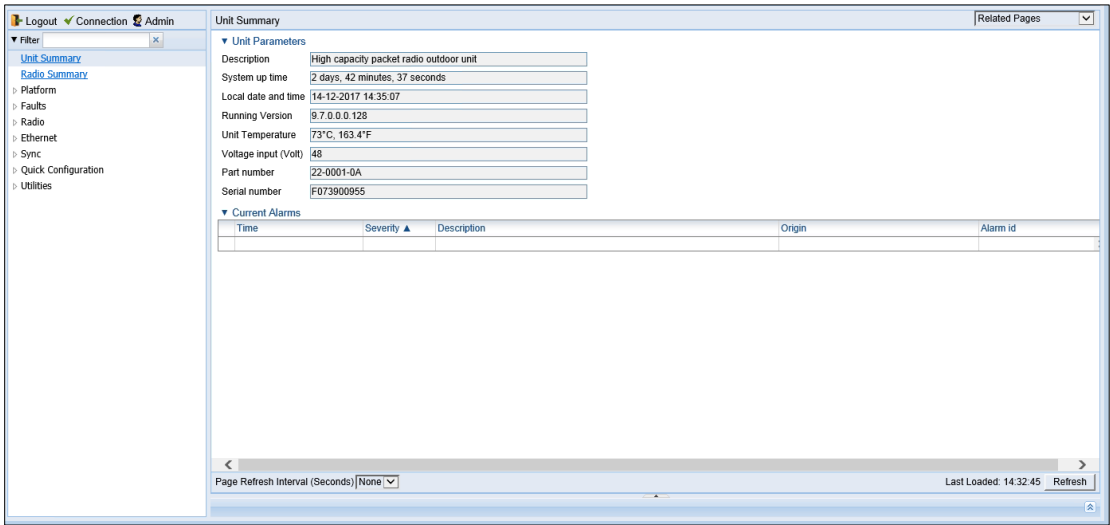
- Click  to hide the sub-options under a menu item.
- The main section of the page provides the page's basic functionality.

Figure 1 Main Web EMS Page



Optionally, you can display a representation of the PTP 820 front panel by clicking either the arrow in the center or the arrow at the right of the bottom toolbar.

Figure 2 Displaying a Representation of the Front Panel

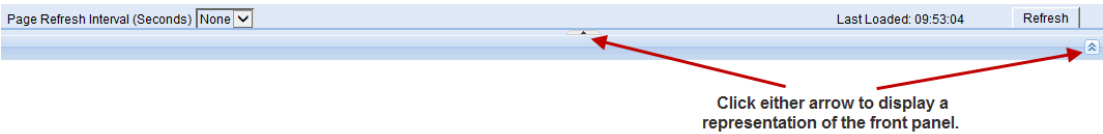
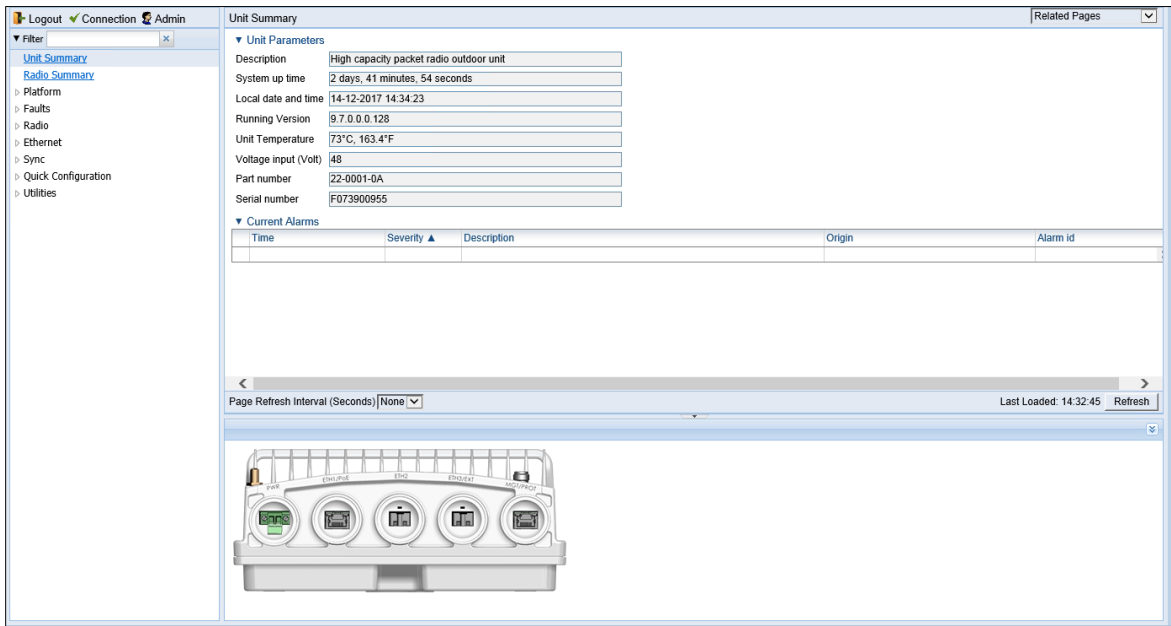


Figure 3 Main Web EMS Page with Representation of Front Panel



Front Panel Representation

Optionally, you can display a representation of the PTP 820 front panel by clicking either the arrow in the center or the arrow at the right of the bottom toolbar.

Figure 4 Displaying a Representation of the Front Panel

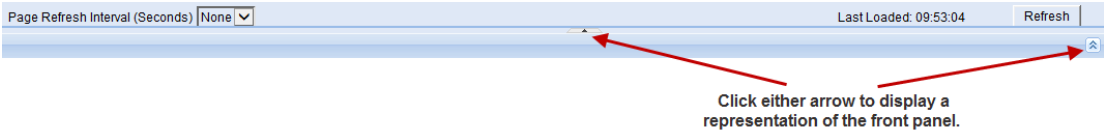
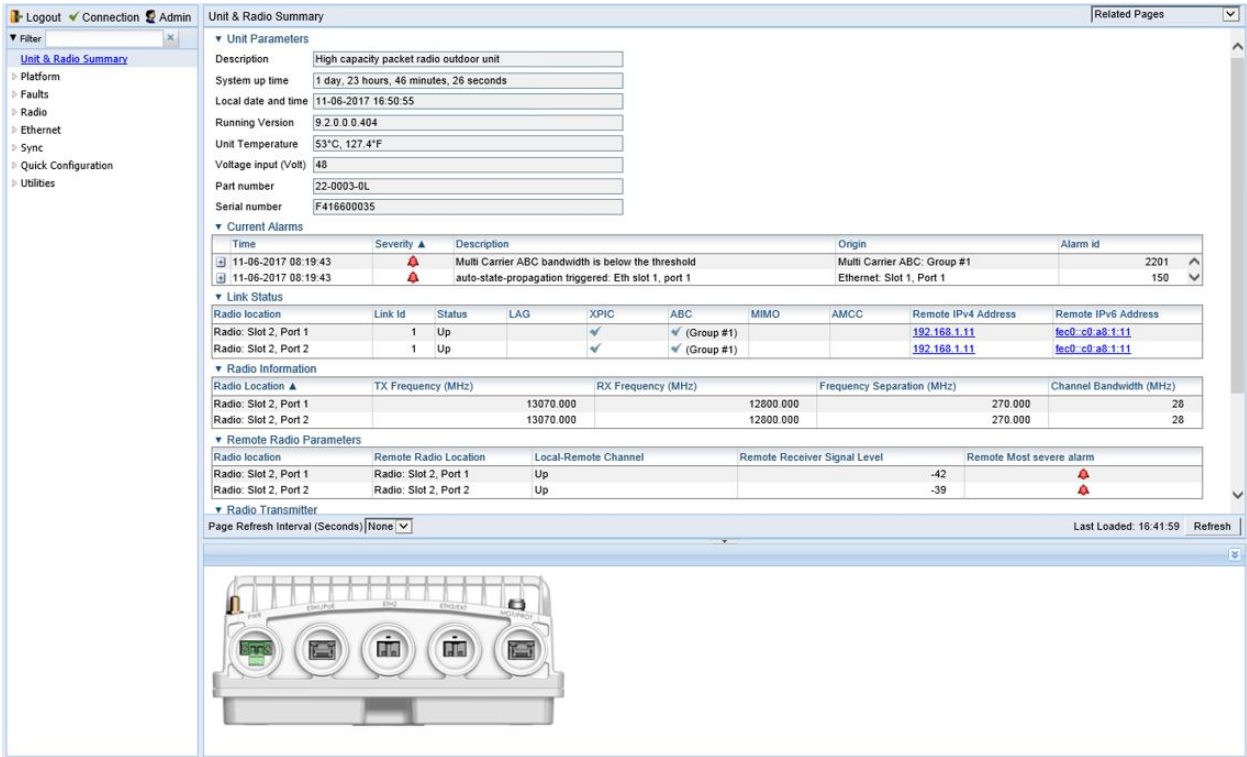


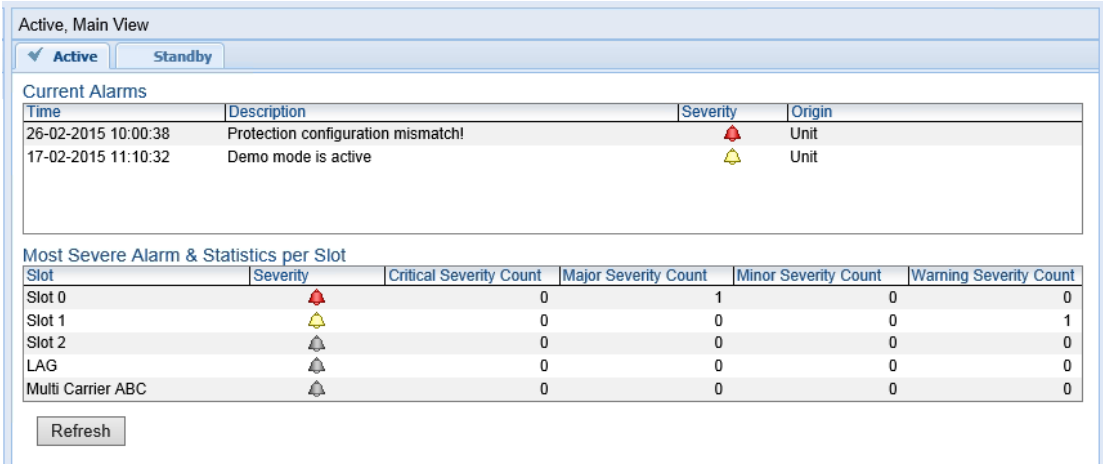
Figure 5 Main Web EMS Page with Representation of Front Panel – PTP 820C and PTP820S



Active and Standby Tabs

When HSB radio 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 TCC. For details on configuring HSB radio protection, see [Configuring Unit Protection with HSB Radio Protection \(External Protection\)](#).

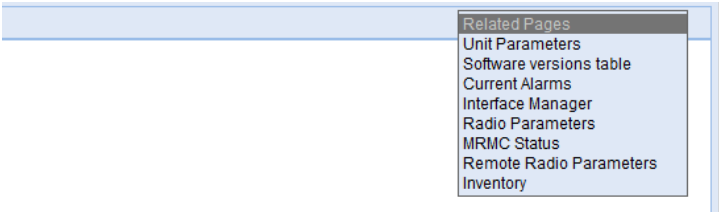
Figure 6 Main Web EMS Page with Active and Standby Tabs



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 7 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 8 Unit Summary Page

Unit Summary																																												
<div> <div>Logout</div> <div>Connection</div> <div>Admin</div> </div>																																												
<div>Filter</div> <div>Unit Summary</div> <div>Radio Summary</div> <div>Platform</div> <div>Faults</div> <div>Radio</div> <div>Ethernet</div> <div>Sync</div> <div>Quick Configuration</div> <div>Utilities</div>	<div>Unit Parameters</div> <div> <div>Description</div> <div>High capacity packet radio outdoor unit</div> </div> <div> <div>System up time</div> <div>15 hours, 9 minutes, 24 seconds</div> </div> <div> <div>Local date and time</div> <div>29-11-2017 05:26:43</div> </div> <div> <div>Running Version</div> <div>9.7.0.0.0.68</div> </div> <div> <div>Unit Temperature</div> <div>46°C, 114.8°F</div> </div> <div> <div>Voltage input (Volt)</div> <div>56</div> </div> <div> <div>Part number</div> <div>27-0001-0A</div> </div> <div> <div>Serial number</div> <div>F123456789</div> </div>																																											
<div>Current Alarms</div> <table border="1"> <thead> <tr> <th>Time</th> <th>Severity</th> <th>Description</th> <th>Origin</th> <th>Alarm id</th> </tr> </thead> <tbody> <tr> <td>28-11-2017 14:19:10</td> <td>▲</td> <td>Radio loss of frame</td> <td>Radio: Slot 2, Port 1</td> <td>603</td> </tr> <tr> <td>28-11-2017 14:19:20</td> <td>▲</td> <td>Loss of Carrier</td> <td>Ethernet: Slot 1, Port 3</td> <td>401</td> </tr> <tr> <td>28-11-2017 14:19:20</td> <td>▲</td> <td>Loss of Carrier</td> <td>Ethernet: Slot 1, Port 2</td> <td>401</td> </tr> <tr> <td>28-11-2017 14:19:20</td> <td>▲</td> <td>Loss of Carrier</td> <td>Ethernet: Slot 1, Port 1</td> <td>401</td> </tr> <tr> <td>28-11-2017 14:19:10</td> <td>▲</td> <td>RFU TX level out of range</td> <td>Radio: Slot 2, Port 1</td> <td>1727</td> </tr> <tr> <td>28-11-2017 14:19:09</td> <td>▲</td> <td>RFU TX Mute</td> <td>Radio: Slot 2, Port 1</td> <td>1735</td> </tr> <tr> <td>28-11-2017 14:17:52</td> <td>▲</td> <td>Demo mode is active</td> <td>Slot 1</td> <td>901</td> </tr> </tbody> </table>					Time	Severity	Description	Origin	Alarm id	28-11-2017 14:19:10	▲	Radio loss of frame	Radio: Slot 2, Port 1	603	28-11-2017 14:19:20	▲	Loss of Carrier	Ethernet: Slot 1, Port 3	401	28-11-2017 14:19:20	▲	Loss of Carrier	Ethernet: Slot 1, Port 2	401	28-11-2017 14:19:20	▲	Loss of Carrier	Ethernet: Slot 1, Port 1	401	28-11-2017 14:19:10	▲	RFU TX level out of range	Radio: Slot 2, Port 1	1727	28-11-2017 14:19:09	▲	RFU TX Mute	Radio: Slot 2, Port 1	1735	28-11-2017 14:17:52	▲	Demo mode is active	Slot 1	901
Time	Severity	Description	Origin	Alarm id																																								
28-11-2017 14:19:10	▲	Radio loss of frame	Radio: Slot 2, Port 1	603																																								
28-11-2017 14:19:20	▲	Loss of Carrier	Ethernet: Slot 1, Port 3	401																																								
28-11-2017 14:19:20	▲	Loss of Carrier	Ethernet: Slot 1, Port 2	401																																								
28-11-2017 14:19:20	▲	Loss of Carrier	Ethernet: Slot 1, Port 1	401																																								
28-11-2017 14:19:10	▲	RFU TX level out of range	Radio: Slot 2, Port 1	1727																																								
28-11-2017 14:19:09	▲	RFU TX Mute	Radio: Slot 2, Port 1	1735																																								
28-11-2017 14:17:52	▲	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 9 Unit Summary Page – Customizing Columns

▼ Radio Information	
<input checked="" type="checkbox"/> All columns	RX Frequency (MHz)
<input checked="" type="checkbox"/> Radio Location	12800.000
<input checked="" type="checkbox"/> TX Frequency (MHz)	12800.000
<input checked="" type="checkbox"/> RX Frequency (MHz)	Local-Remote Channel
<input checked="" type="checkbox"/> Frequency Separation (MHz)	Up
<input checked="" type="checkbox"/> Channel Bandwidth (MHz)	Up
	Maximum TX Level (dBm)

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 10 Radio Summary Page

Logout

Connection

Admin

Filter

Unit Summary

Radio Summary

Platform

Faults

Radio

Ethernet

Sync

Quick Configuration

Utilities

Radio Summary

Related Pages

▼ Link Status

Radio location	Link Id	Status	LAG	XPIC	ABC	MIMO	AMCC	Remote IPv4 Address	Remote IPv6 Address
Radio: Slot 2, Port 1	1	Up			✓ (Unit, Group #1)			192.168.1.31	fec0::c0:a8:1:1
Radio: Slot 2, Port 2		Up			✓ (Unit, Group #1)			192.168.1.31	fec0::c0:a8:1:1

▼ Radio Information

Radio Location ▲	TX Frequency (MHz)	RX Frequency (MHz)	Frequency Separation (MHz)	Channel Bandwidth (MHz)
Radio: Slot 2, Port 1		15200.000	14750.000	450.000
Radio: Slot 2, Port 2		15280.000	14850.000	430.000

▼ 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		
Radio: Slot 2, Port 2	Radio: Slot 2, Port 2	Up	-51	
			-47	

▼ 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	0 ✓		20	15	512
Radio: Slot 2, Port 2	0 ✓		20	15	512

▼ 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 0	-38.75	0	-49	512	200.968
Radio: Slot 2, Port 2	Clear 0	-39.87	0	-48	512	200.968

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 [Configuring the Radio Parameters](#).
- **Radio Information** – The TX and RX frequencies, frequency separation, and channel bandwidth on which the link is operating. For additional information, see [Configuring the Radio Parameters](#).
- **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 [Configuring the Radio Parameters](#).
- **Radio Receiver** – Receiver PMs and statistics, including defective blocks, modem MSE, and RX level, modulation, and bit rate. For additional information, see [Configuring the Radio Parameters](#) and [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 11 Radio Summary Page- Customizing Columns

▼ Radio Information	
<input checked="" type="checkbox"/> All columns	RX Frequency (MHz)
	12800.000
<input checked="" type="checkbox"/> Radio Location	12800.000
<input checked="" type="checkbox"/> TX Frequency (MHz)	
<input checked="" type="checkbox"/> RX Frequency (MHz)	Local-Remote Channel
<input checked="" type="checkbox"/> Frequency Separation (MHz)	Up
<input checked="" type="checkbox"/> Channel Bandwidth (MHz)	Up
	Maximum TX Level (dBm)

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 PTP 820 Web EMS Menu Hierarchy

Root Menu Item	Sub-Menus	For Further Information
Platform	Management > Unit Parameters	Configuring Unit Parameters
	Management > NTP Configuration	Configuring NTP
	Management > Time Services	Setting the Time and Date (Optional)
	Management > Interface Manager	Enabling the Interfaces (Interface Manager)
	Management > Inventory	Displaying Unit Inventory
	Management > Unit Info	Uploading Unit Info
	Management > Reset	Performing a Hard (Cold) Reset
	Management > Set to Factory Default	Setting the Unit to the Factory Default Configuration
	Management > Unit Redundancy	Configuring Unit Protection with HSB Radio
	Management > Networking > Local	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	Configuration SNMP
	Management > SNMP > Trap Managers	Configuring Trap Managers
	Management > SNMP > V3 Users	Configuration SNMP
	Software > Timer Parameters	Configuring a Timed Installation
	Software > Versions	Viewing Current Software Versions
	Software > Download & Install	Downloading and Installing Software

Root Menu Item	Sub-Menus	For Further Information
	Configuration > Timer Parameters	Reserved for future use.
	Configuration > Backup Files	Viewing Current Backup Files
	Configuration > Configuration Management	Backing Up and Restoring Configurations
	Activation Key > Activation Key Configuration	Configuring the Activation Key
	Security > General > Configuration	Operating in FIPS mode
	Security > General > Security Log Upload	Uploading the Security Log
	Security > General > Configuration Log Upload	Uploading the Configuration Log
	Security > X.509 Certificate > CSR	Configuring X.509 CSR Certificates and HTTPS
	Security > X.509 Certificate > Download & Install	Configuring X.509 CSR Certificates and HTTPS
	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	Configuring RADIUS
	Security > Access Control > Radius > Radius Users	Viewing RADIUS User Permissions and Connectivity
	Security > Protocols Control	Configuring the Session Timeout
Faults	Current alarms	Viewing Current Alarms
	Alarm Statistics	Viewing Alarm Statistics

Root Menu Item	Sub-Menus	For Further Information
Radio	Event Log	Viewing the Event Log
	Alarm Configuration	Editing Alarm Text and Severity
	Radio Parameters	Configuring the Radio Parameters
	Remote Radio Parameters	Configuring the Remote Radio Parameters
	Radio Thresholds	Configuring BER Thresholds and displaying current BER
	ATPC	Configuring ATPC
	Payload Encryption	Configuring AES-256 Payload Encryption
	Ethernet Interface > Configuration	Configuring Header De-Duplication and Frame Cut-Through
	Ethernet Interface > Counters	Viewing Header De-Duplication and Frame Cut-Through Counters
	MRMC > Symmetrical Scripts > ETSI	Configuring the Radio (MRMC) Script(s)
	MRMC > Symmetrical Scripts > FCC	Configuring the Radio (MRMC) Script(s)
	MRMC > MRMC > Status	Displaying MRMC Status
	PM & Statistics > Counters	Displaying and Clearing Defective Block Counters
	PM & Statistics > Signal Level	Displaying Signal Level PMs
	PM & Statistics > Diversity	Not relevant for these products
	PM & Statistics > Combined	Not relevant for these products
	PM & Statistics > Aggregate	Displaying Modem BER (Aggregate) PMs
	PM & Statistics > MSE	Displaying MSE PMs and Configuring MSE PM Thresholds
	PM & Statistics > XPI	Displaying XPI PMs and Configuring XPI PM Threshold
	PM & Statistics > MRMC	Displaying MRMC PMs
	PM & Statistics > Traffic > Capacity/Throughput	Displaying Capacity and Throughput PMs
	PM & Statistics > Traffic > Utilization	Displaying Utilization PMs
	PM & Statistics > Traffic > Frame error rate	Displaying Frame Error Rate PMs
	Diagnostics > Loopback	Performing Radio Loopback

Root Menu Item	Sub-Menus	For Further Information
Ethernet	Groups > XPIC	Configuring XPIC
	Groups > Multi Radio	Configuring Multi-Carrier ABC
	Groups > MIMO	Configuring MIMO and Space Diversity Configuring 1+1 HSB with Space Diversity
	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 Service Bundle Shaper Profile to a Service Bundle 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
	Interfaces > Groups > LAG	Configuring Link Aggregation (LAG) and LACP
	PM & Statistics > RMON	RMON Statistics
	PM & Statistics > Egress CoS Statistics	Egress CoS Statistics
	PM & Statistics > Port TX	Port TX Statistics
	PM & Statistics > Port RX	Port RX Statistics
	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

Root Menu Item	Sub-Menus	For Further Information
	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
	QoS > Shaper > Queue Profiles	Configuring Queue Shaper Profiles
	QoS > Shaper > Service Bundle Profiles	Configuring Service Bundle Shaper Profiles
	QoS > Scheduler > Priority Profiles	Configuring Priority Profiles
	QoS > Scheduler > WFQ Profiles	Configuring WFQ Profiles
	Protocols > Adaptive Bandwidth Notification	Configuring Adaptive Bandwidth Notification (ABN)
	Protocols > LLDP > Remote Management	Displaying Peer Status
	Protocols > LLDP > Advanced > Configuration > Parameters	Configuring the General LLDP Parameters
	Protocols > LLDP > Advanced > Configuration > Port Configuration	Configuring the LLDP Port Parameters
	Protocols > LLDP > Advanced > Configuration > Destination Address	Displaying the Unit's Management Parameters
	Protocols > LLDP > Advanced > Configuration > Management TLV	Displaying the Unit's Management Parameters
	Protocols > LLDP > Advanced > Remote System > Management	Displaying Peer Unit's Management Parameters
	Protocols > LLDP > Advanced > Remote System > Remote Table	Displaying Peer Unit's Management Parameters
	Protocols > LLDP > Advanced > Local System > Parameters	Displaying the Local Unit's Parameters
	Protocols > LLDP > Advanced > Local System > Port	Displaying the Local Unit's Parameters
	Protocols > LLDP > Advanced > Local System > Management	Displaying the Local Unit's Parameters

Root Menu Item	Sub-Menus	For Further Information
	Protocols > LLDP > Advanced > Statistic > General	Displaying LLDP Statistics
	Protocols > LLDP > Advanced > Statistic > Port TX	Displaying LLDP Statistics
	Protocols > LLDP > Advanced > Statistic > Port RX	Displaying LLDP Statistics
	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)
Sync	SyncE Regenerator	Configuring the SyncE Regenerator
	Sync Source	Configuring the Sync Source
	Outgoing Clock	Configuring the Outgoing Clock and SSM Messages
	1588 > General Configuration	Configuring 1588 Transparent Clock
	1588 > Transparent Clock	Not relevant for these products
	1588 > Boundary Clock > Clock Parameters > Default	Not relevant for these products
	1588 > Boundary Clock > Clock Parameters > Advanced	Not relevant for these products
	1588 > Boundary Clock > Port Parameters	Not relevant for these products
	1588 > Boundary Clock > Port Statistics	Not relevant for these products
Quick Configuration	From File	Error! Reference source not found.
	Platform Setup	Performing Quick Platform Setup
	Link Setup (PIPE) > 1+0	Configuring a 1+0 Link Using the Quick Configuration Wizard
	Link Setup (PIPE) > 1+0 (Repeater)	Configuring a 1+0 (Repeater) Link Using the Quick Configuration Wizard

Root Menu Item	Sub-Menus	For Further Information
	Link Setup (PIPE) > Multi Carrier ABC > 2 + 0	Configuring a 2+0 Multi-Carrier ABC Link Using the Quick Configuration Wizard
Utilities	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](#)
- [Error! Reference source not found.](#)
- [Performing Quick Platform Setup](#)
- [Mate Management Access \(IP Forwarding\)](#)
- [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 Parameters](#)
- [Configuring the Radio \(MRMC\) Script\(s\)](#)
- [Enabling ACM with Adaptive Transmit Power](#)
- [Operating in FIPS Mode](#)
- [Configuring Grouping \(Optional\)](#)
- [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 820 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 820 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 820 unit to a PC by means of a Twisted Pair cable. The cable is connected to the MGT port on the PTP 820 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 820 unit, it is necessary to configure an IP address on the PC within the same subnet as the PTP 820 unit. The default PTP 820 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 820 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 12 Internet Protocol Properties Window

The screenshot shows the 'Internet Protocol (TCP/IP) Properties' window with the 'General' tab selected. The window title bar includes a question mark icon and a close button. The main text area contains instructions: '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.'

There are two radio button options for IP address assignment:

- ☐ Obtain an IP address automatically
- ☒ Use the following IP address:

Below the second option, there are three input fields:

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

There are two radio button options for DNS server address assignment:

- ☐ Obtain DNS server address automatically
- ☒ Use the following DNS server addresses:

Below the second option, there are two input fields:

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

At the bottom right of the main area is an 'Advanced...' button. At the very bottom of the window are 'OK' and 'Cancel' buttons.

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 13 Login Page



The screenshot shows a web browser window with a title bar that says "Login". Inside the window, there are two text input fields. The first field is labeled "User Name" and the second is labeled "Password". Below these fields are two buttons: "Apply" and "Clear".

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 2 Cables for Direct CPU Connection

Product	Part Number	Description
PTP 820C and PTP 820S	N000082L062A	PTP 820C MIMO or Prot management ODU spltr

To log in using this cable:

1. 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
2. Connect Channel 2 of the cable to the MGT port on the PTP 820

3. Connect the single end of the cable to the LAN port on the PC. Verify that the MGT port LED is orange. (When a connection is established using Channel 1 of the cable, the LED on the MGT port is green.)
4. The system will prompt you for a user name and password (see [Figure 13](#)).
5. Enter the default user name and password:
 - User Name: admin
 - Password: admin
6. Click Apply.
7. 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 14 Change User Password Page

The screenshot shows the 'Change User Password' page. On the left, a navigation tree is visible with the following structure: Platform (Management, Software, Configuration, Activation Key, Security (General, X.509 Certificate, Access Control (General, User Profiles, User Accounts, Password Management, Change Password), Radius, Protocols Control), Faults, Radio, Ethernet, Sync). The 'Change Password' link under 'Access Control' is highlighted. The main content area has a title bar 'Change User Password' and a section 'Change your password' containing four input fields: 'User name' (pre-filled with 'admin'), 'Old password', 'New password', and 'Reenter password'. Below these fields are 'Apply' and 'Clear' buttons.

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.

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 820 unit.

To use the Platform Setup page:

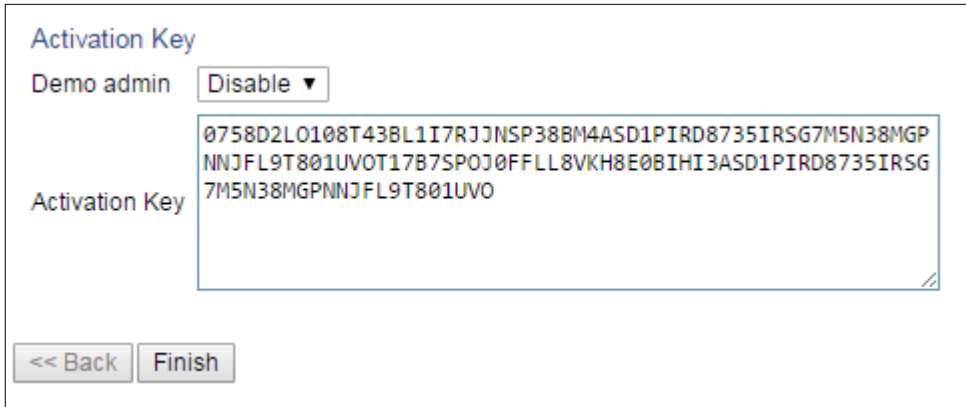
1. Select **Quick Configuration > Platform Setup**. The Quick Configuration – Platform Setup page opens.

Figure 15 Quick Configuration – Platform Setup Page

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

5. In the Activation Key section, you can enable or disable Demo mode in the **Demo admin** field. Demo mode enables all features for 60 days. When demo mode expires, the most recent valid activation key goes into effect. The 60-day period is only counted when the system is powered up. 10 days before demo mode expires, an alarm is raised indicating that demo mode is about to expire.

If you set **Demo admin** to **Disable**, the Activation Key field is displayed. Enter a valid activation key in this field. For a full explanation of activation keys, see [Configuring the Activation Key](#).



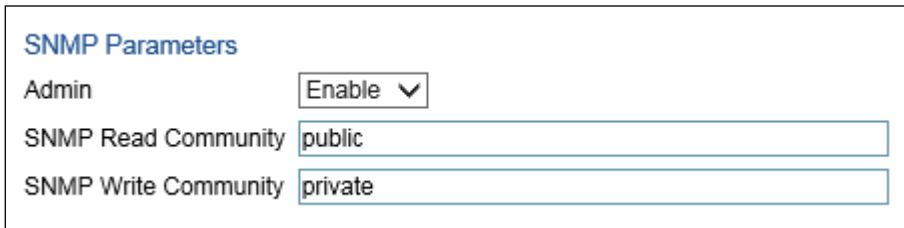
Activation Key

Demo admin **Disable ▼**

Activation Key
0758D2L0108T43BL1I7RJJNSP38BM4ASD1PIRD8735IRSG7M5N38MGP
NNJFL9T801UVOT17B7SPOJ0FFLL8VKH8E0BIHI3ASD1PIRD8735IRSG
7M5N38MGPNNJFL9T801UVO

<< Back Finish

6. 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. For a full explanation of SNMP parameters, see [Configuring SNMP](#).



SNMP Parameters

Admin **Enable ▼**

SNMP Read Community public

SNMP Write Community private

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

Figure 16 Quick Configuration– Platform Setup Summary Page

Logout ✓ Connection Admin

▼ Filter

[Unit & Radio Summary](#)

- ▶ Platform
- ▶ Faults
- ▶ Radio
- ▶ Ethernet
- ▶ Sync
- ▶ Quick Configuration
 - [From File](#)
 - [Platform Setup](#)
- ▶ PIPE
- ▶ Utilities

IP-20N #1: Quick Configuration - Platform

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

<< Back Next >> Submit

Mate Management Access (IP Forwarding)

Mate Management Access enables the use of in-band management for nodes that use two PTP 820C units (4x4 MIMO, 2+2 XPIC, and 4+0 Multi-Carrier ABC), where traffic comes from an external switch operating in LAG mode. When Mate Management Access is enabled, the two units exchange incoming management packets, ensuring that all management data is received by both units.

Mate Management Access must be configured via the CLI. For instructions, see [Mate Management Access \(IP Forwarding\) \(CLI\)](#) on page 13-7.

Configuring In-Band Management

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

To use in-band management for nodes that utilize two PTP 820C units (4x4 MIMO, 2x2 XPIC, and 4+0 Multi-Carrier ABC), you must first configure [Mate Management Access \(IP Forwarding\)](#). For instructions, see on page [2-14](#).

Each PTP 820C unit includes a pre-defined management service with Service ID 257. The management service is a multipoint service that connects the two local management ports and the network element host CPU in a single service. In order to enable in-band management, you must add at least one service point to the management service, in the direction of the remote site or sites from which you want to access the unit for management.

**Note**

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

For instructions on adding service points, see [Configuring Service Points](#).

Changing the Management IP Address

Related Topics:

- [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.

Figure 17 Local Networking Configuration Page

Logout Admin Connection

Filter

Main View

- Platform
 - Management
 - Unit Parameters
 - NTP Configuration
 - Time Services
 - Interface Manager
 - Inventory
 - Unit Info
 - Reset
 - Set to Factory Default
 - Unit Redundancy
 - Networking
 - Local**
 - Remote
 - SNMP
 - Software
 - Configuration
 - Activation Key
 - Security
 - Faults
 - Radio
 - Ethernet
 - Sync

Local Networking Configuration

IP Family Configuration

IP address Family IPv6

Apply

Description	local-management-port
IP address	192.168.1.37
Subnet mask	255.255.255.0
Default gateway	192.168.1.1
IPv6 Address	fe80::c0a8:126
IPv6 Prefix-Length	64 (1..128)
Default Gateway IPv6	::

Apply Refresh

2. Optionally, in the Description field, enter descriptive information about the unit.
3. In the IP 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.
4. In the Subnet mask field, enter the subnet mask.
5. Optionally, in the Default gateway field, enter the default gateway address.

6. 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 IP Address field. The unit will receive communications whether they are sent to its IPv4 address or its IPv6 address.
7. If you entered an IPv6 address, enter the IPv6 prefix length in the IPv6 Prefix-Length field.
8. Optionally, if you entered an IPv6 address, enter the default gateway in IPv6 format in the Default Gateway IPv6 field.
9. Click Apply.

Configuring the Activation Key

This section includes:

- [Activation Key Overview](#)
- [Viewing the Activation Key Status Parameters](#)
- [Entering the Activation Key](#)
- [Activating a Demo Activation Key](#)

Activation Key Overview

PTP 820 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 820 units are delivered with a default activation key that enables you to manage and configure the unit. Additional feature and capacity support requires you to enter an activation key cipher in the Activation Key Configuration page. Contact your vendor to obtain your activation key cipher.



Note

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

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

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

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. 10 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

To display the current activation key status parameters:

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

Figure 18 Activation Key Configuration Page

The screenshot shows the 'Activation Key Configuration' page. On the left is a navigation tree with 'Platform' expanded, showing 'Management', 'Software', 'Configuration', 'Activation Key', 'Security', 'Faults', 'Radio', 'Ethernet', and 'Sync'. 'Activation Key' is expanded, showing 'Activation Key Configuration' and 'Activation Key Overview'. The main content area has a title bar 'Activation Key Configuration'. Below it are three sections: 'Activation Key - Status Parameters' with fields for Type (Demo), Validation number (0x0), Date code (NA), Violation runtime counter (hours) (48), and Sanction state (No); 'Activation Key - Configuration Parameters' with an empty 'Activation Key' field; and 'Demo Mode Configuration' with 'Demo admin' (Enable) and 'Demo timer (hours)' (1225). At the bottom are 'Apply' and 'Refresh' buttons.

Table 3 PTP 820 Web EMS Menu Hierarchy

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

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 18](#)).
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 a demo activation key:

1. Select **Platform > Activation Key > Activation Key Configuration**. The Activation Key Configuration page opens ([Figure 19](#)).
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.

Displaying a List of Activation-Key-Enabled Features

To display the status of activation key coverage for features and capacities in the PTP 820:

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

Figure 19 Activation Key Overview Page

Feature ID	Feature name	Feature description	Activation key-enabled feature usage	Activation key-enabled feature credit	Activation key violation status
10	Per Usage	Post paid model for the activation key	Disable	0	OK
100	Services Mode	Service mode: Smart-Pipe, Edge-CET-Node, Agg-Lvl-1-CET-Node, Agg-Lvl-2-CET-Node	Not used	0	OK
200	Number of Services	Number of allowed Ethernet services	0	0	OK
300	H-QoS	Hierarchical QoS (Quality of Service)	Not used	0	OK
500	Network Resiliency	Network resiliency protocols (Smart-TDM Path Protection, G.8032)	Not used	0	OK
600	Ethernet OAM - Fault Management	Ethernet OAM (Operation Administration and Maintenance) protocols - CFM (802.1ag), EFM (802.3ah)	Not used	0	OK
650	Ethernet OAM - Performance Monitoring	Ethernet OAM (Operation Administration and Maintenance) Performance Monitoring (PM) - Y.1731	Not used	0	OK
1100	Sync Unit	ITU-T G.8262 SyncE and ITU-T G.8264 ESMC (Ethernet Synchronization Message Control)	Not used	0	Violated
1202	IEEE1588 Transparent Clock	Synchronization over Packet	Not used	0	Violated
1300	IEEE1588 Ordinary Clock (quantity)	The allowed number of IEEE1588v2 (PTP - Precision Time Protocol) Ordinary Clocks (OC)	Not used	0	OK
1400	IEEE1588 Boundary Clock (quantity)	The allowed number of IEEE1588v2 (PTP - Precision Time Protocol) Boundary Clocks (BC)	Not used	0	OK
1600	Main card redundancy	Redundancy of the main card	Not used	0	OK
1700	TDM Pseudowire	TDM Pseudowire support	Not used	0	OK
1800	Frame cut-through	Frame cut-through capability	Not used	0	Violated
2100	Secured Management	Secured protocols: SSH, SFTP, HTTPS, RADIUS, SNMPv3	Not used	0	OK
2200	FE traffic ports (quantity)	The allowed number of FE (Fast Ethernet) ports	0	0	OK

The Activation Key Overview page displays the activation-key-enabled features and capacities for the PTP 820, 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 4 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.

Setting the Time and Date (Optional)

Related Topics:

- [Configuring NTP](#)

PTP 820 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 820 unit holds the UTC offset and daylight savings time information for the location of the unit. Each management unit presenting the information uses its own UTC offset to present the information in the correct time.



Note

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

To display and configure the UTC parameters:

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

Figure 20 Time Services Page

Logout Admin Connection

Filter

Main View

- Platform
 - Management
 - Unit Parameters
 - NTP Configuration
 - Time Services**
 - Interface Manager
 - Inventory
 - Unit Info
 - Reset
 - Set to Factory Default
 - Unit Redundancy
 - Networking
 - SNMP
 - Software
 - Configuration
 - Activation Key
 - Security
 - Faults
 - Radio
 - Ethernet
 - Sync
 - Quick Configuration
 - Utilities

Time Services

Date & Time Configuration

UTC date and time

Local date and time

Offset from GMT

UTC offset hours

UTC offset minutes

Daylight Saving Start Time

Month

Day

Daylight Saving End Time

Month

Day

DST offset (hours)

Apply Refresh

2. Configure the fields listed in [Table 5](#).
3. Click Apply.

Table 5 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.

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

PTP 820S units have a single radio interface.

To enable or disable interfaces:

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

Figure 21 Interface Manager Page

Interface location	MAC address	Admin status	Operational Status
<input type="checkbox"/> Ethernet: Slot 1, Port 1	00:0A:25:32:62:27	Up	Up
<input type="checkbox"/> Ethernet: Slot 1, Port 2	00:0A:25:32:62:28	Down	Down
<input type="checkbox"/> Radio: Slot 2, Port 1	00:0A:25:32:62:2A	Up	Up
<input type="checkbox"/> Radio: Slot 2, Port 2	00:00:00:00:00:00	Up	Up
<input type="checkbox"/> Management: Slot 1, Port 1	00:0A:25:32:62:24	Up	Up
<input type="checkbox"/> Multi Carrier ABC (Unit, Group #1)	00:0A:25:32:62:45	Up	Up

Multiple Selection Operation
Admin status: Up ▼ Apply

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 22 Interface Manager – Edit Page

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

To enable or disable multiple interfaces:

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

Figure 23 Multiple Selection Operation Section (Interface Manager Page)

3. Click Apply.

**Note**

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

Configuring the Radio Parameters

In order to establish a radio link, you must:

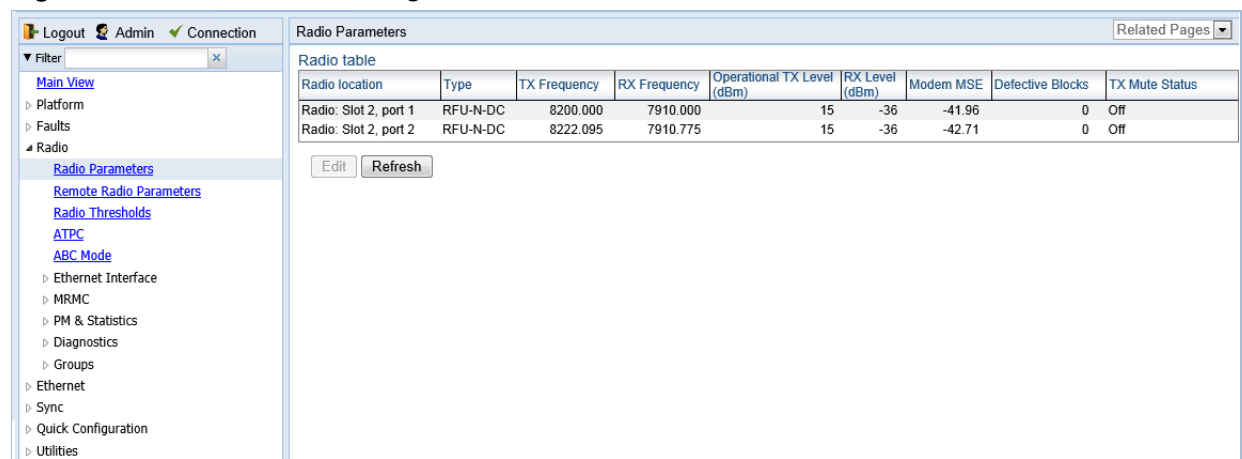
- Unmute the radio carrier.
- Configure the radio frequencies.
- Configure the TX level.

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.
 - For PTP 820C units, the Radio Parameters page initially displays a table as shown in [Figure 24](#).
 - For PTP 820S units, a page appears, similar to [Figure 25](#) (which shows a PTP 820C page).

Figure 24 Radio Parameters Page PTP 820C



2. For PTP 820C units, select the carrier in the Radio table (see [Figure 24](#)) and click Edit. A separate Radio Parameters page opens. The page is essentially identical to the PTP 820C and PTP 820S page, except for the addition of a Radio location parameter.

Figure 25 Radio Parameters Page Per Carrier – PTP 820C

Radio Parameters

Status Parameters

Radio Location	Radio: Slot 2, Port 1
Type	RFU-N-DC
XPIC support	Yes
Radio Interface operational status	Up
Operational TX Level (dBm)	10
RX Level (dBm)	-39
Modem MSE (dB)	-42.40
Modem XPI (dB)	30.80
Defective Blocks	0
TX Mute Status	Off
Adaptive TX power operational status	Down

Frequency control (Local)

TX Frequency (MHz)	13070.000	(13002.000 ... 13141.000)
RX Frequency (MHz)	12800.000	(12747.000 ... 12866.000)
Frequency Separation (MHz)	270.000	

☐ Set also remote unit

Configuration Parameters

TX Level (dBm)	10	(2 ... 18)
TX mute	Off	▼
RSL Connector Source	PHY1	▼
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: 08:25:15 **Refresh** **Close**

3. Set the radio frequency in the Frequency control (Local) section:
 - i. In the TX Frequency (MHz) field, set the transmission radio frequency in MHz.
 - ii. In the RX Frequency (MHz) field, set the received radio frequency in MHz.
 - iii. Click Apply. The system automatically calculates and displays the frequency separation in the TX to RX frequency separation (MHz) field, based on the configured TX and RX frequencies.

- iv. Optionally, select Set also remote unit to apply the frequency settings to the remote unit as well as the local unit.
4. Set the other radio parameters in the Configuration parameters section:
 - i. In the TX Level (dBm) field, enter the desired TX signal level (TSL). The range of values depends on the frequency and RFU type.
 - ii. To mute the TX output of the RFU, select On in the TX Mute field. To unmute the TX output of the RFU, select Off.
 - 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. If Link ID Mismatch Security is enabled, traffic is also blocked on the link. See [Enabling Link ID Mismatch Security](#).
 - iv. In the **RSL degradation alarm admin** 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.
 - v. In the Adaptive TX power admin field, select Enable if you wish the PTP 820 to automatically adjust power levels on the fly in order to optimize the available capacity at every modulation point. See [Enabling ACM with Adaptive Transmit Power](#).

**Note**

The RSL Connector Source field is used in dual-carrier systems to switch between one carrier and the other when measuring RSL at the BNC connector.

For a description of the read-only parameters in the Status parameters section, see [Viewing the Radio Status and Settings](#).

Enabling Link ID Mismatch Security

You can configure the unit to block all Ethernet traffic over the radio link in the event of a Link ID mismatch by enabling Link ID Mismatch Security. When Link ID Mismatch Security is enabled and a Link ID mismatch occurs:

- All Ethernet traffic over the link is blocked.
- The operational status of the radio is set to Down.
- Automatic State Propagation is triggered.

- You cannot change the Link ID of the remote radio, but the local-remote channel remains open for other remote configurations.
- In-band management is lost. Once the mismatch is cleared, in-band management is automatically restored.

Link ID Mismatch Security must be enabled and disabled via CLI.

To enable Link ID Mismatch Security, enter the following command in root view:

```
root> platform security link-id mismatch security set admin enable
```

To disable Link ID Mismatch Security, enter the following command in root view:

```
root> platform security link-id mismatch security set admin disable
```

To display the current Link ID Mismatch Security setting, enter the following command in root view:

```
root> platform security link-id mismatch security show admin
```

By default, Link ID Mismatch Security is disabled.

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

PTP 820S units do not support XPIC or MIMO. For detailed information on the exact scripts and profiles available per unit type, channel, and configuration, refer to the Release Notes for the System Release version you are using.

Figure 26 MRMC Symmetrical Scripts Page (ETSI)

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

Select Radio interface: Slot 2 (Radio: Slot 2, port 1)

▼ MRMC script attribute table (Symmetrical ETSI Scripts)

Script ID	Channel Bandwidth	Occupied Bandwidth	Modulation Scheme	Multi-Carrier	Adjacent Channel	Latency Level	Supported QAM	Bit Rate (Mbps)
1501	80.000	74.100	Adaptive	XPIC	ACCP	Normal	4 .. 2048	114.326 .. 672.601
1502	56.000	53.000	Adaptive	XPIC	ACCP	Normal	4 .. 2048	82.864 .. 489.311
1503	56.000	53.000	Adaptive	Single-Carrier	ACCP	Normal	4 .. 2048	82.864 .. 503.904
✓ 1504	28.000	26.500	Adaptive	XPIC	ACCP	Normal	4 .. 2048	40.978 .. 243.123
1505	28.000	28.000	Adaptive	XPIC	ACAP	Normal	4 .. 2048	43.389 .. 261.357
1506	56.000	55.700	Adaptive	XPIC	ACAP	Normal	4 .. 2048	87.122 .. 529.505
1507	40.000	37.400	Adaptive	XPIC	ACCP	Normal	4 .. 2048	58.224 .. 349.341
1508	7.000	6.500	Adaptive	XPIC	ACCP	Normal	4 .. 2048	9.547 .. 55.151
1509	14.000	13.300	Adaptive	XPIC	ACCP	Normal	4 .. 2048	20.386 .. 116.462
1523	3.500	3.267	Adaptive	XPIC	ACCP	Normal	4 .. 256	4.582 .. 20.344
1901	28.000	26.000	Adaptive	XPIC+MIMO	ACCP	Normal	4 .. 2048	38.841 .. 240.600
1902	40.000	37.600	Adaptive	XPIC+MIMO	ACCP	Normal	4 .. 2048	54.621 .. 341.803
1903	56.000	53.000	Adaptive	XPIC+MIMO	ACCP	Normal	4 .. 2048	77.434 .. 494.360

Configure script Refresh

Note: ✓ Indicates the current configured script

Figure 27 MRMC Symmetrical Scripts Page (PTP 820C) (ETSI)

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

Radio interface: Slot 2 (Radio: Slot 2, Port 1)

▼ MRMC Symmetrical ETSI Scripts (Symmetrical ETSI Scripts)

Script ID ▲	Channel Bandwidth	TX Occupied Bandwidth	Modulation Scheme	Adjacent Channel	Latency Level	Supported QAM	Bit Rate (Mbps)
4700	125.000	119.800	Adaptive	ACCP	Normal	2 .. 512	89.840 .. 914.264
4701	62.500	60.450	Adaptive	ACCP	Normal	2 .. 1024	42.633 .. 500.430
4702	250.000	239.600	Adaptive	ACCP	Normal	2 .. 256	179.679 .. 1636.975
4704	500.000	478.300	Adaptive	ACCP	Normal	2 .. 64	359.358 .. 2426.277

Configure script

Note: ✓ Indicates the current configured script

Figure 28 MRMC Symmetrical Scripts Page (PTP 820C) (FCC)

2.174 IP-20C: MRMC Symmetrical FCC Scripts (Radio: Slot 2, Port 1)

Radio interface: Slot 2 (Radio: Slot 2, Port 1)

▼ MRMC Symmetrical FCC Scripts (Symmetrical FCC Scripts)

Script ID ▲	Channel bandwidth	TX Occupied Bandwidth	Modulation Scheme	Multi-Carrier	Adjacent Channel	Latency Level	Supported QAM	Bit Rate (Mbps)
1501	80.000	74.100	Adaptive	XPIC	ACCP	Normal	4 .. 2048	114.326 .. 672.601
1505	30.000	28.000	Adaptive	XPIC	ACAP	Normal	4 .. 2048	43.389 .. 261.357
1506	60.000	55.700	Adaptive	XPIC	ACAP	Normal	4 .. 2048	87.122 .. 529.505
1507	40.000	37.400	Adaptive	XPIC	ACCP	Normal	4 .. 2048	58.224 .. 349.341
1510	50.000	47.200	Adaptive	XPIC	ACCP	Normal	4 .. 2048	70.683 .. 445.020
1520	10.000	9.110	Adaptive	XPIC	ACAP	Normal	4 .. 2048	13.535 .. 78.319
1521	20.000	18.570	Adaptive	XPIC	ACAP	Normal	4 .. 2048	28.520 .. 165.740
1523	5.000	3.267	Adaptive	XPIC	ACCP	Normal	4 .. 256	4.582 .. 20.344
1525	25.000	23.400	Adaptive	XPIC	ACAP	Normal	4 .. 2048	36.141 .. 214.092
1901	30.000	26.000	Adaptive	XPIC+MIMO	ACCP	Normal	4 .. 2048	38.841 .. 240.600
1902	40.000	37.600	Adaptive	XPIC+MIMO	ACCP	Normal	4 .. 2048	54.621 .. 341.803
1903	56.000	53.000	Adaptive	XPIC+MIMO	ACCP	Normal	4 .. 2048	77.434 .. 494.360
1904	50.000	46.000	Adaptive	XPIC+MIMO	ACCP	Normal	4 .. 2048	69.124 .. 441.302

Configure script

Note: ✓ Indicates the current configured script

- In the Select Radio Interface field, select the slot for which you want to configure the script.

**Note**

This step is only applicable for PTP 820C units.

- Select the script you want to assign to the radio. The currently-assigned script is marked by a check mark (Script ID 1504 in the image above).
- Click Configure Script. A separate MRMC Symmetrical Scripts page opens similar to the page shown below.

Figure 29 MRMC Symmetrical Scripts Page (Configuration) – PTP 820C

MRMC Symmetrical ETSI Scripts

MRMC script configuration - Script: 1504Interface: Radio: Slot 2, Port 1

Script ID	1504
Channel Bandwidth (MHz)	28
TX Occupied Bandwidth (MHz)	26.5
Modulation Scheme	Adaptive
Multi-Carrier	XPIC
Adjacent Channel	ACCP
Latency Level	Normal
Symmetry	Normal
Standard	ETSI

Script configuration parameters - Interface: Slot 2, Port 1

MRMC Script operational mode: Fixed

MRMC Script profile: Profile 10, 2048 QAM, 243.123 Mbps

Apply

Warning: pressing 'Apply' will automatically reset the radio interface and affect traffic.

Page Refresh Interval (Seconds): None Last Loaded: 14:13:06 Refresh Close

5. 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.

Figure 30 MRMC Symmetrical Scripts Page – Configuration – Adaptive Mode (PTP 820C)

MRMC Symmetrical ETSI Scripts

MRMC script configuration - Script: 1007Interface: Radio: Slot 1, Port 1

Script ID

1007

Channel bandwidth (MHz)

40

TX Occupied Bandwidth (MHz)

37.4

Script Name

mdN_A4040N_123_1007

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 10, 2048 QAM, 349.341 Mbps

MRMC Script minimum profile

Profile 3, 32 QAM, 153.976 Mbps

Apply

Refresh

Close

Note: Current configured script is: 1004.
Radio: Slot 1, Port 1: Pressing 'Apply' will configure Radio interface with script: 1007.

Warning: pressing 'Apply' will automatically reset the radio interface and affect traffic.

Page Refresh Interval (Seconds)

None

Last Loaded: 16:52:19

Refresh

Close

6. Define the script profile or profiles

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

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

Note

Refer to [Configuring the Radio \(MRMC\) Scripts\(s\)](#) for a list of available radio profiles.

7. Click Apply.

Note

Changing the script resets the radio interface and affects traffic.

[Configuring the Radio \(MRMC\) Scripts\(s\)](#) describes the MRMC Symmetrical Scripts page parameters.

phn-3963_008v000

Page 2-34

Table 6 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.
Modulation Script	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.
Multi-Carrier	Indicates the Multi-Carrier status of the script (XPIC, MIMO, or Single-Carrier).
Adjacent Channel	Displays the script's adjacent channel polarization mode.
Latency Level	Indicates whether the script is a normal or low-latency script.
Symmetry	Indicates that the script is symmetrical (Normal). Only symmetrical scripts are supported in the current release.
Standard	Indicates whether the script is compatible with ETSI or FCC (ANSI) standards, or both.
MRMC Script operational mode	<p>The ACM mode: Fixed or Adaptive.</p> <ul style="list-style-type: none"> 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	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.

Radio Profiles



Note
For detailed information on the exact profiles available per unit type, channel, and configuration, refer to the Release Notes for the software version you are using.

Table 7 Available Radio Profiles

Parameter	Definition
Profile 0	QPSK
Profile 1	8 QAM
Profile 2	16 QAM
Profile 3	32 QAM
Profile 4	64 QAM
Profile 5	128 QAM
Profile 6	256 QAM
Profile 7	512 QAM
Profile 8	1024 QAM (Strong FEC)
Profile 9	1024 QAM (Light FEC)
Profile 10	2048 QAM

Enabling ACM with Adaptive Transmit Power

When planning ACM-based radio links, the radio planner attempts to apply the lowest transmit power that will perform satisfactorily at the highest level of modulation. During fade conditions requiring a modulation drop, most radio systems cannot increase transmit power to compensate for the signal degradation, resulting in a deeper reduction in capacity. The PTP 820 is capable of adjusting power on the fly, and optimizing the available capacity at every modulation point.

To enable ACM with adaptive transmit power:

1. Select **Radio > Radio Parameters**. The Radio Parameters page opens.
 - For PTP 820C units, the Radio Parameters page initially displays a table as shown in [Figure 24](#).
 - For PTP 820S units and units, a page appears, similar to [Figure 25](#) (which shows a PTP 820C page).
2. For PTP 820C units, select the carrier in the Radio table (see [Figure 24](#)) and click **Edit**. A separate Radio Parameters page opens. The page is essentially identical to the PTP 820C and PTP 820S page, except for the addition of a **Radio location** parameter.

Figure 31 Radio Parameters Page Per Carrier – PTP 820C

Radio Parameters

Status Parameters

Radio Location: Radio: Slot 2, Port 1

Type: RFU-N-DC

XPIC support: Yes

Radio Interface operational status: Up

Operational TX Level (dBm): 10

RX Level (dBm): -39

Modem MSE (dB): -42.40

Modem XPI (dB): 30.80

Defective Blocks: 0 Clear Counter

TX Mute Status: Off

Adaptive TX power operational status: Down

Frequency control (Local)

TX Frequency (MHz): 13070.000 (13002.000 ... 13141.000)

RX Frequency (MHz): 12800.000 (12747.000 ... 12866.000)

Frequency Separation (MHz): 270.000

☐ Set also remote unit

Configuration Parameters

TX Level (dBm): 10 (2 ... 18)

TX mute: Off ▼

RSL Connector Source: PHY1 ▼

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: 08:25:15 Refresh Close

3. In the Adaptive TX power admin field, select Enable. The AdaptiveTX power operational status field should now indicate Up to indicate that the feature is fully functional.

Operating in FIPS Mode

**Note**

New specific FIPS compliance hardware is required for PTP 820C and PTP 820S.

FIPS 140-2 compliance is only available with the PTP 820 Assured platform.

FIPS validation by NIST can be found from below link:

<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm> (Certificate #2752)

The PTP 820 Assured Platform is supported by System release 8.3. It is not supported by System release 10.0.

PTP 820C and PTP 820S can be configured to be FIPS 140-2-compliant in specific hardware and software configurations, as described in this section.

Requirements for FIPS Compliance

For PTP 820C or PTP 820S node to be FIPS-compliant, the unit must be FIPS-compliant hardware.

**Note**

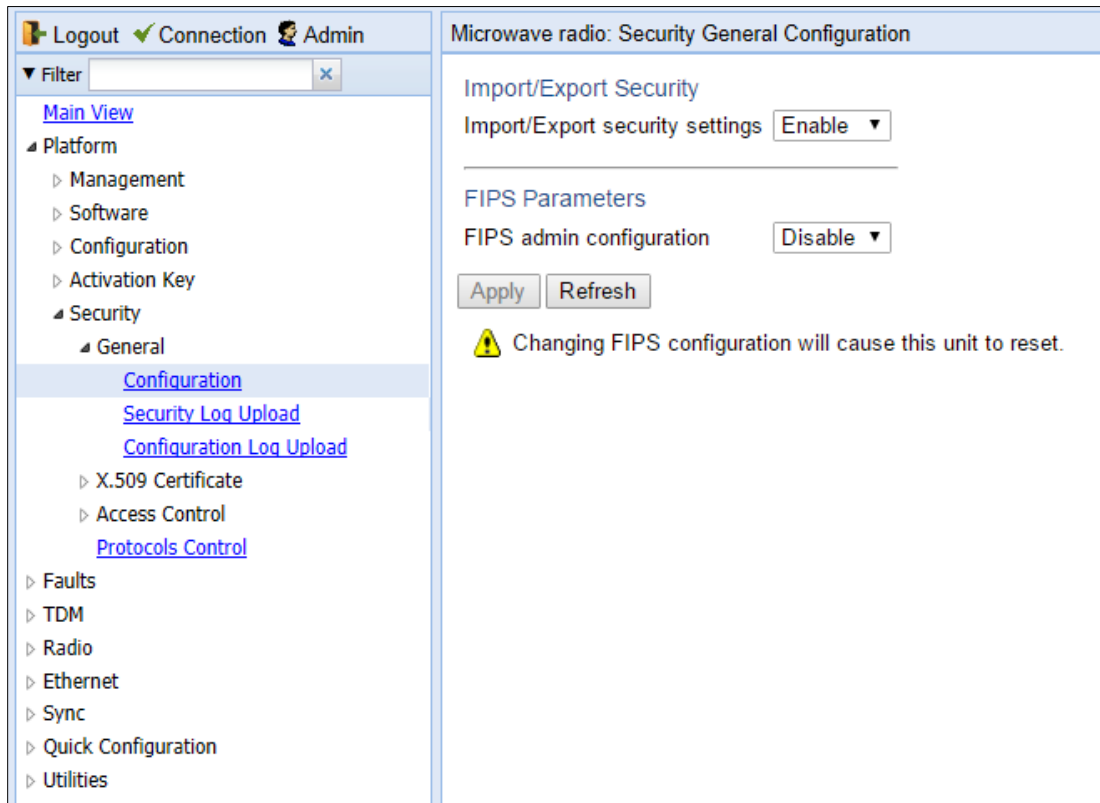
To display the part numbers of the hardware components of your PTP 820 unit, see [Displaying Unit Inventory](#).

Special labels must be affixed to a FIPS-compliant PTP 820C or PTP 820S unit. These labels are tamper-evident and must be applied in such a way that it is not possible to open or tamper with the unit. Tamper-evident labels should be inspected for integrity at least once every six months. For further details, refer to the *PTP 820C Installation Guide* or the *PTP 820S Installation Guide*.

Enabling FIPS Mode

To set the unit to operate in FIPS mode:

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

Figure 32 Security General Configuration Page


Logout ✓ Connection Admin

Filter

Main View

- Platform
 - Management
 - Software
 - Configuration
 - Activation Key
 - Security
 - General
- Configuration
 - Security Log Upload
 - Configuration Log Upload
- X.509 Certificate
- Access Control
- Protocols Control
- Faults
- TDM
- Radio
- Ethernet
- Sync
- Quick Configuration
- Utilities

Microwave radio: Security General Configuration

Import/Export Security

Import/Export security settings **Enable**

FIPS Parameters

FIPS admin configuration **Disable**

Apply Refresh

⚠ Changing FIPS configuration will cause this unit to reset.

- In the **FIPS admin configuration** field, select **Enable**.
- Click **Apply**.

**Note**

Changing the FIPS configuration causes a unit reset.

After enabling FIPS:

- The MD5 option for SNMPv3 is blocked.
- After any system reset, the length of time before users can log back into the system is longer than usual due to FIPS-related self-testing.

Configuring Grouping (Optional)

At this point in the configuration process, you should configure any interface groups that need to be set up according to your network plan. For details on available grouping and other configuration options, as well as configuration instructions, see [System Configurations](#).

Creating Service(s) for Traffic

In order to pass traffic through the PTP 820, you must configure Ethernet traffic services. For configuration instructions, see [Configuring Ethernet Service\(s\)](#).

Chapter 3: Configuration Guide

This section includes:

- [System Configurations](#)
- [Configuring a Link Using the Quick Configuration Wizard](#)
- [Configuring Multi-Carrier ABC](#)
- [Deleting a Multi-Carrier ABC Group](#)
- [Configuring Link Aggregation \(LAG\)](#)[Configuring Link Aggregation \(LAG\) and LACP](#)
- [Configuring XPIC](#)
- [Configuring Unit Protection with HSB Radio](#)
- [Configuring MIMO and Space Diversity](#)
- [Configuring Advanced Frequency Reuse \(AFR\)](#)
- [Operating a PTP 820C in Single Radio Carrier Mode](#)

System Configurations

This section lists the basic system configurations and the PTP 820 product types that support them, as well as links to configuration instructions.

Table 8 System Configurations

Configuration	Supported Products	Link to Configuration Instructions
Multi-Carrier ABC (Multi-Radio)	PTP 820C	Configuring Multi-Carrier ABC
Link Aggregation (LAG)	PTP 820C/S	Configuring Link Aggregation (LAG) and LACP
2+0 XPIC	PTP 820C	Configuring XPIC
HSB Radio Protection	PTP 820C/S	Configuring Unit Protection with HSB Radio
1+1 HSB with Space Diversity	PTP 820C	Configuring 1+1 HSB with Space Diversity
MIMO and Space Diversity	PTP 820C	Configuring MIMO and Space Diversity
AFR 1+0	PTP 820C (hub site or tail site) PTP 820S (tail site only)	Configuring Advanced Frequency Reuse (AFR)
PTP 820C in Single Radio Carrier Mode	PTP 820C	Operating a PTP 820C in Single Radio Carrier Mode

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](#).
- **1+0 Repeater** – Configures a 1+0 radio link that passes traffic between two user-selected radios via a point-to-point pipe service. This type of link is used to configure a node that functions as a repeater, passing traffic between two other nodes. See [Configuring a 1+0 \(Repeater\) Link Using the Quick Configuration Wizard](#).
- **2+0 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*. For a detailed explanation of Multi-Carrier ABC and its requirements, see [Configuring Multi-Carrier ABC](#).

You can also use this wizard to configure XPIC between the radios within the Multi-Carrier ABC group. For a detailed explanation of XPIC and its requirements, see [Configuring XPIC](#).

**Note**

1+0 Repeater links and Multi-Carrier ABC are only available for PTP 820C dual-carrier units.

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 33 1+0 Quick Configuration Wizard – Page 1

- 2 In the **Ethernet Interface** field, select an Ethernet interface or LAG for the link for the link.



Note

To create a LAG, click Create LAG. The Create LAG Group page opens. For instructions on creating LAG groups, see [Configuring Link Aggregation \(LAG\) and LACP](#).

- 3 In the **Radio Interface** field, select a radio interface for the link.
- 4 In the **Pipe Type** field, select the Attached Interface type for the service that will connect the radio and Ethernet interfaces. Options are:
 - o **s-tag** – All VLANs and untagged frames are classified into the service.
 - o **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\(s\)](#).

- 5 Click **Next**. Page 2 of the 1+0 Quick Configuration wizard opens.

Figure 34 1+0 Quick Configuration Wizard – Page 2

Link Setup (PIPE) 1 + 0

Link Setup Progress 30%

Enter the radio interface parameters.

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

TX Frequency (MHz) (0..214748.364)

RX Frequency (MHz) (0..214748.364)

TX Level (dBm)

TX Mute

<< Back Next >> Finish

- 6 In the **TX Frequency (MHz)** field, set the transmission radio frequency in MHz.
- 7 In the **RX Frequency (MHz)** field, set the received radio frequency in MHz.
- 8 In the **TX Level (dBm)** field, enter the desired TX signal level (TSL). The range of values depends on the frequency and RFU type.
- 9 To mute the TX output of the RFU, select **On** in the **TX mute** field. To unmute the TX output of the RFU, select **Off**.
- 10 Click **Next**. Page 3 of the 1+0 Quick Configuration wizard opens.

Figure 35 1+0 Quick Configuration Wizard – Page 3

- 11 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 [Configuring the Radio \(MRMC\) Script\(s\)](#).
- 12 In the **Operational Mode** field, select the ACM mode: **Fixed** or **Adaptive**.
 - Fixed ACM mode applies constant TX and RX rates. However, unlike regular scripts, with a Fixed ACM script you can specify a maximum profile to inhibit inefficient transmission levels.
 - In Adaptive ACM mode, TX and RX rates are dynamic. An ACM-enabled radio system automatically chooses which profile to use according to the channel fading conditions.
- 13 Do one of the following:
 - If you selected **Fixed** in the **Operational Mode** field, the next field is **Profile**. Select the ACM profile for the radio in the **Profile** field.
 - If you selected **Adaptive** in the **Operational Mode** field, the following two fields are displayed:
 - **Maximum Profile:** Enter the maximum profile for the script. See [Configuring the Radio \(MRMC\) Script\(s\)](#).
 - **Minimum Profile:** Enter the minimum profile for the script. See [Configuring the Radio \(MRMC\) Script\(s\)](#).
- 14 Click **Next**. Page 4 of the 1+0 Quick Configuration wizard opens.

Figure 36 1+0 Quick Configuration Wizard – Page 4

Logout Connection Admin

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
- Sync
- Quick Configuration
 - PIPE
 - Single Carrier
 - 1 + 0**
 - 1 + 0 (Repeater)
 - Multi Carrier ABC
 - Utilities

Link Setup (PIPE) 1 + 0

Link Setup Progress 75%

To configure In Band management, choose 'Yes'.
If you choose 'Yes', you will need to select a Management VLAN.

Management Configuration, 1 + 0

In Band Management Yes

Management VLAN 1

☐ In Band includes Ethernet interface

<< Back Next >> Finish

- 15 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.
- 15 If you selected **Yes** in the **In Band Management** field, select the management VLAN in the **Management VLAN** field.
- 16 If you want to use the Ethernet interface as well as the radio interface for in-band management, select **In Band includes Ethernet interface**.
- 17 Click **Finish**. Page 5 of the 1+0 Quick Configuration wizard opens. This page displays the parameters you have selected for the link.

Figure 37 1+0 Quick Configuration Wizard – Page 5 (Summary Page)

- 18 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 1+0 (Repeater) Link Using the Quick Configuration Wizard

To configure a 1+0 repeater (radio-to-radio) link using the Quick Configuration wizard:

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

Figure 38 1+0 Repeater Quick Configuration Wizard – Page 1

- 2 In the **Radio #1 Interface** field, select the first radio interface for the link.
- 3 Click **Next**. Page 2 of the 1+0 Repeater Quick Configuration wizard opens.

Figure 39 1+0 Repeater Quick Configuration Wizard – Page 2

- 4 In the **Radio #2 Interface** field, select the second radio interface for the link.
- 5 In the **Pipe Type** field, select the Attached Interface type for the service that will connect the radios. 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\(s\)](#).

- 6 Click **Next**. Page 3 of the 1+0 Repeater Quick Configuration wizard opens.

Figure 40 1+0 Repeater Quick Configuration Wizard – Page 3

7 For each interface, configure the following parameters:

- I. In the **TX Frequency (MHz)** field, set the transmission radio frequency in MHz.
- II. In the **RX Frequency (MHz)** field, set the received radio frequency in MHz.
- III. In the **TX Level (dBm)** field, enter the desired TX signal level (TSL). The range of values depends on the frequency and RFU type.
- IV. To mute the TX output of the RFU, select **On** in the **TX mute** field. To unmute the TX output of the RFU, select **Off**.

8 Click **Next**. Page 4 of the 1+0 Repeater Quick Configuration wizard opens.

Figure 41 1+0 Repeater Quick Configuration Wizard – Page 4

9 For each interface, configure the following MPMC script parameters:

- I. In the **Script ID** field, select the MPMC script you want to assign to the radio. For a full explanation of choosing an MPMC script, see *Configuring the Radio (MPMC) Script(s)*.

- II. In the **Operational Mode** field, select the ACM mode for the first radio: **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.
 - III. Do one of the following:
 - 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.
 - 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\(s\)](#).
- 10 Click **Next**. Page 5 of the 1+0 Repeater Quick Configuration wizard opens.

Figure 42 1+0 Repeater Quick Configuration Wizard – Page 5

- 11 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.
- 12 If you selected **Yes** in the **In Band Management** field, select the management VLAN in the **Management VLAN** field. Management will be available through both radio interfaces.
- 13 Click **Finish**. Page 6 of the 1+0 Repeater Quick Configuration wizard opens. This page displays the parameters you have selected for the link.

Figure 43 1+0 Repeater Quick Configuration Wizard – Page 6

Link Setup (PIPE) 1 + 0 Repeater

Link Setup Progress 100%

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

Radio #1 Interface: Radio: Slot 2, Port 1
 Radio #1 - TX Frequency: 6400 MHz, RX Frequency: 6150 MHz
 Radio #1 - TX Level (dBm): 5 TX Mute: Off
 Radio #1 - MPMC Script ID: 1505, Operational Mode: Adaptive, Maximum profile: 10, Minimum profile: 0

Radio #2 Interface: Radio: Slot 2, Port 2
 Radio #2 - TX Frequency: 6400 MHz, RX Frequency: 6150 MHz
 Radio #2 - TX Level (dBm): 5 TX Mute: Off
 Radio #2 - MPMC Script ID: 1506, Operational Mode: Adaptive, Maximum profile: 10, Minimum profile: 0

PIPE Type: dot1q
 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.

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

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

To configure a 2+0 Multi-Carrier ABC link using the Quick Configuration wizard:

- 1 Select **Quick Configuration > Link Setup (PIPE) > Multi Carrier ABC > 2+0**. Page 1 of the 2 + 0 Multi Carrier ABC Quick Configuration wizard opens.

Figure 44 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Page 1

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

**Note**

To create a LAG, click **Create LAG**. The **Create LAG Group** page opens. For instructions on creating LAG groups, see [Configuring Link Aggregation \(LAG\) and LACP](#).

- 3 In the **Radio #1 Interface** field, select the first radio interface for the group.

**Note**

The **Number of Radio Interfaces** field is read-only.

- 4 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\(s\)](#).

- 5 Click **Next**. The **Radio #2 Selection** page opens.

Figure 45 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio #2 Selection Page

Link Setup (PIPE) 2 + 0 Multi Carrier ABC

Link Setup Progress 10%

Select the second radio interface.

Radio #2 selection, 2 + 0 ABC

Radio #2 Interface Radio: Slot 2, Port 2

<< Back Next >> Finish

- 6 In the **Radio #2 Interface** field, select the second radio interface for the group.
- 7 Click **Next**. The Radio XPIC Configuration page opens. If you want to set up an XPIC configuration, select the radio pair. For full instructions on configuring XPIC, including antenna alignment instructions, see [Configuring XPIC](#).

Figure 46 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio XPIC Configuration Page

Link Setup (PIPE) 2 + 0 Multi Carrier ABC

Link Setup Progress 25%

Select XPIC groups by checking the desired radio interfaces.

Radio XPIC Configuration

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

<< Back Next >> Finish

- 8 Click **Next**. The Radio Parameters Configuration page opens. You can configure the basic radio parameters for each interface. If you selected XPIC in the Radio XPIC Configuration page, you configure the parameters for the group rather than the individual interfaces.

Figure 47 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio Parameters Configuration Page

Logout Connection Admin

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
- Sync
- Quick Configuration
 - PIPE
 - Single Carrier
 - Multi Carrier ABC
- Utilities

2 + 0

Link Setup (PIPE) 2 + 0 Multi Carrier ABC

Link Setup Progress 30%

Enter the radio parameters for the selected radio interfaces.

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

TX Frequency (MHz) 6400.000 (5850.000..6450.000)

RX Frequency (MHz) 6150.000 (5850.000..6450.000)

TX Level (dBm) 5

TX Mute Off

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

TX Frequency (MHz) 6400.000 (5850.000..6450.000)

RX Frequency (MHz) 6150.000 (5850.000..6450.000)

TX Level (dBm) 5

TX Mute Off

<< Back Next >> Finish

Figure 48 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio Parameters Configuration Page (XPIC)

Logout Connection Admin

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
- Sync
- Quick Configuration
 - PIPE
 - Single Carrier
 - Multi Carrier ABC
- Utilities

2 + 0

Link Setup (PIPE) 2 + 0 Multi Carrier ABC

Link Setup Progress 30%

Enter the radio parameters for the selected radio interfaces.

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

TX Frequency (MHz) 6400.000 (5850.000..6450.000)

RX Frequency (MHz) 6150.000 (5850.000..6450.000)

TX Level (dBm) 5

TX Mute Off

<< Back Next >> Finish

- 9 For each interface or XPIC group, configure the following radio parameters.
 - I. In the **TX Frequency (MHz)** field, set the transmission radio frequency in MHz.
 - II. In the **RX Frequency (MHz)** field, set the received radio frequency in MHz.
 - III. In the **TX Level (dBm)** field, enter the desired TX signal level (TSL). The range of values depends on the frequency and RFU type.
 - IV. To mute the TX output of the RFU, select **On** in the **TX mute** field. To unmute the TX output of the RFU, select **Off**.
- 10 Click **Next**. The Radio MPMC Script Configuration page opens. You can configure the MPMC script parameters for each interface. For an XPIC group, you configure the parameters for the group rather than the individual interfaces.

Figure 49 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio MPMC Script Configuration Page

Logout Connection Admin

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
- Sync
- Quick Configuration
 - PIPE
 - Single Carrier
 - Multi Carrier ABC
 - 2 + 0**
 - Utilities

Link Setup (PIPE) 2 + 0 Multi Carrier ABC

Link Setup Progress 50%

Select an MPMC script and profile for the selected radio interfaces

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

Script ID Script: 1507, XPIC, BW:40 MHz, OBW:37.4 MHz, 58.224-349.341 Mbps, XPIC, ETSI+FCC, ACCP

Operational Mode Adaptive

Maximum profile Profile: 10, 2048 QAM, 349.341 Mbps

Minimum profile Profile: 0, 4 QAM, 58.224 Mbps

Radio #2, Radio MPMC Script Configuration - Radio: Slot 2, Port 2, 2 + 0 ABC

Script ID Script: 1507, XPIC, BW:40 MHz, OBW:37.4 MHz, 58.224-349.341 Mbps, XPIC, ETSI+FCC, ACCP

Operational Mode Adaptive

Maximum profile Profile: 10, 2048 QAM, 349.341 Mbps

Minimum profile Profile: 0, 4 QAM, 58.224 Mbps

<< Back Next >> Finish

Figure 50 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio MPMC Script Configuration Page - XPIC

Logout Connection Admin

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
- Sync
- Quick Configuration
 - PIPE
 - Single Carrier
 - Multi Carrier ABC
 - 2 + 0**
 - Utilities

Link Setup (PIPE) 2 + 0 Multi Carrier ABC

Link Setup Progress 50%

Select an MPMC script and profile for the selected radio interfaces

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

Script ID Script: 1507, XPIC, BW:40 MHz, OBW:37.4 MHz, 58.224-349.341 Mbps, XPIC, ETSI+FCC, ACCP

Operational Mode Adaptive

Maximum profile Profile: 10, 2048 QAM, 349.341 Mbps

Minimum profile Profile: 0, 4 QAM, 58.224 Mbps

<< Back Next >> Finish

- 11 For each interface or XPIC group, configure the following MPMC script parameters:
 - I. In the **Script ID** field, select the MPMC script you want to assign to the radio or XPIC group. For a full explanation of choosing an MPMC script, see Configuring the Radio (MPMC) Script(s).
 - II. In the **Operational Mode** field, select the ACM mode: **Fixed** or **Adaptive**.
 - o 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.
 - o 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.
 - III. Do one of the following:
 - o If you selected **Fixed** in the **Operational Mode** field, the next field is **Profile**. Select the ACM profile in the **Profile** field.
 - o If you selected **Adaptive** in the **Operational Mode** field, the following fields are displayed:

- **Maximum Profile:** Enter the maximum profile for the script. See [Configuring the Radio \(MRMC\) Script\(s\)](#).
- **Maximum Profile:** Enter the maximum profile for the script. See [Configuring the Radio \(MRMC\) Script\(s\)](#).

12 Click **Next**. The Management Configuration page opens.

Figure 51 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Management Configuration Page

- 13 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.
- 14 If you selected **Yes** in the **In Band Management** field, select the management VLAN in the **Management VLAN** field.
- 15 If you want to use the Ethernet interface as well as the radio interface for in-band management, select **In Band includes Ethernet interface**.
- 16 Click **Finish**. The Summary page opens. This page displays the parameters you have selected for the group.

Figure 52 2 + 0 Multi Carrier ABC Quick Configuration Wizard –Summary Page

Logout Connection Admin

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
- Sync
- Quick Configuration
 - PIPE
 - Single Carrier
 - Multi Carrier ABC
- Utilities

2 + 0

Link Setup (PIPE) 2 + 0 Multi Carrier ABC

Link Setup Progress 100%

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

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

TX Frequency: 6400 MHz, RX Frequency: 6150 MHz

TX Level (dBm): 5 TX Mute: Off

MRMC Script ID: 1507, Operational Mode: Adaptive, Maximum profile: 10, Minimum profile: 0

Ethernet Interface: LAG: Group #1

PIPE Type: dot1q

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.

<< Back Next >> Submit

- 17 To complete configuration of the Multi-Carrier ABC group, click Submit. If you want to go back and change any of the parameters, click Back. After you click Submit, the unit is reset.

Configuring Multi-Carrier ABC

**Note**

This option is only relevant for PTP 820C units.

This section includes:

- [Multi-Carrier ABC Overview](#)
- [Configuring a Multi-Carrier ABC Group](#)
- [Configuring the Multi-Carrier ABC Minimum Bandwidth Override Option](#)
- [Adding and Removing Group Members](#)**Error! Reference source not found.**

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 100% utilization of radio resources in which traffic load is balanced based on instantaneous radio capacity per carrier.

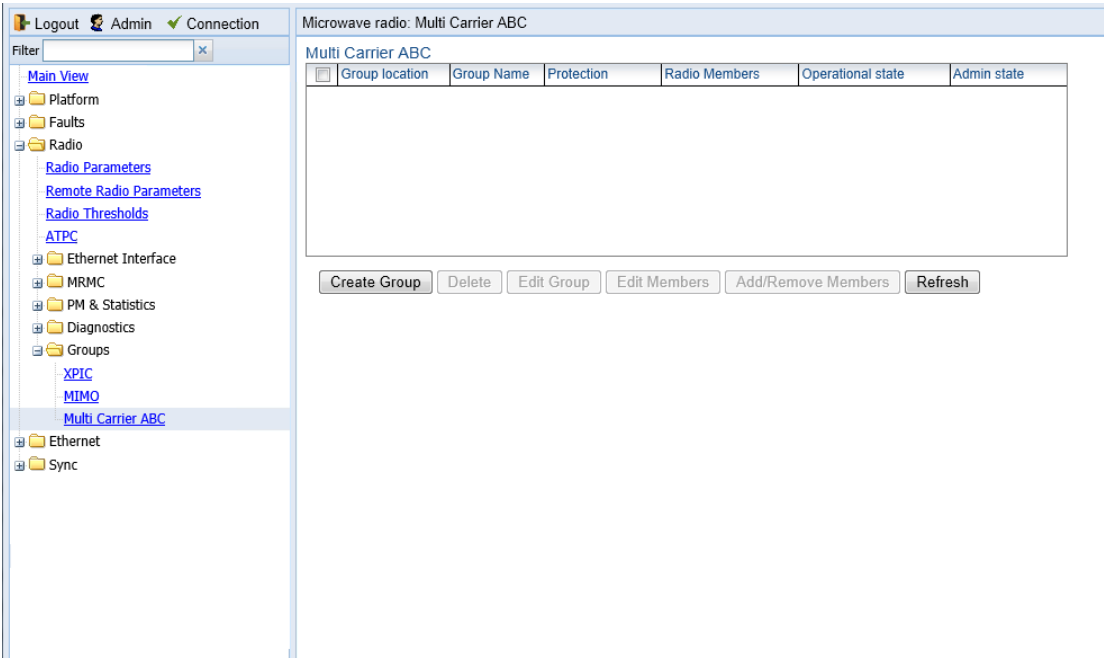
One Multi-Carrier ABC group that includes both radio interfaces can be configured per unit. The MRMC scripts for both radio carriers must be identical.

Configuring a Multi-Carrier ABC Group

To configure a Multi-Carrier ABC group:

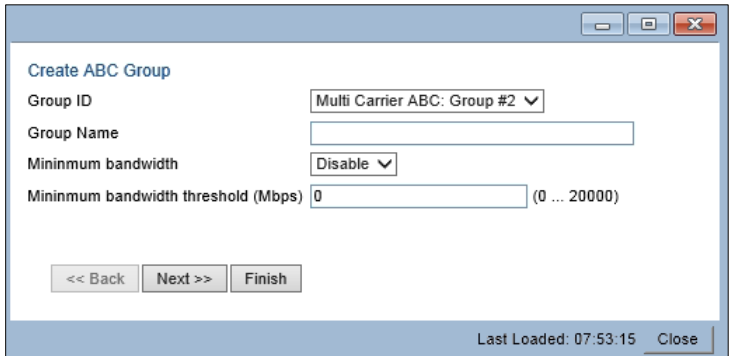
1. Select Radio > Groups > Multi Carrier ABC. The Multi Carrier ABC page opens.

Figure 53 Multi-Carrier ABC Group Page (Empty)



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

Figure 54 Create ABC Group Wizard – First Page



- 3. Optionally, enter a descriptive name for the group in the Group Name field.
- 4. In the **Minimum bandwidth** field, select **Enable** to enable Minimum Bandwidth Override or **Disable** to disable Minimum Bandwidth Override.
- 5. In the **Minimum bandwidth threshold** field, enter the minimum bandwidth override threshold (in Mbps). The threshold can be between 0 – 20000 Mbps, with a resolution of 1 Mbps. If the group’s bandwidth capacity falls beneath this threshold, the group is automatically placed in **Down** state until the bandwidth capacity exceeds this threshold.



Note

For an explanation of Multi-Carrier ABC Minimum Bandwidth Override, see *Configuring the Multi-Carrier ABC Minimum Bandwidth Override Option*.

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

Figure 55 Create ABC Group Wizard – Second Page

- In the Member 1 field, select a radio interface.



Note

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

- Click Next. The next page of the Create Group wizard opens.
- In the Member 2 field, select a radio interface.
- Click Next. A summary page opens.

Figure 56 Create ABC Group Wizard – Finish Page

- Click Submit, A message appears indicating whether or not the operation was successful.
- 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.

Configuring the Multi-Carrier ABC Minimum Bandwidth Override Option

A multi-carrier ABC group can be configured to be placed in **Down** state if the group's capacity falls beneath a user-defined threshold.

By default, the Multi-Carrier ABC minimum bandwidth override option is disabled. When enabled, the Multi-Carrier ABC group is automatically placed in a Down state in the event that the group's aggregated capacity falls beneath the user-configured threshold. The group is returned to an Up state when its aggregated capacity goes above the threshold. An alarm is also raised:

- Alarm ID – 2201
- Alarm Description – Multi Carrier ABC bandwidth is below the threshold

This option is used in conjunction with the LAG group shutdown in case of degradation event option (see [LAG Group Shutdown in Case of Degradation Event](#)) in cases where the operator wants to re-route traffic from an upstream switch connected to an another PTP 820 unit whenever the link is providing less than a certain capacity. To set up a configuration in which a drop in the capacity of the Multi-Carrier ABC group closes the Ethernet port in the upstream PTP 820 unit, you must perform all of the following steps:

- Enable the Multi-Carrier ABC minimum bandwidth option and set a threshold on the PTP 820C unit, as described below.
- Enable an ASP group on the PTP 820C unit, where the Monitored Interface is the Multi-Carrier ABC group and the Controlled Interface is the Ethernet interface that faces the upstream PTP 820 unit. See [Configuring Automatic State Propagation](#).
- Enable the LAG group shutdown in case of degradation event option on the upstream PTP 820 unit.



Note

When using in-band management, management is lost in the event of radio failure and returns when the radio link is restored.

The minimum bandwidth threshold is based on the capacity of the Multi-Carrier ABC group, not the combined capacities of the group's members. The group's aggregated capacity is displayed in the Multi-Carrier ABC Group – Edit Group page ([Figure 57](#)).

You can configure Multi-Carrier ABC Minimum Bandwidth Override when creating the group. See [Configuring a Multi-Carrier ABC Group](#).

To configure Multi-Carrier ABC Minimum Bandwidth Override after the group has been created:

1. Select the group in the Multi-Carrier ABC table and click Edit Group. The Edit Group page opens.

Figure 57 Multi-Carrier ABC Group – Edit Group Page

Multi Carrier ABC configuration table - Edit Group

Group location: Multi Carrier ABC: Group #1

Group Name:

Status Parameters

Operational state: Up

Remote Operational state: Up

Current Aggregated Capacity TX: 484224

Current Aggregated Capacity RX: 484224

Configuration Parameters

Admin state: Enable

Minimum bandwidth: Enable ▾

Minimum bandwidth threshold (Mbps): 350 (0 ... 20000)

Apply

Page Refresh Interval (Seconds): None ▾ Last Loaded: 07:53:22 Refresh Close

2. In the **Minimum bandwidth** field, select **Enable** to enable Minimum Bandwidth Override or **Disable** to disable Minimum Bandwidth Override.
3. In the **Minimum bandwidth threshold** field, enter the minimum bandwidth override threshold (in Mbps). If the group's bandwidth capacity falls beneath this threshold, the group is automatically placed in **Down** state until the bandwidth capacity exceeds this threshold.
4. Click **Apply**.

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 Multi Carrier ABC - Add/Remove Members page opens.

Figure 58 Multi Carrier ABC Group - Add/Remove Members Page

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

**Note**

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

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 ([Figure 53](#)).
2. Select the group in the Multi-Carrier ABC table and click **Add/Remove Members**. The Multi Carrier ABC – Add/Remove Members page opens (Figure 58 Multi Carrier ABC Group - Add/Remove Members Page).
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 Link Aggregation (LAG) and LACP

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 function. PTP 820 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 Link Aggregation \(LAG\) and LACP](#)
- [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 820 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 820 supports LACP, which expands the capabilities of static LAG and provides interoperability with third-party equipment that uses LACP. LACP improves the communication between LAG members. This improves error detection capabilities in situations such as improper LAG configuration or improper cabling. It also enables the LAG to detect uni-directional failure and remove the link from the LAG, preventing packet loss.

LACP is enabled as part of the LAG configuration process. It should only be used if the LAG is in a link with another LACP-enabled LAG.

**Note**

LACP is not supported with unit protection. For unit protection, a special, limited implementation is configured on the logical interface level. See **Error! Reference source not found.**

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 a LAG Group

To create a LAG group:

1. Select Ethernet > Interfaces > Groups > LAG. The LAG page opens.
2. Click Create LAG underneath the Link Aggregation table. The Create LAG Group page opens.

Figure 59 Create LAG Group – Page 1

3. In the Group ID field, select a LAG Group ID. Only LAG IDs that are not already assigned to a LAG group appear in the dropdown list.
4. In the **LACP** field, select **Enable** to enable LACP on the LAG or **Disable** to disable LACP on the LAG. The default value is **Disable**.
5. 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.
6. Click **Next**. A new Create LAG Group page opens.

Figure 60 Create LAG Group – Page 2

7. In the **Member 2** field, select an additional interface to assign to the LAG Group.
8. To add additional interfaces to the LAG group, repeat steps 5 and 6.
9. When you have finished adding interfaces to the LAG group, click **Finish**. A new Create LAG Group page opens displaying all the interfaces you have selected to include in the LAG group.

Figure 61 Create LAG Group – Final Page

LAG

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

<< Back Next >> Submit

Close

10. 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:

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

Figure 62 Link Aggregation - Edit Page

LAG

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 ▼

Apply

Page Refresh Interval (Seconds) None ▼ Last Loaded: 10:13:29 Refresh Close

4. 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 *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.
5. Click **Apply**.
 6. To remove or add additional interfaces, repeat steps 4 and 5.
 7. 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.

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:

1. Select **Ethernet > Interfaces > Groups > LAG** to open the LAG page.
2. Select the LAG group in the Link Aggregation table.
3. Click **Edit** underneath the Link Aggregation table. The Link Aggregation - Edit page opens (Figure 62).
4. In the **LAG degrade** field, select **Enable** to enable the LAG group shutdown in case of degradation event option or **Disable** to disable the LAG group shutdown in case of degradation event option.
5. Click **Apply**.

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:

1. Select **Ethernet > Interfaces > Groups > LAG**. The LAG page opens.
2. Click LAG DF underneath the Link Aggregation table. The LAG Distribution Function (DF) page opens.

Figure 63 Link Aggregation - Edit Page

LAG Distribution Function (DF)

Group Location

Distribution Function

Member #1 (Slot 1, Port 1)

TX byte count

Clear on read

Member #2 (Slot 1, Port 2)

TX byte count

Clear on read

Changing Distribution Function may cause traffic hit

Page Refresh Interval (Seconds) Last Loaded: 11:52:57 Refresh Close

115%

3. 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.
4. 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.

5. Click **Apply** to apply the selected distribution scheme.

Deleting a LAG Group

In order to delete a LAG group, you must first make sure that no service points are attached to the LAG group.

To delete a LAG group:

1. Select **Ethernet > Interfaces > Groups > LAG**. The LAG page opens.
2. Select the LAG group you want to delete in the Link Aggregation table.
3. Click **Delete** underneath the Link Aggregation table. The LAG group is deleted.

To delete multiple LAG groups:

1. Select the LAG groups in the Link Aggregation table or select all the LAG groups by selecting the check box in the top row.
2. 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 820 does not support any LACP write parameters.

Displaying LACP Aggregation Status Parameters

To Display LACP aggregation status parameters:

1. Select **Ethernet > Protocols > LACP > Aggregation** to open the LACP Aggregation page.

Figure 64 LACP Aggregation Page

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

The following table describes the LACP aggregation status parameters.

Table 9 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:

1. Select **Ethernet > Protocols > LACP > Port > Status** to open the LACP Port Status page.

Figure 65 LACP Port Status Page

Logout

Connection

Admin

Filter

Unit Summary

Radio Summary

Platform

Faults

Radio

Ethernet

General Configuration

Services

Interfaces

PM & Statistics

QoS

Protocols

Adaptive Bandwidth Notification

LLDP

SOAM

LACP

Aggregation

Port

Status

Statistics

Debug

Groups

Sync

Quick Configuration

Utilities

LACP Port Status

Related Pages

LACP Port Status

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

View

2. The LACP Port Status page displays the major port status parameters, per port. To display all the available LACP port status parameters, select a port and click View. The LACP Port Status – View page is displayed.

Figure 66 LACP Port Status – View Page

LACP Port Status

LACP Port Status - View

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

Refresh

Close

Table 10 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 via LACPDUs.
Actor Operational Key	The current operational value of the Key for the Aggregation Port.
Actor Operational State	The current operational values of the Actor's state as transmitted by the Actor via LACPDUs.
Partner Operational Key	The current operational value of the Key for the protocol Partner.
Partner Operational State	The current values of Actor State in the most recently received LACPDU transmitted by the protocol Partner.
Partner Operational 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.

Figure 67 LACP Port Statistics Page

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

Table 11 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 Staistics

To Display LACP port debug statistics:

1. Select **Ethernet > Protocols > LACP > Port > Debug** to open the LACP Port Debug page.

Figure 68 LACP Port Debug Page

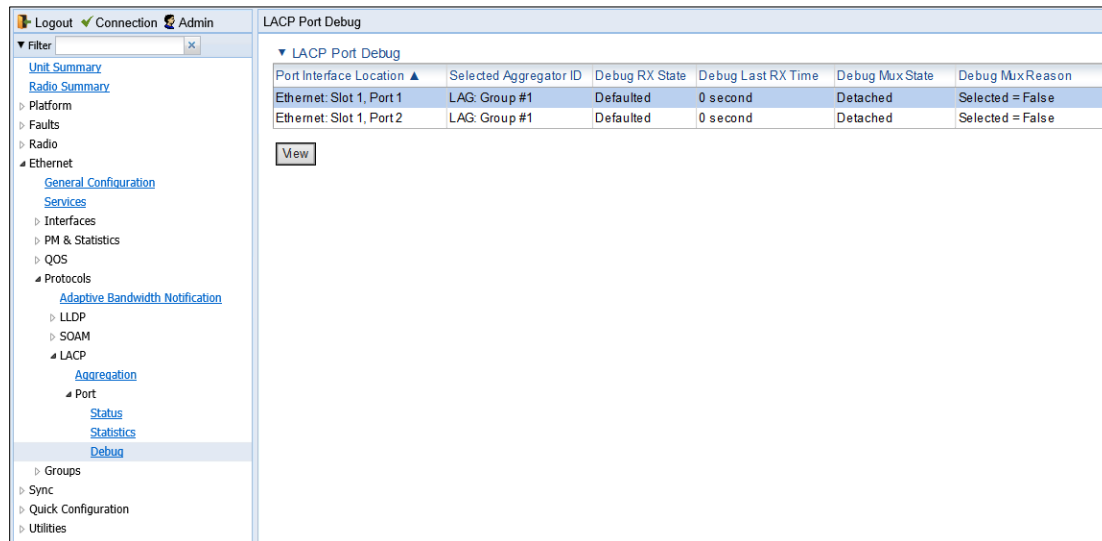


Table 12 LACP Port Debug Statistics

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	<p>The state of the receive state machine for the Aggregation port. Possible values are:</p> <ul style="list-style-type: none"> • 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.

Configuring XPIC

**Note**

This option is only relevant for PTP 820C units.

This section includes:

- [XPIC Overview](#)
- [Configuring the Radio Carriers](#)
- [Creating an XPIC Group](#)
- [Performing Antenna Alignment for XPIC](#)

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.

In addition, XPIC includes an automatic recovery mechanism that ensures that if one carrier fails, or a false signal is received, the mate carrier will not be affected. This mechanism also ensures that both carriers will be operational, after the failure is cleared.

To configure and enable XPIC, first configure the carriers and then perform antenna alignment, as described below.

For 2+2 XPIC using an external switch operating in LAG mode, Mate Management Access enables users to manage both units via in-band management. See [Mate Management Access \(IP Forwarding\) \(CLI\)](#).

Configuring the Radio Carriers

To configure the radio carriers:

1. Configure the carriers on both ends of the link to the desired frequency channel. Both carriers must be configured to the same frequency channel.
2. Assign an XPIC (CCDP operational mode) support-enabled script to the carriers on both ends of the link. Each carrier must be assigned the same script. For details, refer to [Configuring the Radio \(MRMC\) Script\(s\)](#).

**Note**

XPIC support is indicated by an X in the script name. For example, mdN_A2828X_111_1205 is an XPIC-enabled script. mdN_A2828N_130_100 is not an XPIC-enabled script. For a list of XPIC support-enabled scripts, refer to the most recent PTP 820C Release Notes.

3. In the XPIC page, create an XPIC group that consists of the two RMCs that will be in the XPIC group. See [Creating an XPIC Group](#).

Creating an XPIC Group

To create an XPIC group:

1. Select **Radio > Groups > XPIC**. The XPIC page opens.

Figure 69 XPIC Configuration Page

2. In the XPIC Configuration page, select **Enable** in the Admin state field and click **Apply**.
To disable XPIC, select **Disable** in the Admin state field and click **Apply**.

Performing Antenna Alignment for XPIC

1. Align the antennas for the first carrier. For a 2+2 XPIC configuration (or a 4x4 MIMO configuration), align the antennas for the first carrier on the upper PTP 820C units. While you are aligning these antennas, mute the second carrier. See [Configuring the Radio Parameters](#). For a 2+2 XPIC configuration (or a 4x4 MIMO configuration), mute all the carriers except the first carrier on the upper PTP 820C units.
2. Adjust the antenna alignment until you achieve the maximum RSL for the first-carrier link (the "RSLwanted"). This RSL should be no more than +/-2 dB from the expected level. Record the RSL of the first carrier as the "RSLwanted".
 - Measure the RSL of the second carrier and record it as the "RSLunwanted").

**Note**

To measure the second carrier, leave the Voltmeter connected to the BNC connector. In the Radio Parameters page of the Web EMS, change the **RSL Connector Source** field from **PHYS1** to **PHYS2** (or **2** to **1**). The BNC connector will now measure RSL from the other carrier.

3. Determine the XPI, using either of the following two methods:
 - To calculate the XPI, subtract $RSL_{unwanted}$ from the RSL_{wanted} .
 - Read the XPI from the **Modem XPI** field of the Radio Parameters page in the Web EMS. See *Viewing the Radio Status and Settings*.
4. The XPI 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 XPI, 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 XPI.

**Note**

As an extra step, to check the veracity of the initial measurements, you can mute the first carrier and unmute the second carrier on the upper PTP 820C units on both sides of the link. Then measure the RSL of the second carrier link (the " RSL_{wanted} "), measure the RSL of the first carrier (the " $RSL_{unwanted}$ ") and determine the XPI. The XPI should match the XPI with the second carriers muted.

5. 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 ± 2 dB. The RSL of the vertical carrier of the local unit should match the RSL of the horizontal carrier of the remote unit, within ± 2 dB.
6. For a 2x2 configuration, repeat Steps **Error! Reference source not found.** through **Error! Reference source not found.** for the lower PTP 820C units.
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.

Configuring Unit Protection with HSB Radio Protection (External Protection)

This section explains how to configure unit protection, including HSB radio protection and Ethernet interface protection, and includes the following topics:

- [Unit Protection Overview](#)
- [Configuring Ethernet Interface Protection](#)
- [Configuring 2+2 HSB Protection on a PTP 820C Unit](#)
- [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](#)
- [Configuring 1+1 HSB Unit Protection with Space Diversity](#)

**Note**

For instructions on configuring 1+1 unit protection with Space Diversity, see **Error!** *Reference source not found.* on page

Unit Protection Overview

PTP 820C and PTP 820S support 1+1 HSB radio protection. PTP 820C also supports 2+2 HSB radio protection. In HSB radio protection, one PTP 820 operates in active mode and the other operates in standby mode. If a protection switchover occurs, the Active unit goes into standby mode and the Standby unit goes into active mode.

- For a full explanation of 1+1 HSB radio protection and 2+2 HSB radio protection support in PTP 820C, refer to the PTP 820C Technical Description.
- For a full explanation of 1+1 HSB radio protection support in PTP 820S, refer to the PTP 820S Technical Description.

To configure unit protection, you must perform the following steps:

- 1 Configure Ethernet interface protection – See [Configuring Ethernet Interface Protection](#).
- 2 Configure HSB radio protection – See [Configuring HSB Radio Protection](#).
- 3 For 2+2 HSB configurations (PTP 820C only), perform the additional steps described in [Configuring 2+2 HSB Protection on a PTP 820C Unit](#).

Configuring Ethernet Interface Protection

There are two modes for Ethernet interface protection in an HSB radio protection configuration:

- Line Protection Mode – Traffic is routed to the Ethernet ports via two ports on an external switch (only Cisco Switch has been certified).
- Split Protection Mode – Only available for optical Ethernet ports. An optical splitter cable is used to connect to both the active and the standby optical Ethernet ports.

Configuring Line Protection Mode with Cisco Switch

To configure line protection mode:

- 1 Configure the GE ports on the external switch in LACP mode. The external switch must support LACP.

**Note**

PTP 820 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 Connect one port on the external switch to an Ethernet port on the active PTP 820, and the other port on the external switch to an Ethernet port on the standby PTP 820.
- 3 Enable LACP on the Ethernet interface connected to the external switch on the active PTP 820:
 - i Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens .
 - ii Select the interface and click **Edit**. The Logical Interfaces – Edit page opens.

Figure 70 Logical Interfaces – Edit Page

Logical Interfaces - Edit

Interface location: Ethernet: Slot 1, Port 1

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

Buttons: Apply, Refresh, Close

Zoom: 100%

- iii In the **Interface Mode** field, select **LACP**.
- iv Click **Apply**, then **Close**.

Configuring Split Ethernet Interface Protection Mode (CLI)

To configure split Ethernet interface protection mode:

- 1 Use an optical splitter to route traffic to an optical Ethernet port on each PTP 820 unit.
- 2 Proceed to [Configuring HSB Radio Protection](#).

Configuring HSB Radio Protection

You must perform the initial configuration of a 1+1 or 2+2 HSB system using a splitter cable for each unit to provide a management connection to each unit. For instructions on preparing and connecting the splitter cables, refer to the Installation Guide for PTP 820C or PTP 820S.

To configure HSB radio 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](#).

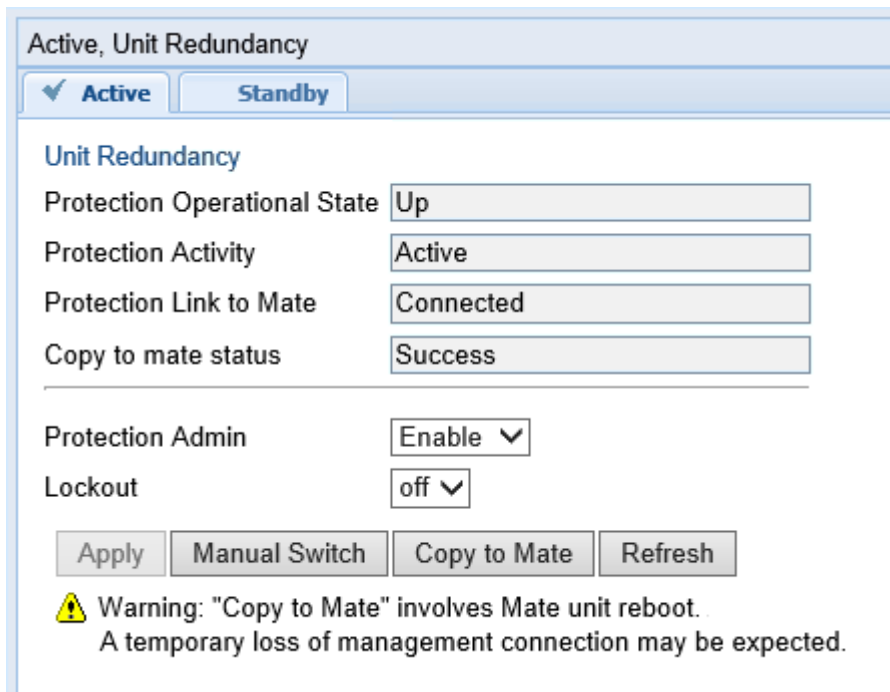
- iii. Establish a management connection to one of the units. You can select either unit; once you enable Protection Administration, the system will determine which unit becomes the Active unit.
2. Select Platform > Management > Unit Redundancy. The Unit Redundancy (HSB Protection) page opens.

Figure 71 Unit Redundancy Page

The screenshot shows the 'Unit Redundancy' configuration page. The left sidebar contains a navigation tree with the following items: Main View, Platform, Management, Unit Parameters, NTP Configuration, Time Services, Interface Manager, Inventory, Unit Info, Reset, Set to Factory Default, Unit Redundancy (selected), Networking, SNMP, Software, Configuration, Activation Key, Security, Faults, Radio, Ethernet, and Sync. The main content area has a title bar 'Unit Redundancy' and the following configuration fields:

Unit Redundancy	
Protection Operational State	Down
Protection Activity	Active
Protection Link to Mate	Connected
Protection Admin	Disable ▼
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>	

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 MIMO/Prot ports on the splitters connecting the two units.
 - HSB protection is enabled on both units.
 - The Unit Redundancy page refreshes to include additional radio protection fields.

Figure 72 Unit Redundancy Page when Redundancy Enabled


In addition, almost every Web EMS page will now include two tabs on top of the main section of the page:

- Active – Enables you to configure the Active unit.
- Standby – In most cases, this tab is read-only and enables you to display Standby unit parameters. Even when a switchover occurs, the unit displayed in the Web EMS is always the currently Active unit.

**Note**

The parameters that are editable on the Standby tab are described in [Editing Standby Unit Settings](#).

5. Once you have enabled Protection:

- i. Perform all necessary radio configurations on the Active unit, such as setting the frequency, assigning MRMC scripts, unmuting the radio, and setting up radio groups such as XPIC or Multi-Carrier ABC (Multi-Radio).
- ii. Perform all necessary Ethernet configurations on the Active unit, such as defining Ethernet services.
- iii. In the Unit Redundancy page, click Copy to Mate to copy the configuration of the Active unit to the Standby unit. Confirm the action in the confirmation window that appears.

**Note**

While the system is performing the copy-to-mate operation, a temporary loss of management connection will occur.

To keep the Standby unit up-to-date, after any change to the configuration of the Active unit click Copy to Mate to copy the configuration to the Standby unit.

If you change the configuration of the Active unit but do not perform Copy to Mate, a Configuration Mismatch alarm appears in the Faults > Current Alarms page.



Note

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

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

Configuring 2+2 HSB Protection on a PTP 820C Unit

In order to configure 2+2 HSB unit protection on a PTP 820C unit, you must simply enable the second radio carrier on both units on both sides of the link. No other configuration is necessary other than the configuration described above.

- To enable the second radio carrier on both units, use the Interface Manager page (see [Figure 21](#)). The following figure shows the Interface Manager page with both radio carriers enabled.

Figure 73 Interface Manager Page – Both Radio Carriers Enabled

<div> <div>Active</div> <div>Standby</div> </div>		
Interface Manager		
<input type="checkbox"/> Interface location	Admin status	Operational Status
<input type="checkbox"/> Ethernet: Slot 1, port 1	Down	Down
<input type="checkbox"/> Ethernet: Slot 1, port 2	Up	Up
<input type="checkbox"/> Radio: Slot 2, port 1	Up	Up
<input type="checkbox"/> Radio: Slot 2, port 2	Up	Up

Edit

Refresh

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 74 Standby Tab of Radio Parameters Page

Radio Parameters

Related Pages

Active

Standby

Radio table

Radio location	Type	TX Frequency	RX Frequency	Operational TX Level (dBm)	RX Level (dBm)	Modem MSE	Defective Blocks	TX Mute Status
Radio: Slot 2, port 1	RFU-N-DC	8200.000	7910.000	15	-36	-41.96	0	Off
Radio: Slot 2, port 2	RFU-N-DC	8222.095	7910.775	15	-36	-42.71	0	Off

Edit

Refresh

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:

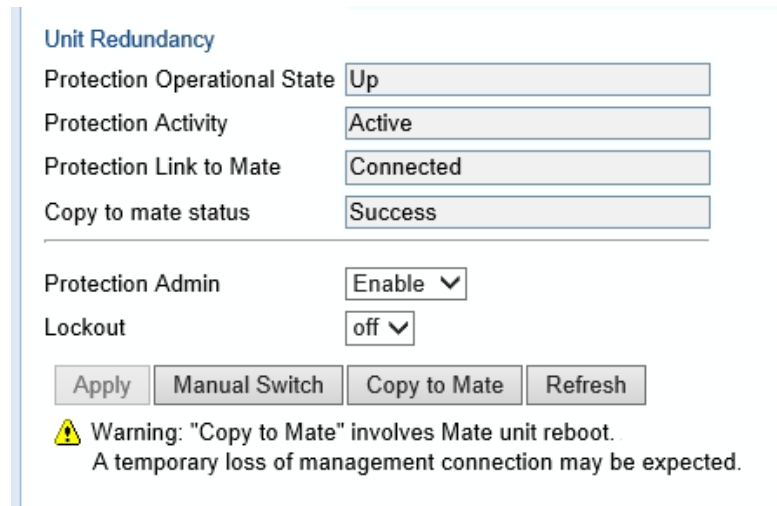
- Setting the Unit Name – in the Name field of the Unit Parameters page (see [Configuring Unit Parameters](#)).
- Disabling/enabling Radio TX-mute – in the TX mute field of the Edit Radio Parameters window. Refer to [Configuring the Radio Parameters](#).
- Clearing the Radio and RMON counters – in the TX mute 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 [Figure 19 Activation Key Overview Page](#) (see [Configuring the Activation Key](#)).
- Defining user accounts – Refer to the [Access Control User Accounts Page](#) (see [Configuring Users](#)).
- Setting synchronization settings – Refer to the [SyncE Regenerator page](#) (see [Configuring the SyncE Regenerator](#)).

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 > Management > Unit Redundancy. The Unit Redundancy (HSB Protection) page opens.

Figure 75 Unit Redundancy Page


Unit Redundancy

Protection Operational State


Protection Activity

Protection Link to Mate

Copy to mate status

Protection Admin

Lockout

 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). Radio protection is not functional if any of the following occurred:
 - MIMO is configured.
 - The management connection to the mate is down.
- **Protection Activity** – The activity state of the device: Active or Standby.
- **Protection Link to Mate** – 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 or disabled.

Manually Switching to the Standby Unit

The following events trigger switchover for HSB radio protection according to their priority, with the highest priority triggers listed first.

- 1 Loss of active unit
- 2 Lockout
- 3 Radio/Ethernet interface failure
- 4 Manual switch

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 (HSB Protection) page opens.
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 > Management > Unit Redundancy**. The Unit Redundancy (HSB Protection) page opens.
2. Select **On** in the **Lockout** field.
3. Click **Apply**.

To re-enable automatic switchover, select **Off** in the **Lockout** field and then click **Apply**.

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 > Management > Unit Redundancy**. The Unit Redundancy (HSB Protection) page opens.
2. Select **Disable** in the **Protection Admin** field.
3. Click **Apply**.

Configuring 1 + 1 HSB with Space Diversity



Note

This feature is only relevant to PTP 820C. It can be used with all PTP 820 hardware versions.

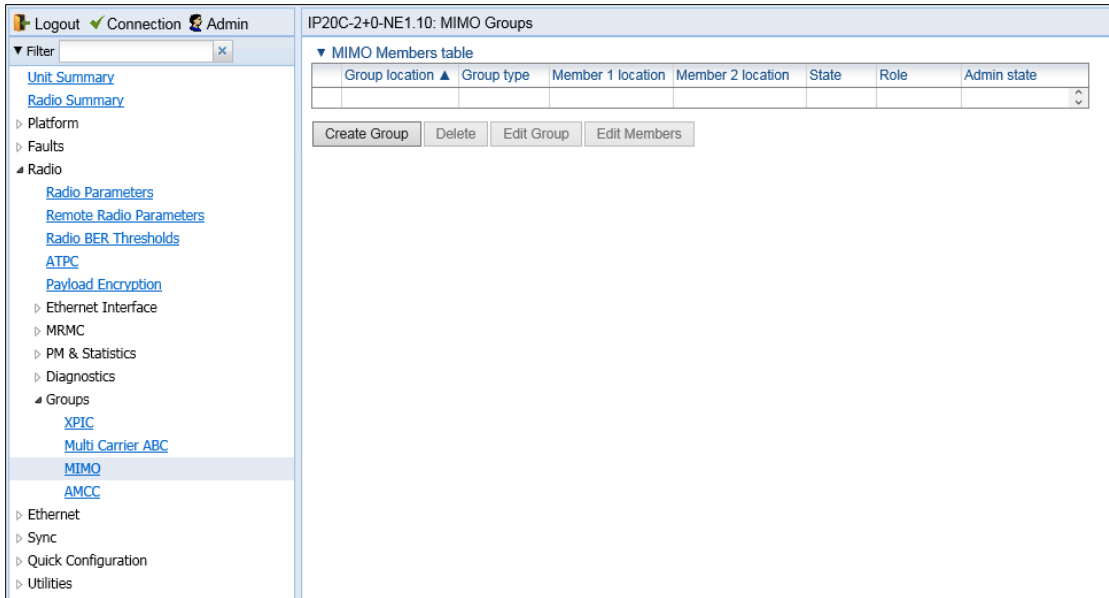
A 1+1 HSB-SD configuration utilizes two PTP 820C units on each side of the link, with both radio carriers activated. The PTP 820C units are combined and connected to the primary and diversity antennas via a dual coupler and two flexible waveguides.

Radio carrier 2 is muted on each unit. On the receiving side, the signals are combined in the active unit to produce a single, optimized signal. The link is protected via external protection, so that if a protection switchover occurs, the standby unit becomes the active unit, and the link continues to function with full space diversity.

To configure a 1+1 HSB link with Space Diversity:

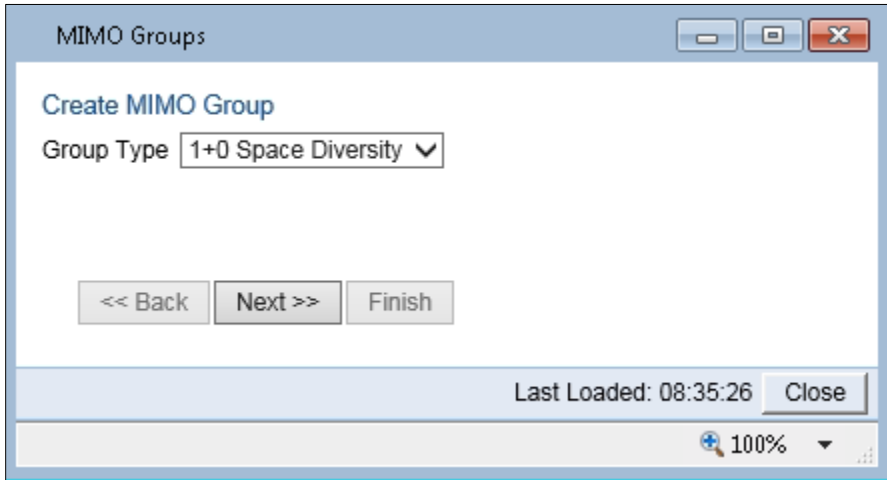
1. For one PTP 820 unit, select **radio > Groups > MIMO**. The MIMO page opens.

Figure 76 MIMO Page.



2. Click **Create Group**. The Create MIMO Group page opens.

Figure 77 Create Space Diversity Group- Page 1.



- 3. In the **Group Type** Field, select **1+0 Space Diversity**.
- 4. Click **Next**. The Selection Summary page opens.

Figure 78 Create Space Diversity Group- Selection Summary

Create MIMO Group (Selection Summary)

Group Type: 1+0 Space Diversity

Group ID: MIMO: Group #1

Member #1: Radio: Slot 2, Port 1

Member #2: Radio: Slot 2, Port 2

<< Back Next >> Submit

Last Loaded: 08:36:07 Close

100%

5. Click **Submit**. The create MIMO Group page is updated and displays your system configuration.

Figure 79 MIMO page – populated

Logout Connection Admin

Filter

- Unit Summary
- Radio Summary
- Platform
- Faults
- Radio
 - Radio Parameters
 - Remote Radio Parameters
 - Radio BER Thresholds
 - ATPC
 - Payload Encryption
- Ethernet Interface
- MRMC
- PM & Statistics
- Diagnostics
- Groups
 - XPIC
 - Multi Carrier ABC
 - MIMO**
 - AMCC
- Ethernet
- Sync
- Quick Configuration
- Utilities

IP20C-2+0-NE1.10: MIMO Groups

MIMO Members table

<input type="checkbox"/>	Group location	Group type	Member 1 location	Member 2 location	State	Role	Admin state
<input type="checkbox"/>	MIMO: Group #1	1+0 Space Diversity	Radio: Slot 2, Port 1	Radio: Slot 2, Port 2	Disabled	Not-relevant	Disable

Create Group Delete Edit Group Edit Members

6. Click **Submit**

7. In the MIMO page, select the group you just created and click **Edit Group**. The MIMO edit page opens.

Figure 80 MIMO – Edit Page (Space Diversity Group)

MIMO Members table - Edit

Group location: MIMO: Group #1

Group type: 1+0 Space Diversity

Member 1 location: Radio: Slot 2, Port 1

Member 2 location: Radio: Slot 2, Port 2

State: Disabled

Advanced state: Disabled

Role: Not-relevant

Admin state: Enable

Apply Reset State Machine

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

Page Refresh Interval (Seconds): None Last Loaded: 08:38:42 Refresh Close

100%

8. In the **Admin State** field, select **Enable**
9. Click **Apply**.
10. Repeat Steps 1 through 9 for the second unit.

**Note**

The identity of the active and standby units is not determined until unit protection is configured.

11. Configure Unit Protection, according to the instructions in [Configuring Unit Protection with HSB Radio Protection \(External Protection\)](#).
12. On the active PTP 820 unit, mute the transmitter of radio carrier 2. For instructions, see [configuring the radio parameters](#).
13. Perform Copy to Mate. See Step 5 in [configuring HSB Radio Protection](#).

**Note**

It is crucial to ensure that the port connected to the Diversity antenna is muted in each PTP 820 unit. If you perform Copy to Mate after configuring unit protection, as indicated above, the mute configuration will be copied to the standby unit. If you mute the interface before configuring unit protection, you must make sure to manually mute the interface on both PTP 820 units. Otherwise, configuring unit protection will override the mute configuration.

Configuring MIMO and Space Diversity

**Note**

This feature is only relevant for PTP 820C units.

This section describes how to configure MIMO and space diversity, and include the following topics:

- [MIMO and Space Diversity Overview](#)
- [Configuring a MIMO Link](#)
- [Creating a MIMO or Space Diversity Group](#)
- [Enabling/Disabling a MIMO or Space Diversity Group](#)
- [Setting the Role of a MIMO or Space Diversity Group](#)
- [Resetting MIMO](#)
- [Viewing MMI and XPI Levels](#)
- [Deleting a MIMO or Space Diversity Group](#)

MIMO and Space Diversity Overview

Line-of-Sight (LoS) Multiple Input Multiple Output (MIMO) achieves spatial multiplexing by creating an artificial phase de-correlation by deliberate antenna distance at each site in deterministic constant distance. At each site in a LoS MIMO configuration, data to be transmitted over the radio link is split into two bit streams (MIMO 2x2) or four bit streams (MIMO 4x4). These bit streams are transmitted via two antennas. In MIMO 2x2, the antennas use a single polarization. In MIMO 4x4, each antenna uses dual polarization. The phase difference caused by the antenna separation enables the receiver to distinguish between the streams.

PTP 820C supports both MIMO 2x2 and MIMO 4x4. For a full explanation of MIMO support in PTP 820C, refer to the PTP 820C Technical Description.

The same hardware configurations can also be used to implement BBS Space Diversity. PTP 820C supports 1+0, 2+0 and 2+2 Space Diversity. For a full explanation of Space Diversity support in PTP 820C, refer to the PTP 820C Technical Description.

**Note**

Only one MIMO or Space Diversity group can be created per PTP 820C unit. All MPMC scripts that support MIMO also support Space Diversity.

2+2 Space Diversity (CLI)

2+2 HSB Space Diversity provides both equipment protection and signal protection. If one unit goes out of service, the other unit takes over and maintains the link until the other unit is restored to service and Space Diversity operation resumes.

2+2 HSB Space Diversity utilizes two PTP 820C units operating in dual core mode. In each PTP 820C unit, both radio carriers are connected to a single antenna. One optical GbE port on each PTP 820C is connected to an optical splitter. Traffic must be routed to an optical GbE port on each PTP 820C unit.

In effect, a 2+2 HSB configuration is a protected 2+0 Space Diversity configuration. Each PTP 820C monitors both of its cores. If the active PTP 820C detects a radio failure in either of its cores, it initiates a switchover to the standby PTP 820C.

Configuring a MIMO Link

To configure a MIMO link, you must perform the following steps:

1. If you are configuring a 4x4 MIMO link, verify that the following three cables are connected between the Master and Slave PTP 820C units on each side of the link. For details, refer to the PTP 820C Installation Guide:
 - Source sharing cable between both EXT REF PTP 820C radio connectors.
 - MIMO data sharing cable between both PTP 820C ETH3/EXT ports.
 - MIMO signaling cable between both PTP 820C MGT/PROT ports.
2. If you are configuring a 4x4 MIMO link, you must initially configure the PTP 820C carriers as XPIC links, using XPIC scripts, and configuring the carriers as XPIC groups. See [Configuring XPIC](#).
3. Perform antenna alignment for XPIC. See [Performing Antenna Alignment for XPIC](#).
4. Configure MIMO groups on each PTP 820C unit. See [Creating a MIMO or Space Diversity Group](#).
5. If you are configuring a 4x4 MIMO link, configure the groups in the following order:
 - i Upper unit (Master) on the local side of the link.
 - ii Upper unit (Master) on the remote side of the link.
 - iii Lower unit (Slave) on the local side of the link.
 - iv Lower unit (Slave) on the remote side of the link.
6. After enabling the MIMO groups and setting their roles on the Master units on both sides of the link, reset the MIMO state machine. See [Resetting MIMO](#).
7. For a 4x4 MIMO link, configure LAG on the two Ethernet ports of the external switches connected to the PTP 820C units on both sides of the link.
8. For a 4x4 MIMO link, configure Automatic State Propagation with **ASP trigger by remote fault** enabled on the MIMO group in all four PTP 820C units that make up the link. See [Configuring Automatic State Propagation and Link Loss Forwarding](#).



Note

The last two steps are crucial to ensure that the link continues to function via the MIMO resiliency mechanism in the event of a hardware failure scenario. See [Resetting MIMO](#).

Creating a MIMO or Space Diversity Group

**Note**

Only one MIMO or Space Diversity group can be created per PTP 820C unit.

To create a MIMO or Space Diversity group:

1. Select **Radio > Groups > MIMO**. The MIMO page opens.
2. Click **Create MIMO**. The Create MIMO Group page opens.

Figure 81 Create MIMO Group – Page 1



3. In the Group Type field, select one of the following according to your desired system configuration:
 - MIMO 2x2
 - MIMO 4x4
 - 1+0 Space Diversity
 - 2+0 Space Diversity

**Note**

To enable 2+2 Space Diversity, select 2+0 Space Diversity after setting up the hardware configuration for 2+2 Space Diversity. See [2+2 Space Diversity](#).

4. Click Next. The Create MIMO Group page is updated and displays your system configuration.

Figure 82 Create MIMO Group – Page 2

Create MIMO Group

Group Type

Group #

Member 1

Member 2

<< Back Next >> Submit Close

100%

5. Click **Submit**, to create the MIMO or Space Diversity group.
Click **Close** to cancel and close the window.
6. After creating the group, you must enable the group in the MIMO - Edit page.
See [Enabling/Disabling a MIMO or Space Diversity Group](#).
7. For 4x4 MIMO configurations and 2+2 Space Diversity configurations, you must set the role of the group to Master or Slave. See [Setting the Role of a MIMO or Space Diversity Group](#).

Enabling/Disabling a MIMO or Space Diversity Group

To set the admin state of a MIMO or Space Diversity group:

1. Select **Radio > Groups > MIMO**. The MIMO page opens.
2. Select a MIMO group from the table, then click **Edit Group**. The MIMO - Edit page opens.

Figure 83 MIMO - Edit Page

3. In the Admin state field:
 - Select Enable to enable the MIMO or Space Diversity configuration.
 - Select Disable to disable the MIMO or Space Diversity configuration
4. Click Apply.

Setting the Role of a MIMO or Space Diversity Group

For 4x4 MIMO configurations and 2+2 Space Diversity configurations, you must set the role of the group to Master or Slave. This determines the role of the PTP 820C unit in the overall MIMO or Space Diversity configuration.

To set the role of a MIMO or Space Diversity group:

1. Select **Radio > Groups > MIMO**. The MIMO page opens.
2. Select a MIMO group from the table
3. Click **Edit Group**. The MIMO - Edit page opens.

Figure 84 MIMO - Edit Page

4. Perform the following:
 - For 4x4 MIMO configurations and 2+2 Space Diversity configurations, select Master or Slave in the Role field. This determines the role of the PTP 820C unit in the overall MIMO or Space Diversity configuration.
 - For MIMO 2x2 configurations and 1+0 Space Diversity configurations, select Not-Relevant in the Role field.
5. Click **Apply**.

Resetting MIMO

In hardware failure scenarios, MIMO 4x4 provides a resiliency mechanism that enables the link to continue functioning as a 2+0 XPIC link.

To restore full MIMO operation, the faulty equipment must be replaced. The replacement equipment must be pre-configured to the same configuration as the equipment being replaced. Once the new equipment has been properly installed and, if necessary, powered up, you must reset MIMO.



Note

MIMO reset causes a traffic interruption. It is recommended to rest MIMO on the remote side of the link first, then on the local side.

To reset MIMO:

1. Select Radio > Groups> MIMO. The MIMO page opens.
2. Select the MIMO group from the table.
3. Click Edit Group. The MIMO - Edit page opens.

Figure 85 MIMO - Edit Page

4. Click Reset State Machine.
5. Confirm the reset operation.

Viewing MMI and XPI Levels

You can view MMI and XPI levels for the individual radio carriers in a MIMO group.

Note that the MMI value can also be calculated manually. To calculate it manually, you must measure the following RSL levels per receiver:

1. Mute all remote transmitters except the transmitter for the link you want to measure, and measure the local RSL level (RSL_Wanted).
2. Mute all remote transmitters except the same polarization interferer and measure the local RSL2 (RSL_Int).

The MMI is equal to $RSL_Wanted - RSL_Int$

To view MMI and XPI Levels:

1. Select Radio > Groups> MIMO. The MIMO page opens.
2. Select the MIMO group from the table.

3. Click Edit Members. The MIMO - Edit Members page opens.

Figure 86 MIMO - Edit Members Page

Member	MMI	XPI
Radio: Slot 2, port 1	0	17.70
Radio: Slot 2, port 2	0	16.70

Apply Refresh Close

100%

The MIMO - Edit Members page provides the following information for each radio carrier in the MIMO group:

- **MMI** – MIMO Mate Interference. MMI represents the difference between the RSL1 and the RSL2 of the remote Master and Slave transmitters with the same polarization. The nominal range is 0. The range should be from -3 dB to +3 dB. This parameter is not relevant for 1+0 Space Diversity (as indicated by a value of -99).
- **XPI** – Cross Polarization Interference. This is only relevant in 4x4 configurations, where each unit operates in dual polarization (XPIC) mode. The XPI value should be at least 25 dB. For further information, see [Configuring XPIC](#).

Deleting a MIMO or Space Diversity Group

You can delete a MIMO or Space Diversity Group.

To delete a MIMO or Space Diversity Group:

1. Before deleting a MIMO or Space Diversity group, you must disable the group. To disable the group, set the Admin State to Disable in the [MIMO - Edit Page](#).



Note

When the MIMO or Space Diversity group is disabled, the system is automatically reset.

2. Select a MIMO group from the table.
3. Click **Delete**. The Delete MIMO confirmation page opens.
4. Confirm the operation.

Configuring Advanced Frequency Reuse (AFR)

AFR Overview

AFR works in conjunction with ACM to enable links to achieve high modulations and high capacities despite the presence of adjacent links transmitting at the same frequency. By mitigating the effects of side lobe interference (SLI) completely, or nearly completely, AFR can reduce adjacent link interference to levels that enable links that would otherwise be limited to QPSK modulation to transmit at modulations of up to 2048 QAM. This enables the placement of links that would otherwise be impractical due to high interference.

In an AFR 1+0 configuration, a dual-modem PTP 820C unit is deployed at the hub site and two PTP 820C or PTP 820S units are deployed in two tail sites. Each carrier at the hub site is known as an “aggregator.”

The hub site utilizes a single PTP 820C unit with two radio carriers. Each carrier is in a link, via its own directional antenna, with a tail site that consists of a PTP 820C or PTP 820S unit.

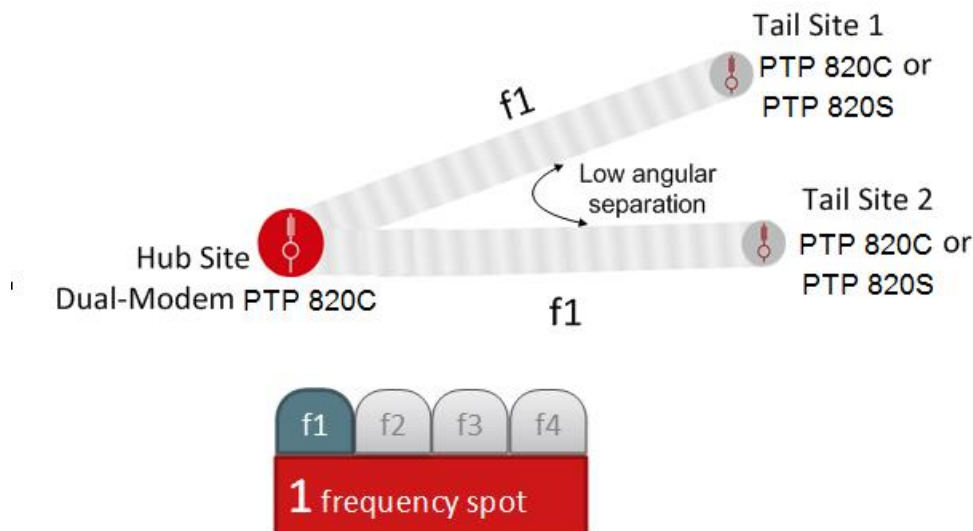
One hub site cannot have more than two tail sites. Also, a hub site cannot be a tail site for another AFR hub site.



Note

The links should be located so as to ensure that the two data streams do not cross.

Figure 87 AFR 1+0 Deployment



For information about planning links with AFR, contact Cambium support.

Initial Link Configuration and Alignment for AFR

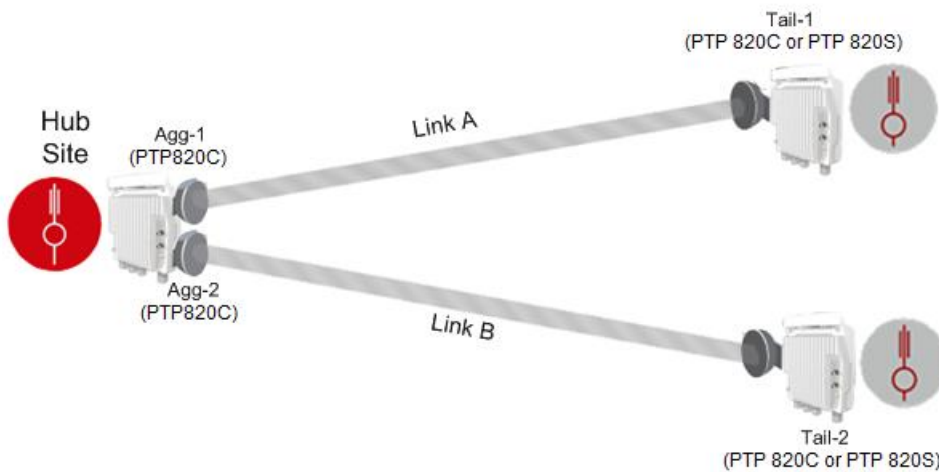
AFR 1+0 requires the following hardware configurations:

- **Hub Site** – Install a single PTP 820C unit with two antennas using a PTP 820C Dual Core kit, as described in Section 6.12 of the PTP 820C Installation Guide, *2x2 LoS MIMO Direct Mount*.
- **Tail Sites** – Install a 1+0 PTP 820C or PTP 820S configuration.

Before performing the software configuration for AFR, you must set up and align the two links as individual 1+0 links. Use Script 1801 for the alignment, but *do not* enable AFR before aligning the links.

When aligning Link A, mute both sides of Link B. When you are finished aligning Link A, mute both sides of Link A, unmute both sides of Link B, and align link B. When you are finished aligning Link B, unmute both sides of both links.

Figure 88 AFR 1+0 Configuration



Software Configuration for AFR



Note

AFR is not supported with ATPC. ATPC should be disabled before configuring AFR. See [Configuring ATPC and ATPC Override Timer](#).

Perform the following steps for each site in the AFR configuration.

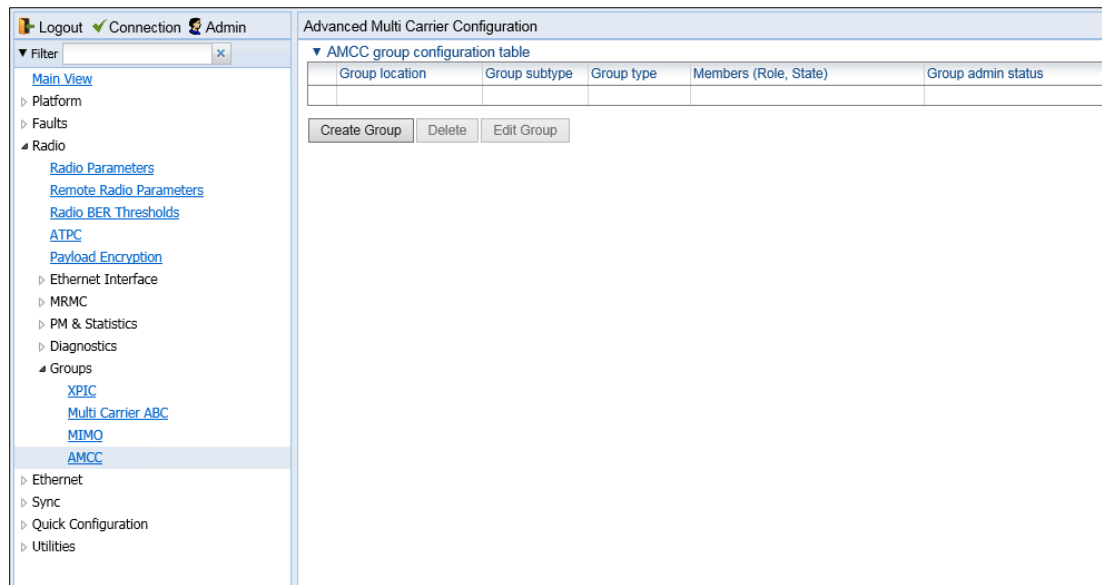
- If you are performing the configuration locally at the Hub site and each Tail site, the order in which you configure the sites does not matter.
- If you are performing the configuration for all three sites remotely from the Hub Site, you must configure the sites in the following order:
 - Tail Site 1

- Tail Site 2
- Hub Site

After you configure AFR on the Tail Sites, the link between the Hub Site and the Tail Sites will be lost. The links will be restored after you configure AFR on the Hub site and the Hub site comes back up after unit reset.

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

Figure 89 Advanced Multi Carrier Configuration Page (Empty)



1 Click Create Group. The AMCC Group – Select Group Parameters page opens.

Figure 90 AMCC Group – Select Group Parameters Page

- 2 In the Group type field, select one of the following:
- If you are configuring the Hub site, select **AFR Aggregate**.
 - If you are configuring a Tail site, select **AFR Tail**.

- 3 In the Group admin status field, select Enable.
- 4 Click Next. The AMCC Group – Select Members Parameters page opens.

Figure 91 AMCC Group – Select Group Parameters Page (Hub Site)

AMCC Group - Select Members Parameters

Group ID: AMCC: Group #1

Group subtype: AFR 1+0

Group type: AFR Aggregate

Group admin status: Enable

Member #1: Radio: Slot 2, Port 1 ▼

Member role: Aggregate #1 ▼

☒ Set MRMC Script (1801)

MRMC Script maximum profile: 10 ▼

Member #2: Radio: Slot 2, Port 2

Member role: Aggregate #2

☒ Set MRMC Script (1801)

MRMC Script maximum profile: 10 ▼

<< Back Next >> Finish

Last Loaded: 15:13:15 Close

Figure 92 AMCC Group – Select Group Parameters Page (Tail Site)

- 5 In the **Member #1** field, select a radio interface.
- 6 In the **Member role** field, select the role of the interface in the AFR 1+0 configuration:
 - If you are configuring the Hub site, select **Aggregate #1** or **Aggregate #2**.
 - If you are configuring the Tail site, select **Tail #1** or **Tail #2**.

Make sure the interface you configure as Aggregate #1 is part of the link with Tail #1 and that the interface you configure as Aggregate #2 is part of the link with Tail #2.

- 7 Select **Set MPMC Script (1801)**.

**Note**

Script 1801 is a 28/30 MHz script, with a maximum ACM profile of 10 (2048 QAM). For additional details, refer to the relevant Release Notes or product Technical Description.

- 8 In the **MPMC Script maximum profile** field, select the maximum ACM profile for the links.
- 9 Click **Finish**. This page displays the parameters you have selected for the link.

Figure 93 AMCC Group – Selection Summary Page

AMCC Group - Selection Summary

Group ID: AMCC: Group #1

Group subtype: AFR 1+0

Group type: AFR Aggregate

Group admin status: Enable

Member #1: Radio: Slot 2, Port 1

Member role: Aggregate #1

☒ Set MRMC Script (1801) (1801, Minimum profile: 0, Maximum profile: 10)

Member #2: Radio: Slot 2, Port 2

Member role: Aggregate #2

☒ Set MRMC Script (1801) (1801, Minimum profile: 0, Maximum profile: 10)

Pressing 'Submit' will cause unit to reset.

<< Back Next >> Submit

Last Loaded: 15:17:07 Close

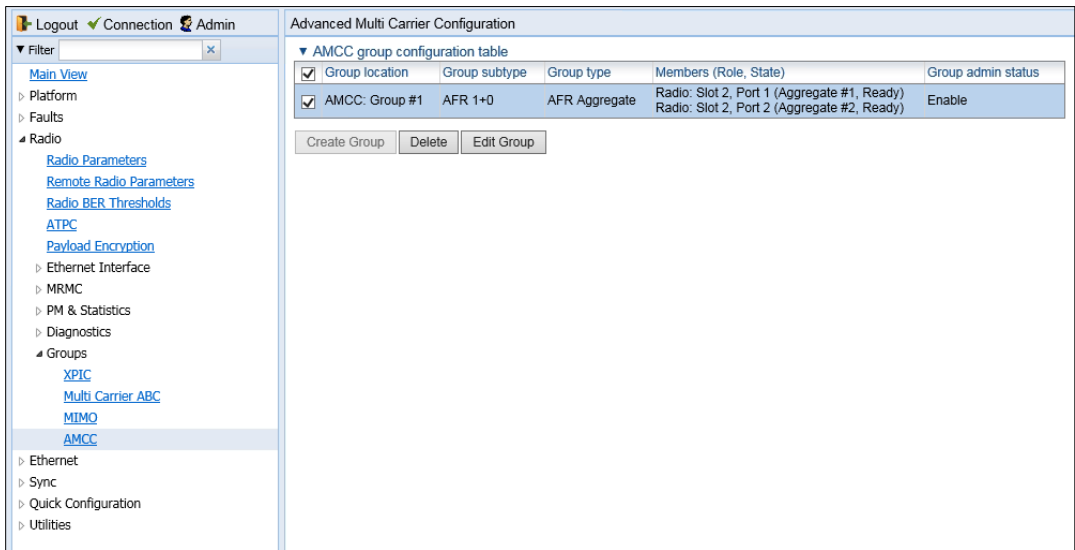
- 10 Click **Submit**. The unit is automatically reset. Once AFR has been configured on the Hub site and both Tail sites, the configuration is complete.

Deleting an AFR Group

If you want to disable AFR and convert the two links into non-AFR links, you must perform the following steps for each site in the AFR configuration. If you are managing the links by in-band management from the hub site, you must disable AFR at the tail sites first, then disable AFR at the hub site. Once AFR has been disabled at all of the sites, you can delete the AFR groups in any order.

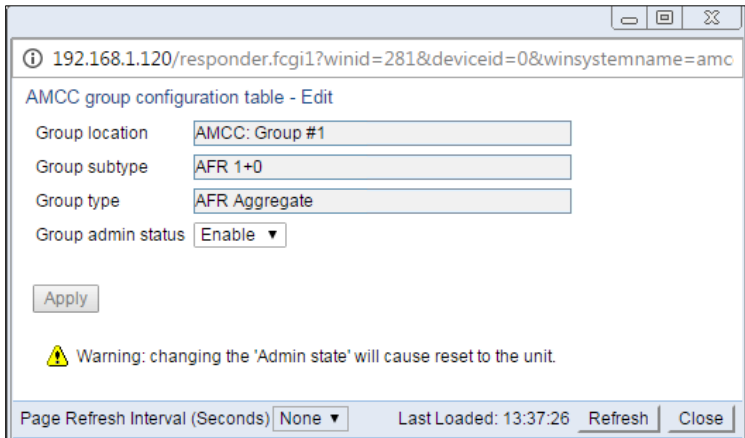
- 1 Select **Radio > Groups > AMCC**. The Advanced Multi Carrier Configuration page opens.

Figure 94 Advanced Multi Carrier Configuration Page (Populated)



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

Figure 95 AMCC Group – Edit Page



- 3 In the **Group admin status** field, select **Disable**.
- 4 Click **Apply**, then **Close**. The unit is automatically reset.
- 5 In the Advanced Multi Carrier Configuration page, select the group and click **Delete**.

Once you have performed this procedure for the Hub site and both Tail sites, you can reconfigure the links according to the new network plan.

Operating a PTP 820C in Single Radio Carrier Mode

If you wish to operate a PTP 820C unit in single radio carrier mode, you must perform the following steps:

1. Verify that XPIC is disabled. See [Configuring XPIC](#).
2. Disable Multi-Carrier ABC, as described in [Error! Reference source not found.](#).
3. Disable one of the two radio interfaces, as described in [Enabling the Interfaces \(Interface Manager\)](#).
4. Mute the disabled radio interface, as described in [Configuring the Radio Parameters](#).

Chapter 4: Unit Management

This section includes:

- [Defining the IP Protocol Version for Initiating Communications](#)
- [Configuring the Remote Unit's IP Address](#)
- [Configuration 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](#)

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 96 Local Networking Configuration Page

Logout Admin Connection

Filter

Main View

Platform

Management

Unit Parameters

NTP Configuration

Time Services

Interface Manager

Inventory

Unit Info

Reset

Set to Factory Default

Unit Redundancy

Networking

Local

Remote

SNMP

Software

Configuration

Activation Key

Security

Faults

Radio

Ethernet

Sync

Quick Configuration

Utilities

Local Networking Configuration

IP Family Configuration

IP address Family IPv4

Apply

Description	local-management-port
IP address	192.168.1.34
Subnet mask	255.255.255.0
Default gateway	192.168.1.1
IPv6 Address	fec0::c0:a8:1:1
IPv6 Prefix-Length	120 (1..128)
Default Gateway IPv6	::

Apply Refresh

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.
 - For PTP 820C units, the Radio Parameters page initially displays a table as shown in [Figure 97](#).
 - For PTP 820S units, the page appears as shown in [Figure 98](#).

Figure 97 Remote Networking Configuration Page – PTP 820C

Radio location	Remote radio location	Remote IP Address	Remote Subnet mask	Remote default gateway	Remote IPv6 Prefix Length	Remote IPv6 Default Gateway
Radio: Slot 2, port 1	Unknown	0.0.0.0	255.255.255.0	0.0.0.0	64	--
Radio: Slot 2, port 2	Unknown	0.0.0.0	255.255.255.0	0.0.0.0	64	--

Buttons:

Figure 98 Remote Networking Configuration Page – PTP 820S

Logout Admin Connection

Filter

Main View

Platform

Management

Unit Parameters

NTP Configuration

Time Services

Interface Manager

Inventory

Unit Info

Reset

Set to Factory Default

Unit Redundancy

Networking

Local

Remote

SNMP

Software

Configuration

Activation Key

Security

Faults

Radio

Ethernet

Sync

Quick Configuration

Remote Networking Configuration

Remote IP Configuration

Radio location: Radio: Slot 2, port 1

Remote radio location: Radio: Slot 2, port 1

Remote IP Address: 192.168.1.35

Remote Subnet mask: 255.255.255.0

Remote default gateway: 192.168.1.1

Remote IPv6 Address: fe80::c0a8:124

Remote IPv6 Prefix-Length: 64 (1..128)

Remote IPv6 Default Gateway: ::

Apply Refresh

- For PTP 820C units, select the carrier in the Radio table (see [Figure 97](#)) and click **Edit**. A separate Remote IP Configuration page opens. The page is identical to the PTP 820C and PTP 820S page.

Figure 99 Remote IP Configuration Page Per Carrier – PTP 820C

Remote

Remote IP Configuration

Radio location Radio: Slot 2, port 1

Remote radio location Radio: Slot 2, port 1

Remote IP Address 192.168.1.222

Remote Subnet mask 255.255.255.0

Remote default gateway 192.168.1.211

Remote IPv6 Address 2001:200::222

Remote IPv6 Prefix-Length 64 (1..128)

Remote IPv6 Default Gateway 2001:200::1

Apply Refresh Close

3. In the **Remote IP address** field, enter an IP 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.
4. In the **Remote Subnet mask** field, enter the subnet mask of the remote radio.
5. Optionally, in the **Remote default gateway** field, enter the default gateway address for the remote radio.
6. Optionally, in the **Remote IPv6 Address** field, enter an IPv6 address for the remote unit. You can enter the address in IPv6 format in this field, and/or in IPv4 format in the **IP Address** field. The unit will receive communications whether they are sent to its IPv4 address or its IPv6 address.
7. If you entered an IPv6 address, enter the IPv6 prefix length in the **Remote IPv6 Prefix-Length** field.
8. Optionally, if you entered an IPv6 address, enter the default gateway in IPv6 format in the **Remote default Gateway IPv6** field.
9. Click **Apply**.

Changing the Subnet of the Remote IP Address

If you wish to change the **Remote IP 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 IP 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.

Configuration SNMP

PTP 820C and PTP 820S support SNMP v1, V2c, and v3. You can set community strings for access to PTP 820 units.

PTP 820C and PTP 820S 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 100 SNMP Parameters Page

The screenshot displays the 'SNMP Parameters' configuration page. The left-hand navigation pane shows a tree structure with 'SNMP Parameters' highlighted. The main content area is titled 'SNMP Parameters' and contains the following fields:

- Admin:** A dropdown menu set to 'Enable'.
- Operational Status:** A text field containing 'Up'.
- SNMP Read Community:** A text field containing 'public'.
- SNMP Write Community:** A text field containing 'private'.
- SNMP Trap Version:** A dropdown menu set to 'V1'.
- SNMP MIB Version:** A text field containing '1.8.2.2.1.3.2'.
- V1V2 Blocked:** A dropdown menu set to 'No'.

At the bottom of the configuration area, there are two buttons: 'Apply' and 'Refresh'.

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.

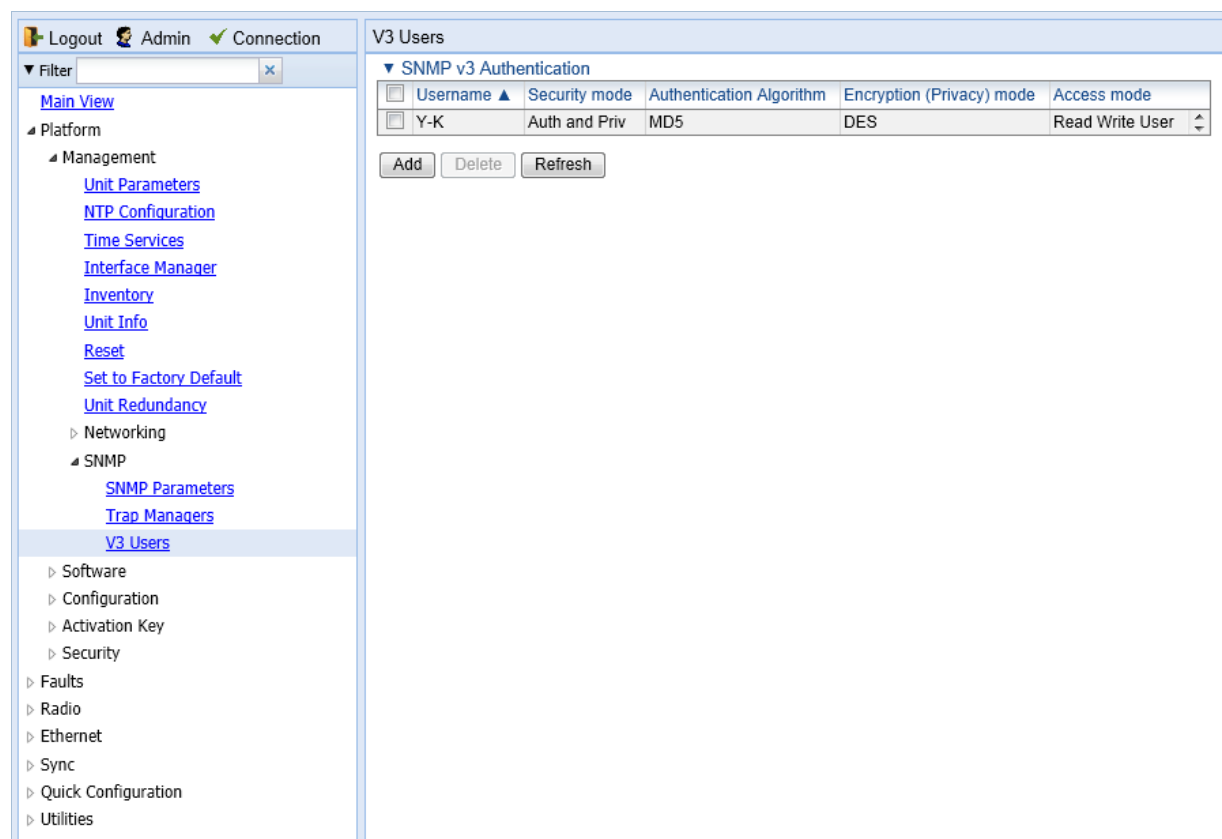
6. In the **V1V2 Blocked** field, select **Yes** if you want to block SNMPv1 and SNMPv2 access so that only SNMPv3 access will be enabled.
7. Click **Apply**.

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 101 V3 Users Page



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

Figure 102 V3 Users - Add Page

The screenshot shows a web-based configuration window titled "V3 Authentication" with a subtitle "SNMP v3 Authentication - Add". The window contains the following fields and controls:

- User Name:** A text input field.
- Password:** A text input field.
- Authentication Algorithm:** A dropdown menu with "MD5" selected.
- Encryption (Privacy) mode:** A dropdown menu with "DES" selected.
- Access mode:** A dropdown menu with "Read Write User" selected.
- Buttons:** "Apply", "Refresh", and "Close" buttons are located at the bottom left of the form area.

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

Table 13 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: <ul style="list-style-type: none">• None• SHA• MD5
Encryption (Privacy) Mode	Select an encryption (privacy) protocol for the user. Options are: <ul style="list-style-type: none">• None• DES• AES
Access Mode	Select an access permission level for the user. Options are: <ul style="list-style-type: none">• 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 103 Trap Managers Page

The screenshot shows the 'Trap Managers' configuration page. The left sidebar contains a navigation menu with the following items: Main View, Platform (expanded), Management (expanded), Unit Parameters, NTP Configuration, Time Services, Interface Manager, Inventory, Unit Info, Reset, Set to Factory Default, Unit Redundancy, Networking (expanded), SNMP (expanded), **Trap Managers** (selected), V3 Users, Software, Configuration, Activation Key, Security, Faults, Radio, Ethernet, Sync, Quick Configuration, and Utilities. The main content area is titled 'Trap Managers' and contains a table labeled 'Trap managers table'. The table has the following columns: Id, IPv4 Address, IPv6 Address, Description, Admin, Community, Port, Heartbeat period (minutes), CLI, and V3 User Name. There are four rows of data, all with 'Disable' as the Admin and 'public' as the Community. Below the table are 'Edit' and 'Refresh' buttons.

Id	IPv4 Address	IPv6 Address	Description	Admin	Community	Port	Heartbeat period (minutes)	CLI	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 104 Trap Managers - Edit Page

3. Configure the trap manager parameters, as described in [Table 14 Trap Manager Parameters](#).
4. Click **Apply**, then **Close**.

Table 14 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	<ul style="list-style-type: none"> Enter a description of the trap manager (optional).
Admin	<ul style="list-style-type: none"> Select Enable or Disable to enable or disable the selected trap manager.
Community	<ul style="list-style-type: none"> Enter the community string for the SNMP read community.
Port	<ul style="list-style-type: none"> Enter the number of the port through which traps will be sent.
Heartbeat Period	<ul style="list-style-type: none"> Enter the interval, in minutes, between each heartbeat trap.

Parameter	Definition
CLLI	<ul style="list-style-type: none">Enter a Common Language Location Identifier (CLLI). The CLLI is free text that will be sent with the trap. You can enter up to 100 characters.
V3 User Name	<p>If the SNMP Trap version selected in Figure 100 SNMP Parameters Page is V3, enter the name of a V3 user defined in the system.</p> <p>To view or define a V3 user, use the Figure 101 V3 Users Page page.</p> <p>Note: Make sure that an identical V3 user is also defined on the manager's side.</p>

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 820 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).

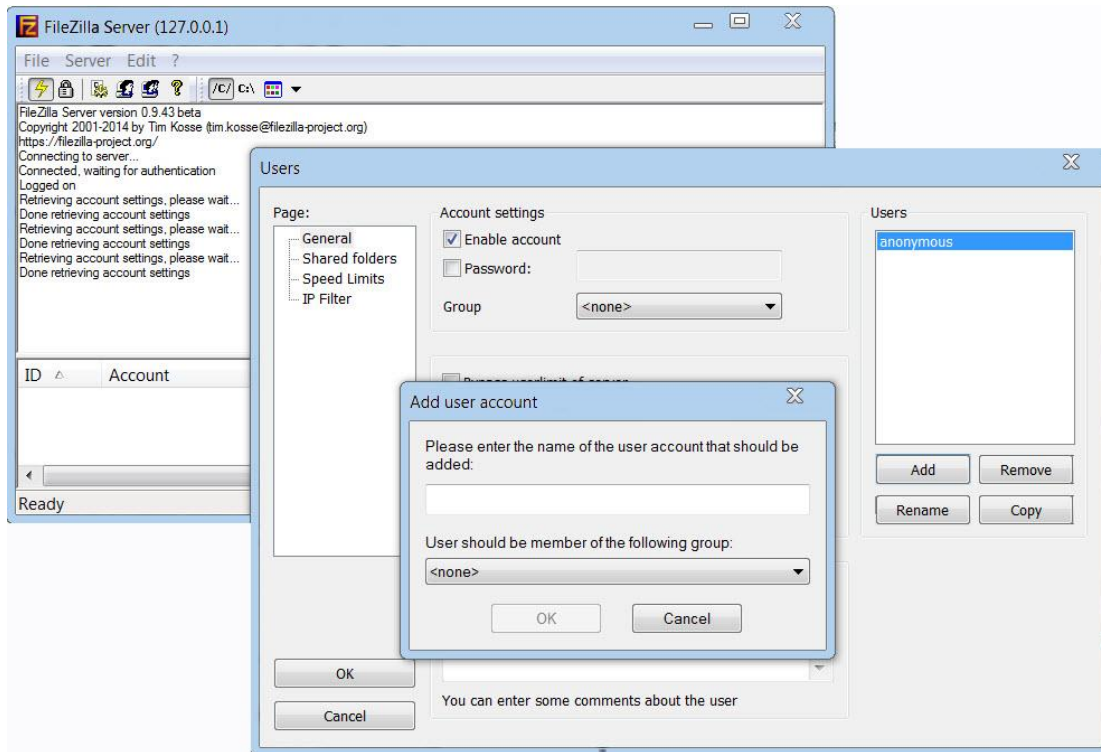
If you are using IPv6 to perform the operation, make sure to use FileZilla version 0.9.38 or higher to ensure IPv6 support. If you are using another type of FTP or SFTP server, make sure the application version supports IPv6.

To install and configure FTP or SFTP server software on the PC or laptop:

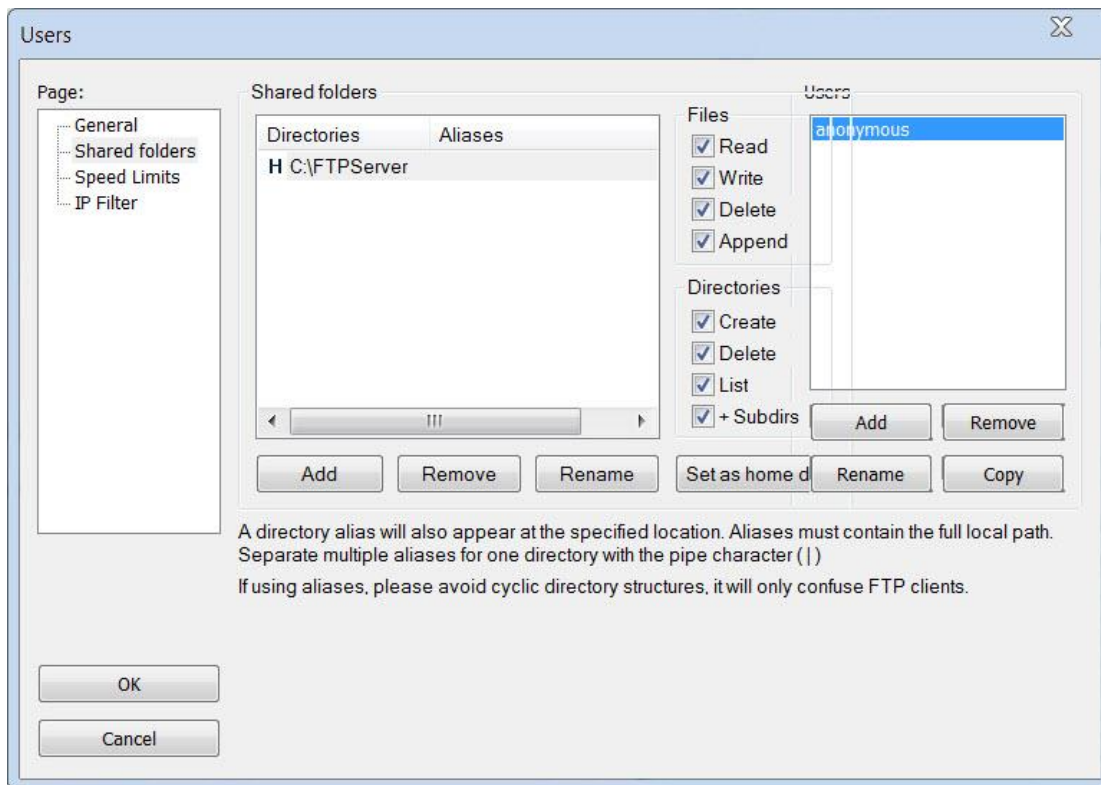
1. Create a user and (optional) password on the FTP/SFTP server. For example, in FileZilla Server, perform the following:

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 105 FileZilla Server User Configuration

2. Create a shared FTP/SFTP folder on the PC or laptop you are using to perform the software upgrade (for example, *C:\FTPServer*).
3. In the FTP/SFTP server, set up the permissions for the shared FTP/SFTP folder. For example, in FileZilla Server:
 - I. From the **Edit** menu, select **Users**.
 - II. In the Users window, select **Shared folders**.
 - III. Underneath the Shared folders section, click **Add** and browse for your shared FTP folder.
 - IV. Select the folder and click **OK**.
 - V. In the Shared folders section, select your shared FTP folder.
 - VI. In the Files and Directories sections, select all of the permissions.
 - VII. Click Set as home directory to make the Shared folder the root directory for your FTP server
 - VIII. Click **OK** to close the Users window.

Figure 106 FileZilla Server Shared Folder Setup

Configuring the Internal Ports for FTP or SFTP

By default, the following PTP 820 ports are used for FTP and SFTP when the PTP 820 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 > 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 107 FTP Port Page

FTP Port

File transfer protocol	File transfer port number
FTP	21
SFTP	22

Apply

Last Loaded: 15:35:32 Refresh Close

110%

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

Upgrading the Software

PTP 820 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 15 Versions Page Columns](#).

Figure 108 Versions Page

Package Name	Target Device	Running Version	Installed Version	Downloaded version	Reset Type
nou	Cleared	8.2.0.0.0.303	8.2.0.0.0.303	N/A	Main board cold reset
nou-nhc	Cleared	8.2.0.0.0.303	8.2.0.0.0.303	N/A	Main board cold reset
nou-nrc	Cleared	22.33	23.7	N/A	Main board cold reset
nou-management	Cleared	1.8.2.13	1.8.2.13	N/A	Main board cold reset
nou-fpga-fw	Cleared	10.0.874	11.0.5	N/A	Main board cold reset
nou-modem-fw	Cleared	223	2.25.2.23	N/A	Main board cold reset
nou-mmio-scripts	Cleared	9.2	9.2	N/A	Main board cold reset
nou-rfu-tables	Cleared	2.4	2.4	N/A	Main board cold reset
nou-vm-control	Cleared	1.0.2.11	N/A	N/A	No Reset

Table 15 Versions Page Columns

Parameter	Definition
Package Name	The name of the software package.
Target Device	The specific component on which the software runs.
Running Version	The software version currently running on the component.
Installed Version	The software version currently installed for the component. If the installed version is not already the running version, it will become the running version after the next reset takes place.

Parameter	Definition
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 820 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 820 that are currently running an older version.
3. **Reset** – The PTP 820 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 820 and its components, so that only files that need to be updated are actually downloaded. A message is displayed for each file that is actually downloaded.



Note

When downloading an older version, all files in the bundle may be downloaded, including files that are already installed.

Software bundles can be downloaded via HTTP, HTTPS, FTP or SFTP. After the software download is complete, you can initiate the installation.



Note

Before performing a software upgrade, it is important to verify that the system date and time are correct. See [Setting the Time and Date \(Optional\)](#).

When upgrading a node with unit protection, upgrade the standby unit first, followed by the active unit.

Downloading and Installing Software

You can download software using HTTP, HTTPS, FTP or SFTP.

When downloading software via HTTPS or HTTPS, the PTP 820 functions as the server, and you can download the software directly to the PTP 820 unit.



Note

HTTP and HTTPS can only be used to download files for System release 9.5 and later. If there is a requirement to downgrade from System release 9.5 or higher to an earlier version using HTTP or HTTPS, contact Cambium Customer Support for assistance.

When downloading software via FTP or SFTP, the PTP 820 functions as an FTP or SFTP client. You must install FTP or SFTP server software on the PC or laptop you are using to perform the software upgrade. For details, see [Installing and Configuring an FTP or SFTP Server](#).

Downloading Software Via HTTP or HTTPS

To download and install a new software version using HTTP or HTTPS:

1. Before performing a software upgrade, it is important to verify that the system date and time are correct. See [Setting the Time and Date \(Optional\)](#).
2. In the PTP 820's Web EMS, select **Platform > Software > Download & Install**. The Download & Install page opens.

Figure 109 Download & Install Page – HTTP/ HTTPS Download – No File Selected

Logout Connection Admin

Filter

[Unit & Radio Summary](#)

Platform

- Management
- Software
 - [Versions](#)
 - Download & Install**
 - Configuration
 - Activation Key
 - Security
- Faults
- Radio
- Ethernet
- Sync
- Quick Configuration
- Utilities

Microwave radio: Download & Install

Software Download

☒ HTTP ☐ FTP

Download status: Ready

Download progress: 0%

File Name: No file chosen for download

Choose File Abort Download

Software Install

Installation status: Ready

Installation progress: 0%

Install Parameters Install

3. Select **HTTP**
4. Click **Choose File**. A browser window opens.

5. Navigate to the directory in which the software file is located and selected the file. The selected file must be a ZIP file.
6. Click **Open**. The file name of the selected file appears in the **File Name** field.

Figure 110 Download & Install page – HTTP/ HTTPS Download – File Selected

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



Note

To Discontinue the download process, Click **Abort**.

8. Once the download has been completed, verify that the version you want to install has been downloaded. You can check the downloaded version for each component by viewing the *Downloaded Version* column in the Versions page. See [Viewing Current Software versions](#).

Downloading Software Via FTP or SFTP

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

1. Before performing a software upgrade, it is important to verify that the system date and time are correct. See [Setting the Time and Date \(Optional\)](#).
2. Install and configure FTP or SFTP server software on the PC or laptop you are using to perform the software upgrade, as described in [Installing and Configuring an FTP or SFTP Server](#).
3. Unzip the new software package for PTP 820 into your shared FTP or SFTP folder.
4. In the PTP 820's Web EMS, select **Platform > Software > Download & Install**. The Download & Install page opens.
5. Select **FTP**.

Figure 111 Download & Install Page - FTP

The screenshot displays a web interface for managing a microwave radio. On the left is a navigation menu with links for Logout, Connection, and Admin. Below these is a 'Filter' box and a list of categories: Unit & Radio Summary, Platform (with sub-items Management, Software, Versions, and Download & Install), Configuration, Activation Key, Security, Faults, Radio, Ethernet, Sync, Quick Configuration, and Utilities. The 'Download & Install' section is highlighted. The main content area is titled 'Microwave radio: Download & Install' and is divided into two sections: 'Software Download' and 'Software Install'. In the 'Software Download' section, the 'FTP' radio button is selected, and the 'Download status' is 'Ready'. The 'Download progress' bar shows 0%. Below this are buttons for 'FTP Parameters', 'FTP Port', and 'Download'. The 'Software Install' section shows the 'Installation status' as 'Ready' and the 'Installation progress' bar at 0%. Below this are buttons for 'Install Parameters' and 'Install'.

Logout Connection Admin

Filter

[Unit & Radio Summary](#)

Platform

- Management
- Software
 - Versions
 - Download & Install**
- Configuration
- Activation Key
- Security

Faults

Radio

Ethernet

Sync

Quick Configuration

Utilities

Microwave radio: Download & Install

Software Download

☐ HTTP ☒ FTP

Download status Ready

Download progress 0%

FTP Parameters FTP Port Download

Software Install

Installation status Ready

Installation progress 0%

Install Parameters Install

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

Figure 112 FTP Parameters Page

7. In the **File Transfer Protocol** field, select the file transfer protocol you want to use (**FTP** or **SFTP**).
8. In the **User name** field, enter the user name you configured in the FTP server.
9. In the **User password** field, enter the password you configured in the FTP server. If you did not configure a password for your FTP/SFTP user, simply leave this field blank.
10. If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the FTP/SFTP server in the **Server IPv4 address** field. See [Defining the IP Protocol Version for Initiating Communications](#).
11. If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the FTP/SFTP server in the **Server IPv6 Address** field. See [Defining the IP Protocol Version for Initiating Communications](#).
12. In the **Path** field, enter the directory path from which you are downloading the files. Enter the path relative to the FTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "/".
13. Click **Apply** to save your settings, and **Close** to close the FTP Parameters page.
14. Click **Download**. The download begins. You can view the status of the download in the **Download Status** field of the Download & Install page. See [Table 16 Download & Install Status Parameters](#).
15. Once the download has been completed, verify that the version you want to install has been downloaded. You can check the downloaded version for each component by viewing the *Downloaded Version* column in the Versions page. See [Viewing Current Software Versions](#).

**Note**

If upgrading from version 7.9 or earlier:

Before you proceed to install the software, repeat the download process even if Download Success is displayed in the Download status field, until the unit displays the message No new software modules found.

In case of failure, wait at least 30 minutes and repeat the software download.

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 111](#)).
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 16 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 16 Download & Install Status Parameters

Parameter	Definition
Download status	<p>The status of any pending software download. Possible values are:</p> <ul style="list-style-type: none"> • 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. <p>If an error occurs during the download, an appropriate error message is displayed in this field.</p> <p>When the download is complete, one of the following status indications appears:</p> <ul style="list-style-type: none"> • Download Success • Download Failure • All components already found in the system <p>When the system is reset, the Download Status returns to Ready.</p>
Download progress	Displays the progress of the current software download.
Install status	<p>The status of any pending software installation. Possible values are:</p> <ul style="list-style-type: none"> • 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. <p>If an error occurs during the installation, an appropriate error message is displayed in this field.</p> <p>When the installation is complete, one of the following status indications appears:</p> <ul style="list-style-type: none"> • Installation Success • Installation Partial Success • Installation Failure • incomplete-sw-version <p>When the system is reset, the Installation Status returns to Ready.</p>
Install progress	Displays the progress of the current software installation.

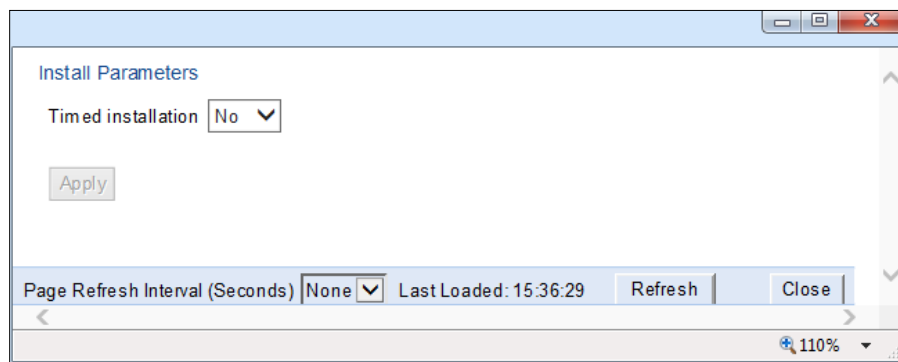
Configuring a Timed Installation

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:

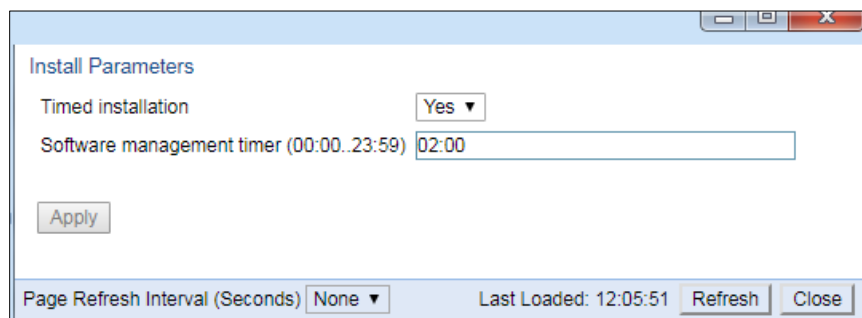
1. Download the software version you want to install. See [Downloading and Installing Software](#).
2. Select **Platform > Software > Download & Install**. The **Download & Install** page opens.
3. Click **Install Parameters**. The **Install Parameters** page opens.

Figure 113 Install parameters Page.



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

Figure 114 Install parameters page- Software Management Timer.



6. In the **Software management timer** field, enter the amount of time, in hours and minutes, you want to defer the installation. For example, in Figure 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 820 configuration files. This enables you to copy the system configuration to multiple PTP 820 units. You can also backup and save configuration files.

Configuration files can only be copied between units of the same type, i.e., PTP 820C to PTP 820C and PTP 820S to PTP 820S.

This section includes:

- [Configuration Management Overview](#)
- [Viewing Current Backup Files](#)
- [Setting the Configuration Management Parameters](#)
- [Exporting a Configuration File](#)
- [Importing a Configuration File](#)
- [Deleting a Configuration File](#)
- [Backing Up the Current Configuration](#)
- [Restoring a Saved Configuration](#)
- [Editing CLI Scripts](#)

Configuration Management Overview

System configuration files consist of a zip file that contains three components:

- A binary configuration file used by the system to restore the configuration.
- A text file which enables users to examine the system configuration in a readable format. The file includes the value of all system parameters at the time of creation of the backup file.
- An additional text file which enables you to write CLI scripts in order to make desired changes in the backed-up configuration. This file is executed by the system after restoring the configuration.

The system provides three restore points to manage different configuration files. Each restore point contains a single configuration file. Files can be added to the restore points by creating backups of the current system state or by importing them from an external server. For example, you may want to use one restore point to keep a last good configuration, another to import changes from an external server, and the third to store the current configuration.

You can apply a configuration file to the system from any of the restore points.

Viewing Current Backup Files

The system provides three restore points to manage different configuration files. Each restore point contains a single configuration file. Files can be added to the restore points by creating backups of the current system state or by importing them from an external server. For example, you may want to use one restore point to keep a last good configuration, another to import changes from an external server, and the third to store the current configuration.

To display the configuration files currently saved at the system restore points:

1. Select **Platform > Configuration > Backup Files**. The Backup Files page opens. For a description of the information provided in the Backup Files page, see [Table 17 Backup Files Page Columns](#).

Figure 115 Backup Files Page

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 17 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 820 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 [Setting the Time and Date \(Optional\)](#).
2. Install and configure an FTP server on the PC or laptop you are using to perform the import or export. See [Installing and Configuring an FTP or SFTP Server](#).
3. In the PTP 820's Web EMS, select **Platform > Configuration > Configuration Management**. The Configuration Management page opens.

Figure 116 Configuration Management Page

The screenshot shows the 'Configuration Management' page. On the left is a navigation menu with options like 'Unit & Radio Summary', 'Platform', 'Configuration', 'Timer Parameters', 'Backup Files', 'Configuration Management', 'Activation Key', 'Security', 'Faults', 'Radio', 'Ethernet', 'Sync', 'Quick Configuration', and 'Utilities'. The 'Configuration Management' option is selected. The main content area is titled 'Microwave radio: Configuration Management'. It contains several sections: 'Export/Import file status' with 'File transfer status' set to 'ready' and 'File transfer progress' at '0'; 'Backup file creation status' with 'Backup file creation status' set to 'Ready' and 'Backup file creation progress' at '0'; 'Configuration restore status' with 'Configuration restore status' set to 'ready'; and 'Configuration Parameters' with 'File number' set to 'Restore point 1' and 'Timed installation' set to 'No'. At the bottom are buttons for 'Apply', 'Export', 'Import', 'Delete', 'Backup', 'Restore', 'FTP Parameters', and 'FTP Port'.

4. Click FTP Parameters to display the FTP Parameters page.

Figure 117 FTP Parameters Page

The screenshot shows the 'FTP Parameters' page. It has a title bar 'FTP Parameters'. Below the title are input fields for 'Username' (containing 'anonymous'), 'Password' (masked with dots), 'Server IP address' (containing '0.0.0.0'), 'Server IPv6 address' (containing '::'), 'Path', and 'File name'. There is an 'Apply' button below these fields. At the bottom of the page, there is a 'Page Refresh Interval (Seconds)' dropdown set to 'None', a 'Last Loaded: 15:38:38' timestamp, and 'Refresh' and 'Close' buttons. The browser's status bar at the very bottom shows '110%' zoom.

5. In the **User name** 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 IP 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 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 "/".
10. In the **FileName** 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.

11. Click **Apply**, then **Close**, to save the FTP parameters and return to the Configuration Management page
12. 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.

13. 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:

1. Verify that you have followed all the steps in [Setting the Configuration Management Parameters](#).
2. Select **Platform > Configuration > Configuration Management**. The Configuration Management page opens ([Figure 116](#)).
3. In the **File Number** field, select the restore point from which you want to export the file.
4. Click **Apply** to save your settings.
5. 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.

To import a configuration file:

1. Verify that you have followed all the steps in [Setting the Configuration Management Parameters](#).
2. Select **Platform > Configuration > Configuration Management**. The Configuration Management page opens ([Figure 116](#)).
3. In the **File Number** field, select the restore point to which you want to import the file.
4. Click **Apply** to save your settings.
5. 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](#).

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 116](#)).
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 116](#)).
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 116 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 [Importing a Configuration File](#).
7. Restore the imported configuration file. See [Restoring a Saved Configuration](#). The unit is automatically reset. During initialization, the CLI script is executed, line by line.

**Note**

If any specific command in the CLI script requires reset, the unit is reset when that command is executed. During initialization following the reset, execution of the CLI script continues from the following command.

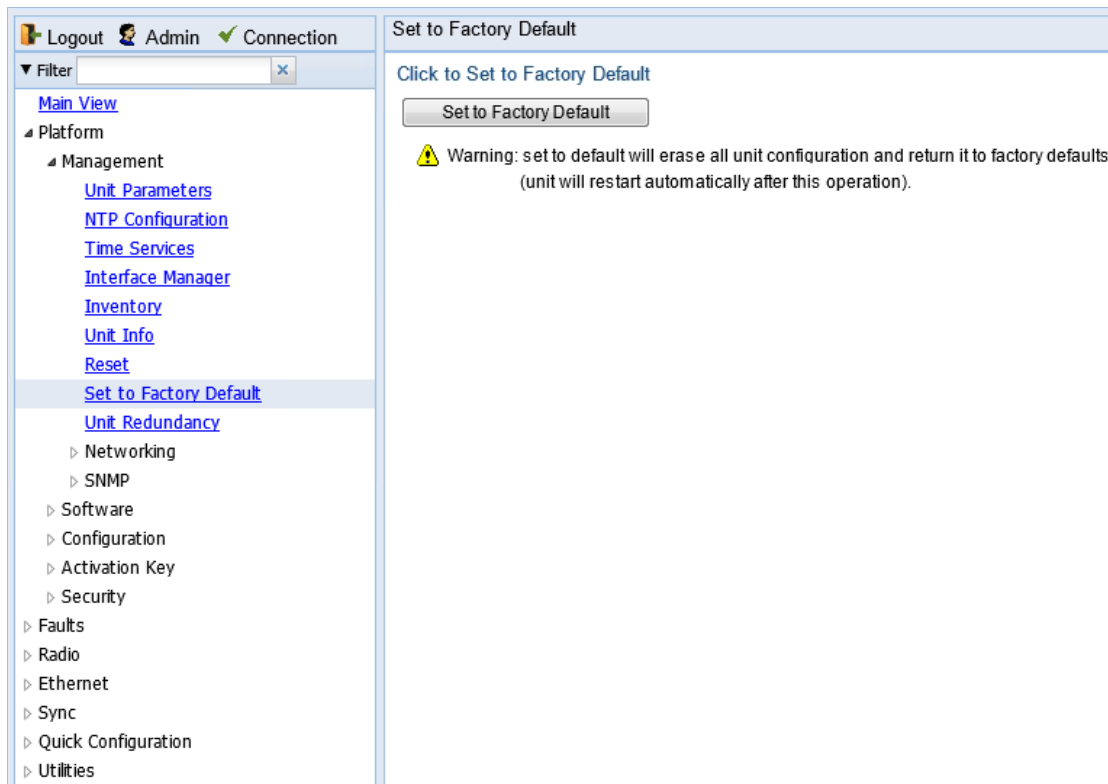
Setting the Unit to the Factory Default Configuration

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

To restore the factory default settings:

1. Select **Platform > Management > Set to Factory Default**. The Set to Factory Default page opens.

Figure 118 Set to Factory Default Page



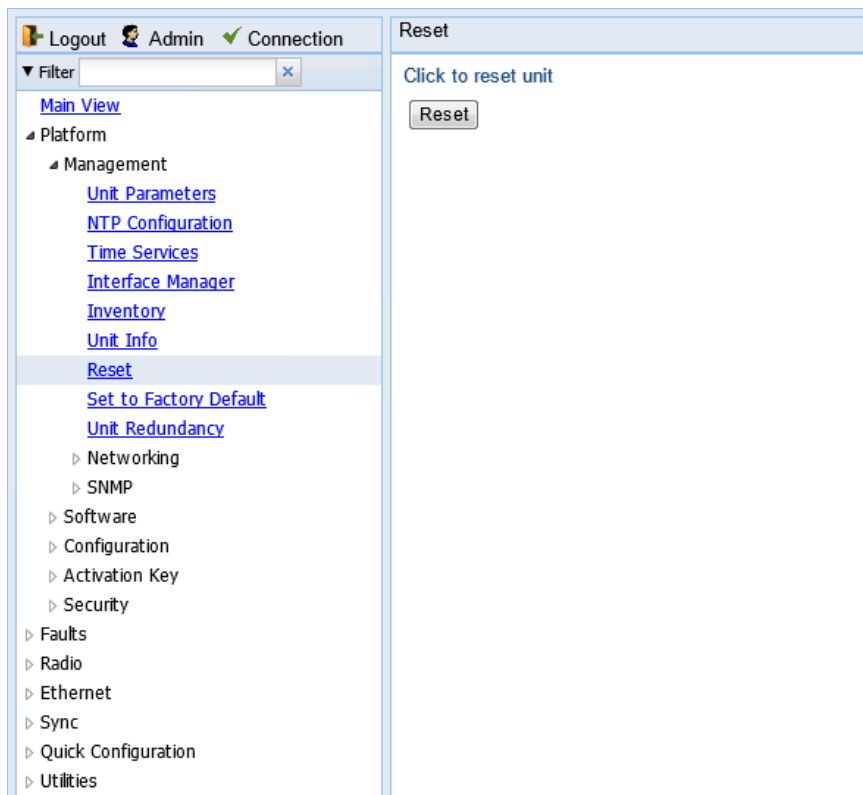
2. Click **Set to Factory Default**. The unit is restored to its factory default settings. This does not change the unit's IP address.

Performing a Hard (Cold) Reset

To initiate a hard (cold) reset on the unit:

1. Select **Platform > Management > Reset**. The Reset page opens.

Figure 119 Reset Page



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 18](#) describes the fields in the Unit Parameters page.

Figure 120 Unit Parameters Page

Table 18 Unit Parameters

Parameter	Definition
Name	A name for the unit (optional). 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 chassis 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.
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. If the voltage exceeds 60V, the unit raises a high voltage alarm (Alarm ID 27). This alarm is cleared when the voltage goes lower than 58V. If the voltage goes lower than 32V, the unit raises a low voltage alarm (Alarm ID 26). This alarm is cleared when the voltage rises above 34V.
User Comment	A free text field for any information you want to record (up to 500 characters)

Configuring NTP

PTP 820 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.

To view and configure the NTP Parameters:

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

Figure 121 NTP Configuration Page

2. In the **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 19 describes the status parameters that appear in the NTP Configuration page.

Table 19 NTP Status Parameters

Parameter	Definition
Poll interval	Displays the interval used by the NTP client to maintain synchronization with the current NTP server.

Parameter	Definition
Sync on NTP server IP address	Displays the IP address of the remote NTP server on which the NTP client is currently locked.
Client lock status	<p>Indicates if the NTP client is locked on a remote NTP server. Possible values are:</p> <ul style="list-style-type: none">• LOCK – The NTP client is locked on the remote server.• LOCAL – The NTP client is locked on the local system clock (free running clock).• N/A – The NTP client is not locked on any clock.

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 122 Inventory Page

The screenshot shows a web interface with a top navigation bar containing 'Logout', 'Admin', and 'Connection' status. Below this is a left sidebar menu with a 'Filter' box and a tree structure. The tree structure includes 'Main View', 'Platform' (expanded), 'Management' (expanded), and a list of sub-items: 'Unit Parameters', 'NTP Configuration', 'Time Services', 'Interface Manager', 'Inventory' (highlighted), 'Unit Info', 'Reset', 'Set to Factory Default', 'Unit Redundancy', 'Networking', 'SNMP', 'Software', 'Configuration', 'Activation Key', 'Security', 'Faults', 'Radio', 'Ethernet', 'Sync', 'Quick Configuration', and 'Utilities'. The main content area is titled 'Inventory' and displays two input fields: 'Part number' with the value '22-0001-0A' and 'Serial number' with the value 'F073900955'. Below these fields is a 'Refresh' button.

Inventory	
Part number	22-0001-0A
Serial number	F073900955
<button>Refresh</button>	

Chapter 5: Radio Configuration

This section includes:

- [Viewing the Radio Status and Settings](#)
- [Configuring the Remote Radio Parameters](#)
- [Configuring ATPC](#)
- [Configuring Header De-Duplication and Frame Cut-Through](#)
- [Configuring AES-256 Payload Encryption](#)
- [Configuring and Viewing Radio PMs and Statistics](#)

Related topics:

- [Configuring the Radio Parameters](#)
- [Configuring the Radio \(MRMC\) Script\(s\)](#)
- [System Configurations](#)
- [Configuring Multi-Carrier ABC](#)
- [Configuring XPIC](#)
- [Configuring Unit Protection with HSB Radio](#)
- [Configuring MIMO and Space Diversity](#)
- [Configuring Advanced Frequency Reuse \(AFR\)](#)

Viewing the Radio Status and Settings

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



Note

For instructions how to configure the radio parameters, see [Configuring the Radio Parameters](#).

To display the radio parameters:

1. Select **Radio > Radio Parameters**. The Radio Parameters page opens.
 - For PTP 820C units, the Radio Parameters page initially displays a table as shown in [Figure 123](#).
 - For PTP 820S units, a page appears, similar to [Figure 25](#) (which shows a PTP 820C page).

Figure 123 Radio Parameters Page – PTP 820C

Logout

Admin

Connection

Filter

Main View

Platform

Faults

Radio

Radio Parameters

Remote Radio Parameters

Radio Thresholds

ATPC

ABC Mode

Ethernet Interface

MRMC

PM & Statistics

Diagnostics

Groups

Ethernet

Sync

Quick Configuration

Utilities

Radio Parameters

Related Pages

Radio table

Radio location	Type	TX Frequency	RX Frequency	Operational TX Level (dBm)	RX Level (dBm)	Modem MSE	Defective Blocks	TX Mute Status
Radio: Slot 2, port 1	RFU-N-DC	8200.000	7910.000	15	-36	-41.96	<div>Clear</div>	0 Off
Radio: Slot 2, port 2	RFU-N-DC	8222.095	7910.775	15	-36	-42.71	<div>Clear</div>	0 Off

Edit

Refresh

2. For PTP 820C units, select the carrier in the Radio table (see [Figure 123](#)) and click **Edit**. A separate Radio Parameters page opens. The page is essentially identical to the PTP 820S page, except for the addition of a **Radio location** parameter.

Figure 124 Radio Parameters Page Per Carrier – PTP 820C

Radio Parameters

Status Parameters

Radio Location

Radio: Slot 2, Port 1

Type

RFU-N-DC

XPIC support

Yes

Radio Interface operational status

Up

Operational TX Level (dBm)

10

RX Level (dBm)

-39

Modem MSE (dB)

-42.40

Modem XPI (dB)

30.80

Defective Blocks

0

Clear Counter

TX Mute Status

Off

Adaptive TX power operational status

Down

Frequency control (Local)

TX Frequency (MHz)

13070.000

(13002.000 ... 13141.000)

RX Frequency (MHz)

12800.000

(12747.000 ... 12866.000)

Frequency Separation (MHz)

270.000

☐ Set also remote unit

Configuration Parameters

TX Level (dBm)

10

(2 ... 18)

TX mute

Off

RSL Connector Source

PHY1

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: 08:25:15

Refresh

Close

Table 20 lists and describes the parameters in the Radio table of the PTP 820C Radio Parameters page and the **Status parameters** section of the Radio Parameters configuration page.

Table 20 Radio Status Parameters

Parameter	Definition
Type	The RF module type.
XPIC Support	Indicates whether the carrier is operating in XPIC mode. For instructions on configuring XPIC, refer to Configuring XPIC . Note: Only relevant for PTP 820C units.
TX Frequency	The configured TX radio frequency. The TX radio frequency is configured in the Frequency control (Local) section of the Radio Parameters page. See Configuring the Radio Parameters .
RX Frequency	The configured RX radio frequency. The RX radio frequency is configured in the Frequency control (Local) section of the Radio Parameters page. See Configuring the Radio Parameters .
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. Note: Only relevant for PTP 820C units.
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.

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**. The Remote Radio Parameters page opens.
 - For PTP 820C units, the Radio Parameters page initially displays a table as shown in [Figure 125](#).
 - For PTP 820S units, the page appears as shown in [Figure 126](#)

Figure 125 Remote Radio Parameters Page – PTP 820C

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 IP Address	Remote IPv6 Address
Radio: Slot 2, port 1	Radio: Slot 2, port 1	Up	-39		18	Off	192.168.1.33	fec0::c0a8:1:1
Radio: Slot 2, port 2	Radio: Slot 2, port 2	Up	-38		17	Off	192.168.1.33	fec0::c0a8:1:1

Figure 126 Remote Radio Parameters Page – PTP 820S

Remote Radio Parameters (Radio: Slot 2, port 1)

Remote Status

Radio location: Radio: Slot 2, port 1

Remote radio location: Radio: Slot 2, port 1

Local remote Channel Operational status: Up

Remote Receiver Signal Level: -42

Remote Most severe alarm: warning

Remote Unit link ID: 1 (1..65535)

Remote Configuration

Remote Tx output level: 10 (-50..34)

Remote Radio Mute: Off

Remote IP Address: 192.168.1.35

Remote IPv6 Address: fe80::c0a8:124

Apply Reset Remote Unit Refresh

- For PTP 820C units, select the carrier in the Remote Radio table (see [Figure 125](#)) and click **Edit**. A separate Remote Radio Parameters page opens. The page is identical to the PTP 820S page.

Figure 127: Remote Radio Parameters Page Per Carrier – PTP 820C

Remote Radio

Remote Status

Radio location: Radio: Slot 2, port 1

Remote radio location: Radio: Slot 2, port 1

Local remote Channel Operational status: Up

Remote Receiver Signal Level: -39

Remote Most severe alarm: major

Remote Unit link ID: 1 (1..65535)

Remote Configuration

Remote Tx output level: 13 (-50..34)

Remote Radio Mute: Off

Remote IP Address: 192.168.1.222

Remote IPv6 Address: 2001:200::222

Buttons: Apply, Reset Remote Unit, Refresh, Close

- Configure the remote radio parameters. For a description of these parameters, see [Table 21 Remote Radio Parameters](#).
- Click **Apply**.

You can also reset the remote unit from the Remote Radio Parameters – Edit page:

To reset the remote unit, click **Reset Remote Unit**.

Table 21 Remote Radio Parameters

Parameter	Definition
Radio Location	Read-only. Identifies the carrier.
Remote Radio Location	Read-only. Identifies the location of the remote radio.
Local Remote Channel Operational Status	Read-only. The operational status of the active (in a protection configuration) remote channel.
Remote Receiver Signal Level	Read-only. The Rx level of the remote radio, in dBm.

Parameter	Definition
Remote Most Severe Alarm	Read-only. The level of the most severe alarm currently active on the remote unit.
Remote Unit Link ID	Edit page only. Identifies the link, in order to distinguish it from other links. Enter a unique identifier from 1 to 65535.
Remote Tx Output Level	The remote unit's Tx output level, if the remote unit has been configured to operate at a fixed Tx 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

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 820C and PTP 820S provide an ATPC override mechanism. If ATPC override is enabled, a timer begins whenever 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.

You cannot use ATPC in MIMO mode. See [Configuring MIMO and Space Diversity](#)

To enable and configure ATPC and display ATPC settings:

1. Select **Radio > ATPC**. The ATPC page opens.
 - For PTP 820C units, the Radio Parameters page initially displays a table as shown in [Figure 128](#).
 - For PTP 820S units, a page appears, similar to [Figure 129](#) (which shows a PTP 820C page).

Figure 128 ATPC Page – PTP 820C

Radio ATPC									
▼ ATPC table									
Radio Location ▲	ATPC Admin	Reference RX Level (dBm)	ATPC Override Admin	ATPC Override State	Override TX Level (dBm)	Override Timeout (seconds)	Remote Radio Location	Remote ATPC Admin	Remote Reference RX Level (dBm)
Radio: Slot 2, Port 1	Enable	-42	Enable	Disabled	15	0	Radio: Slot 2, Port 1	Enable	-42
Radio: Slot 2, Port 2	Disable	-42	Disable	Disabled	15	0	Radio: Slot 2, Port 1	Disable	-42

- For PTP 820C units, select the carrier you wish to configure in the ATPC table (see [Figure 128](#)) and click **Edit**. A separate ATPC –Edit page opens.

Figure 129 ATPC – Edit Page per Carrier – PTP 820C

Radio ATPC

Local ATPC

Radio Location: Radio: Slot 2, Port 1
ATPC Admin: Enable ▼
Reference RX Level (dBm): -42 ▼
ATPC Override Admin: Enable ▼
ATPC Override State: Disabled
Override TX Level (dBm): 15 ▼
Override Timeout (seconds): 0 ▼

Remote ATPC

Remote Radio Location: Radio: Slot 2, Port 1
Remote ATPC Admin: Enable ▼
Remote Reference RX Level (dBm): -42 ▼

Apply Cancel Override

Page Refresh Interval (Seconds): None ▼ Last Loaded: 09:15:25 Refresh Close

- In the **ATPC Admin** field, select **Enable** to enable ATPC or **Disable** to disable ATPC.
- Click **Apply**. If you selected **ATPC -Admin – Enable**, the **Reference RX Level (dBm)** and **ATPC Override Admin** fields are now displayed.
- 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, MPMC script, and RFU type.
- 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.

7. Click **Apply**. If you selected **ATPC Override Admin – Enable**, the **ATPC Override State**, **Override TX Level**, and **ATPC Override Admin** fields are now displayed.
8. 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, MPMC script, and RFU type.
9. 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.
10. In the **Remote ATPC Admin** field, select **Enable** to enable ATPC or **Disable** to disable ATPC on the remote radio carrier.
11. Click **Apply**. If you selected **Remote ATPC Admin – Enable**, the **Remote Reference RX Level (dBm)** field is now displayed.
12. 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.
13. Click **Apply**.

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

Configuring Header De-Duplication and Frame Cut-Through

Header De-Duplication enables operators to significantly improve Ethernet throughput 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 configuration must be identical on both sides of the link.

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. Transmission of the pre-empted frames is resumed after the cut-through with no capacity loss or re-transmission required.



Note

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.

To configure Header De-Duplication and Frame Cut-Through:

1. Select **Radio > Ethernet Interface > Configuration**. The Radio Ethernet Interface Configuration page opens.
 - For PTP 820C units, the Radio Ethernet Interface Configuration page initially displays a table as shown in [Figure 130](#).
 - For PTP 820S units, a page appears, similar to [Figure 131](#) (which shows a PTP 820C page).

Figure 130 Radio Ethernet Interface Configuration Page – PTP 820C

Interface location	Header Deduplication type	Header Deduplication mode	Header Deduplication operational state	Cut through mode state
Radio: Slot 2, port 1	No Deduplication	Disabled	Disabled	No
Radio: Slot 2, port 2	No Deduplication	Disabled	Disabled	No

**Note**

The **Header De-duplication type** column in the Main page and the **Header De-duplication type** field in the Edit page are not operational. To monitor the Header De-Duplication setting and status, use the **Header De-duplication mode** and **Header De-duplication operational state** columns and fields.

2. For PTP 820C units, select the carrier in the Radio Ethernet and Compression table (see [Figure 130](#)) and click **Edit**. A separate Radio Ethernet Interface Configuration page opens. The page is essentially identical to the PTP 820S page.
3. Click **Edit**. The Radio Ethernet Interface Configuration – Edit page opens.

Figure 131 Radio Ethernet Interface Configuration – Edit Page Per Carrier – PTP 820C

The screenshot shows the 'Radio Ethernet Interface Configuration' window. At the top, the title is 'Radio Ethernet Interface Configuration'. Below it, the 'Interface location' is set to 'Radio: Slot 2, port 1'. A section titled 'Header Compression' contains the following fields: 'Header Deduplication type' is 'No Deduplication', 'Header Deduplication mode' is 'Disabled' (with a dropdown arrow), 'Header Deduplication operational state' is 'Disabled', 'User flow type' is '0' (with a range '(0..65535)' to its right), 'Utilization threshold' is '100' (with a range '(-1..100)' to its right), and 'Cut through mode' is 'No' (with a dropdown arrow). At the bottom left of the form are three buttons: 'Apply', 'Refresh', and 'Close'. The window has a standard scrollbar on the right and a status bar at the bottom.

4. In the **Cut through mode** field, select **Yes** to enable Frame Cut-Through or **No** to disable Frame Cut-Through.
5. In the **Header Compression 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.
6. 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.
 - For PTP 820C units, the Radio Ethernet Interface Configuration page initially displays a table as shown in [Figure 132](#).
 - For PTP 820S units, the page appears as shown in [Figure 133](#).

Figure 132 Radio Ethernet Interface Counters Page – PTP 820C

Radio Ethernet Interface Counters										
▼ Header Compression counters										
Interface location ▲	TX bytes before enhanced HC	TX compressed bytes	TX frames before enhanced HC	TX frames compressed by enhanced HC	TX learning frames	TX frames not compressed due to excluding rule	TX frames not compressed due to other reasons	TX number of active flows	Number of active flows of user selected flow type	Cut through TX frames
Radio: Slot 2, port 1	0	0	0	0	0	0	0	0	0	0
Radio: Slot 2, port 2	0	0	0	0	0	0	0	0	0	0

Figure 133 Radio Ethernet Interface Counters Page – PTP 820S

Radio Ethernet Interface Counters

Interface location: Radio Slot 2, port 1

Header Compression Counters

TX bytes before enhanced HC	4760
TX compressed bytes	4760
TX frames before enhanced HC	70
TX frames compressed by enhanced HC	0
TX learning frames	0
TX frames not compressed due to excluding rule	0
TX frames not compressed due to other reasons	70
TX number of active flows	0
Number of active flows of user selected flow type	0

Ethernet Port Counters

Port RX good bytes	0
Port RX good frames	0
Port TX total bytes	4760
Port TX frames	70
Port TX idle bytes	0

Cut Through Counters

Cut through TX frames	0
-----------------------	---

Clear Counters Refresh Close

- For PTP 820C units, select the carrier in the Header Compression Counters table (Figure 132) and click **View**. A separate Radio Ethernet Interface Configuration page opens. The page is essentially identical to the PTP 820S page.

Figure 134 Radio Ethernet Interface Counters Page Per Carrier – PTP 820C

Radio Ethernet Interface Counters

Interface location

Radio: Slot 2, port 1

Header Compression Counters

TX bytes before enhanced HC

4760

TX compressed bytes

4760

TX frames before enhanced HC

70

TX frames compressed by enhanced HC

0

TX learning frames

0

TX frames not compressed due to excluding rule

0

TX frames not compressed due to other reasons

70

TX number of active flows

0

Number of active flows of user selected flow type

0

Ethernet Port Counters

Port RX good bytes

0

Port RX good frames

0

Port TX total bytes

4760

Port TX frames

70

Port TX idle bytes

0

Cut Through Counters

Cut through TX frames

0

Clear Counters

Refresh

Close

Table 22 lists and describes the fields in the Radio Ethernet Interface Counters page.

Table 22: Radio Ethernet Interface Counters Fields

Parameter	Definition
Interface Location	Identifies the radio interface.
Header Compression Counters	
TX bytes before enhanced HC	Bytes on the TX side before Header De-Duplication.
TX compressed bytes	Bytes on the TX side that were compressed by Header De-Duplication.

Parameter	Definition
TX frames before enhanced HC	Frames on the TX side before Header De-Duplication.
TX frames compressed by enhanced HC	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	
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 820C and PTP 820S units.

This feature is not supported with MIMO or space diversity links.

This feature requires:

- Requires an activation key per radio. If no valid AES activation key has been applied to the unit, AES will not operate on the unit. See [Configuring the Activation Key](#). For PTP 820S and PTP 820C, any radio manufactured after July 1, 2015, is AES hardware-ready. An easy way to validate this is to check the radio's S/N number. S/N's starting F265xxx and above are AES hardware-ready.

**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 820C and PTP 820S support AES-256 payload encryption. AES is enabled and configured separately for each radio carrier.

PTP 820 uses a dual-key encryption mechanism for AES:

- 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.

AES key generation is completely hitless, and has no effect on ACM operation.

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. In a protected link, enable protection lockout, first on the remote and then on the local unit. See [Disabling Automatic Switchover to the Standby Unit](#).
4. On the remote unit, select **Radio > Payload Encryption**. The Payload Encryption page opens.

- For PTP 820C units, the Payload Encryption page initially displays a table as shown in [Figure 135](#) Payload Encryption Page
- For PTP 820S units, a page appears, similar to [Figure 136](#)(which shows in PTP 820C page).

Figure 135 Payload Encryption Page

Interface ID ▲	Admin Mode	Crypto Validation State	Session Key Period
Radio: Slot 2, port 1	AES-256	Not Valid	01:00
Radio: Slot 2, port 2	Disable	Not Valid	01:00

5. Select the carrier you want to configure and click **Edit**. The Payload Encryption – Edit page opens.

Figure 136 Payload Encryption – Edit Page

6. Configure the master key by doing one of the following:
 - Enter a master key in the **Master Key** field. You must enter between 8 and 32 ASCII characters.

- Click **Generate key** to generate a master key automatically.

You must use the same master key on both sides of the link. This means that if you generate a master key automatically on one side of the link, you must copy that key and for use on the other side of the link. Once payload encryption has been enabled on both sides of the link, the Key Exchange Protocol periodically verifies that both ends of the link have the same master key. If a mismatch is detected, an alarm is raised and traffic transmission is stopped for the mismatched carrier at both sides of the link. The link becomes non-valid and traffic stops being forwarded.

When you enter a master key, or when the master key is automatically generated, the key is hidden behind dots. To copy the master key, you must display the key. To display the master key, click **Show Key**. A new **Master key** field appears, displaying the master key. You can copy the key to the clipboard from this field.

Figure 137 Payload Encryption – Edit Page with Master Key Displayed

- Record and save the master key generated in Step 6.
- On the local unit, follow Steps 4 through 6 to configure the same master key configured on the remote unit also on the local unit.
- Enable payload encryption on the remote unit:
 - In the **Admin Mode** field, select **AES-256** to enable payload encryption.
 - 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.



Note

The Session Key Period must be the same on both sides of the link.

- 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.

10. Enable payload encryption on the local unit by following the procedure described in [Step 9](#). 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.
11. In a protected link, perform copy-to-mate, first on the remote and then on the local unit. See [Step 5](#) in [Configuring HSB Radio Protection](#). After the copy-to-mate operation, wait for both standby units to re-boot and verify that there are no alarms.

**Note**

The standby unit may have a *payload encryption failure* alarm for up to about one minute after the unit is up and running.

12. In a protected link, remove the protection lockout, first on the remote and then on the local unit. See [Disabling Automatic Switchover to the Standby Unit](#).
13. Verify that there are no alarms on the link.

**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

This section includes:

- [Configuring BER Thresholds and Displaying Current BER](#)
- [Displaying MPMC Status](#)
- [Displaying MPMC PMs](#)
- [Displaying and Clearing Defective Block Counters](#)
- [Displaying Signal Level PMs and Configuring Signal Level PM Thresholds](#)
- [Displaying Modem BER \(Aggregate\) PMs](#)
- [Displaying MSE PMs and Configuring MSE PM Thresholds](#)
- [Displaying XPI PMs and Configuring XPI PM Threshold](#)
- [Displaying Traffic PMs](#)



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](#).
- XPI PM Thresholds are configured from the XPI PM Report page. See [Displaying XPI PMs and Configuring XPI PM Threshold](#).

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 138 Radio BER Thresholds Page

Radio Location	Excessive BER Threshold	Signal Degrade BER Threshold	Radio BER
Radio: Slot 2, Port 1	1e-3	1e-6	1e-2
Radio: Slot 2, Port 2	1e-3	1e-6	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 Thresholds table, select the radio for which you want to configure thresholds.
4. Click **Edit**. The Radio BER Thresholds – Edit page opens.

Figure 139 Radio BER Thresholds – Edit Page

5. In the Excessive BER Threshold field, select the level above which an excessive BER alarm is issued for errors detected over the radio link.

6. 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.
7. Click **Apply**, then **Close**.

Displaying MPMC Status

Related Topics:

- [Configuring the Radio \(MPMC\) Script\(s\)](#)

To display the current modulation and bit rate per radio:

1. Select **Radio > MPMC > MPMC Status**. The MPMC Status page opens.

Figure 140 MPMC Status Page

Radio location	Configured MPMC Script	Tx profile	Tx QAM	Tx bit-rate (Mbps)	Rx profile	Rx QAM	Rx bit-rate (Mbps)
Radio: Slot 2, Port 1	mdN_A2828X_157_1504 (1504)	10	2048	243.123	10	2048	243.123
Radio: Slot 2, Port 2	mdN_A2828X_157_1504 (1504)	10	2048	243.123	10	2048	243.123

Table 23 describes the MPMC status parameters.



Note

To display the same parameters for an individual radio in a separate page, select the radio in the MPMC script status table and click **Edit**. You can configure Adaptive TX Power from the MPMC Status – Edit page. See [Enabling ACM with Adaptive Transmit Power](#).

Table 23 MRMC Status Parameters

Parameter	Definition
Radio Location	Identifies the carrier (Slot 2, port 1 or Slot 2, port 2). Note: Only relevant for PTP 820C units.
Configured MRMC Script	The current MRMC script.
TX profile	The current TX profile.
TX QAM	The current TX modulation.
TX bit-rate	The current TX bit-rate.
RX profile	The current RX profile.
RX QAM	The current RX modulation.
RX bit-rate	The current RX bit-rate.

Displaying MRMC PMs

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:

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

Figure 141 MRMC PM Report Page

MRMC PM report (Radio: Slot 2, Port 1, 15 minutes)

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

PM Table

#	Interval	Min profile	Max profile	Min bitrate	Max bitrate	Integrity
	Current (20:01:52)	10	10	243123	243123	✓
1	09-Feb-00 20:00	10	10	243123	243123	✓
2	09-Feb-00 19:45	10	10	243123	243123	✓
3	09-Feb-00 19:30	10	10	243123	243123	✓
4	09-Feb-00 19:15	10	10	243123	243123	✓
5	09-Feb-00 19:00	10	10	243123	243123	✓
6	09-Feb-00 18:45	10	10	243123	243123	✓
7	09-Feb-00 18:30	10	10	243123	243123	✓
8	09-Feb-00 18:15	10	10	243123	243123	✓
9	09-Feb-00 18:00	10	10	243123	243123	✓
10	09-Feb-00 17:45	10	10	243123	243123	✓
11	09-Feb-00 17:30	10	10	243123	243123	✓
12	09-Feb-00 17:15	10	10	243123	243123	✓
13	09-Feb-00 17:00	10	10	243123	243123	✓
14	09-Feb-00 16:45	10	10	243123	243123	✓
15	09-Feb-00 16:30	10	10	243123	243123	✓

View Graph

2. For the PTP 820C, In the **Port** field, select the port that holds the radio for which you want to display PMs.
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 24 describes the MPMC PMs.



Note

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

Table 24 MPMC PMs

Parameter	Definition
PM Interval	The length of the interval for which the PMs were measured (15 Minutes or 24 Hours).
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.
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.

- For PTP 820C units, the Counters page initially displays a table as shown in [Figure 142](#).
- For PTP 820S unit, the Counters page appears as shown in [Figure 143](#).

Figure 142 Counters Page – PTP 820C

Logout Connection Admin

Filter

Unit & Radio Summary

- Platform
- Faults
- Radio
 - Radio Parameters
 - Remote Radio Parameters
 - Radio BER Thresholds
 - ATPC
 - Payload Encryption
- Ethernet Interface
- MRMC
- PM & Statistics
 - Counters**
 - Signal Level
 - Diversity
 - Combined
 - Aggregate
 - MSE
 - XPI
 - MRMC
- Traffic
- Diagnostics
- Groups
- Ethernet
- Sync
- Quick Configuration
- Utilities

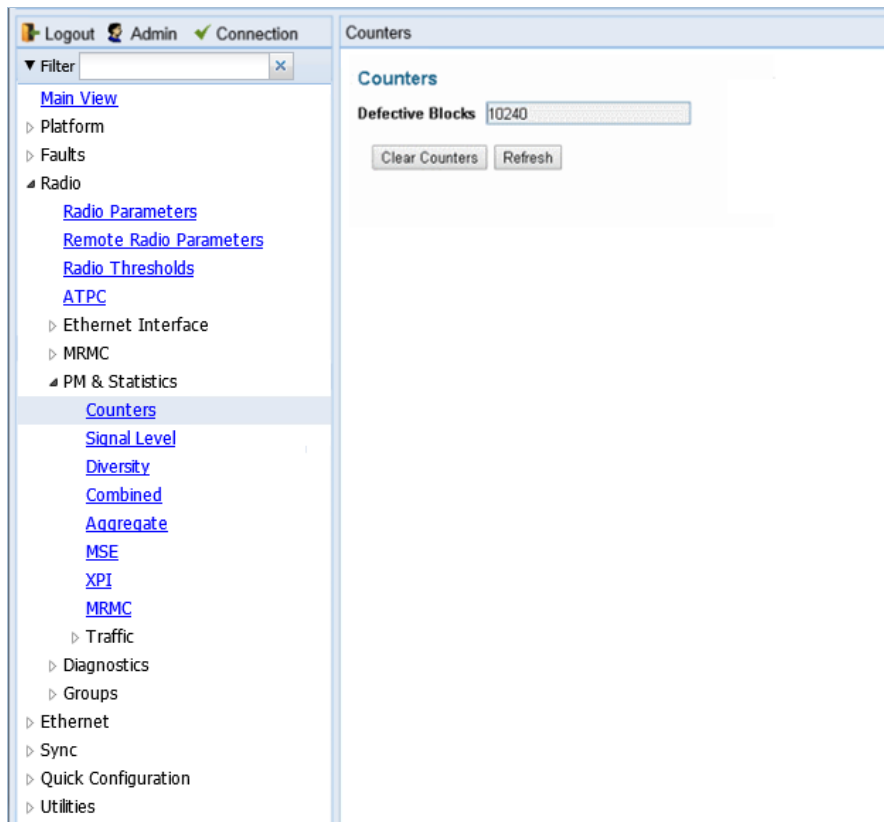
Radio Counters

Radio Counters

Radio Location ▲	Defective Blocks
Radio: Slot 2, Port 1	0
Radio: Slot 2, Port 2	19

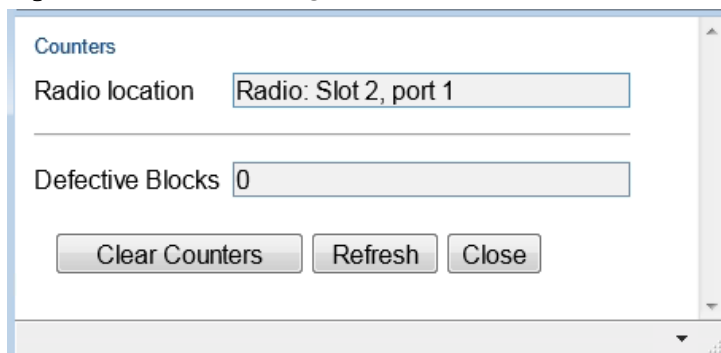
View Clear Counter

Figure 143 Counters Page – PTP 820S



- For PTP 820C units, you can select the carrier in the Radio table (see [Figure 142](#)) and click **View** to display a page for that carrier. A separate Counters page opens.

Figure 144 Counters Page Per Carrier – PTP 820C



- 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 145 Signal Level PM Report Page

#	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 (17:20:57)		10	10	-39	-39	0	0	0	✓
1	11-Jun-17 17:15	10	10	-39	-39	0	0	0	✓
2	11-Jun-17 17:00	10	10	-39	-39	0	0	0	✓
3	11-Jun-17 16:45	10	10	-39	-39	0	0	0	✓
4	11-Jun-17 16:30	10	10	-39	-39	0	0	0	✓
5	11-Jun-17 16:15	10	10	-39	-39	0	0	0	✓
6	11-Jun-17 16:00	10	10	-39	-39	0	0	0	✓
7	11-Jun-17 15:45	10	10	-39	-39	0	0	0	✓
8	11-Jun-17 15:30	10	10	-39	-39	0	0	0	✓
9	11-Jun-17 15:15	10	10	-39	-39	0	0	0	✓
10	11-Jun-17 15:00	10	10	-39	-39	0	0	0	✓
11	11-Jun-17 14:45	10	10	-39	-39	0	0	0	✓
12	11-Jun-17 14:30	10	10	-39	-39	0	0	0	✓
13	11-Jun-17 14:15	10	10	-39	-39	0	0	0	✓
14	11-Jun-17 14:00	10	10	-39	-39	0	0	0	✓
15	11-Jun-17 13:45	10	10	-39	-39	0	0	0	✓

2. For the PTP 820C, in the **Interface** field, select the radio for which you want to display PMs.
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 25 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 25 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.

Parameter	Definition
Max RSL (dBm)	The maximum RSL (Received Signal Level) that was measured during the interval.
Min RSL (dBm)	The minimum RSL (Received Signal Level) that was measured during the interval.
TSL exceed 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 26](#), and click **Apply**.

Figure 146 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 2, Port 1	-50	-68	25
Radio: Slot 2, Port 2	-50	-68	25

Apply

Page Refresh Interval (Seconds) None Last Loaded: 17:21:40 Refresh Close

95%

Table 26 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 147 Aggregate PM Report Page

#	Interval	ES	SES	UAS	BBE	Integrity
	Current (21:03:43)	0	0	0	0	✓
1	09-Feb-00 21:00	0	0	0	0	✓
2	09-Feb-00 20:45	0	0	0	0	✓
3	09-Feb-00 20:30	0	0	0	0	✓
4	09-Feb-00 20:15	0	0	0	0	✓
5	09-Feb-00 20:00	0	0	0	0	✓
6	09-Feb-00 19:45	0	0	0	0	✓
7	09-Feb-00 19:30	0	0	0	0	✓
8	09-Feb-00 19:15	0	0	0	0	✓
9	09-Feb-00 19:00	0	0	0	0	✓
10	09-Feb-00 18:45	0	0	0	0	✓
11	09-Feb-00 18:30	0	0	0	0	✓
12	09-Feb-00 18:15	0	0	0	0	✓
13	09-Feb-00 18:00	0	0	0	0	✓
14	09-Feb-00 17:45	0	0	0	0	✓
15	09-Feb-00 17:30	0	0	0	0	✓

2. For the PTP 820C, in the **Interface** field, select the radio for which you want to display PMs.
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 27](#) 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 27 Modem BER (Aggregate) PMs

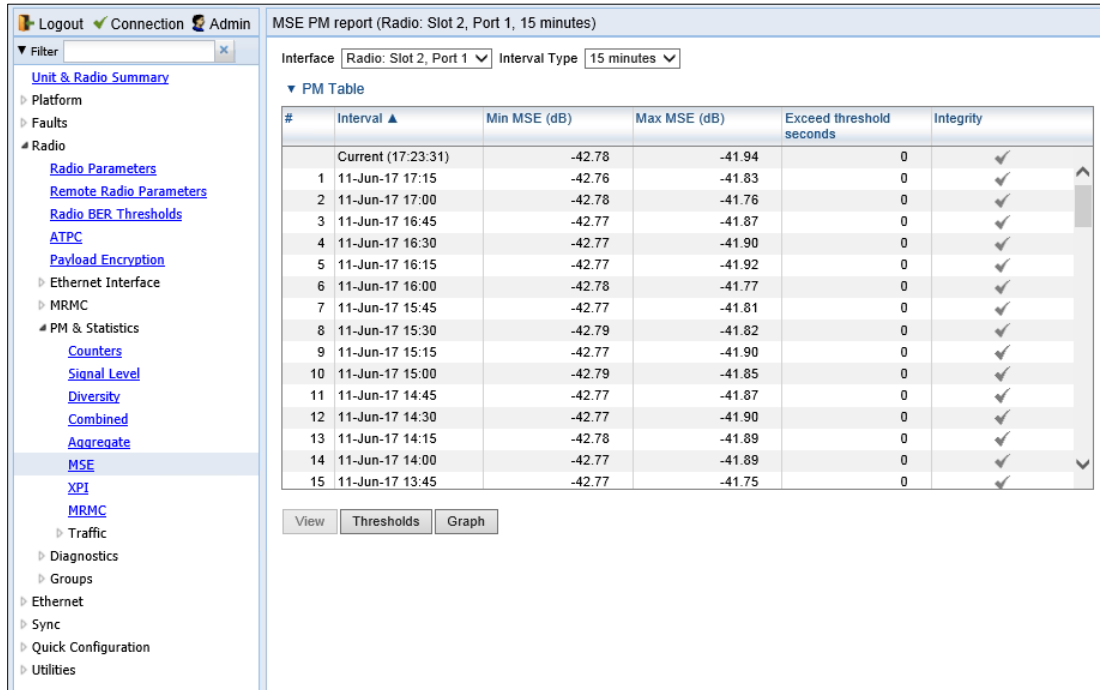
Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
ES	Displays the number of seconds in the measuring interval during which errors occurred.
SES	Displays the number of severe error seconds 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 148 MSE PM Report Page



MSE PM report (Radio: Slot 2, Port 1, 15 minutes)

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

PM Table

#	Interval ▲	Min MSE (dB)	Max MSE (dB)	Exceed threshold seconds	Integrity
	Current (17:23:31)	-42.78	-41.94	0	✓
1	11-Jun-17 17:15	-42.76	-41.83	0	✓
2	11-Jun-17 17:00	-42.78	-41.76	0	✓
3	11-Jun-17 16:45	-42.77	-41.87	0	✓
4	11-Jun-17 16:30	-42.77	-41.90	0	✓
5	11-Jun-17 16:15	-42.77	-41.92	0	✓
6	11-Jun-17 16:00	-42.78	-41.77	0	✓
7	11-Jun-17 15:45	-42.77	-41.81	0	✓
8	11-Jun-17 15:30	-42.79	-41.82	0	✓
9	11-Jun-17 15:15	-42.77	-41.90	0	✓
10	11-Jun-17 15:00	-42.79	-41.85	0	✓
11	11-Jun-17 14:45	-42.77	-41.87	0	✓
12	11-Jun-17 14:30	-42.77	-41.90	0	✓
13	11-Jun-17 14:15	-42.78	-41.89	0	✓
14	11-Jun-17 14:00	-42.77	-41.89	0	✓
15	11-Jun-17 13:45	-42.77	-41.75	0	✓

View Thresholds Graph

2. For the PTP 820C, in the **Interface** field, select the radio for which you want to display PMs.

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 28 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 28 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.

Parameter	Definition
Min MSE (dB)	Displays the minimum MSE in dB, measured during the interval. A 0 in this field and an X in the Integrity field may also indicate that the modem was unlocked during the entire interval.
Max MSE (dB)	Displays the maximum MSE in dB, measured during the interval. A 0 in this field and an X in the Integrity field may also indicate that the modem was unlocked.
Exceed threshold seconds	Displays the number of seconds the MSE exceeded the MSE PM threshold during the interval. 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 149 Modem MSE Thresholds Configuration – Edit Page

Thresholds Configuration - Edit

Radio location	MSE PM Threshold (dB)
Radio: Slot 2, Port 1	-34
Radio: Slot 2, Port 2	-34

Apply

Page Refresh Interval (Seconds) None Last Loaded: 17:23:28 Refresh Close

95%

Displaying XPI PMs and Configuring XPI PM Threshold

Related topics:

- [Configuring XPIC](#)

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

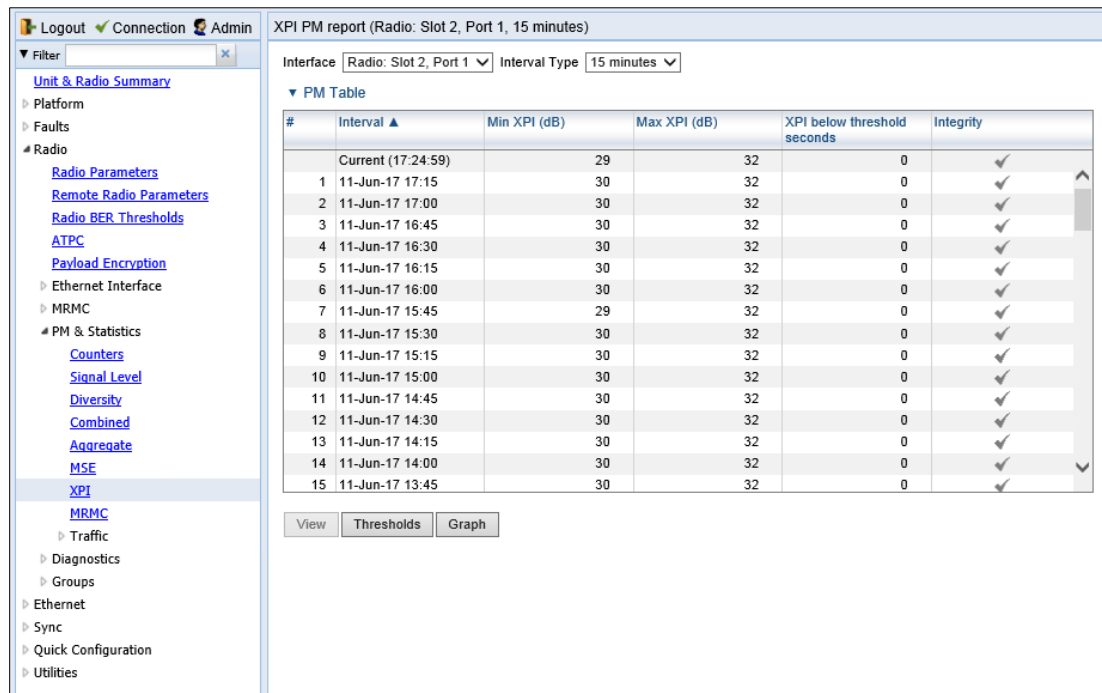
Select **Radio > PM & Statistics > XPI**. The XPI PM report page opens.



Note

The XPI page only appears if XPIC is configured on the unit.

Figure 150 XPI PM Report Page



4. For the PTP 820C, in the **Interface** field, select the radio for which you want to display PMs.

5. 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 29 describes the XPI PMs.



Note

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

Table 29 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 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. For each radio, specify the modem XPI threshold for calculating XPI Exceed Threshold seconds, and click **Apply**.

Figure 151 XPI Thresholds Configuration – Edit Page

Thresholds Configuration - Edit

Radio location	XPI PM Threshold (dB)
Radio: Slot 2, Port 1	15
Radio: Slot 2, Port 2	14

Apply

Page Refresh Interval (Seconds) None Last Loaded: 17:24:58 Refresh Close

95%

Displaying Traffic PMs

This section includes:

- [Displaying Capacity and Throughput PMs](#)
- [Displaying Utilization PMs](#)
- [Displaying Frame Error Rate 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 152 Capacity PM Report Page

Capacity PM report (Slot 2, Port 1, 15 minutes)

Slot: Slot #2 Port: 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 (18:13:54)	0	0	0	0	0	0	✓
1	20-Sep-15 16:00	0	0	0	0	0	0	✓
2	20-Sep-15 15:45	0	0	0	0	0	0	✓
3	20-Sep-15 15:30	0	0	0	0	0	0	✓
4	20-Sep-15 15:15	0	0	0	0	0	0	✓
5	20-Sep-15 15:00	0	0	0	0	0	0	✓
6	20-Sep-15 14:45	0	0	0	0	0	0	✓
7	20-Sep-15 14:30	0	0	0	0	0	0	✓
8	20-Sep-15 14:15	0	0	0	0	0	0	✓
9	20-Sep-15 14:00	0	0	0	0	0	0	✓
10	20-Sep-15 13:45	0	0	0	0	0	0	✓
11	20-Sep-15 13:30	0	0	0	0	0	0	✓
12	20-Sep-15 13:15	0	0	0	0	0	0	✓
13	20-Sep-15 13:00	0	0	0	0	0	0	✓
14	20-Sep-15 12:45	0	0	0	0	0	0	✓

View Threshold Graph Refresh

- For the PTP 820C, in the **Port** field, select the port that holds the radio for which you want to display PMs.
- 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 30 describes the capacity and throughput PMs.



Note

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

Table 30 Capacity/Throughput PMs

Parameter	Definition
Time interval index	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Peak capacity (Mbps)	Displays the highest L1 bandwidth, in Mbps, sent through the selected radio during the measured time interval.
Average capacity (Mbps)	Displays the average L1 bandwidth, in Mbps, during the measured time interval.
Seconds exceeding Threshold	Displays the number of seconds during the measured time interval during which the L1 bandwidth exceeded 0.

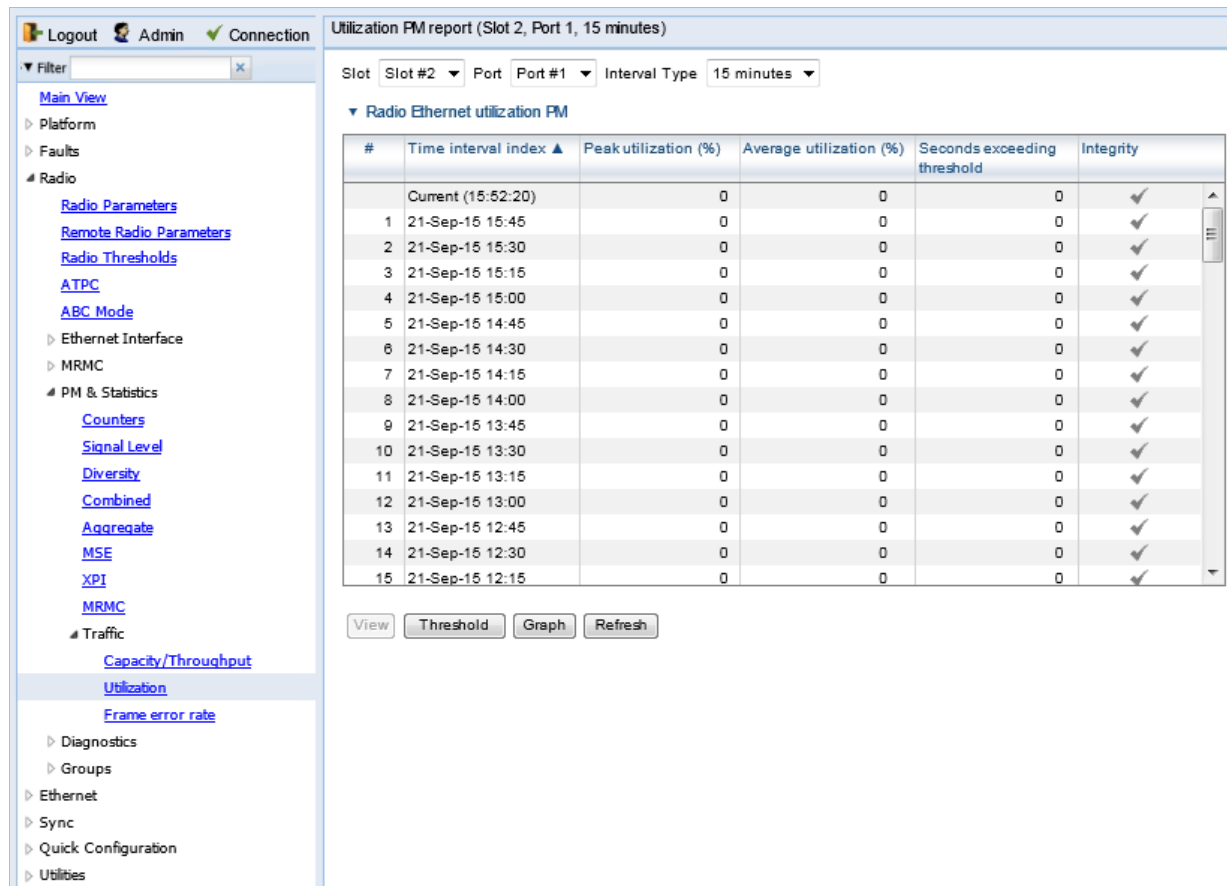
Parameter	Definition
Peak throughput (Mbps)	Displays the highest throughput, in Mbps, that occurred for the selected radio during the measured time interval.
Average throughput (Mbps)	Displays the average throughput, in Mbps, for the selected radio during the measured time interval.
Seconds exceeding Threshold	Displays the number of seconds during the measured time interval during which the throughput exceeded 0.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.

Displaying Utilization PMs

To display radio capacity utilization PMs per radio:

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

Figure 153 Utilization PM Report Page



2. For the PTP 820C, in the **Port** field, select the port that holds the radio for which you want to display PMs.
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 **Threshold**. The Ethernet Radio Capacity & Throughput Threshold page opens.

Figure 154 Ethernet Radio Capacity and Throughput Threshold Page

- 2 Enter the capacity and throughput thresholds you want, in Mbps. The range of values is 0 to 4294967295. The default value for is 1000.
- 3 Click **Apply**, then **Close**

Table 31 describes the capacity and throughput PMs.



Note

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

Table 31 Utilization PMs

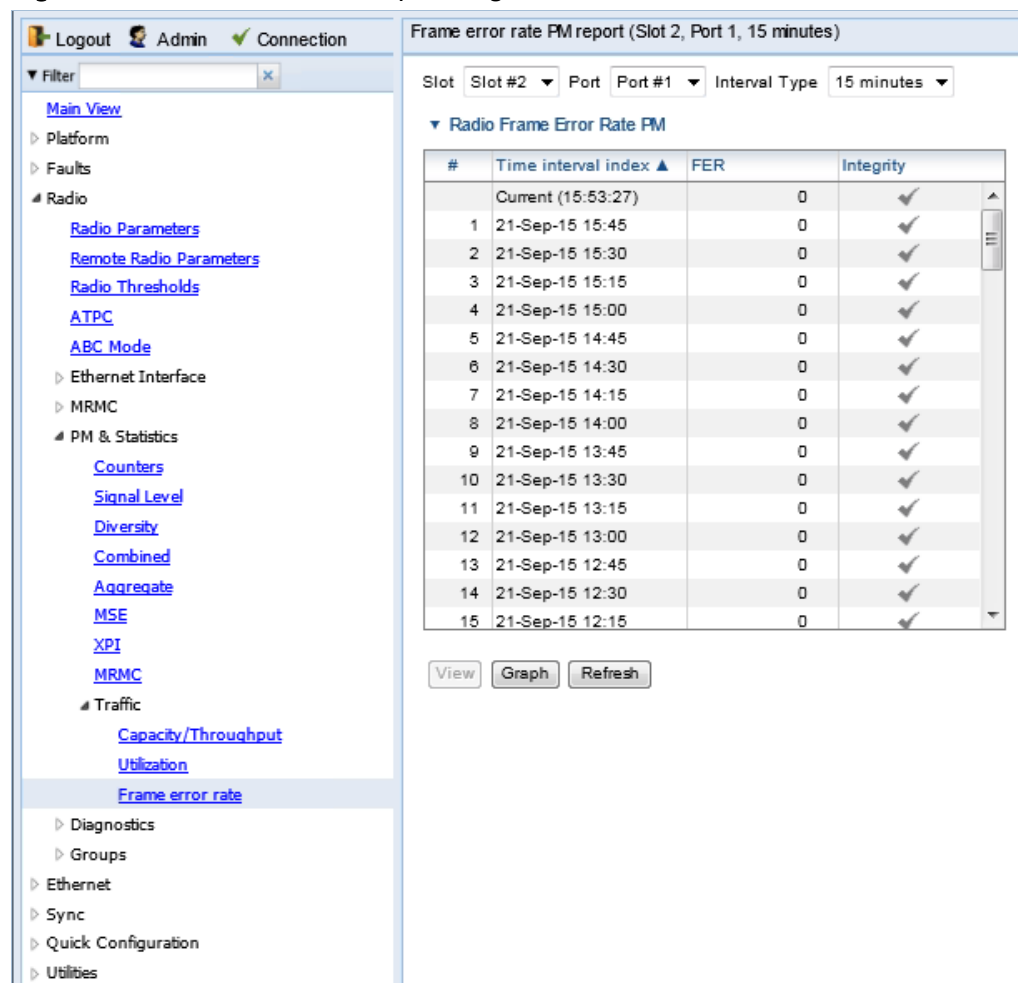
Parameter	Definition
Time interval index	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Peak capacity (Mbps)	Displays the highest L1 bandwidth, in Mbps, sent through the selected radio during the measured time interval.
Average capacity (Mbps)	Displays the average L1 bandwidth, in Mbps, during the measured time interval.

Parameter	Definition
Seconds exceeding Threshold	Displays the number of seconds during the measured time interval during which the L1 bandwidth exceeded the configured capacity threshold.
Peak throughput (Mbps)	Displays the highest throughput, in Mbps, that occurred for the selected radio during the measured time interval.
Average throughput (Mbps)	Displays the average throughput, in Mbps, for the selected radio during the measured time interval.
Seconds exceeding Threshold	Displays the number of seconds during the measured time interval during which the L1 bandwidth exceeded the configured throughput threshold.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.

Displaying Frame Error Rate PMs

To display frame error rate PMs per radio or Multi-Carrier ABC group:

1. Select **Radio > PM & Statistics > Traffic > Frame error rate**. The Frame error rate PM report page opens.

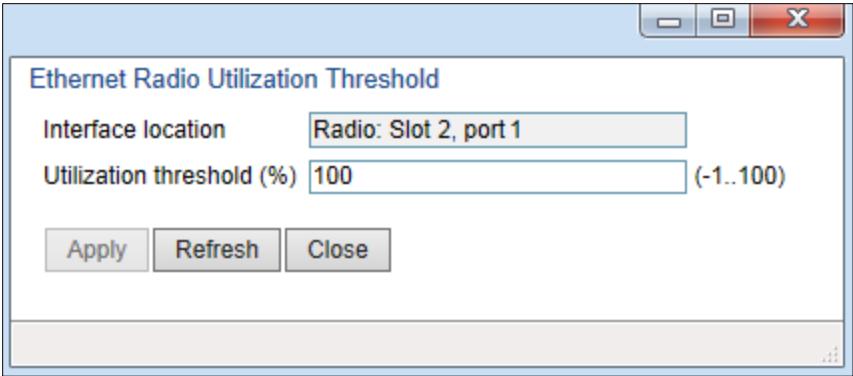
Figure 155 Frame Error PM Report Page

- For the PTP 820C, in the **Port** field, select the port that holds the radio for which you want to display PMs.
- 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:


- Select **Threshold**. The Utilization Threshold page opens.

Figure 156 Ethernet Radio Utilization Threshold Page



- 2 Enter the utilization threshold you want, in % (1-100). The default value for is 100.
- 3 Click Apply, then Close.

Table 32 describes the capacity and throughput PMs.



Note

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

Table 32 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.

Chapter 6: Ethernet Services and Interfaces

This section includes:

- [Configuring Ethernet Service\(s\)](#)
- [Setting the MRU Size and the S-VLAN Ethertype](#)
- [Configuring Ethernet Interfaces](#)
- [Configuring Automatic State Propagation and Link Loss Forwarding.](#)
- [Viewing Ethernet PMs and Statistics](#)

Related topics:

- [Deleting a Multi-Carrier ABC Group](#)
- [Configuring Link Aggregation \(LAG\)Configuring Link Aggregation \(LAG\) and LACP](#)
- [Quality of Service \(QoS\)](#)
- [Ethernet Protocols](#)
- [Performing Ethernet Loopback](#)

Configuring Ethernet Service(s)

This section includes:

- [Ethernet Services Overview](#)
- [General Guidelines for Provisioning Ethernet Services](#)
- [The Ethernet Services Page](#)
- [Adding an Ethernet Service](#)
- [Editing a Service](#)
- [Deleting a Service](#)
- [Enabling, Disabling, or Deleting Multiple Services](#)
- [Viewing Service Details](#)
- [Configuring Service Points](#)

Ethernet Services Overview

Users can define up to 64 Ethernet services. Each service constitutes a virtual bridge that defines the connectivity between logical ports in the PTP 820 network element.

This version of PTP 820 supports the following service types:

- Multipoint (MP)
- Point-to-Point (P2P)
- Management (MNG)

In addition to user-defined services, PTP 820 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 [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 to 30 service points.

For a more detailed overview of PTP 820's service-oriented Ethernet switching engine, refer to the Technical Description for the PTP 820 product type you are using.

General Guidelines for Provisioning Ethernet Services

When provisioning Ethernet services, it is recommended to follow these guidelines:

- Use the same Service ID for all service fragments along the path of the service.
- Do not re-use the same Service ID within the same region. A region is defined as consisting of all PTP 820 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 820.

To open the Ethernet Services page:

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

Figure 157 Ethernet Services Page

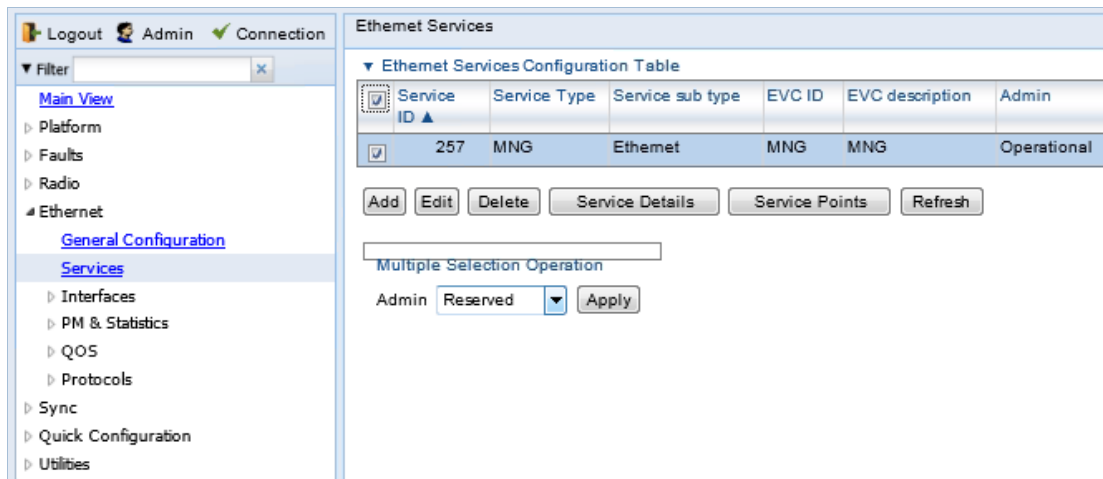


Figure 36 describes the parameters displayed in the Ethernet Services page.

Table 33 Ethernet Services Page Parameters

Parameter	Definition
Services ID	A unique ID for the service.
Service Type	The service type: <ul style="list-style-type: none">• 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 157](#)).
2. In the Ethernet Services page, click **Add**. The Ethernet Services – Add page opens.

Figure 158 Ethernet Services - Add page

Ethernet Services Configuration Table - Add

Service ID 2 ▾

Service Type P2P ▾

EVC ID N.A.

EVC description N.A.

Admin Operational ▾

MAC table size 131072 ▾

Default CoS 0 ▾

CoS Mode Preserve-SP-COS-Decision ▾

Apply Refresh Close

3. In the **Service ID** field, select a unique ID for the service. You can choose any unused value from 1 to 1024. 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 131,072, 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 157](#)).
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 158](#)). 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 157](#)).
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 157](#)).
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 159 Multiple Selection Operation Section (Ethernet Services)



Note

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

When setting multiple services to **Reserve** state, make sure to avoid setting the management service to **Reserve** state

Viewing Service Details

To view the full service parameters:

1. Select **Ethernet > Services**. The Ethernet Services page opens ([Figure 157](#)).
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 157](#)). However, in the Service Details page, these fields are read-only.

Configuring Service Points

This section includes:

- [Ethernet Services Points Overview](#)
- [The Ethernet Service Points Page](#)
- [Adding a Service Point](#)
- [Editing a Service Point](#)

- [Deleting a Service Point](#)
- [Attaching VLANs](#)

Ethernet Services Points Overview

Service points are logical interfaces within a service. A service point is a logical entity attached to a physical or logical interface. Service points define the movement of frames through the service. Each service point includes both ingress and egress attributes.

Each service point for a Point-to-Point or Multipoint service can be either a Service Access Point (SAP) or a Service Network Point (SNP). A Point-to-Point service can also use Pipe service points.

- An SAP is equivalent to a UNI in MEF terminology and defines the connection of the user network with its access points. SAPs are used for Point-to-Point and Multipoint traffic services.
- An SNP is equivalent to an NNI or E-NNI in MEF terminology and defines the connection between the network elements in the user network. SNPs are used for Point-to-Point and Multipoint traffic services.
- A Pipe service point is used to create traffic connectivity between two ports in a port-based manner (Smart Pipe). In other words, all the traffic from one port passes to the other port.

Management services utilize Management (MNG) service points.

A Point-to-Point or Multipoint service can hold up to 32 service points. A management service can hold up to 30 service points.

The Ethernet Service Points Page

The Ethernet Service Points page is the starting point for configuring Ethernet service points.

To open the Ethernet Service Points page:

1. Select **Ethernet > Services**. The Ethernet Services page opens ([Figure 157](#)).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens.

Figure 160 Ethernet Service Points Page

You can choose to display the following sets of attributes by selecting the appropriate button above the SP Attributes table:

- **General** – See [Ethernet Service Points – General SP Attributes Table](#)
- **Ingress** – See [2. Ethernet Service Points – Ingress Attributes](#)
- **Egress** – See [3. Ethernet Service Points – Egress Attributes](#)

To return to the Ethernet Services page at any time, click **Back to Services table** at the top of the Ethernet Service Points page.

1. Ethernet Service Points – General SP Attributes Table

The General SP Attributes table is shown in [Figure 160 Ethernet Service Points Page](#). [Table 34](#) describes the parameters displayed in the General SP Attributes table.

Table 34 General Service Point Attributes

Parameter	Definition
Service point ID	<p>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.</p> <p>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.</p>
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	<p>The service point type. Options are:</p> <ul style="list-style-type: none"> • SAP – Service Access Point. • SNP – Service Network Point. • MNG – Management service point. • PIPE – Pipe service point. <p>The following rules apply to the mixing of different types of service points on a single logical interface:</p> <p>You cannot configure both SAPs and SNPs on the same logical interface.</p> <ul style="list-style-type: none"> • 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	<p>The physical or logical interface on which the service point is located. Once you have added the service point, you cannot change this parameter.</p>
Attached interface type	<p>The encapsulation type (Ethertype) for frames entering the service point. Once you have added the service point, you cannot change this parameter.</p> <p>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.</p> <p>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 35.</p>
C-Vlan encapsulation	<p>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.</p> <p>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.</p>

Parameter	Definition
S-Vlan encapsulation	<p>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.</p> <p>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.</p>

[Table 35](#) describes the available Attached Interface Types.

Table 35 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 36](#) describes the parameters displayed in the Ingress SP Attributes table.

Figure 161 Ethernet Service Points Page – Ingress Attributes

The screenshot shows the 'Ethernet Service Points (Service ID - 257)' configuration page. On the left is a navigation menu with 'Services' selected. The main area has a 'Back to Services table' link and a 'Select Service Point Attribute' section with radio buttons for General, Ingress (selected), and Egress. Below this is a table titled 'Ethernet Service Points - Ingress Attributes' with the following columns: Service point ID, Service point name, Service point type, Learning admin, Allow flooding, Allow broadcast, CoS Mode, and Default CoS. The table is currently empty. At the bottom of the table are buttons for 'Add', 'Edit', 'Delete', 'Attached VLAN', and 'Refresh'.

Table 36 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: <ul style="list-style-type: none"> • 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	<p>Indicates how the service point handles the CoS of frames that pass through the service point. Options are:</p> <ul style="list-style-type: none"> 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.
Split horizon group	Reserved for future use.

3. Ethernet Service Points – Egress Attributes

Select **Egress** in the Ethernet Service Points page to display the Ethernet Service Points – Egress Attributes table. [Table 37](#) describes the parameters displayed in the General SP Attributes table.

Figure 162 Ethernet Service Points Page – Egress Attributes

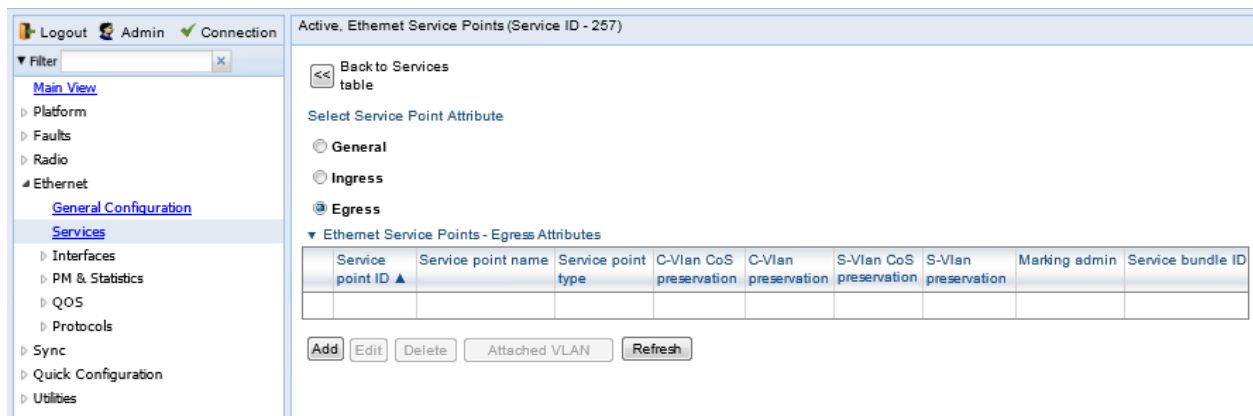


Table 37 Service Point Egress Attributes

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.

Parameter	Definition
Service point name	A descriptive name for the service point (optional). The Service Point Name can be up to 20 characters.
Service point type	<p>The service point type. Options are:</p> <ul style="list-style-type: none"> • SAP – Service Access Point. • SNP – Service Network Point. • MNG – Management service point. • PIPE – Pipe service point.
C-Vlan CoS preservation	<p>Determines whether the original C-VLAN CoS value is preserved or restored for frames egressing from the service point.</p> <p>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.</p> <p>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.</p>
C-Vlan preservation	<p>Determines whether the original C-VLAN ID is preserved or restored for frames egressing from the service point.</p> <p>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.</p> <p>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</p>
S-Vlan CoS preservation	<p>Determines whether the original S-VLAN CoS value is preserved or restored for frames egressing from the service point.</p> <p>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.</p> <p>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</p>

Parameter	Definition
S-Vlan preservation	<p>Read-only. Indicates whether the original S-VLAN ID is preserved or restored for frames egressing from the service point.</p> <p>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.</p> <p>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</p>
Marking admin	<p>Determines whether re-marking of the outer VLAN (C-VLAN or S-VLAN) of tagged frames that pass through the service point is enabled.</p> <p>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.</p> <p>If Marking admin and CoS preservation for the relevant outer VLAN are both set to Enable, re-marking is not performed.</p> <p>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.</p>
Service Bundle ID	<p>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.</p>

Adding a Service Point

To add a service point:

1. Select **Ethernet > Services**. The Ethernet Services page opens ([Figure 157](#)).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens ([Figure 160](#)).
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 163 Ethernet Service Points - Add Page

Ethernet Service Points - Add (Multi Point Service)

Pre defined options: Option #1 (SAP, dot1q)

Service ID: 1

Service point ID: 4

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: 1

S-Vlan encapsulation: N.A.

Ingress Attributes

Learning admin: Enable

Allow flooding: Allow

Allow broadcast: Allow

CoS Mode: Interface-Decision

Default CoS: 0

Split horizon group: Group-A

Egress Attributes

C-Vlan CoS preservation: Enable

C-Vlan preservation: Disable

S-Vlan CoS preservation: Enable

Marking admin: Enable

Service bundle ID: 1

Apply Refresh Close

6. Configure the service point attributes, as described in [Table 34](#), [Table 36](#), and [Table 37](#).

**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 157](#)).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens ([Figure 160](#)).
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 163](#)). 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 34](#), [Table 36](#), and [Table 37](#).
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 157](#)).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens ([Figure 160](#)).
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 157](#)).

2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens (Figure 160).
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 164 Attached VLAN List Page

Attached VLAN List (Ethernet: Slot 1, port 1, Service ID - 1, Service Point ID - 3)

<< Back to Service points table (Service ID: 1)

VLAN classification table

<input type="checkbox"/>	C-Vlan Encapsulation	S-Vlan Encapsulation	CoS overwrite Valid	CoS Value	Color

Add Edit Delete Refresh

6. Click **Add**. The Attached VLAN List - Add page opens.

Figure 165 Attached VLAN List - Add Page

Attached VLAN List

VLAN classification table - Add

Interface Location: Ethernet 1

Service ID: 1

Service Point ID: 1

C-Vlan Encapsulation: 3

S-Vlan Encapsulation: N.A.

CoS overwrite Valid: false

CoS Value: 0

Color: Green

Buttons: Apply, Refresh, Close

7. Configure the VLAN Classification parameters, described in *Table 38*.
8. Click **Apply**, then **Close**.

Table 38 VLAN Classification Parameters

Parameter	Definition
Interface Location	Read-only. The physical or logical interface on which the service point is located.
Service ID	Read-only. The ID of the service to which the service point belongs.
Service Point ID	Read-only. The ID of the service point.
C-Vlan Encapsulation	Select the C-VLAN you want to add to the service point.
S-Vlan Encapsulation	Read-only. If the Attached Interface Type for the service point is Bundle-S , this field displays the S-VLAN encapsulation selected when the service point was created. If the Attached Interface Type for the service point is Bundle-C , this field is inactive.

Parameter	Definition
CoS Overwrite Valid	If you want to assign a specific CoS and Color to frames with the C-VLAN or S-VLAN defined in the C-VLAN Encapsulation field, select true . This CoS and Color values defined below override the CoS and Color decisions made at the interface level. However, if the service point or service are configured to apply their own CoS and Color decisions, those decisions override the decision made here.
CoS Value	<p>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.</p> <p>If CoS Overwrite Valid is set to false, this parameter has no effect.</p>
Color	<p>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.</p> <p>If CoS Overwrite Valid is set to false, this parameter has no effect.</p>

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 166 Ethernet General Configuration Page

Ethernet General Configuration

General Parameters

MRU: (64..9612)

S VLAN Ether type:

C VLAN Ether type:

▼ Instance per Service mapping

Service ID ▲	Instance ID
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0

Page: **1** 2 3 4 5 Rows per page: 1000

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 820's switching fabric distinguishes between physical interfaces and logical interfaces. Physical and logical interfaces serve different purposes in the switching fabric. In some cases, a physical interface corresponds to a logical interface on a one-to-one basis. For some features, such as LAG, a group of physical interfaces can be joined into a single logical *interface*.

The basic interface characteristics, such as media type, port speed, duplex, and auto-negotiation, are configured 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 167 Physical Interfaces Page

Interface location ▲	Description	Operational Status	Admin status	Media type	Auto negotiation	Actual port speed	Actual port duplex
Ethernet: Slot 1, port 1		Down	Down	RJ45	On	10	Full Duplex
Ethernet: Slot 1, port 2		Down	Up	SFP	On	10	Full Duplex
Radio: Slot 2, port 1		Up	Up	Radio	Off	1000	Full Duplex
Radio: Slot 2, port 2		Up	Up	Radio	Off	1000	Full Duplex

2. Select the interface you want to configure and click **Edit**. The Physical Interfaces - Edit page opens.

Figure 168 Physical Interfaces - Edit Page

Physical Interfaces - Edit

Interface location: Ethernet: Slot 1, port 1

Operational Status: Down

Admin status: Down

Media type: RJ45

Actual port speed: 10

Actual port duplex: Full Duplex

Description:

Media type: RJ45 ▼

Auto negotiation: On ▼

Speed: 1000 ▼

Duplex: Full Duplex ▼

Apply Refresh Close

3. Optionally, in the **Description** field, enter a description of the interface.
4. In the **Media type** field, select the physical interface layer 1 media type. Options are:
 - **Auto-Type** – NA.
 - **RJ45** – An electrical (RJ-45) Ethernet interface.
 - **SFP** – An optical (SFP) Ethernet interface.
 - **Radio** – A radio interface.
5. 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**.
6. In the **Speed** field, select the maximum speed of the interface. Options are:
 - Ethernet RJ-45 interfaces – **100** and **1000**.
 - Ethernet SFP interfaces – Only **1000** is supported.
 - Radio interfaces – The parameter is read-only and set by the system to **1000FD**.
7. In the **Duplex** field, select the interface's duplex setting (**Full-Duplex** or **Half-Duplex**). Only **Full-Duplex** is available in this release.
8. Click **Apply**, then **Close**.

[Table 39](#) describes the status parameters that appear in the Physical Interfaces page.

Table 39 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).

Parameter	Definition
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 <i>Enabling the Interfaces (Interface Manager)</i> .
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.

The following events in the Monitored Interface trigger ASP:

- Radio LOF
- Radio Excessive BER
- Remote Radio LOF
- Remote Excessive BER
- Remove LOC

The user can also configure the ASP pair so that Radio LOF, Radio Excessive BER, or loss of the Ethernet connection at the remote side of the link will also trigger ASP.

In addition, ASP is triggered if the Controlled Interface is a LAG, and the physical interfaces that belong to the LAG are set to **Admin = Down** in the Interface Manager.

When a triggering event takes place:

- If the Controlled Interface is an electrical GbE port, the port is closed.
- If the Controlled Interface is an optical GbE port, the port is muted.

The Controlled Interface remains closed or muted until all triggering events are cleared.

In addition, when a local triggering event takes place, the ASP mechanism sends an indication to the remote side of the link. Even when no triggering event has taken place, the ASP mechanism sends periodic update messages indicating that no triggering event has taken place.

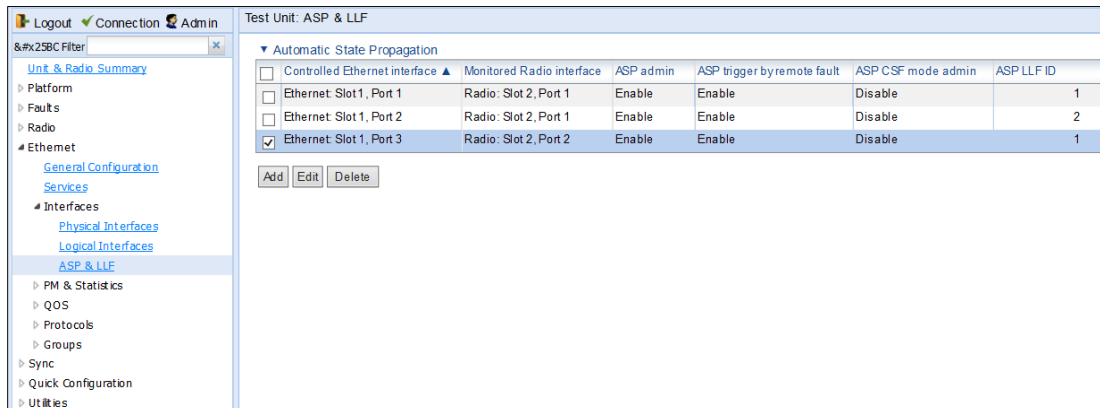
A trigger delay time can be configured, so that when a triggering event takes place, the ASP mechanism does not propagate the event until this delay time has elapsed. A trigger delay from 0 to 10,000 ms can be set per LLD ID. The delay time must be configured via CLI. See [Configuring Automatic State Propagation and Link Loss Forwarding \(CLI\)](#).

It is recommended to configure both ends of the link to the same Automatic State Propagation configuration.

To configure an Automatic State Propagation interface pair:

1. Select **Ethernet > Interfaces > Automatic State Propagation**. The Automatic State Propagation page opens.

Figure 169 Automatic State Propagation Page



2. Click **Add**. The Automatic State Propagation - Add page opens.

Figure 170 Automatic State Propagation - Add Page

3. In the **Controlled Ethernet interface** field, select an interface that will be disabled upon failure of the Monitored Radio Interface, defined below.
4. In the **Monitored Radio interface** field, select the Monitored Radio Interface. The Controlled Ethernet Interface, defined above, is disabled upon a failure indication on the Monitored Radio Interface.
5. In the **ASP admin** field, select **Enable** to enable Automatic State Propagation on the interface pair, or **Disable** to disable Automatic State Propagation on the pair.
6. Optionally, in the **ASP trigger by remote fault** field, select **Enable** if you want to configure the system to disable the Controlled Ethernet Interface upon a radio failure at the remote side of the link from the Monitored Radio Interface. ASP events will only be propagated to Controlled Interfaces with LLF IDs that match LLF IDs of affected Controlled Interfaces at the other side of the link.

7. Optionally, in the **ASP CSF mode admin** field, select **Enable** or **Disable** to enable or disable Client Signal Failure (CSF) mode. In CSF 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 (a CSF message). The CSF 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 170](#)), 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 820 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](#)
- [Egress CoS Statistics](#)
- [Port TX Statistics](#)
- [Port RX Statistics](#)

RMON Statistics

To view and reset RMON statistics:

1. Select **Ethernet > PM & Statistics > RMON**. The RMON page opens.

Figure 171 RMON Page

	Ethernet: Slot 1, port 1	Ethernet: Slot 1, port 2	Radio: Slot 2, port 1	Radio: Slot 2, port 2
Clear on read	No	No	No	No
TX byte count	222724	222660	0	0
TX frame count	3466	3465	0	0
TX multicast frame count	3465	3465	0	0
TX broadcast frame count	1	0	0	0
TX control frame count	0	0	0	0
TX pause frame count	0	0	0	0
TX fcs error frame count	0	0	0	0
TX length error frame count	0	0	0	0
TX oversize frame count	0	0	0	0
TX undersize frame count	0	0	0	0
TX fragment frame count	0	0	0	0
TX jabber frame count	0	0	0	0
TX 64 frame count	3430	3429	0	0
TX 65-127 frame count	36	36	0	0
TX 128-255 frame count	0	0	0	0
TX 256-511 frame count	0	0	0	0
TX 512-1023 frame count	0	0	0	0
TX 1024-1518 frame count	0	0	0	0
TX 1519-1522 frame count	0	0	0	0

- To clear the statistics, click **Clear All** at the bottom of the page.
- To refresh the statistics, click **Refresh** at the bottom of the page.

Each column in the RMON page displays RMON statistics for one of the unit's interfaces. To hide or display columns:

1. In the header row, select the arrow next to any of the columns.
2. Select **Columns**.

3. Mark the interfaces you want to display and clear the interfaces you do not want to display.

Figure 172 RMON Page – Hiding and Displaying Columns

RMON			
Interface physical Port RMON statistics			
	Ethernet: Slot 1, port 1	Ethernet: Slot 1, port 2	Radio: Slot 2, port 1
Clear on read		0	0
TX byte count	579562	795626	0
TX frame count	8674	86748	0
TX multicast frame count	3473		0
TX broadcast frame count	5201		0
TX control frame count			0
TX pause frame count			0
TX fcs error frame count	0	0	0
TX length error frame count	0	0	0
TX oversize frame count	0	0	0
TX undersize frame count	0	0	0
TX fragment frame count	0	0	0
TX jabber frame count	0	0	0

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 173 Egress Cos Statistics Page

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	17301239	13684841578	0	0	0	0	0	0	0	0	No
1	17307193	13690538658	0	0	0	0	0	0	0	0	No
2	17307269	13685998077	0	0	0	0	0	0	0	0	No
3	17304780	13687762286	0	0	0	0	0	0	0	0	No
4	17298291	13685264466	0	0	0	0	0	0	0	0	No
5	17295050	13679871485	0	0	0	0	0	0	0	0	No
6	17304365	13685719752	0	0	0	0	0	0	0	0	No
7	17306134	13690473705	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**.

3. 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 174 Egress CoS Statistics – Edit Page

Egress CoS Statistics - Edit	
Interface location	Ethernet: Slot 1, Port 2
Service bundle ID	1
CoS queue index	3
Transmitted green packets	17304780
Transmitted green bytes	13687762286
Transmitted green bits per second	0
Dropped green packets	0
Dropped green bytes	0
Transmitted yellow packets	0
Transmitted yellow bytes	0
Transmitted yellow bits per second	0
Dropped yellow packets	0
Dropped yellow bytes	0
Clear on read	No

Apply

Page Refresh Interval (Seconds) None Last Loaded: 12:13:02 Refresh Close

4. In the **Clear on read** field, select **Yes** to have statistics for the CoS value cleared every time you open the page.
5. 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 175 Ethernet Port TX PM Report Page

#	Interval	Peak TX bytes Layer 2	Average TX bytes Layer 2	Peak TX bytes Layer 1	Average TX bytes Layer 1	Peak TX packets	Average TX packets	Peak TX broadcast packets	Average TX broadcast packets	Peak TX multicast packets	Average TX multicast packets	Tx bytes Layer 1 exceed threshold (sec)	Invalid data flag
	Current (15:11:59)	11139913	10010064	12880573	12500067	878337	846599	0	0	0	0	719	✓
1	25-Sep-14 15:00	115511793	10010069	123580573	125001099	902439	846082	0	0	0	0	900	✓
2	25-Sep-14 14:45	110836337	10010042	120154577	125001080	865912	846081	0	0	0	0	900	✓
3	25-Sep-14 14:30	116385905	100100182	108620394	125001150	1940234133	846082	0	0	0	0	441	✓

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 40 describes the Ethernet TX port PMs.

Table 40 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).

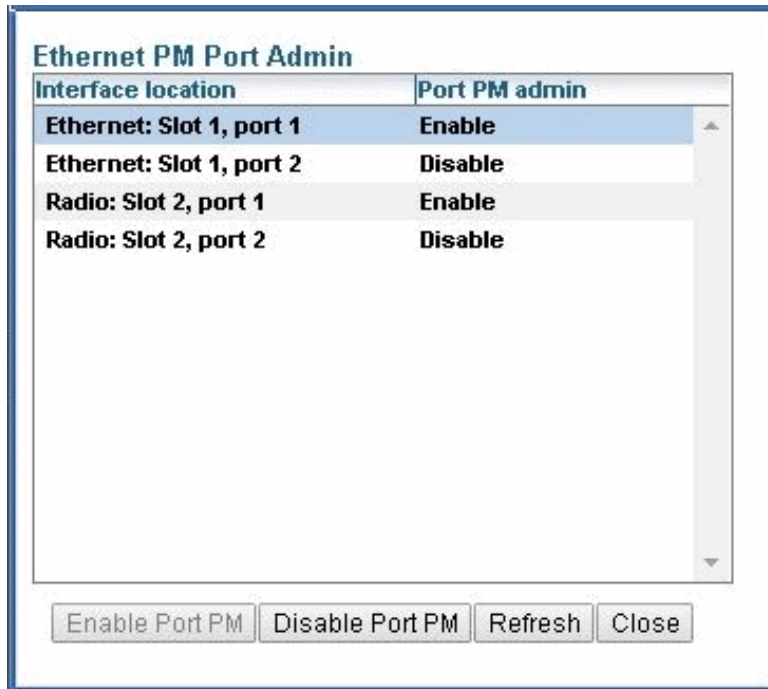
To clear the PMs, click **Clear All**.

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 176 Ethernet PM Port Admin Page



The screenshot shows a web interface titled "Ethernet PM Port Admin". It contains a table with two columns: "Interface location" and "Port PM admin". The table lists four interfaces: "Ethernet: Slot 1, port 1" (Enable), "Ethernet: Slot 1, port 2" (Disable), "Radio: Slot 2, port 1" (Enable), and "Radio: Slot 2, port 2" (Disable). Below the table are four buttons: "Enable Port PM", "Disable Port PM", "Refresh", and "Close".

Interface location	Port PM admin
Ethernet: Slot 1, port 1	Enable
Ethernet: Slot 1, port 2	Disable
Radio: Slot 2, port 1	Enable
Radio: Slot 2, port 2	Disable

Enable Port PM Disable Port PM Refresh Close

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**.

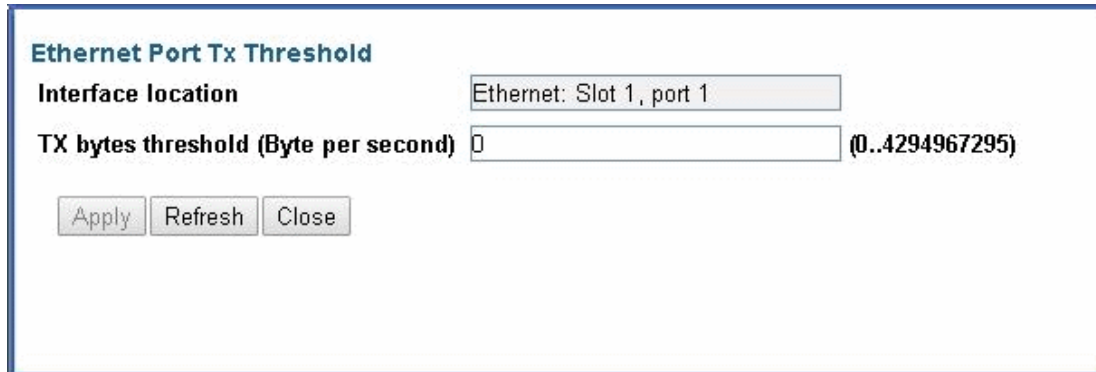
Setting the Ethernet Port TX Threshold

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 177 Ethernet Port Tx Threshold Page



Ethernet Port Tx Threshold

Interface location

TX bytes threshold (Byte per second) (0..4294967295)

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:

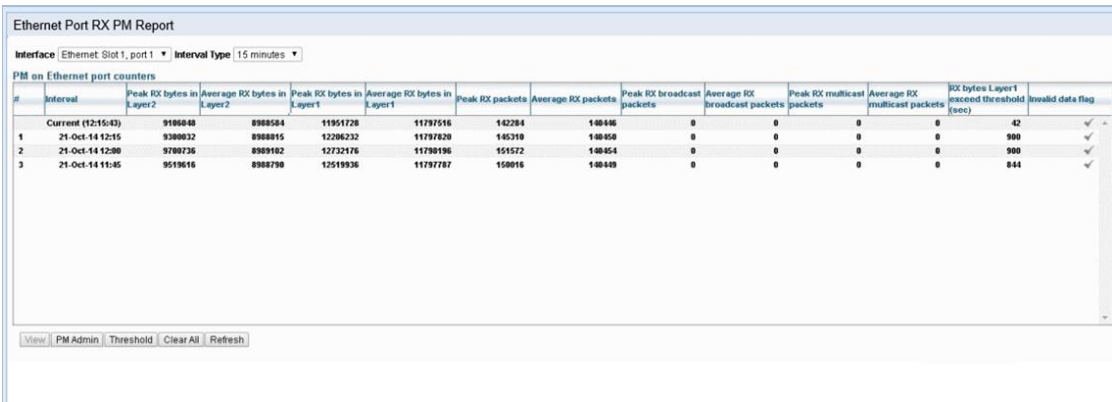
- [Displaying Ethernet Port RX PMs](#)
- [Enabling or Disabling Gathering of Port RX PM Statistics per Interface](#)
- [Setting the Ethernet Port RX Threshold](#)

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 178: Ethernet Port RX PM Report Page



2. In the **Interface** field, select the interface for which you want to display PMs.
3. In the **Interval Type** field:
 - To display reports for the past 24 hours, in 15 minute intervals, select **15 minutes**.
 - To display reports for the past month, in daily intervals, select **24 hours**.

Table 41 describes the Ethernet RX port PMs.

Table 41 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 179 Ethernet PM Port Admin Page

Interface location	Port PM admin
Ethernet: Slot 1, port 1	Enable
Ethernet: Slot 1, port 2	Disable
Radio: Slot 2, port 1	Enable
Radio: Slot 2, port 2	Disable

Buttons: Enable Port PM, Disable Port PM, Refresh, Close

2. Select the interface.
3. Click **Enable Port PM** or **Disable Port PM** to enable or disable the gathering of Port RX PMs on the selected interface.
4. 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 180 Ethernet Port Rx Threshold Page

Ethernet Port Rx Threshold

Interface location: Ethernet: Slot 1, port 1

RX bytes threshold (Byte per second): 0 (0..4294967295)

Buttons: Apply, Refresh, Close

2. Enter a threshold, between 0 and 4294967295.
3. Click **Apply**, then **Close**.

Chapter 7: Quality of Service (QoS)

This section includes:

- [QoS Overview](#)
- [Configuring Classification](#)
- [Configuring Policers \(Rate Metering\)](#)
- [Configuring Marking](#)
- [Configuring WRED](#)
- [Configuring Egress Shaping](#)
- [Configuring Scheduling](#)

**Note**

You can display QoS egress statistics, but only via CLI. For information, see [Displaying Egress Statistics \(CLI\)](#).

QoS Overview

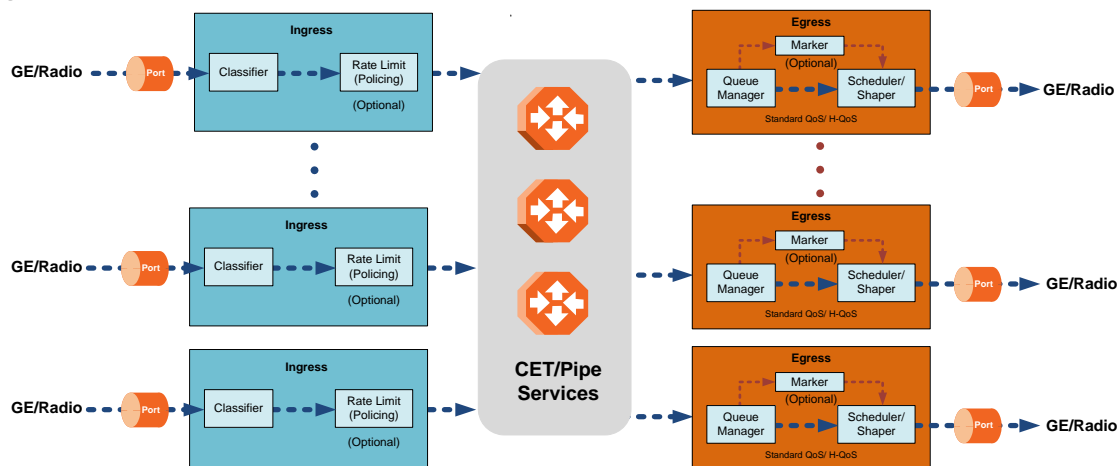
Quality of Service (QoS) deals with the way frames are handled within the switching fabric. QoS is required in order to deal with many different network scenarios, such as traffic congestion, packet availability, and delay restrictions.

PTP 820's personalized QoS enables operators to handle a wide and diverse range of scenarios. PTP 820'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 181 shows the basic flow of PTP 820'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 181 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.

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 820, refer to the Technical Description for the PTP 820 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 820 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
- MPLS EXP field
- Default interface CoS

PTP 820 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.

For example, if the frame is an untagged IP Ethernet frame, a match will not be found until the third priority level (DSCP). The CoS and Color values defined for the frame's DSCP value will be applied to the frame.

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.

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 182 Logical Interfaces Page

Logical Interfaces

▼ Ethernet Logical Port Configuration Table

Interface location ▲	Trust VLAN UP bits	Trust DSCP	Trust MPLS	Default port CoS	Ingress byte compensation	Egress byte compensation
Ethernet: Slot 1, port 1	Trust	Trust	Trust	0	20	0
Ethernet: Slot 1, port 2	Trust	Trust	Trust	0	20	0
Radio: Slot 2, port 1	Trust	Trust	Trust	0	20	0
Radio: Slot 2, port 2	Trust	Trust	Trust	0	20	0

Edit Policers WRED Shaper Scheduler Loopback Refresh

2. Select the interface you want to configure and click **Edit**. The Logical Interfaces - Edit page opens.

Figure 183 Logical Interfaces - Edit Page

3. Configure the parameters described in [Table 42](#).
4. Click **Apply**, then **Close**.



Note

The **Edge mode** field is reserved for future use. The **Ingress byte compensation** and **Egress byte compensation** fields are described in [Configuring the Ingress and Egress Byte Compensation](#).

Table 42 Logical Interface Classification Parameters

Parameter	Definition
Trust VLAN UP bits	<p>Select the interface's trust mode for user priority (UP) bits:</p> <p>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). VLAN UP bit classification has priority over DSCP and MPLS classification, so that if a match is found with the UP bit of the ingressing frame, DSCP values and MPLS bits are not considered.</p> <p>Un-Trust – The interface does not consider 802.1 UP bits during classification.</p>

Parameter	Definition
Trust DSCP	<p>Select the interface's trust mode for DSCP:</p> <p>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.</p> <p>Un-Trust – The interface does not consider DSCP during classification.</p>
Trust MPLS	<p>Select the interface's trust mode for MPLS bits:</p> <p>Trust – The interface performs QoS and color classification according to a user-configurable table for MPLS EXP to CoS and color classification.</p> <p>Un-Trust – The interface does not consider MPLS bits during classification.</p>
Default port CoS	<p>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.</p>

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 184 802.1Q Classification Page

Logout Admin Connection

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
 - General Configuration
 - Services
 - Interfaces
 - PM & Statistics
 - QOS
 - Classification

802.1Q

802.1AD

DSCP

MPLS

- Policer
- Marking
- WRED
- Shaper
- Scheduler
- Protocols
- Sync
- Quick Configuration
- Utilities

802.1Q Classification

802.1Q Classification Table

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

Edit Refresh

- Select the row you want to modify and click **Edit**. The 802.1Q Classification – Edit page opens.

Figure 185 802.1Q Classification - Edit Page

802.1Q Classification Table - Edit

802.1Q UP

802.1Q CFI

802.1Q CoS (0..7)

802.1Q Color Green ▼

Apply Refresh Close

- 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.
- 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 186 802.1AD Classification Page

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 187 802.1Q Classification - Edit Page

802.1AD Classification Table - Edit

802.1AD UP

802.1AD DEI

802.1AD CoS (0..7)

802.1AD Color Green ▼

3. Modify the parameters you want to change:
 - **802.1AD UP** – Read-only. The User Priority (UP) bit to be mapped.
 - **802.1ADQ DEI** – Read-only. The DEI bit to be mapped.
 - **802.1AD CoS** – The CoS assigned to frames with the designated UP and DEI.
 - **802.1AD Color** – The Color assigned to frames with the designated UP and DEI.
4. Click **Apply**, then **Close**.

Modifying the DSCP Classification Table

You can configure the classification criteria for Differentiated Service Code Point (DSCP) priority values. The DSCP is a 6-bit length field inside the IP datagram header carrying priority information. Classification by DSCP can be used for untagged frames, as well as 802.1Q tagged or provider VLAN tagged frames.

To modify the classification criteria for DSCPs:

1. Select **Ethernet > QoS > Classification > DSCP**. The DSCP Classification page opens.

Figure 188 DSCP Classification Page

The screenshot shows the 'DSCP Classification' page. On the left, a navigation pane lists various configuration options, with 'DSCP' highlighted under the 'Classification' section. The main content area features a table titled 'DSCP Classification Table' with the following data:

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

Below the table, there are 'Edit' and 'Refresh' buttons.

2. Select the row you want to modify and click **Edit**. The DSCP Classification - Edit page opens.

Figure 189 DSCP Classification - Edit Page

DSCP Classification Table - Edit

DSCP: 0

Binary: 000000

Description: BE(CS0)

CoS: 0 (0..7)

Color: Green ▼

Apply Refresh Close

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**.

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 190 MPLS Classification Page

Logout Admin Connection

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
 - General Configuration
 - Services
- Interfaces
- PM & Statistics
- QOS
 - Classification
 - 802.1Q
 - 802.1AD
 - DSCP
 - MPLS**
 - Policer
 - Marking
 - WRED
 - Shaper
 - Scheduler
 - Protocols
 - Sync
 - Quick Configuration
 - Utilities

MPLS Classification

MPLS Classification Table

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

Edit Refresh

- Select the row you want to modify and click **Edit**. The MPLS Classification - Edit page opens.

Figure 191 MPLS Classification - Edit Page

MPLS Classification Table - Edit

MPLS EXP

CoS (0..7)

Color

Apply Refresh Close

- 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.
- Click **Apply**, then **Close**.

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 820 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 820'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 192 Policer Profile Page

Logout Admin Connection

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
 - General Configuration
 - Services
 - Interfaces
 - PM & Statistics
 - QOS
 - Classification
 - Policer
 - Policer Profile**
 - Marking
 - WRED
 - Shaper
 - Scheduler
 - Protocols
 - Sync
 - Quick Configuration
 - Utilities

Policer Profile

Policer Profile Table

<input checked="" type="checkbox"/>	Profile ID	Description	Policer type	CIR	CBS	EIR	EBS	Color mode	Coupling flag
<input checked="" type="checkbox"/>	1	N.A.	MEF-TRTCM	84000	32	84000	32	Color Blind	Disable

Add Edit Delete Refresh

- Click **Add**. The Policer Profile - Add page opens.

Figure 193 Policer Profile - Add Page

Policer Profile Table - Add

Profile ID

Description

Policer type

CIR (0..1000000000)

CBS (0..8192)

EIR (0..1000000000)

EBS (0..8192)

Color mode

Coupling flag

Apply Refresh Close

- Configure the profile's parameters. See [Table 43 Policer Profile Parameters](#) for a description of the policer profile parameters.
- Click **Apply**, then **Close**.

Table 43 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 2 through 128 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 2 through 128 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 193](#)). 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 182](#)).
2. Select the interface in the Ethernet Logical Port Configuration table and click **Policies**. The Policies page opens.

Figure 194 Logical Interfaces – Policies Page – Unicast Policer (Default)

Logout Admin Connection

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
 - General Configuration
 - Services
 - Interfaces
 - Physical Interfaces
 - Logical Interfaces
 - Automatic State Propagation
 - Groups
 - PM & Statistics
 - QOS
 - Protocols
 - Sync
 - Quick Configuration
 - Utilities

Logical Interfaces - Policies (Ethernet: Slot 1, port 1)

<< Back to Logical Interfaces

Select Policer (Ethernet: Slot 1, port 1)

☒ Unicast Policer

☐ 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 1

Policer profile: None

Unicast admin: Disable

Apply Refresh

For a logical interface, you can assign policers to the following traffic flows:

- Unicast Policer
- Multicast Policer
- Broadcast Policer
- Ethertype Policers

Assigning Unicast Policers

To assign a policer for unicast traffic to a logical interface:

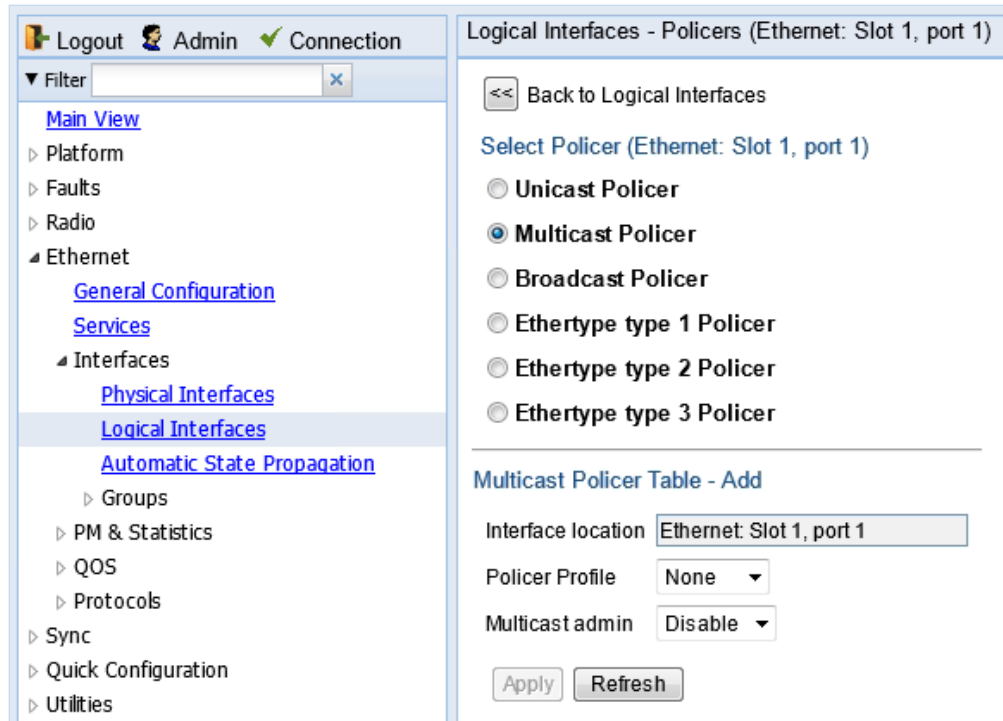
1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens ([Figure 182](#)).
2. Select the interface in the Ethernet Logical Port Configuration Table and click **Policies**. The Policies page opens. By default, the Policies page opens to the Unicast Policer table ([Figure 194](#)).
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 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 182](#)).
2. Select the interface in the Ethernet Logical Port Configuration table and click **Policies**. The Policies page opens. By default, the Policies page opens to the Unicast Policer table ([Figure 194](#)).
3. Select **Multicast Policer**. The Multicast Policer table appears.

Figure 195 Logical Interfaces – Policies Page – Multicast Policer



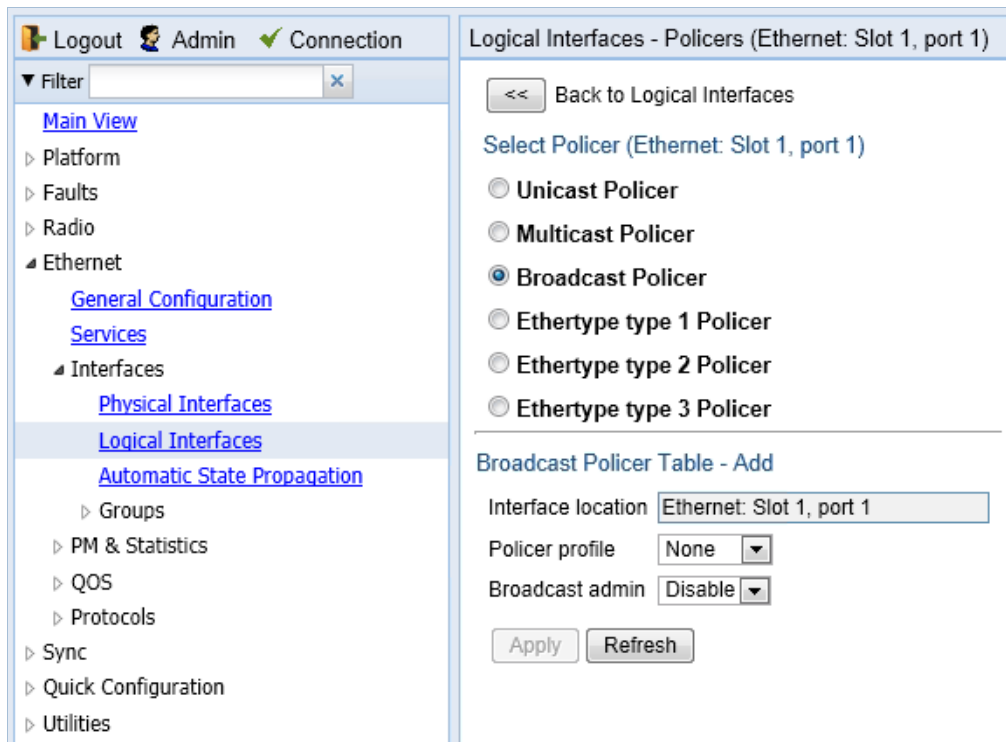
4. In the Policer profile field, select a profile from the policer profiles defined in the system. The Policer profile drop-down list includes the ID and description of all defined profiles.
5. In the Multicast admin field, select Enable to enable policing on multicast traffic flows from the logical interface, or Disable to disable policing on multicast traffic flows from the logical interface.
6. Click Apply.

Assigning 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 182).
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 194).
3. Select **Broadcast Policer**. The Broadcast Policer table appears.

Figure 196 Logical Interfaces – Policers Page – Broadcast Policer



4. In the **Policer profile** field, select a profile from the policer profiles defined in the system. The **Policer profile** drop-down list includes the ID and description of all defined profiles.
5. In the **Broadcast admin** field, select **Enable** to enable policing on broadcast traffic flows from the logical interface, or **Disable** to disable policing on broadcast traffic flows from the logical interface.
6. Click **Apply**.

Assigning Ethertype Policers

You can define up to three policers per Ethertype value.

To assign a policer to an Ethertype:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (Figure 182).
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 194).
3. Select **Ethertype type 1 Policer**. The Ethertype type 1 Policer table appears.

Figure 197 Logical Interfaces – Policers Page – Ethertype Policer

Logout Admin Connection

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
 - General Configuration
 - Services
 - Interfaces
 - Physical Interfaces
 - Logical Interfaces
 - Automatic State Propagation
 - Groups
 - PM & Statistics
 - QOS
 - Protocols
 - Sync
 - Quick Configuration
 - Utilities

Logical Interfaces - Policers (Ethernet: Slot 1, port 1)

<< Back to Logical Interfaces

Select Policer (Ethernet: Slot 1, port 1)

☐ Unicast Policer
☐ 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 1

Ethertype1 profile: None

Ethertype1 user value: 0x0 (0x1..0xffff)

Ethertype1 admin: Disable

Apply Refresh

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 Ethernets, 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 182).
2. Select the interface you want to configure and click **Edit**. The Logical Interfaces - Edit page opens (Figure 183).
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 820'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](#).

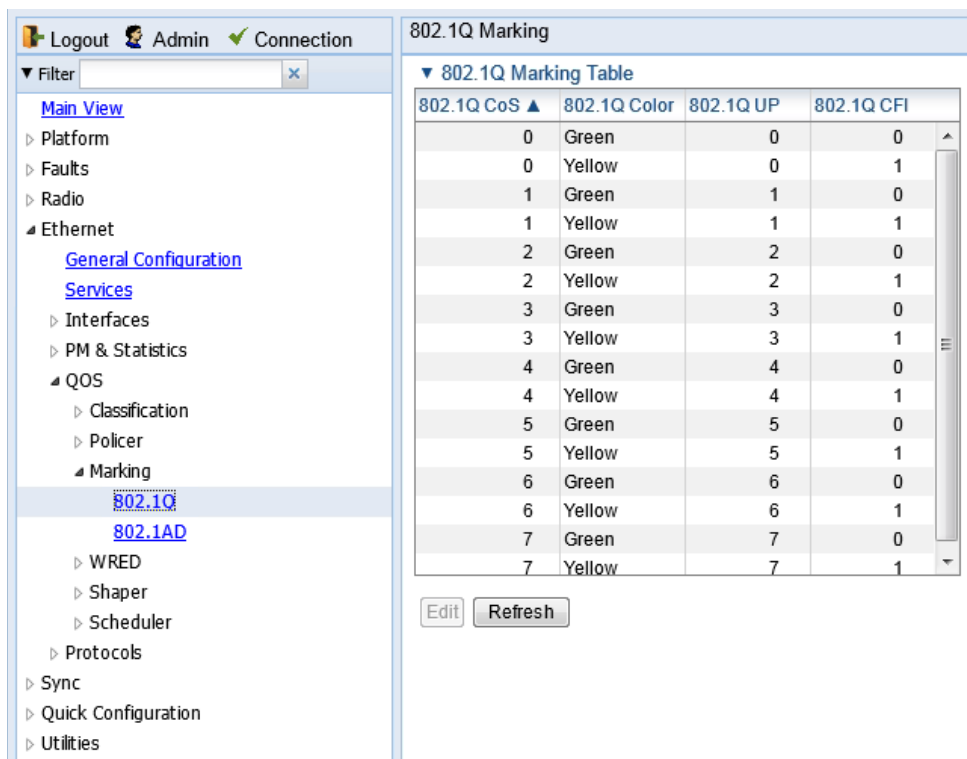
Modifying the 802.1Q Marking Table

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:

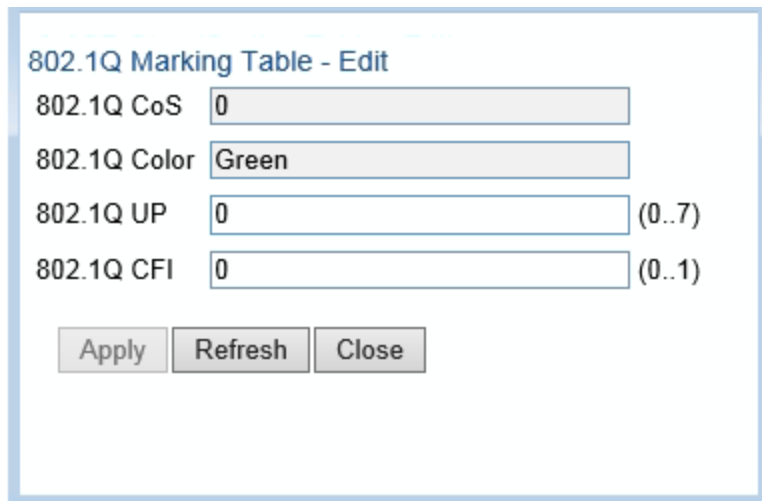
1. Select **Ethernet > QoS > Marking > 802.1Q**. The 802.1Q Marking page opens. Each row in the 802.1Q Marking page represents a CoS and color combination.

Figure 198 802.1Q Marking Page



2. Select the row you want to modify and click **Edit**. The 802.1Q Marking - Edit page opens.

Figure 199 802.1Q Marking - Edit Page



The screenshot shows a configuration window titled "802.1Q Marking Table - Edit". It contains four input fields: "802.1Q CoS" with the value "0", "802.1Q Color" with the value "Green", "802.1Q UP" with the value "0" and a range "(0..7)" to its right, and "802.1Q CFI" with the value "0" and a range "(0..1)" to its right. At the bottom of the window are three buttons: "Apply", "Refresh", and "Close".

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 200 802.1AD Marking Page

802.1AD Marking

▼ 802.1AD Marking Table

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

Edit Refresh

2. Select the row you want to modify and click **Edit**. The 802.1AD Marking - Edit page opens.

Figure 201 802.1AD Marking - Edit Page

802.1AD Marking Table - Edit

802.1AD CoS

802.1AD Color

802.1AD UP (0..7)

802.1AD DEI (0..1)

Apply Refresh Close

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 202 WRED Profile Page

WRED Profile Configuration Table

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
33						

Buttons: Add, Edit, Delete, Refresh

- Click **ADD**. The WRED Profile - Add page opens, with default values displayed.

Figure 203 WRED Profile - Add Page

WRED Profile Configuration Table - Add

WRED Profile ID: 1

Green curve min point: 128 (0..8192)

Green curve max point: 128 (0..8192)

Green curve max drop ratio: 100 (1..100)

Yellow curve min point: 64 (0..8192)

Yellow curve max point: 64 (0..8192)

Yellow curve max drop ratio: 100 (1..100)

Buttons: Apply, Refresh, Close

- In the **WRED Profile ID** field, select a unique ID to identify the profile. Permitted values are 1-30.
- In the **Green curve min point** field, enter the minimum throughput of green packets for queues with this profile, in Kbytes (0-8192). When this value is reached, the system begins dropping green packets in the queue.
- In the **Green curve max point** field, enter the maximum throughput of green packets for queues with this profile, in Kbytes (0-8192). When this value is reached, all green packets in the queue are dropped.
- In the **Green curve max drop ratio** field, enter the maximum percentage (1-100) of dropped green packets for queues with this profile.
- In the **Yellow curve min point** field, enter the minimum throughput of yellow packets for queues with this profile, in Kbytes (0-8192). 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 (0-8192). 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 203](#)). 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 202](#)) 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 182).
2. Select an interface in the Ethernet Logical Port Configuration table and click **WRED**. The WRED page opens.

Figure 204 Logical Interfaces – WRED Page

Logout Admin Connection

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
 - General Configuration
 - Services
 - Interfaces
 - Physical Interfaces
 - Logical Interfaces
 - Automatic State Propagation
 - Groups
 - PM & Statistics
 - QOS
 - Protocols
 - Sync
 - Quick Configuration
 - Utilities

Logical Interfaces - WRED (Ethernet: Slot 1, port 1)

<< Back to Logical Interfaces

WRED (Ethernet: Slot 1, port 1)

Show Service bundle ID: 1

▼ 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

Edit Refresh

3. 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.

4. Select a CoS Queue ID and click **Edit**. The Logical Interfaces – WRED – Edit page opens.

Figure 205: Logical Interfaces – WRED - Edit Page

Egress Queue WRED Configuration Table - Edit

Interface location Ethernet: Slot 1, port 1

Service bundle ID 1

CoS queue ID 0

Profile ID 31

Apply Refresh Close

5. In the **Profile ID** field, select the WRED profile you want to assign to the selected queue.
6. Click **Apply**, then **Close**.

Configuring Egress Shaping

This section includes:

- [Egress Shaping Overview](#)
- [Configuring Queue Shaper Profiles](#)
- [Configuring Service Bundle Shaper Profiles](#)
- [Assigning a Queue Shaper Profile to a Queue](#)
- [Assigning a Service Bundle Shaper Profile to a Service Bundle](#)

Egress Shaping Overview

Egress shaping determines the traffic profile for each queue. PTP 820 can perform queue shaping on the following levels:

- **Queue Level** – Single 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.
- **Service Bundle Level** – Dual leaky bucket shaping. On the service bundle level, users can configure up to 256 dual leaky bucket shaper profiles. If no profile is attached to the service bundle, no egress shaping is performed on that service bundle.
- **Interface Level** – Single leaky bucket shaping.



Note

Egress shaping on the interface level is planned for future release.

Configuring Queue Shaper Profiles

This section includes:

- [Adding a Queue Shaper Profile](#)
- [Editing a Queue Shaper Profile](#)
- [Deleting a Queue Shaper Profile](#)

Adding a Queue Shaper Profile

To add a queue shaper profile:

1. Select **Ethernet > QoS > Shaper > Queue Profiles**. The Queue Shaper Profile page opens.

Figure 206 Queue Shaper Profile Page

Logout Admin Connection

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
 - General Configuration
 - Services
 - Interfaces
 - PM & Statistics
 - QOS
 - Classification
 - Policer
 - Marking
 - WRED
 - Shaper
- Queue Profiles
- Service Bundle Profiles
 - Scheduler
 - Protocols
- Sync
- Quick Configuration
- Utilities

Queue Shaper Profile

Queue Shaper Profiles Configuration Table

Profile ID	Description	CIR
1	N.A.	131008000

Add Edit Delete Refresh

- Click **Add**. The Queue Shaper – Add page opens, with default values displayed.

Figure 207 Queue Shaper Profile – Add Page

Queue Shaper Profiles Configuration Table - Add

Profile ID 2

Description N.A.

CIR 131008000 (16000..131008000)

Apply Refresh Close

- In the **Profile ID** field, select a unique ID to identify the profile. Permitted values are 1-31.
- Optionally, in the **Description** field, enter a description of the profile.
- In the **CIR** field, enter the Committed Information Rate (CIR) 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 - 131,008,000 bps, with granularity of 64,000.
- Click **Apply**, then **Close**.

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 206](#)).
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 207](#)). 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 206](#)) and click **Delete**. The profile is deleted.

To delete multiple queue shaper profiles:

1. Select the profiles in the Queue Shaper Profiles Configuration table or select all the profiles by selecting the check box in the top row.
2. Click **Delete**. The profiles are deleted.

Configuring Service Bundle Shaper Profiles

This section includes:

- [Adding a Service Bundle Shaper Profile](#)
- [Editing a Service Bundle Shaper Profile](#)
- [Deleting a Service Bundle Shaper Profile](#)

Adding a Service Bundle Shaper Profile

To add a service bundle shaper profile:

1. Select **Ethernet > QoS > Shaper > Service Bundle Profiles**. The Service Bundle Shaper Profile page opens.

Figure 208 Service Bundle Shaper Profile Page

Logout Admin Connection

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
 - General Configuration
 - Services
 - Interfaces
 - PM & Statistics
 - QOS
 - Classification
 - Policer
 - Marking
 - WRED
 - Shaper
 - Queue Profiles
 - Service Bundle Profiles
 - Scheduler
 - Protocols
 - Sync
 - Quick Configuration
 - Utilities

Service Bundle Shaper Profile

Service Shaper Profiles Configuration Table

Profile ID	Description	CIR	PIR
1	N.A.	1000000000	1000000000

Add Edit Delete Refresh

- Click **Add**. The Service Bundle Shaper Profile – Add page opens, with default values displayed.

Figure 209 Service Bundle Shaper Profile – Add Page

Service Shaper Profiles Configuration Table - Add

Profile ID: 2

Description: N.A.

CIR: 1000000000 (0..1000000000)

PIR: 1000000000 (16000..1000000000)

Apply Refresh Close

- In the **Profile ID** field, select a unique ID to identify the profile. Permitted values are 1-31.
- Optionally, in the **Description** field, enter a description of the profile.
- 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.
- 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.
- Click **Apply**, then **Close**.

Editing a Service Bundle Shaper Profile

To edit a service bundle shaper profile:

1. Select **Ethernet > QoS > Shaper > Service Bundle Profiles**. The Service Bundle Shaper Profile page opens ([Figure 208](#)).
2. Select the profile you want to edit and click **Edit**. The Service Bundle Shaper Profile – Edit page opens. This page is similar to the Service Bundle Shaper Profile – Add page ([Figure 209](#)). You can edit any parameter except the **Profile ID**.
3. Modify the profile.
4. Click **Apply**, then **Close**.

Deleting a Service Bundle Shaper Profile

You cannot delete a service bundle shaper profile that is assigned to a service bundle. You must first remove the profile from the service bundle, then delete the profile.

To delete a service bundle shaper profile, select the profile in the Service Bundle Shaper Profiles Configuration table ([Figure 208](#)) and click **Delete**. The profile is deleted.

To delete multiple service bundle shaper profiles:

1. Select the profiles in the Service Bundle Shaper Profiles Configuration table or select all the profiles by selecting the check box in the top row.
2. Click **Delete**. The profiles are deleted.

Assigning a Queue Shaper Profile to a Queue

To assign a queue shaper profile to a queue:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens ([Figure 182](#)).
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 210 Logical Interfaces – Shaper – Egress Queue Shaper

Logout Admin Connection

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
 - General Configuration
 - Services
 - Interfaces
 - Physical Interfaces
 - Logical Interfaces
 - Automatic State Propagation
 - Groups
 - PM & Statistics
 - QOS
 - Protocols
 - Sync
 - Quick Configuration
 - Utilities

Logical Interfaces - Shaper (Ethernet: Slot 1, port 1)

<< Back to Logical Interfaces

Select Shaper (Ethernet: Slot 1, port 1)

☒ Egress Queue Shaper

☐ Egress Service Bundle Shaper

▼ Egress Queue Shaper Configuration

Service bundle ID	CoS queue ID	Profile ID	Shaper admin

Add Edit Delete Refresh

3. Click **Add**. The Egress Queue Shaper Configuration – Add page opens.

Figure 211 Logical Interfaces – Egress Queue Shaper Configuration – Add Page

Egress Queue Shaper Configuration - Add

Interface location Ethernet: Slot 1, port 1

Service bundle ID 1 ▼

CoS queue ID 0 ▼

Profile ID 1 - N.A. ▼

Shaper admin Disable ▼

Apply Refresh Close



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:

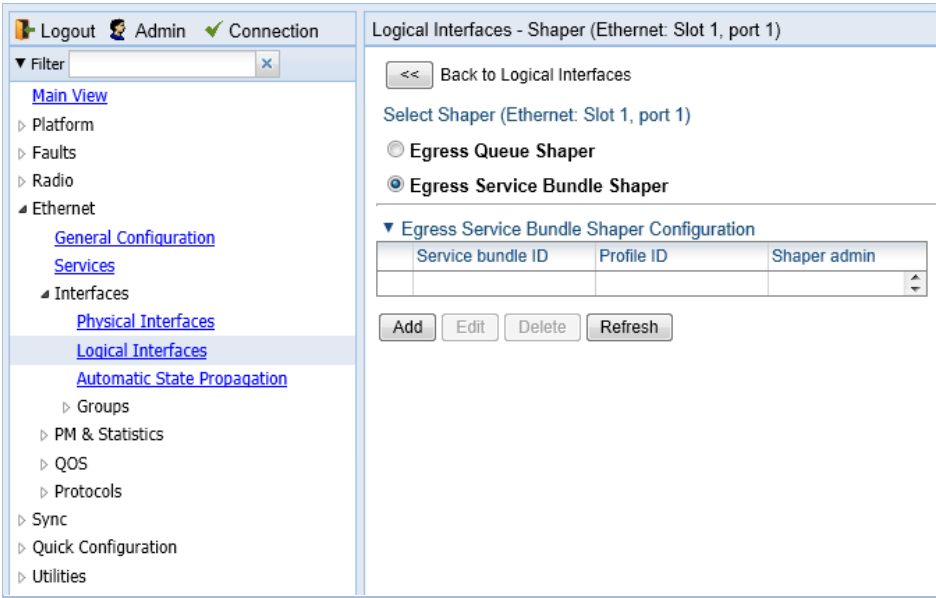
1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens ([Figure 182](#)).
2. Select an interface in the Ethernet Logical Port Configuration table and click **Shaper**. The Logical Interfaces – Shaper page opens, with the Egress Queue Shaper Configuration table open by default ([Figure 210](#)).
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 210](#)).
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 211](#)).
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**.

Assigning a Service Bundle Shaper Profile to a Service Bundle

To assign a service bundle shaper profile to a service bundle:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens ([Figure 182](#)).
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 210](#)).
3. Select **Egress Service Bundle Shaper**. The Egress Service Bundle Shaper Configuration table appears. All service bundle shaper profiles defined in the system are listed in the table.

Figure 212 Logical Interfaces – Shaper – Egress Service Bundle Shaper



4. Click **Add**. The Egress Service Bundle Shaper Configuration – Add page opens.

Figure 213 Logical Interfaces – Egress Service Bundle Shaper Configuration – Add Page

Egress Service Bundle Shaper Configuration - Add

Interface location

Service bundle ID

Profile ID

Shaper admin

**Note**

In this release, only one service bundle (Service Bundle ID 1) is supported.

5. In the **Profile ID** field, select from a list of configured service bundle shaper profiles. See [Configuring Service Bundle Shaper Profiles](#).
6. In the **Shaper Admin** field, select **Enable** to enable egress service bundle shaping, or **Disable** to disable egress service bundle shaping.
7. Click **Apply**, then **Close**.

To assign a different service bundle shaper profile:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens ([Figure 182](#)).
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 210](#)).
3. Select **Egress Service Bundle Shaper**. The Egress Service Bundle Shaper Configuration table appears ([Figure 212](#)). All service bundle shaper profiles defined in the system are listed in the table.
4. Select the row you want to edit and click **Edit**. The Egress Service Bundle Shaper Configuration – Edit page opens. This page is similar to the Egress Service Bundle Shaper Configuration – Add page ([Figure 213](#)).
5. To assign a different egress queue shaper profile, select the profile in the **Profile ID** field.
6. To enable or disable egress service bundle shaping, select **Enable** or **Disable**.
7. Click **Apply**, then **Close**.

Configuring Scheduling

This section includes:

- [Scheduling Overview](#)
- [Configuring Priority Profiles](#)
- [Configuring 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 820 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:

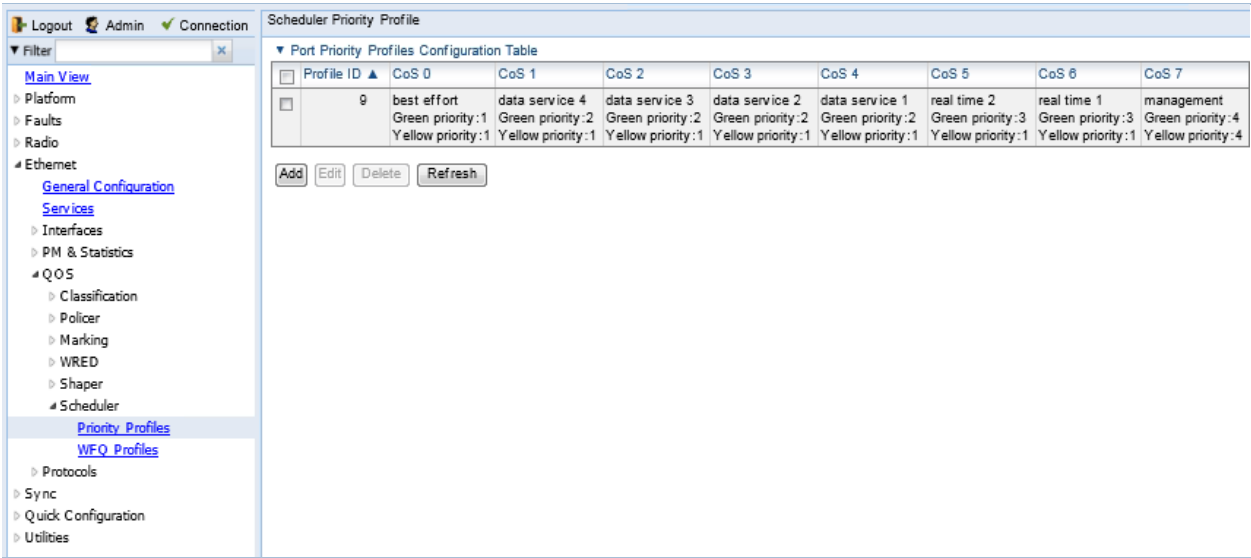
- [Adding a Scheduler Priority Profile](#)
- [Editing a Service Scheduler Priority Profile](#)
- [Deleting a Scheduler Priority Profile](#)

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 214 Scheduler Priority Profile Page



2. Click **Add**. The Scheduler Priority Profile – Add page opens, with default values displayed.

Figure 215 Scheduler Priority Profile – Add Page

Port Priority Profiles Configuration Table - Add			
Profile ID	1		
CoS 0	best effort		
Green CoS 0 priority	1	(1..4)	
Yellow CoS 0 priority	1		
CoS 1	data service 4		
Green CoS 1 priority	2	(1..4)	
Yellow CoS 1 priority	1		
CoS 2	data service 3		
Green CoS 2 priority	2	(1..4)	
Yellow CoS 2 priority	1		
CoS 3	data service 2		
Green CoS 3 priority	2	(1..4)	
Yellow CoS 3 priority	1		
CoS 4	data service 1		
Green CoS 4 priority	2	(1..4)	
Yellow CoS 4 priority	1		
CoS 5	real time 2		
Green CoS 5 priority	3	(1..4)	
Yellow CoS 5 priority	1		
CoS 6	real time 1		
Green CoS 6 priority	3	(1..4)	
Yellow CoS 6 priority	1		
CoS 7	management		
Green CoS 7 priority	4		
Yellow CoS 7 priority	4		

Apply Refresh Close

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 214](#)).
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 215](#)). 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 214](#)) 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:

- [Adding a WFQ Profile](#)
- [Editing a WFQ Priority Profile](#)
- [Deleting a WFQ Profile](#)

Adding a WFQ Profile

To add a WFQ profile:

1. Select **Ethernet > QoS > Scheduler > WFQ Profiles**. The Scheduler WFQ Profile page opens.

Figure 216 Scheduler WFQ Profile Page

The screenshot displays the 'Scheduler WFQ Profile' configuration page. On the left is a navigation sidebar with a tree view. The 'Ethernet' section is expanded, and 'Scheduler' is selected, with 'WFQ Profiles' highlighted. The main area is titled 'Scheduler WFQ Profile' and contains a 'Port WFQ Profiles Configuration Table'. The table has columns for Profile ID and CoS weights (0-7). Profile 1 is listed with all weights set to 20. Below the table are buttons for 'Add', 'Edit', 'Delete', and 'Refresh'.

Profile ID	CoS 0 weight	CoS 1 weight	CoS 2 weight	CoS 3 weight	CoS 4 weight	CoS 5 weight	CoS 6 weight	CoS 7 weight
1	20	20	20	20	20	20	20	20

2. Click **Add**. The Scheduler WFQ Profile – Add page opens, with default values displayed.

Figure 217 Scheduler WFQ Profile – Add Page

Scheduler WFQ Profile

Port WFQ Profiles Configuration Table - Add

Profile ID

CoS 0 weight	<input type="text" value="20"/>	(1..256)
CoS 1 weight	<input type="text" value="20"/>	(1..256)
CoS 2 weight	<input type="text" value="20"/>	(1..256)
CoS 3 weight	<input type="text" value="20"/>	(1..256)
CoS 4 weight	<input type="text" value="20"/>	(1..256)
CoS 5 weight	<input type="text" value="20"/>	(1..256)
CoS 6 weight	<input type="text" value="20"/>	(1..256)
CoS 7 weight	<input type="text" value="20"/>	(1..256)

3. In the **Profile ID** field, select a unique Profile ID between 2 and 7. Profile ID 1 is used for a pre-defined WFQ profile.
4. For each CoS value, enter the weight for that CoS, from 1 to 20.
5. Click **Apply**, then **Close**.

Editing a WFQ Priority Profile

To edit a scheduler WFQ profile:

1. Select **Ethernet > QoS > Scheduler > WFQ Profiles**. The Scheduler WFQ Profile page opens ([Figure 216](#)).
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 206](#)). 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 216](#)) and click **Delete**. The profile is deleted.

To delete multiple scheduler WFQ profiles:

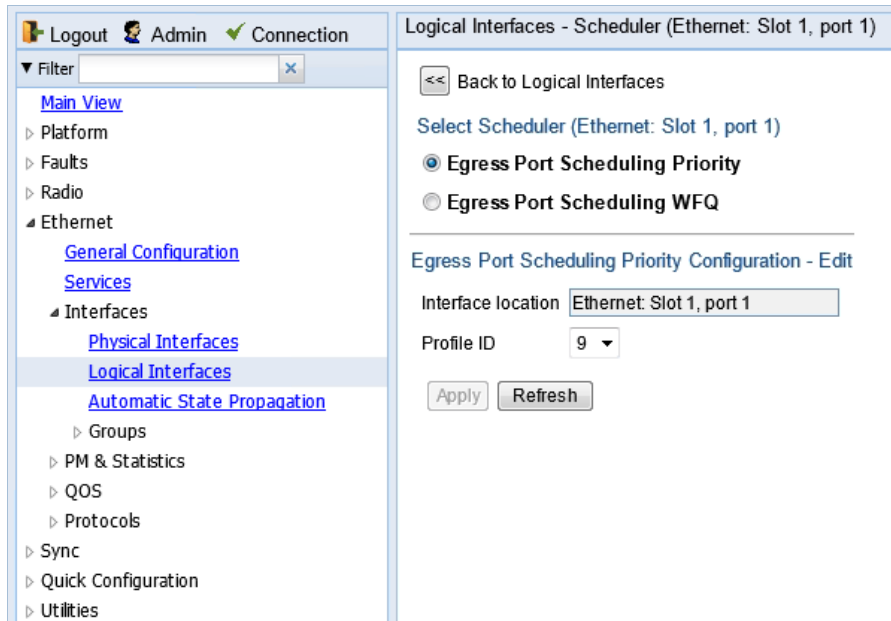
1. Select the profiles in the Scheduler WFQ Profiles page or select all the profiles by selecting the check box in the top row.
2. Click **Delete**. The profiles are deleted.

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 182).
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 218 Logical Interfaces – Scheduler – Egress Port Scheduling Priority



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 182).
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 218).

3. Select **Egress Port Scheduling WFQ**. The Egress Port Scheduling WFQ Configuration – Edit page opens.

Figure 219 Logical Interfaces – Scheduler – Egress Port Scheduling WFQ

Logout Admin Connection

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
 - General Configuration
 - Services
 - Interfaces
 - Physical Interfaces
 - Logical Interfaces
 - Automatic State Propagation
 - Groups
 - PM & Statistics
 - QOS
 - Protocols
- Sync
- Quick Configuration
- Utilities

Logical Interfaces - Scheduler (Ethernet: Slot 1, port 1)

<< Back to Logical Interfaces

Select Scheduler (Ethernet: Slot 1, port 1)

☒ Egress Port Scheduling Priority

☐ Egress Port Scheduling WFQ

Egress Port Scheduling Priority Configuration - Edit

Interface location Ethernet: Slot 1, port 1

Profile ID 9

Apply Refresh

4. In the **Profile ID** field, select from a list of configured scheduling priority profiles. See [Configuring WFQ Profiles](#).
5. Click **Apply**, then **Close**.

Chapter 8: Ethernet Protocols

This section includes:

- [Configuring LLDP](#)

Related Topics:

- [Configuring Service OAM \(SOAM\) Fault Management \(FM\)](#)

Configuring Adaptive Bandwidth Notification (ABN)

This section includes:

- [Adaptive Bandwidth Notification Overview](#)
- [Adding an ABN entity](#)
- [Editing an ABN Entity](#)
- [Deleting an ABN Entity](#)
- [Viewing the Statistics for an ABN Entity](#)

Adaptive Bandwidth Notification Overview

Adaptive Bandwidth Notification (ABN), also known as Ethernet Operation and Maintenance (EOAM), enables third party applications to learn about bandwidth changes in a radio link when ACM is active. Once ABN is enabled, the radio unit reports bandwidth information to upstream third-party switches.

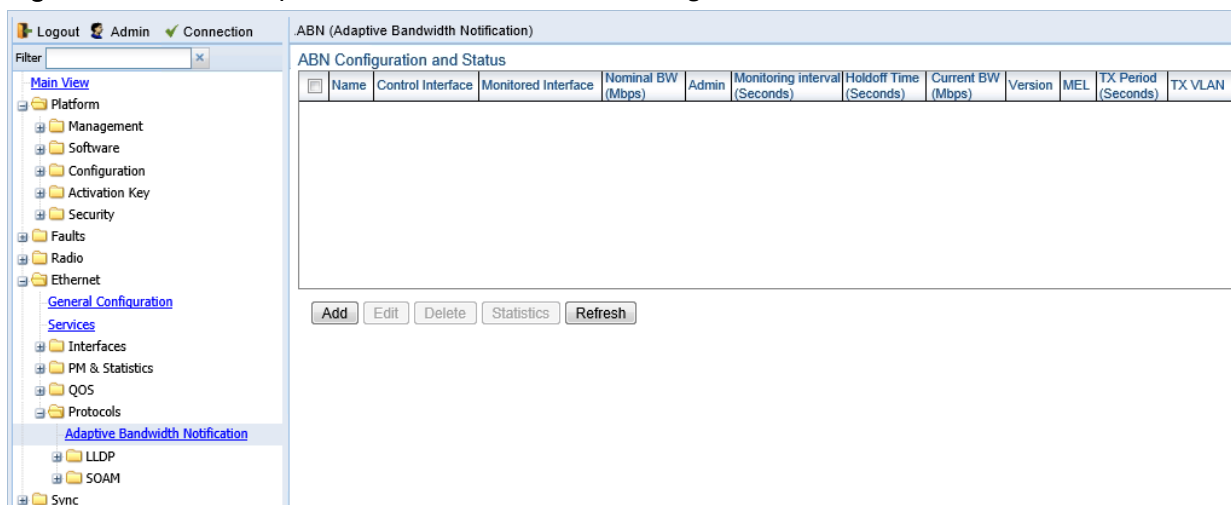
The ABN entity creates a logical relationship between a radio interface or a logical group of radio interfaces, called the Monitored Interface, and an Ethernet interface or a logical group of Ethernet interface, called the Control Interface. When bandwidth degrades from the nominal value in the Monitored Interface, messages relaying the actual bandwidth values are periodically sent over the Control Interface. A termination message is sent once the bandwidth returns to its nominal level.

Adding an ABN entity

To add an ABN entity:

1. Select **Ethernet > Protocols > Adaptive Bandwidth Notification**. The ABN (Adaptive Bandwidth Notification) page opens.

Figure 220 ABN (Adaptive Bandwidth Notification) Page



2. Click **Add** underneath the ABN Configuration and Status table. The ABN Configuration and Status – Add page opens.

Figure 221 ABN Configuration and Status – Add Page

3. In the **Name** field, enter a name for the ABN entity.
4. 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.
5. In the **Monitored Interface** field, select the Monitored Interface. This is the interface which is constantly monitored for its bandwidth value.
6. In the **Admin** field, select **is-Up** to enable ABN monitoring or **is-Down** to disable ABN monitoring.
7. In the **Monitoring Interval** field, select the interval for which a weighted average of the bandwidth readings is calculated.
8. In the **Holdoff Time** field, specify 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.
9. In the **MEL** field, select the Maintenance Level in the messages.
10. In the **Tx Period** field, specify how often messages are transmitted when bandwidth is below the nominal value. Options are:
 - **4** – One second.
 - **5** – Ten seconds.
 - **6** – One minute.
11. In the **Tx VLAN** field, specify the VLAN on which messages are transmitted. Options are:
 - Untagged.
 - 1 – 4090.

12. Click **Apply**, then **Close**.

[Table 44](#) describes the status (read-only) fields in the ABN Configuration and Status table.

Table 44 ABN Status Parameters

Parameter	Definition
Nominal BW	The nominal bandwidth of the link.
Current BW	The weighted average of the bandwidth readings taken during the last Monitoring Interval.
Version	The ABN version used.

Editing an ABN Entity

To edit an ABN entity:

1. Select **Ethernet > Protocols > Adaptive Bandwidth Notification**. The ABN (Adaptive Bandwidth Notification) page opens ([Figure 220](#)).
2. Select the ABN entity in the ABN Configuration and Status Table.
3. Click **Edit**. The ABN Entity - Edit page opens.
The Edit page is similar to the ABN Configuration and Status – Add page ([Figure 221](#)). However, the **Control interface** and **Monitored interface** parameters are read-only, and additional read-only parameters display the **Nominal BW**, the **Current BW**, and the **Version**.
4. Edit the ABN entity attributes, as described in Adding an ABN entity.
5. Click **Apply**, then **Close**.

Deleting an ABN Entity

To delete an ABN entity:

1. Select **Ethernet > Protocols > Adaptive Bandwidth Notification**. The ABN (Adaptive Bandwidth Notification) page opens ([Figure 220](#)).
2. Select the ABN entity in the ABN Configuration and Status Table.
3. Click **Delete**. The ABN entity is removed from the ABN Configuration and Status Table.

Viewing the Statistics for an ABN Entity

To view the statistics for an ABN entity:

1. Select **Ethernet > Protocols > Adaptive Bandwidth Notification**. The ABN (Adaptive Bandwidth Notification) page opens ([Figure 220](#)).
2. Select the ABN entity in the ABN Configuration and Status Table.
3. Click **Statistics**. The ABN Configuration and Status - Statistics page opens.

Figure 222 ABN Configuration and Status - Statistics Page

ABN Configuration and Status - Statistics

Name: ABN-1

TX Messages Counter: 0

Holdoff State: Off

Holdoff Start Time (centi-sec): 0

Last TX message: 00

Buttons: Apply, Clear Counter, Refresh, Close

Table 45 describes the ABN entity statistics.

Table 45 ABN Entity Statistics Parameters

Parameter	Definition
Name	The name of the ABN entity.
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.
Holdoff Start Time (mSec)	The Holdoff start time for the last event.
Last Tx message	The last transmitted bandwidth message, in hexadecimal notation.

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.

Figure 223 LLDP Remote System Management Page

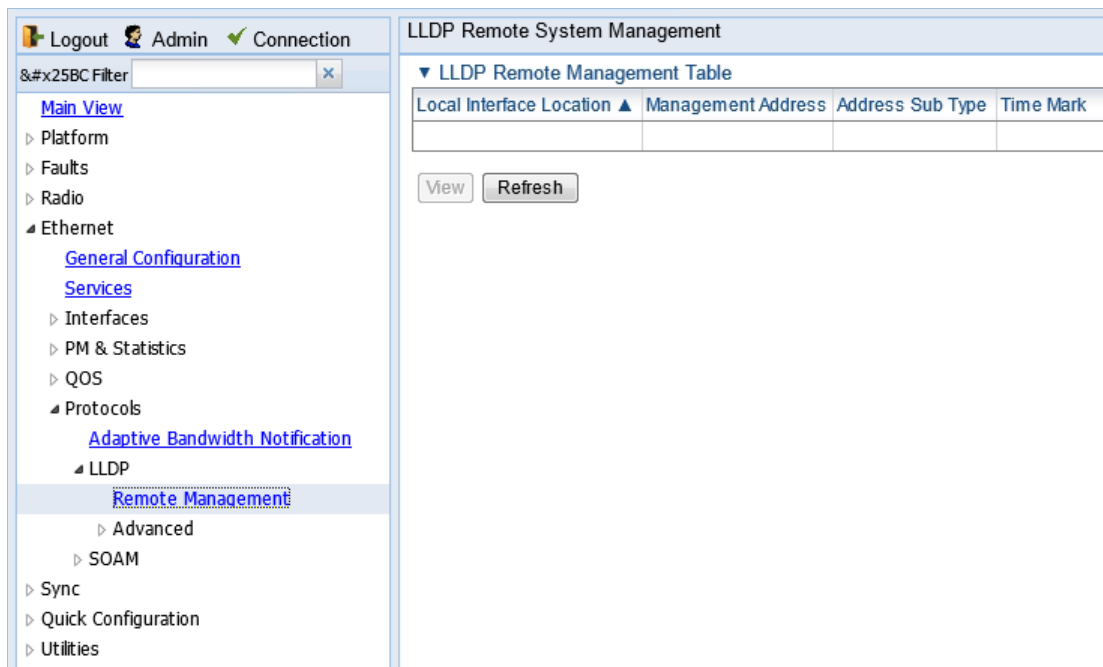


Table 46 describes the LLDP remote system management parameters. These parameters are read-only.

Table 46 LLDP Remote System Management Parameters

Parameter	Definition
Local Interface Location	The location of the local interface.
Management Address	The octet string used to identify the management address component associated with the remote system.
Address Sub Type	The type of management address identifier encoding used in the associated LLDP Agent Remote Management Address.
Time Mark	The time the entry was created.

Configuring the General LLDP Parameters

This section explains how to define the general LLDP parameters for the unit. For instructions on defining port-specific parameters, see [Configuring the LLDP Port Parameters](#).



Note

The management IP address advertised by the local element depends on the IP protocol (IPv4 or IPv6) configured for the unit. See [Defining the IP Protocol Version for Initiating Communications](#).

To display and configure the general LLDP parameters for the unit:

1. Select **Ethernet > Protocols > LLDP > Advanced > Configuration > Parameters**. The LLDP Configuration Parameters page opens.

Figure 224 LLDP Configuration Parameters Page

The screenshot shows the 'LLDP Configuration Parameters' page. On the left is a navigation tree with the following structure:

- ▼ Filter
- Main View
- Platform
- Faults
- Radio
- Ethernet
 - General Configuration
 - Services
 - Interfaces
 - PM & Statistics
 - QOS
 - Protocols
 - Adaptive Bandwidth Notification
 - LLDP
 - Remote Management
 - Advanced
 - Configuration
 - Parameters**
 - Port Configuration
 - Destination Address
 - Management TLV
 - Remote System
 - Local System
 - Statistic
 - SOAM
 - Sync
 - Quick Configuration
 - Utilities

The main content area is titled 'LLDP Configuration Parameters' and contains the following fields:

- Max TX Credit: 5
- Fast TX Interval (Seconds): 1
- Fast TX: 4
- Reinit Delay (Seconds): 2
- TX Interval (Seconds): 30 (range 5..32768)
- Notification Interval (Seconds): 30 (range 5..3600)
- Hold Multiplier: 4 (dropdown)

At the bottom of the main area are 'Apply' and 'Refresh' buttons.

2. Modify the configurable parameters, described in *Table 48*.
3. Click **Apply**.

Table 47 lists and describes the status parameters in the LLDP Configuration Parameters page.

Table 47 LLDP Read-Only Configuration Parameters

Parameter	Definition
Max TX Credit	Displays the maximum number of consecutive LLDPDUs that can be transmitted at any one time. In this release, the Max TX Credit is set at 5.
Fast TX Interval (Seconds)	Displays, in seconds, the interval at which LLDP frames are transmitted during fast transmission periods, such as when the unit detects a new peer. In this release, the Fast TX Interval is set at 1.

Parameter	Definition
Fast TX	The initial value used to initialize the variable which determines the number of transmissions that are made during fast transmission periods. In this release, the Fast TX No. is set at 4.
Reinit Delay (Seconds)	Defines the minimum time, in seconds, the system waits after the LLDP Admin status becomes Disabled until it will process a request to reinitialize LLDP. For instructions on disabling or enabling LLDP on a port, see Configuring the LLDP Port Parameters . In this release, the Reinit Delay is set at 2.

Table 48 LLDP Configurable Configuration Parameters

Parameter	Definition
TX Interval (Seconds)	Defines the interval, in seconds, at which LLDP frames are transmitted. You can select a value from 5 to 32768. The default value is 30.
Notification Interval (Seconds)	Defines the interval, in seconds, between transmissions of LLDP notifications during normal transmission periods. You can select a value from 5 to 3600. The default value is 10.
Hold Multiplier	Defines the time-to-live (TTL) multiplier. The TTL determines the length of time LLDP frames are retained by the receiving device. The TTL is determined by multiplying the TX Interval by the Hold Multiplier. You can select a value from 2 to 10. The default value is 4.

Configuring the LLDP Port Parameters

To enable LLDP per port and determine how LLDP operates and which TLVs are sent for each port:

1. Select **Ethernet > Protocols > LLDP > Advanced > Configuration > Port Configuration**. The LLDP Port Configuration page opens.

Figure 225 LLDP Port Configuration Page

Logout Admin Connection

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
 - General Configuration
 - Services
 - Interfaces
 - PM & Statistics
 - QOS
 - Protocols
 - Adaptive Bandwidth Notification
 - LLDP
 - Remote Management
 - Advanced
 - Configuration
 - Parameters
 - Port Configuration
 - Destination Address
 - Management TLV
 - Remote System
 - Local System
 - Statistic
- SOAM
- Sync
- Quick Configuration
- Utilities

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

Edit Refresh

2. Select an interface and click **Edit**. The LLDP Port Configuration - Edit page opens.

Figure 226 LLDP Port Configuration - Edit Page

Active, LLDP Port Configuration - Edit

Interface Location Ethernet: Slot 1, port 1

Destination Address 1

TLV TX None

Admin TX and RX

Notification Enable False

Apply Refresh Close

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 49](#) lists and describes the status parameters in the LLDP Port Configuration page.

Table 49 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	<p>Indicates which of the unit's capabilities is transmitted by the LLDP agent for the port:</p> <ul style="list-style-type: none"> • PortDesc – The LLDP agent transmits Port Description TLVs. • SysName – The LLDP agent transmits System Name TLVs. • SysDesc – The LLDP agent transmits System Description TLVs. • SysCap – The LLDP agent transmits System Capabilities TLVs.

Displaying the Unit's Management Parameters

To display the unit's destination LLDP MAC address:

1. Select **Ethernet > Protocols > LLDP > Advanced > Configuration > Destination Address**. The LLDP Destination Address Table page opens.

Figure 227 LLDP Destination Address Table Page

The screenshot shows a web-based network management interface. On the left is a navigation pane with a tree structure. The 'Destination Address' link under the 'LLDP' section is highlighted. The main content area is titled 'LLDP Destination Address Table'. It contains a table with two columns: 'Index ▲' and 'Destination Address'. There is one row in the table with the value '1' in the Index column and '01:80:C2:00:00:0E' in the Destination Address column. Below the table are two buttons: 'View' and 'Refresh'.

Index ▲	Destination Address
1	01:80:C2:00:00:0E

To displays the MAC address associated with the unit for purposes of LLDP transmissions:

1. Select **Ethernet > Protocols > LLDP > Advanced > Configuration > Management TLV**. The LLDP Management TLV Configuration page opens.

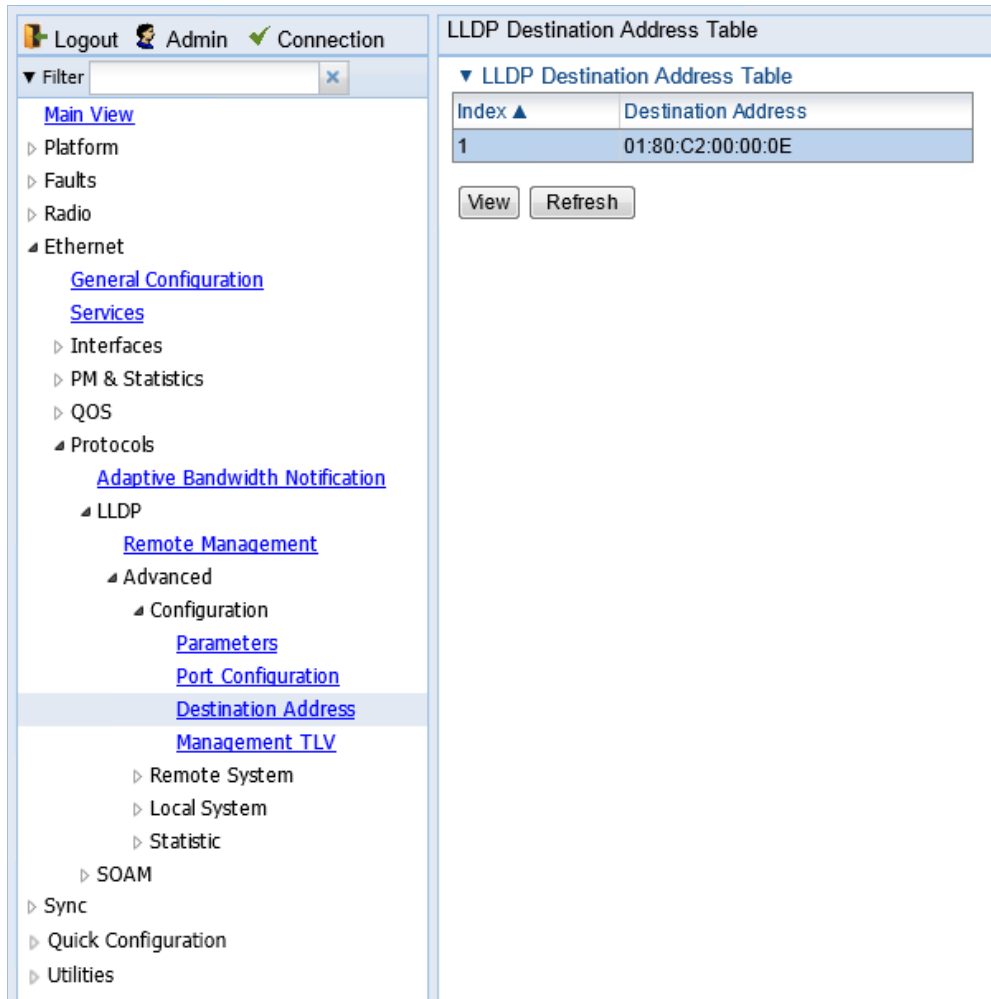
Figure 228 LLDP Management TLV Configuration Page

Table 50 lists and describes the status parameters in the LLDP Management TLV Configuration page.

Table 50 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 sent.

Displaying Peer Unit's Management Parameters

To display LLDP management information about the unit's nearest neighbor (peer):

1. Select **Ethernet > Protocols > LLDP > Advanced > Remote System > Management**. The LLDP Remote System Management page opens.

Figure 229 LLDP Remote System Management Page

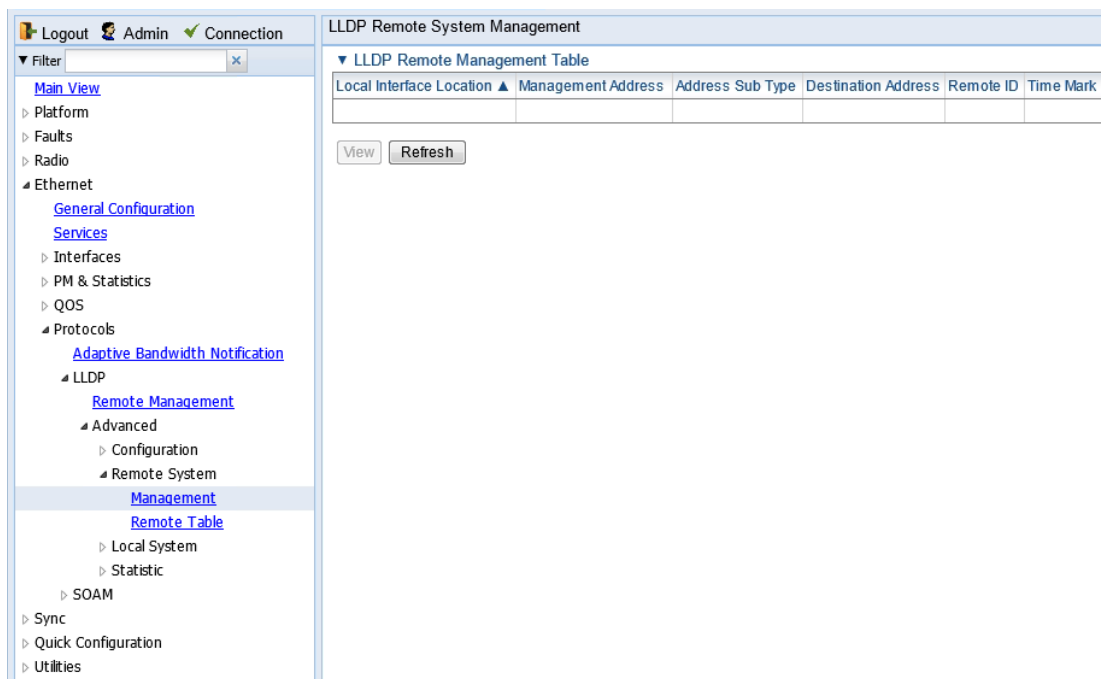


Table 51 describes the LLDP remote system management parameters. These parameters are read-only.

Table 51 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.

Parameter	Definition
Time Mark	The time the entry was created.

To display unit parameter information received via LLDP from the unit's nearest neighbor (peer):

1. Select **Ethernet > Protocols > LLDP > Advanced > Remote System > Remote Table**. The LLDP Remote System Table page opens.

Figure 230 LLDP Remote System Table Page

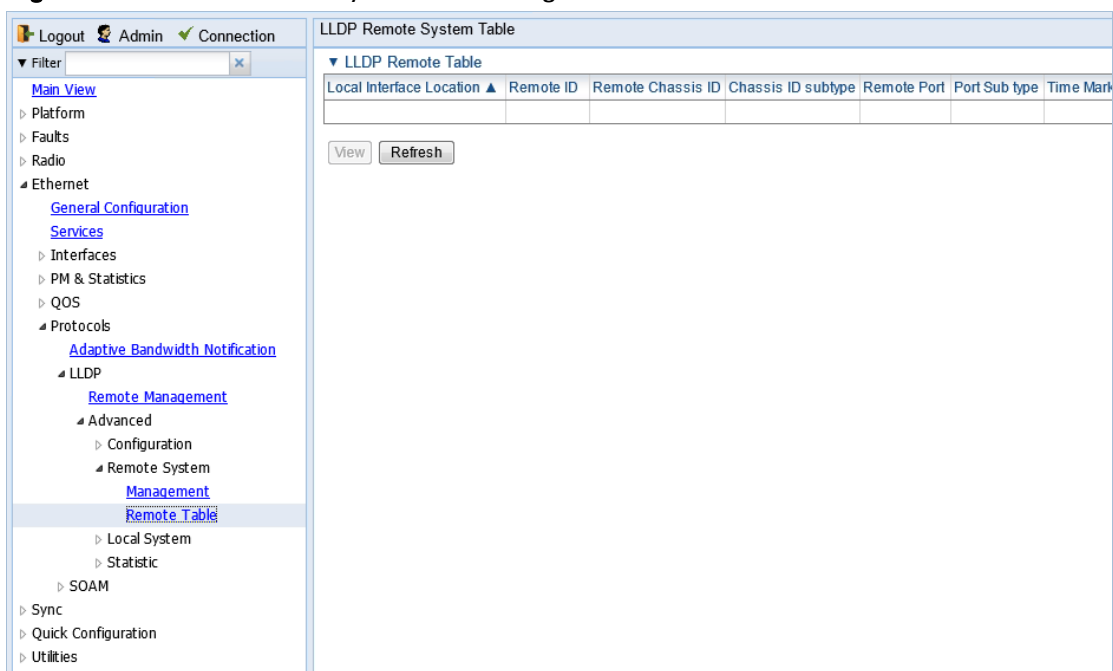


Table 52 describes the parameters in the LLDP Remote System Table page. These parameters are read-only.

Table 52 LLDP Remote System Table Parameters

Parameter	Definition
Local Interface Location	The location of the local interface.
Remote ID	An arbitrary local integer value used by this agent to identify a particular connection instance, unique only for the indicated peer.
Remote Chassis ID	An octet string used to identify the peer's chassis.
Chassis ID Subtype	The type of encoding used to identify the peer's chassis.

Parameter	Definition
Remote Port	An octet string used to identify the port component associated with the remote system.
Port Sub type	The type of port identifier encoding used in the peer's Port ID.
Time Mark	The time the entry was created.

Displaying the Local Unit's Parameters

To display the unit parameters, as transmitted by the LLDP agents:

1. Select **Ethernet > Protocols > LLDP > Advanced > Local System > Parameters**. The LLDP Local System Parameters page opens.

Figure 231 LLDP Local System Parameters Page

The screenshot shows the 'LLDP Local System Parameters' page. The left sidebar contains a navigation tree with the following structure:

- Logout, Admin, Connection (top bar)
- Filter (input field)
- Main View (link)
- Platform (expandable)
- Faults (expandable)
- Radio (expandable)
- Ethernet (expandable)
 - General Configuration (link)
 - Services (link)
 - Interfaces (expandable)
 - PM & Statistics (expandable)
 - QOS (expandable)
 - Protocols (expandable)
 - Adaptive Bandwidth Notification (link)
 - LLDP (expandable)
 - Remote Management (link)
 - Advanced (expandable)
 - Configuration (expandable)
 - Remote System (expandable)
 - Local System (expandable)
 - Parameters (selected, link)
 - Port (link)
 - Management (link)
 - Statistic (expandable)
 - SOAM (expandable)
 - Sync (expandable)
 - Quick Configuration (expandable)
 - Utilities (expandable)

The main content area, titled 'LLDP Local System Parameters', contains the following fields:

- System Name:
- System Description:
- Chassis ID:
- Chassis ID SubType:
- Capabilities Supported:
- Capabilities Enabled:
- Refresh button

Table 53 describes the parameters in the LLDP Local System Parameters page. These parameters are read-only.

Table 53 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	<p>A bitmap value used to identify which system capabilities are supported on the local system, as included in TLVs transmitted by the LLDP agent.</p> <p>The bitmap is defined by the following parameters:</p> <ul style="list-style-type: none"> 0 – other 1 – repeater 2 – bridge 3 – wlanAccessPoint 4 – router 5 – telephone 6 – docsisCableDevice 7 – stationOnly 8 – cVLANComponent 9 – sVLANComponent 10 – twoPortMACRelay

Parameter	Definition
Capabilities Enabled	<p>A bitmap value used to identify which system capabilities are enabled on the local system, as included in TLVs transmitted by the LLDP agent.</p> <p>The bitmap is defined by the following parameters:</p> <ul style="list-style-type: none">0 – other1 – repeater2 – bridge3 – wlanAccessPoint4 – router5 – telephone6 – docsisCableDevice7 – stationOnly8 – cVLANComponent9 – sVLANComponent10 – twoPortMACRelay

To display the unit's port parameters, as transmitted by the LLDP agents:

1. Select **Ethernet > Protocols > LLDP > Advanced > Local System > Port**. The LLDP Local System Port page opens.

Figure 232 LLDP Local System Port Page

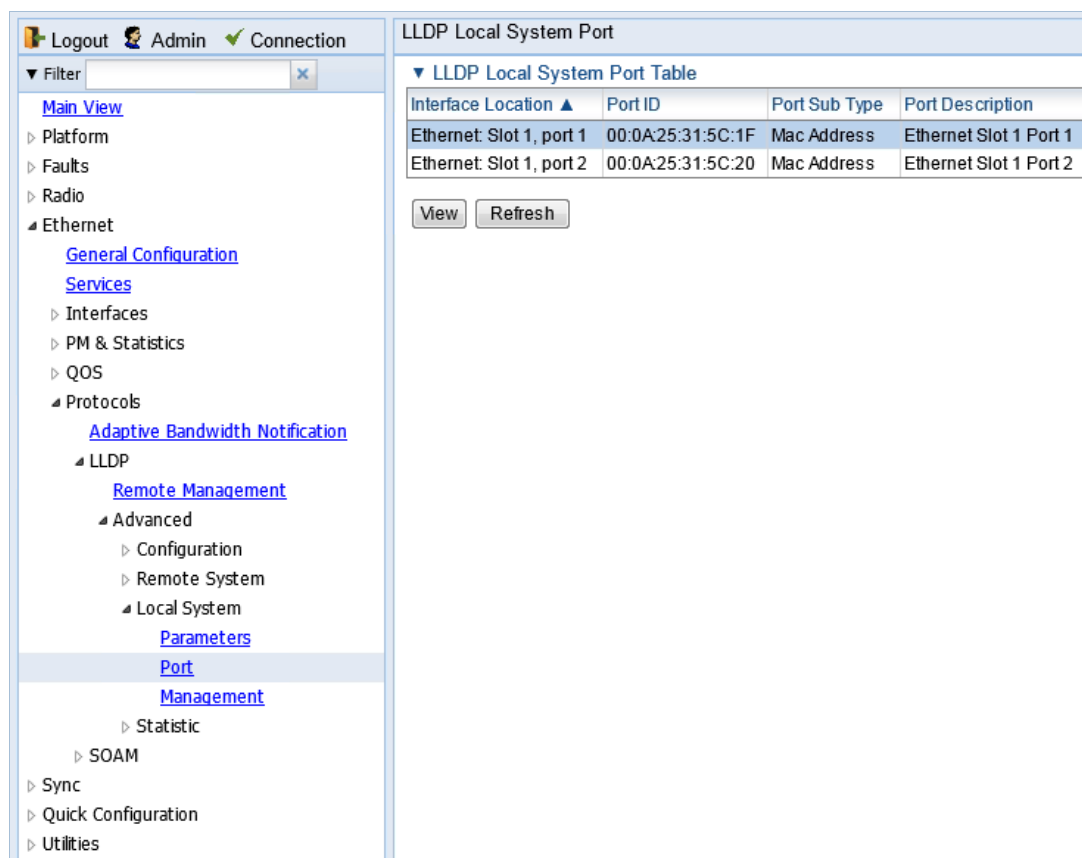


Table 54 describes the parameters in the LLDP Local System Port page. These parameters are read-only.

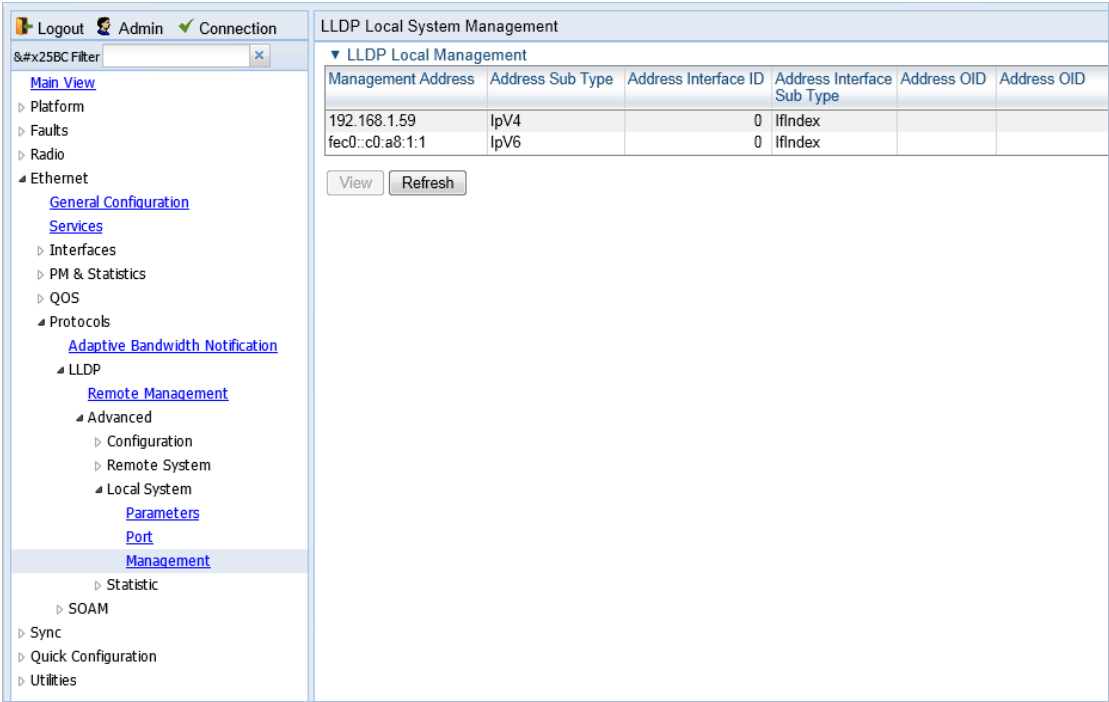
Table 54 LLDP Local System Port Parameters

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.

Figure 233 LLDP Local System Management Page



2. To display all the parameters, select a row and click **View**.

Figure 234 LLDP Local System Management – View Page

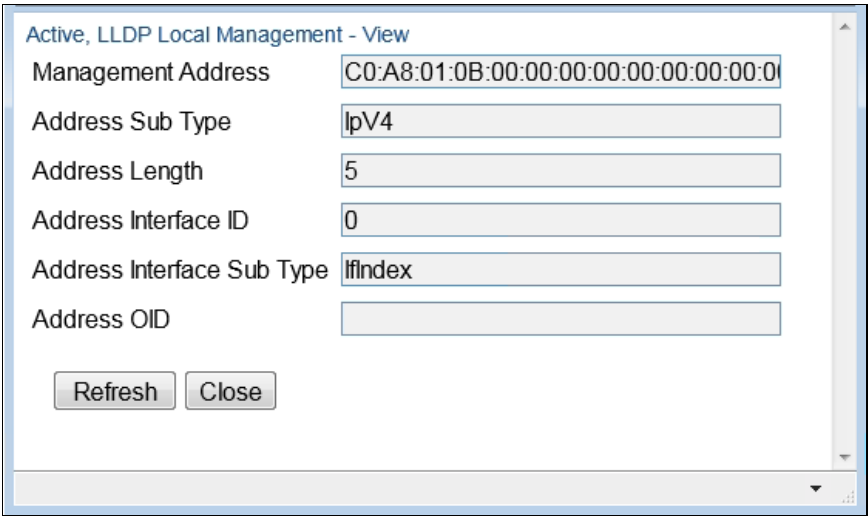


Table 55 describes the parameters in the LLDP Local System Management page. These parameters are read-only.

Table 55 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.

Parameter	Definition
Address Interface ID	Reserved for future use.
Address Interface Sub Type	Reserved for future use.
Address OID	Reserved for future use.

Displaying LLDP Statistics

To display statistics about changes reported via LLDP by the remote unit:

1. Select **Ethernet > Protocols > LLDP > Advanced > Statistic > General**. The LLDP Statistic page opens.

Figure 235 LLDP Statistic Page

The screenshot shows the LLDP Statistic page. On the left, the navigation menu is expanded to 'LLDP > Advanced > Statistic > General'. The main content area is titled 'LLDP Statistic' and contains the following fields:

- Last Change Time: 0 second
- Inserts: 0
- Deletes: 0
- Drops: 0
- Ageouts: 0

A 'Refresh' button is located below the statistics fields.

Table 56 describes the statistics in the LLDP Statistic page.

Table 56 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	<p>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.</p> <p>The RX Ageouts counter in the Port RX page is similar to this counter, but is for specific ports rather than the entire unit.</p>

To display statistics about LLDP transmissions and transmission errors:

1. Select **Ethernet > Protocols > LLDP > Advanced > Statistic > Port TX**. The LLDP Port TX Statistic page opens.

Figure 236 LLDP Port TX Statistic Page

The screenshot shows the LLDP Port TX Statistic page. The left sidebar contains a navigation menu with the following items: Logout, Admin, Connection, Filter, Main View, Platform, Faults, Radio, Ethernet (expanded), General Configuration, Services, Interfaces, PM & Statistics, QOS, Protocols (expanded), Adaptive Bandwidth Notification, LLDP (expanded), Remote Management, Advanced (expanded), Configuration, Remote System, Local System, Statistic (expanded), General, Port TX (selected), Port RX, SOAM, Sync, Quick Configuration, and Utilities. The main content area is titled 'LLDP Port TX Statistic' and contains a table titled 'LLDP Port TX Statistics Table'. The table has four columns: Interface Location, Destination Address, Total Frames, and Errored Length Frames. The table contains two rows of data: 'Ethernet: Slot 1, port 1' with destination address '1:80:c2:0:0:e', total frames '11616', and errored length frames '0'; and 'Ethernet: Slot 1, port 2' with destination address '1:80:c2:0:0:e', total frames '11616', and errored length frames '0'. Below the table are 'View' and 'Refresh' buttons.

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

[Table 57](#) describes the statistics in the LLDP Port TX Statistic page.

Table 57 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	<p>The number of LLDPDU Length Errors recorded for this port and destination MAC address.</p> <p>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.</p>

To display statistics about LLDP frames received by the unit:

Select **Ethernet > Protocols > LLDP > Advanced > Statistic > Port RX**. The LLDP Port TX Statistic page opens.

Figure 237 LLDP Port RX Statistic Page

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

View Refresh

[Table 58](#) describes the statistics in the LLDP Port TX Statistics page.

Table 58 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 agent.
Ageouts	<p>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.</p> <p>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.</p> <p>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.</p>

Chapter 9: Synchronization

This section includes:

- [Configuring the SyncE Regenerator](#)
- [Configuring the Sync Source](#)
- [Configuring the Outgoing Clock and SSM Messages](#)
- [Configuring 1588 Transparent Clock](#)

Configuring the SyncE Regenerator

In SyncE PRC pipe regenerator mode, frequency is transported between two interfaces through the radio link.

With the system acting as a simple link, no distribution mechanism is necessary, resulting in improved frequency distribution performance with PRC quality and a simplified configuration.



Note

SyncE Regenerator currently supports only a single pipe configuration.

To add a pipe configuration:

1. Set the Sync mode to **Pipe**. You must do this via the CLI. Enter the following command in root view:

```
root> platform sync mode set pipe
```



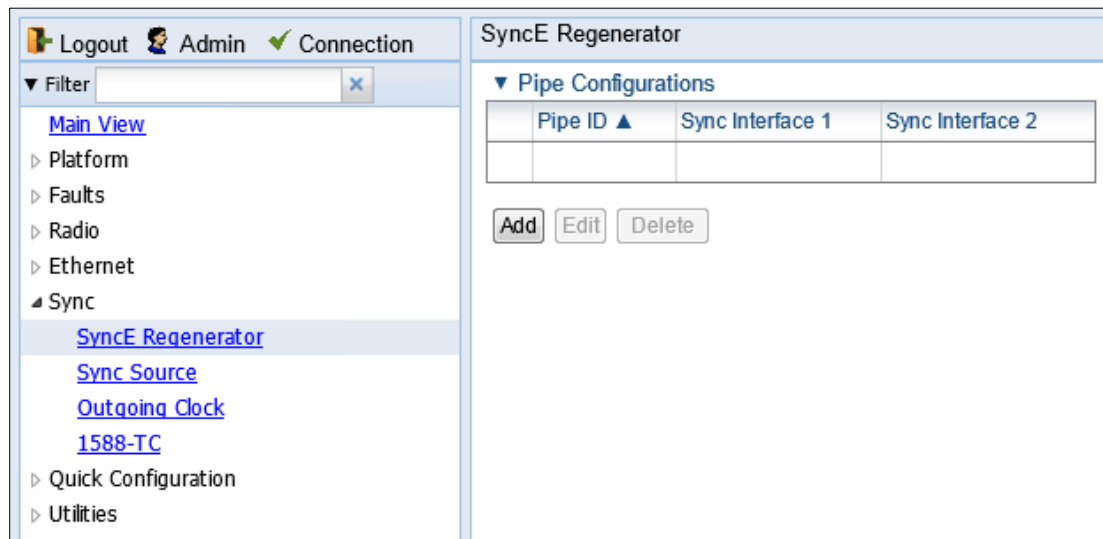
Note

By default, the Sync mode is set to **Automatic**. To display the current Sync mode, enter the following command in root view:

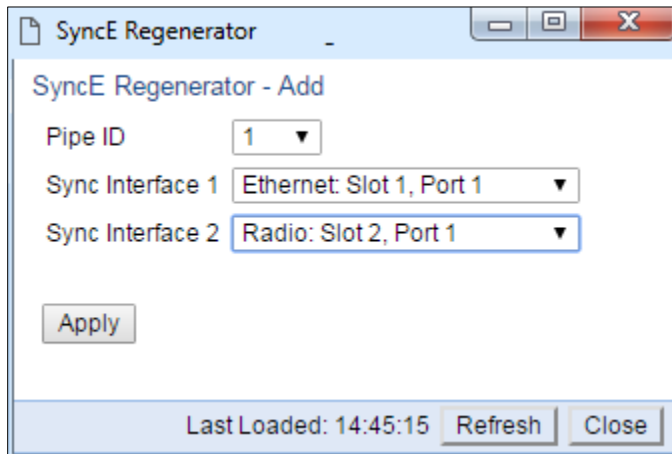
```
root> platform sync mode show
```

2. In the Web EMS, select **Sync > SyncE Regenerator**. The SyncE Regenerator page opens.

Figure 238 SyncE Regenerator Page



3. Click **Add** underneath the Pipe Configurations Table. The Pipe Configuration - Add window opens.

Figure 239 Pipe Configurations - Add PageThe screenshot shows a window titled "SyncE Regenerator" with a subtitle "SyncE Regenerator - Add". Inside the window, there are three configuration fields: "Pipe ID" with a dropdown menu showing "1", "Sync Interface 1" with a dropdown menu showing "Ethernet: Slot 1, Port 1", and "Sync Interface 2" with a dropdown menu showing "Radio: Slot 2, Port 1". Below these fields is an "Apply" button. At the bottom of the window, there is a status bar showing "Last Loaded: 14:45:15" and two buttons, "Refresh" and "Close".

4. Select a Pipe ID.
5. Select one of the available interfaces for each Sync Interface.

**Note**

One of the Sync Interfaces must be a Radio interface and the other must be an Ethernet interface. If the two interfaces are the same type, the operation will fail.
Only one radio port is available for PTP 820S unit.

6. Click **Apply**.

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. 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. To view and configure the Media Type of an Ethernet interface, see [Configuring Ethernet Interfaces](#).

Viewing the Sync Source Status

To view the current sync source and its quality:

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

Figure 240 Sync Source Page

Table 59 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	<p>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.</p> <p>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.</p>

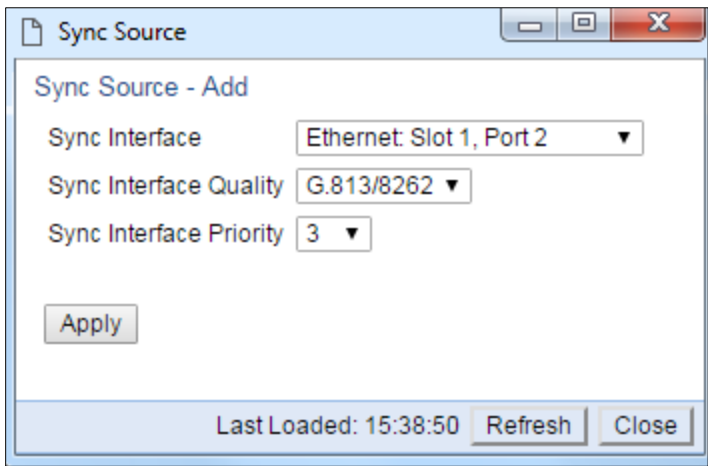
Parameter	Definition
Sync Interface Priority	Displays the priority assigned to this synchronization source.
Sync Interface Quality Status	Displays the current actual synchronization quality of the interface.

Adding a Sync Source

To add a synchronization source:

- 1 In the Sync Source page ([Figure 240](#)), click **Add**. The Sync Source – Add page opens.

Figure 241 Sync Source – Add Page



- 2 In the **Sync Interface** field, select the interface you want to define as a synchronization source. You can select from the following interface types:
 - Ethernet interfaces
 - Radio interface



Note

In order to select an Ethernet interface, you must first specify the media type for this interface. See [Configuring Ethernet Interfaces](#).

- 3 In the **Sync Interface Quality** field, select the quality level applied to the selected synchronization source. This enables the system to select the source with the highest quality as the current synchronization source.
 - If the **Sync Interface Quality** is set to **Automatic**, the quality is determined by the received SSMs. If no valid SSM messages are received or in case of interface failure (such as LOS, LOC, LOF), the quality becomes **Failure**. SSM must be enabled on the remote interface in order for the interface to receive SSM messages. For instructions how to enable SSM, see [Configuring the Outgoing Clock and SSM Messages](#).
 - If the **Sync Interface Quality** is set to a fixed value, then the quality status becomes **Failure** upon interface failure (such as LOS, LOC, LOF).

- 4 In the **Sync Interface Priority** field, select the priority of this synchronization source relative to other synchronization sources configured in the unit (1-16). You cannot assign the same priority to more than one synchronization source. Once a priority value has been assigned, it no longer appears in the **Sync Interface Priority** dropdown list.
- 5 Click **Apply**, then **Close**.

Editing a Sync Source

To edit a synchronization source:

- 1 In the Sync Source page ([Figure 240](#)), 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 240](#)).
- 2 Click **Delete**. The synchronization source is deleted.

Configuring the Outgoing Clock and SSM Messages

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 820C implements the passing of SSM messages over the radio interfaces. SSM timing in PTP 820C 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
```

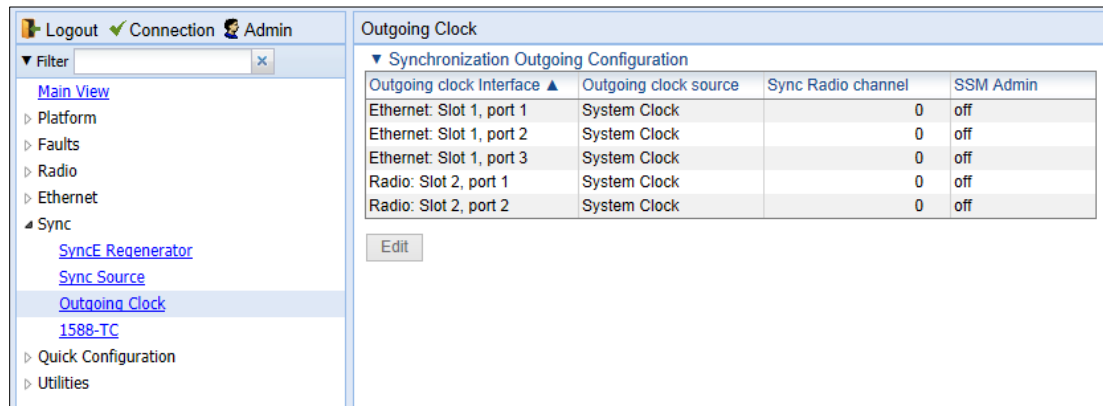
If the Sync mode is set to pipe, you must set it to automatic by entering the following CLI command in root view:

```
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](#).

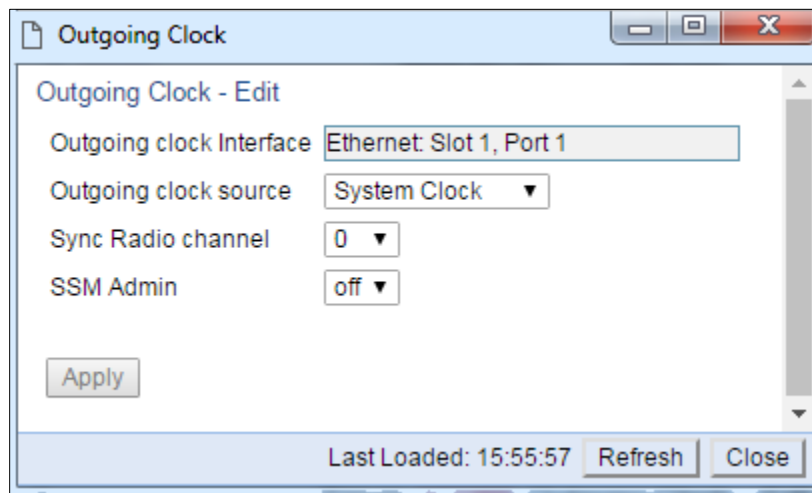
To view and configure the synchronization parameters of the unit’s interfaces:

- 1 Select **Sync > Outgoing Clock**. The Outgoing Clock page opens.

Figure 242 Outgoing Clock Page

2 Select

the interface you want to configure and click **Edit**. The Outgoing Clock – Edit page opens.

Figure 243 Outgoing Clock – Edit Page

- 3 In the **Outgoing clock source** field, select the interface's synchronization source. Options are:
 - **Local Clock** – The interface uses its internal clock as its synchronization source.
 - **System Clock** – Default value. The interface uses the system clock as its synchronization source.
 - **Source Interface** – Reserved for future use.
 - **Time Loop** – Reserved for future use.
- 4 In **Sync Radio Channel** field, use the default value of 0.
- 5 In the **SSM Admin** field, select **On** or **Off** to enable or disable SSM for the interface. By default, SSM is disabled on all interfaces.

Configuring 1588 Transparent Clock

**Note**

1588 Transparent Clock is supported by PTP 820C and PTP 820S.

PTP 820 uses 1588v2-compliant Transparent Clock to counter the effects of delay variation. Transparent Clock measures and adjusts for delay variation, enabling the PTP 820 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 G10.0:

- 1588 TC is not supported when Master-Slave communication is using the IPv6 transport layer.
 - 1588 TC cannot be used on 1+1 HSB links.
 - 1588 TC is not supported with Frame Cut-Through.
-

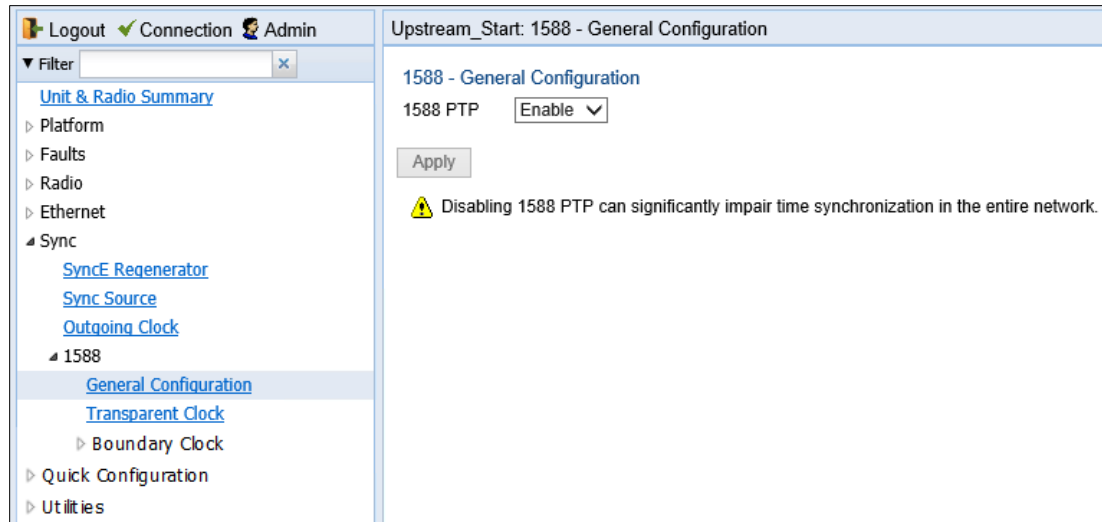
**Note**

Make sure to enable Transparent clock on the remote side of the link before enabling it on the local side.

To configure Transparent Clock:

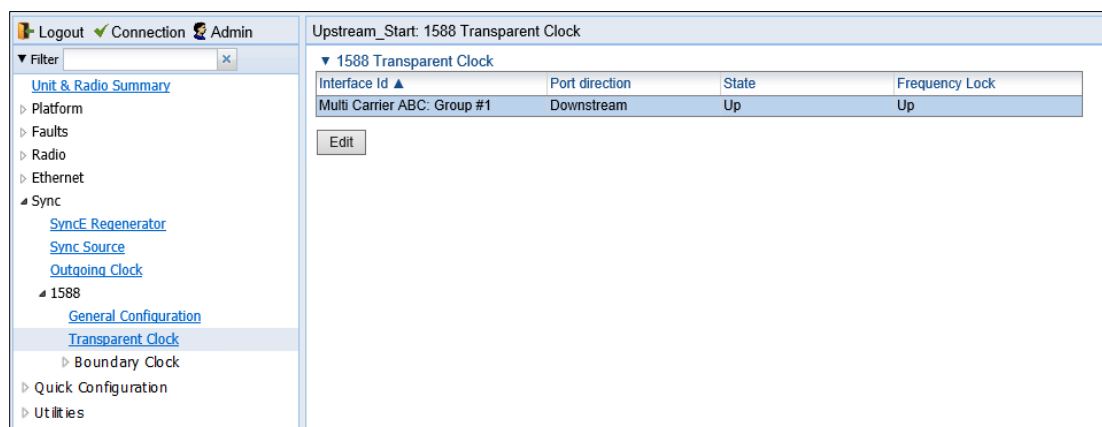
1. Add the port receiving synchronization from the customer side as a Sync source, with Sync Interface Priority 1. See [Adding a Sync Source](#).
2. Add a radio interface as a Sync source, with lower priority than the port receiving synchronization from the customer side. See [Adding a Sync Source](#).
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.

Figure 244 1588-TC Page



7. In the **1588 PTP** field, select **Enable**.
8. Click **Apply**.
9. Select **Sync > 1588 > Transparent Clock**. The 1588 Transparent Clock page opens.

Figure 245 1588 Transparent Clock Page



10. Select a radio interface or Multi-Carrier ABC group and click **Edit**. The 1588 Transparent Clock – Edit page opens.

Figure 246 1588-TC – Edit Page

11. In the **Port direction** field, select **Upstream** or **Downstream**. This field must be set to different values on two sides of the link so that if local side is set to **Upstream**, then the remote side of the link must be set to **Downstream** and vice versa. Otherwise than the mentioned configuration, it does not matter how this field is set.
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:
14. To map 1588 packets to CoS 7, enter the following command:

```
root> ethernet generalcfg ptp-tc cos-preserve set admin disable
```

```
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.

Chapter 10: Access Management and Security

This section includes:

- [Configuring the General Access Control Parameters](#)
- [Configuring the Password Security Parameters](#)
- [Configuring the Session Timeout](#)
- [Configuring Users](#)
- [Configuring RADIUS](#)
- [Configuring X.509 CSR Certificates](#)
- [Uploading the Security Log](#)
- [Uploading the Configuration Log](#)

Related topics:

- [Changing Your Password](#)
- [Operating in FIPS Mode](#)
- [Configuring AES-256 Payload Encryption](#)

Configuring the General Access Control Parameters

To avoid unauthorized login to the system, PTP 820 automatically blocks users upon a configurable number of failed login attempts. You can also configure PTP 820 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 247 Access Control General Configuration Page

The screenshot shows the 'Access Control General Configuration' page. The left sidebar has a tree view with the following structure:

- Platform
 - Management
 - Software
 - Configuration
 - Activation Key
 - Security
 - General (selected)
 - X.509 Certificate
 - Access Control
 - General (selected)
 - User Profiles
 - User Accounts
 - Password Management
 - Change Password
 - Radius
 - Protocols Control
 - Faults
 - Radio
 - Ethernet
 - Sync
 - Quick Configuration
 - Utilities

The main content area is titled 'Access Control General Configuration' and contains the following fields:

- Failure login attempts to block user: (1..10)
- Blocking period (Minutes): (1..60)
- Unused account period for blocking (Days): (0..90)

At the bottom of the main content area are two buttons: 'Apply' and 'Refresh'.

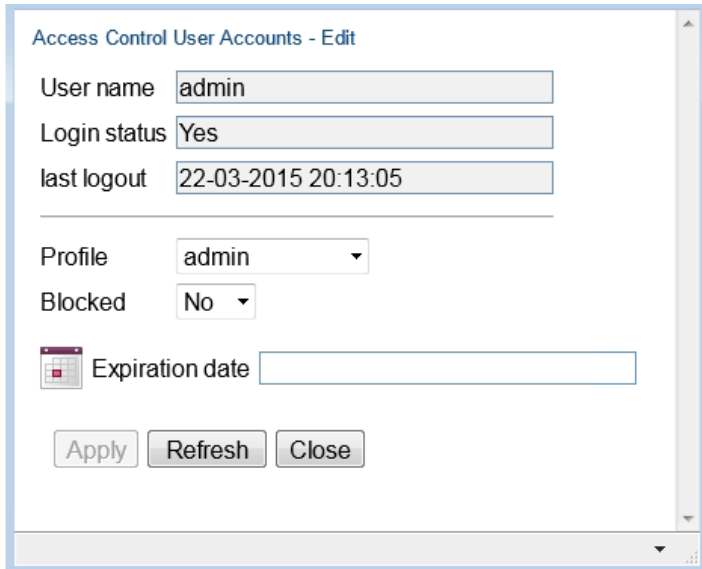
2. In the **Failure login attempts to block user** field, select the number of failed login attempts that will trigger blocking. If a user attempts to login to the system with incorrect credentials this number of times consecutively, the user will temporarily be prevented from logging into the system 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 253).
2. Select the user and click **Edit**. The Access Control User Accounts - Edit page opens.

Figure 248 Access Control User Accounts - Edit Page



Access Control User Accounts - Edit


User name

Login status

last logout

Profile

Blocked

 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 249 Access Control Password Management Page

The screenshot shows the 'Access Control Password Management' page. On the left, a navigation pane lists various system components. Under 'Platform', 'Security' is expanded, and 'Access Control' is selected. Within 'Access Control', 'Password Management' is highlighted. The main area displays three configuration options: 'Enforce password strength' set to 'No', 'Password change for first login' set to 'Yes', and 'Password aging (Days)' set to 'No Aging'. There are 'Apply' and 'Refresh' buttons at the bottom of the configuration section.

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.
 - A password cannot be repeated within five changes in password.
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**.

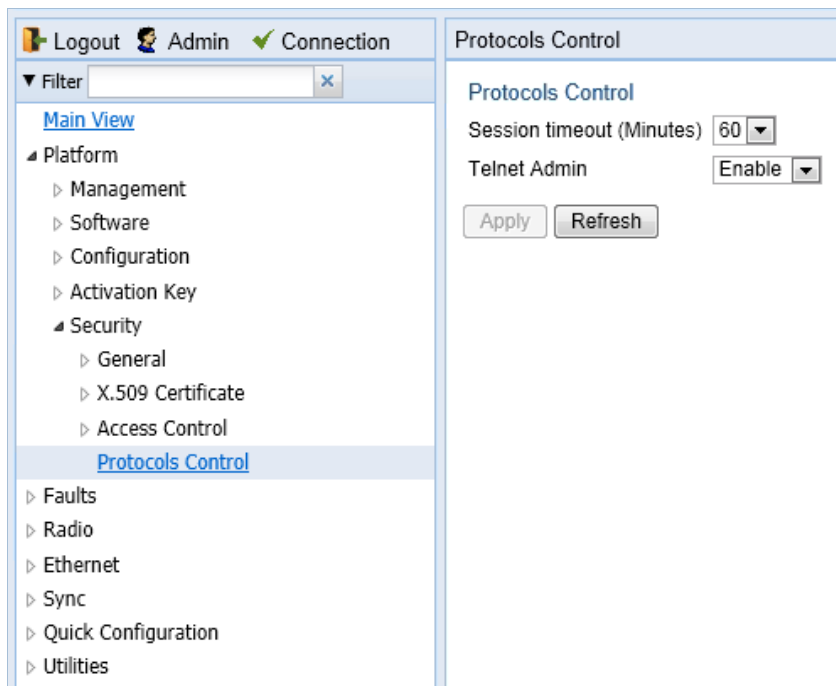
Configuring the Session Timeout

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 250 Protocols Control Page



2. In the **Session timeout (Minutes)** field, select a session timeout, in minutes, from 1 to 60.
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 820 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 251 Access Control User Profiles Page

The screenshot shows the 'Access Control User Profiles' page. On the left is a sidebar with a 'Filter' box and a 'Main View' section. The 'Main View' contains a tree structure with 'Platform' expanded, showing 'Management', 'Software', 'Configuration', 'Activation Key', and 'Security'. Under 'Security', 'General' is selected, and 'User Profiles' is highlighted. Other links include 'User Accounts', 'Password Management', 'Change Password', 'Radius', and 'Protocols Control'. The main content area is titled 'Access Control User Profiles' and contains a table labeled 'Users profile configuration table'. The table has four columns: 'Profile', 'Permitted access channels', and 'Usage counter'. Below the table are buttons for 'Add', 'Edit', 'Delete', and 'Refresh'.

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 252 Access Control User Profiles - Add Page

3. In the **Profile** field, enter a name for the profile. The profile name can include up to 49 characters. Once you have created the user profile, you cannot change its name.

**Note**

The **Usage counter** field displays the number of users to whom the user profile is assigned.

4. In the **Permitted access channels** row, select the access channels the user will be permitted to use to access the system.
5. For each functionality group, select one of these options for write level and read level. All users with this profile will be assigned these access levels:
 - **None**
 - **Normal**
 - **Advanced**
6. Click **Apply**, then **Close**.

To view a user profile, click + next to the profile you want to view.

To edit a user profile, select the profile and click **Edit**. You can edit all of the profile parameters except the profile name.

To delete a user profile, select the profile and click **Delete**.

**Note**

You cannot delete a user profile if the profile is assigned to any users.

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 253 Access Control User Accounts Page

The screenshot shows the 'Access Control User Accounts' page. On the left is a navigation pane with a tree structure. The 'Security' section is expanded, and 'User Accounts' is selected. The main content area has a title 'Access Control User Accounts' and a 'Users table' section. The table has columns: Username, Profile, Blocked, Login status, last logout, and Expiration date. There is one row for the user 'admin' with profile 'admin', blocked status 'No', login status 'Yes', and last logout '21-09-2015 10:52:35'. Below the table are buttons for 'Add', 'Edit', 'Delete', and 'Refresh'.

Username	Profile	Blocked	Login status	last logout	Expiration date
admin	admin	No	Yes	21-09-2015 10:52:35	

2. Click **Add**. The Access Control User Profiles - Add page opens.

Figure 254 Access Control User Accounts - Add Page

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](#)
- [Viewing RADIUS User Permissions and Connectivity](#)
- [Configuring a RADIUS Server](#)

RADIUS Overview

The RADIUS protocol provides centralized user management services. PTP 820 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 820 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 > Radius > Radius Configuration**. The Radius Configuration page opens.

Figure 255 Radius Configuration Page

Logout Admin Connection

Filter

Main View

- Platform
 - Management
 - Software
 - Configuration
 - Activation Key
- Security
 - General
 - X.509 Certificate
 - Access Control
 - General
 - User Profiles
 - User Accounts
 - Password Management
 - Change Password
 - Radius
 - Radius Configuration**
 - Radius Users
 - Protocols Control
- Faults
- Radio
- Ethernet
- Sync
- Quick Configuration
- Utilities

Radius Configuration

Radius Enabled

Radius Admin Disable

Apply

Radius Configuration Table

Server Id ▲	Connectivity Status	IPv4 address	Port	Retries	Timeout
1	False	0.0.0.0	1812	3	5
2	False	0.0.0.0	1812	3	5

Edit Refresh

2. In the **Radius Admin** field, select **Enable**.
3. Click **Apply**.

Configuring the RADIUS Server Attributes

To configure the RADIUS server attributes:

1. Select **Platform > Security > Access Control > Radius > Radius Configuration**. The Radius Configuration page opens (Figure 255).
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 256 Radius Configuration – Edit Page

Active, Radius Configuration Table - Edit

Server Id	1
Connectivity Status	False
IPV4 address	0.0.0.0
Port	1812 (0..65535)
Retries	3 (3..30)
Timeout	5 (1..10)
Secret	••••••••

Apply Refresh Close

4. In the **IPV4 address** field, enter the IP address of the RADIUS server.
5. In the **Port** field, enter the port ID of the RADIUS protocol in the RADIUS server.
6. In the **Retries** field, enter the number of times the unit will try to communicate with the RADIUS server before declaring the server to be unreachable.
7. In the **Timeout** field, enter the timeout (in seconds) that the agent will wait in each communication with the selected RADIUS server before retrying if no response is received.
8. In the **Secret** field, enter the shared secret of the RADIUS server. The string must be between 22-128 characters long.
9. Click **Apply**, then **Close**.

In addition to the configurable parameters described above, the Radius Configuration page displays the following information for each RADIUS server:

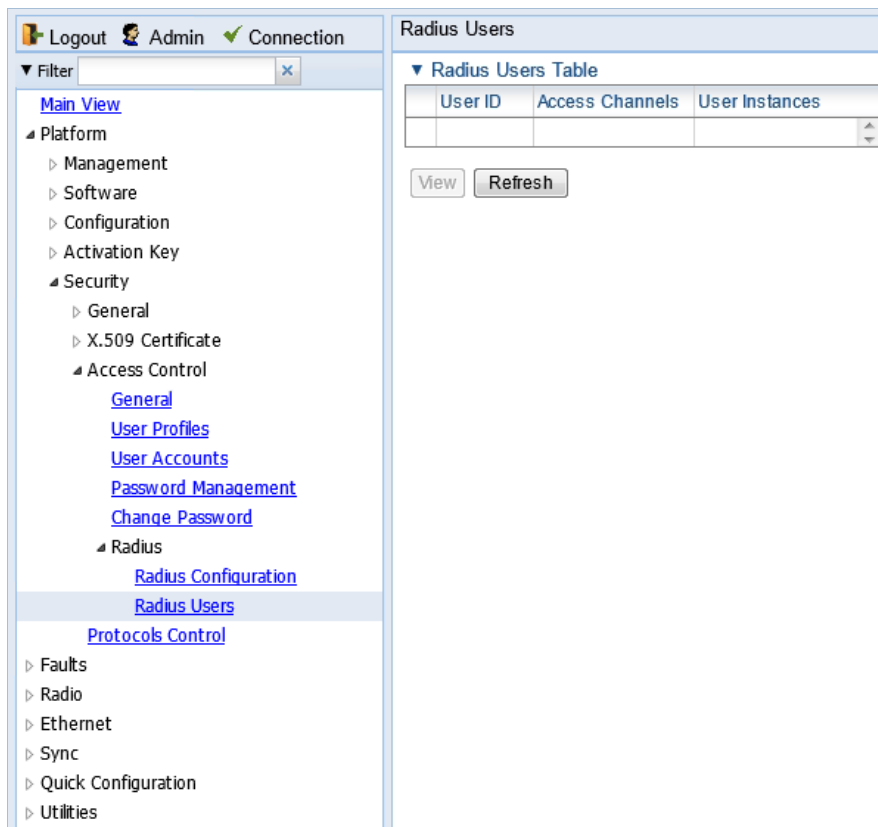
- **Server Id** – The server ID of the Radius server:
 - **1** – The primary Radius server.
 - **2** – The secondary Radius server.
- **Connectivity Status** – The connectivity status of the Radius server in the last attempted connection:
 - **True** – The last connection attempt succeeded.
 - **False** – The last connection attempt failed.

Viewing RADIUS User Permissions and Connectivity

You can view RADIUS user connectivity and permissions information for all Radius users currently connected.

To view RADIUS users:

1. Select **Platform > Security > Access Control > Radius > Radius Users**. The Radius Users page opens.

Figure 257 Radius Users Page

- The **User ID** column displays the user's name.
- The **Access Channels** column displays the access channels the user is allowed to use to access the unit.
- The **User Instances** column displays the number of open sessions the user currently has.

To view the user's authorized access levels, click + next to the user name. The page refreshes and displays the additional access level information.

Figure 258 Radius Users Page – Expanded

Radius table		
User ID	Access Channels	User Instances
u1	Serial+Telnet+SSH+Web+NMS+SNMP+SNMPv3	4
Ethernet access levels Write - Advanced; Read - Advanced		
Management access levels Write - Advanced; Read - Advanced		
Radio access levels Write - Advanced; Read - Advanced		
Security access levels Write - Advanced; Read - Advanced		
Sync access levels Write - Advanced; Read - Advanced		
TDM access levels Write - Advanced; Read - Advanced		

For each of the six functional groups (**Ethernet**, **Management**, **Radio**, **Security**, **Sync**, **TDM**), the page displays the Read access level (**None**, **Regular**, or **Advanced**), and the Write access level (**None**, **Regular**, or **Advanced**).

Configuring a RADIUS Server

If you want to use the PTP 820 RADIUS feature, you must first install a RADIUS server and configure it to work with the PTP 820 device.

The following subsections describe how to configure a Win2008 RADIUS server and a Linux FreeRADIUS server to work with a PTP 820. 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.

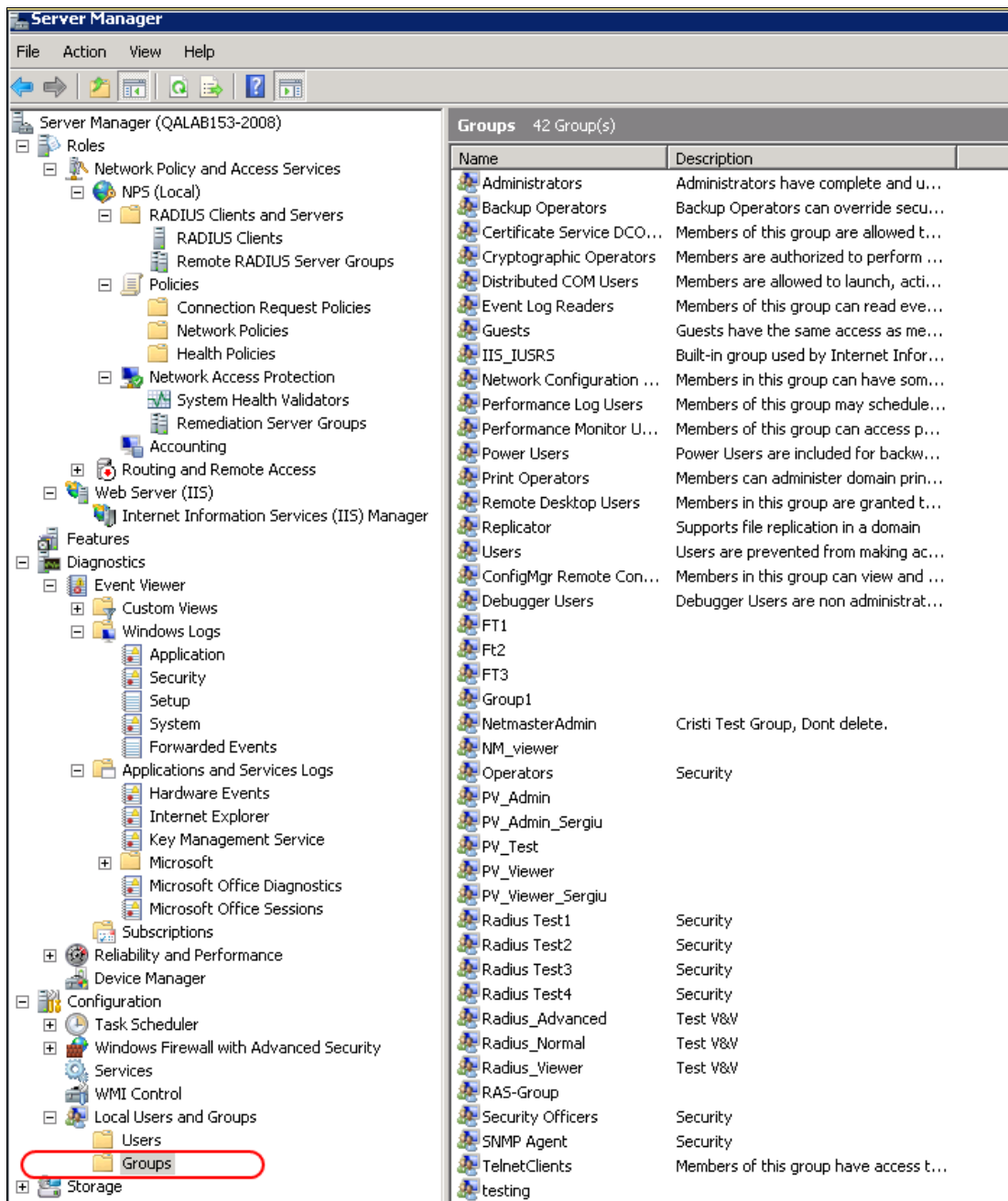
Configuring a Win 2008 RADIUS Server

The following sub-sections describe how to configure a Win 2008 RADIUS Server to work with a PTP 820 device.

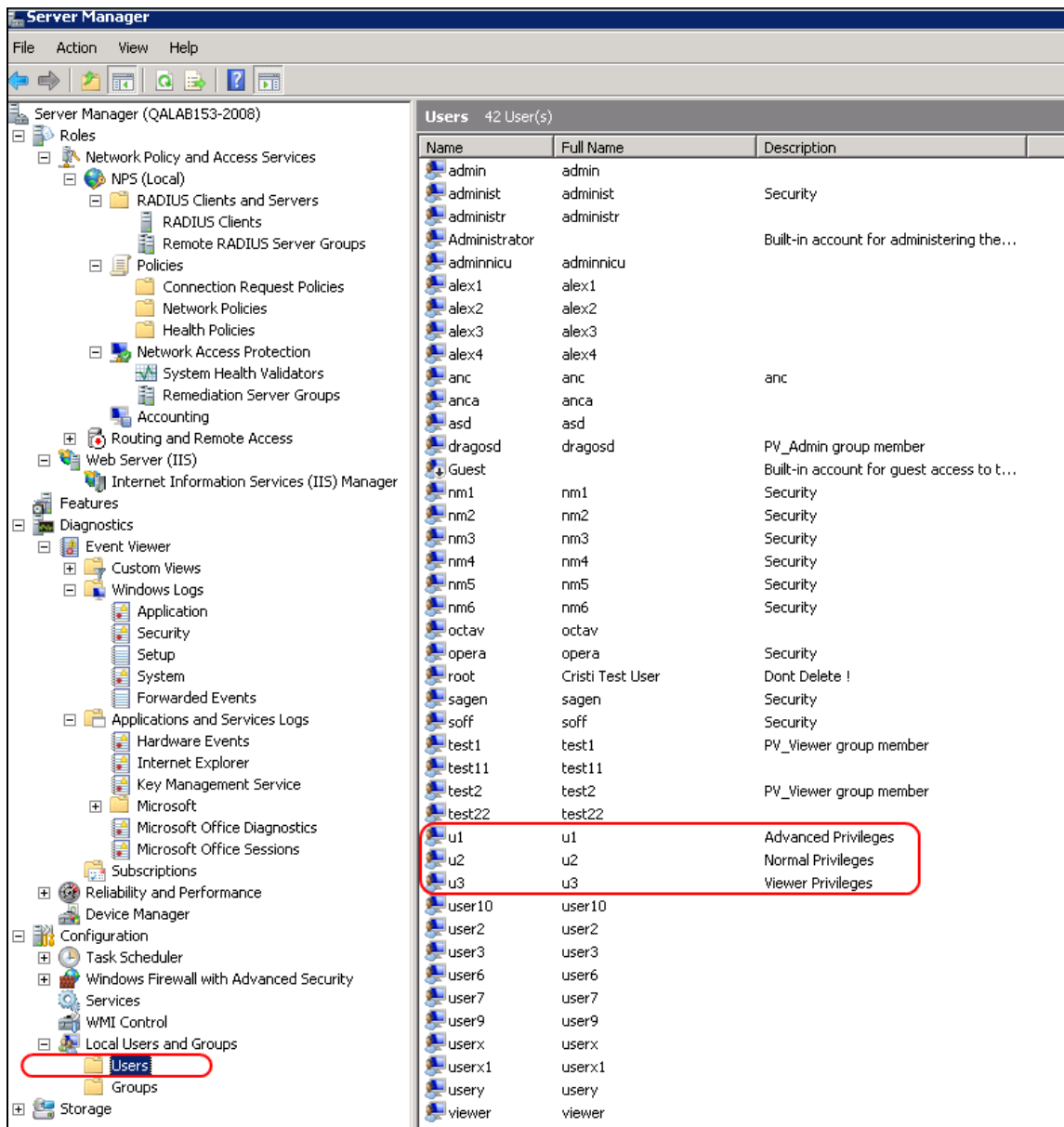
Step 1 – Creating Groups and Users

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 259 Server Manager – Creating User Groups**2 Create three users:**

- u1
- u2
- u3

Figure 260 Server Manager – Creating Users

3 Attach each user to a group, as follows:

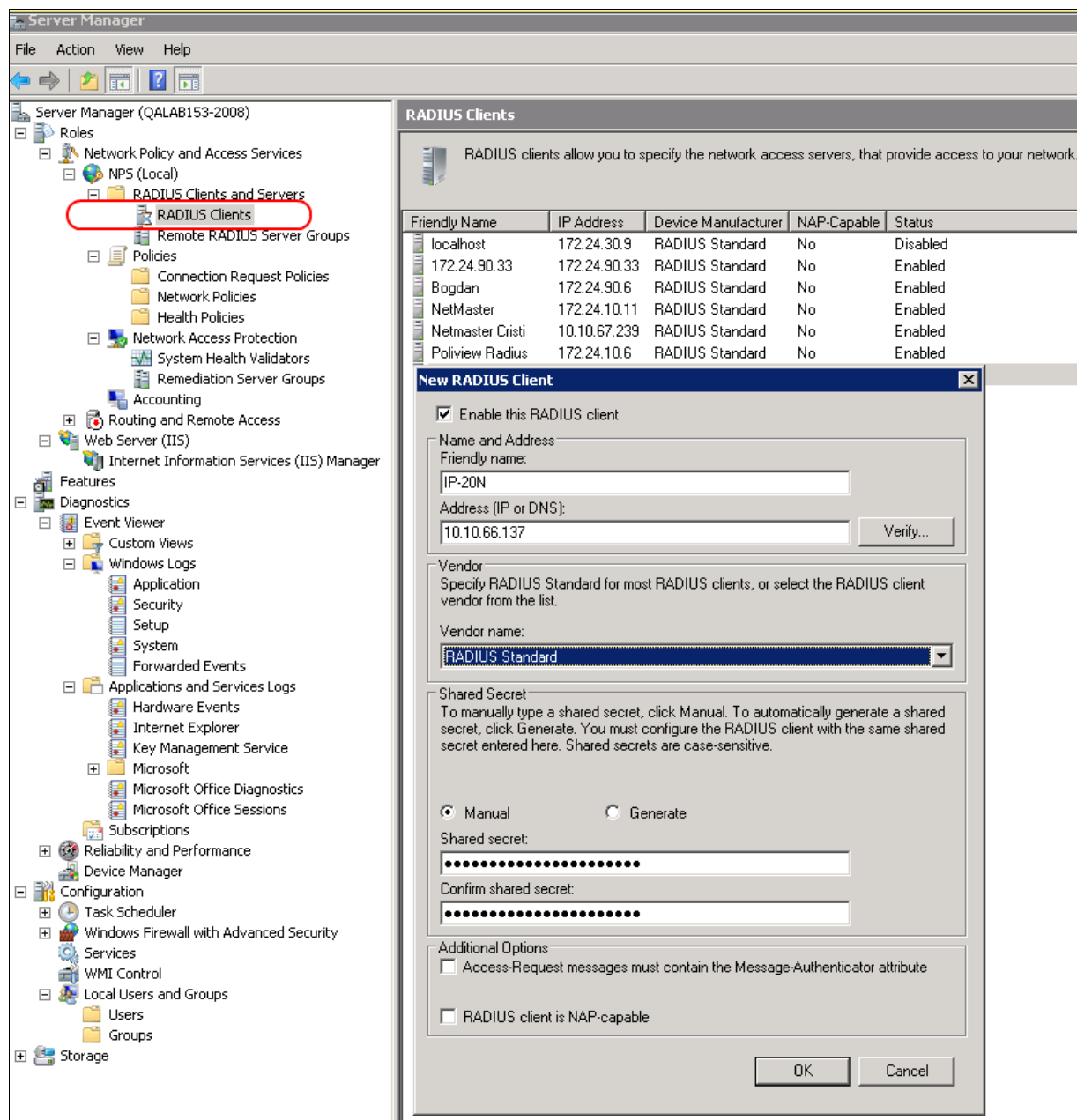
- Attach u1 to Radius_Advanced
- Attach u2 to Radius_Normal
- Attach u3 to Radius_Viewer

Step 2 – Creating a RADIUS Client

Define the PTP 820 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 261 Server Manager – Creating a RADIUS Client



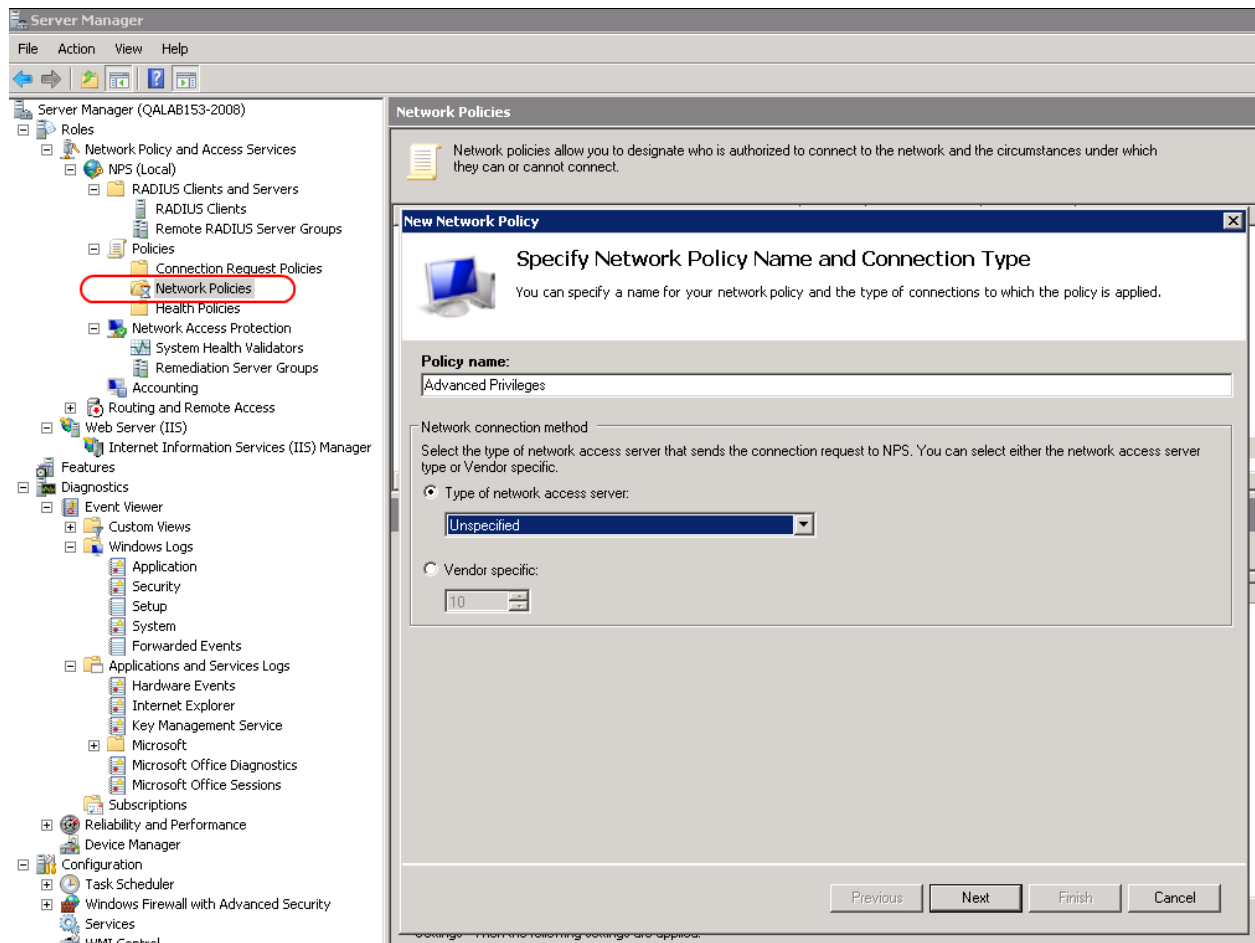
- 3 In the New RADIUS Client window:
 - i Select the **Enable this RADIUS client** check box.
 - ii Enter a descriptive **Friendly name** for the device, such as **PTP 820X**.
 - iii Enter the device IP **Address**.
 - iv Select **RADIUS Standard** as the **Vendor name**.
 - v In the **Shared Secret** 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 ([Figure 256](#)).

Step 3 – Creating a Network Policy

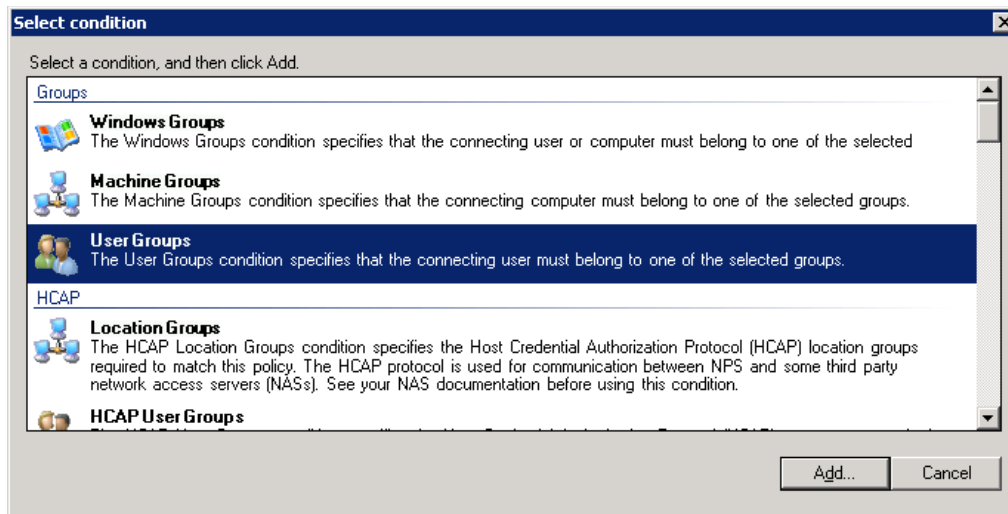
Create a network policy for each of the three groups you created: Radius_Advanced, Radius_Normal, Radius_Viewer. That is, follow the instructions in this section, for each of the three groups.

To create a network policy:

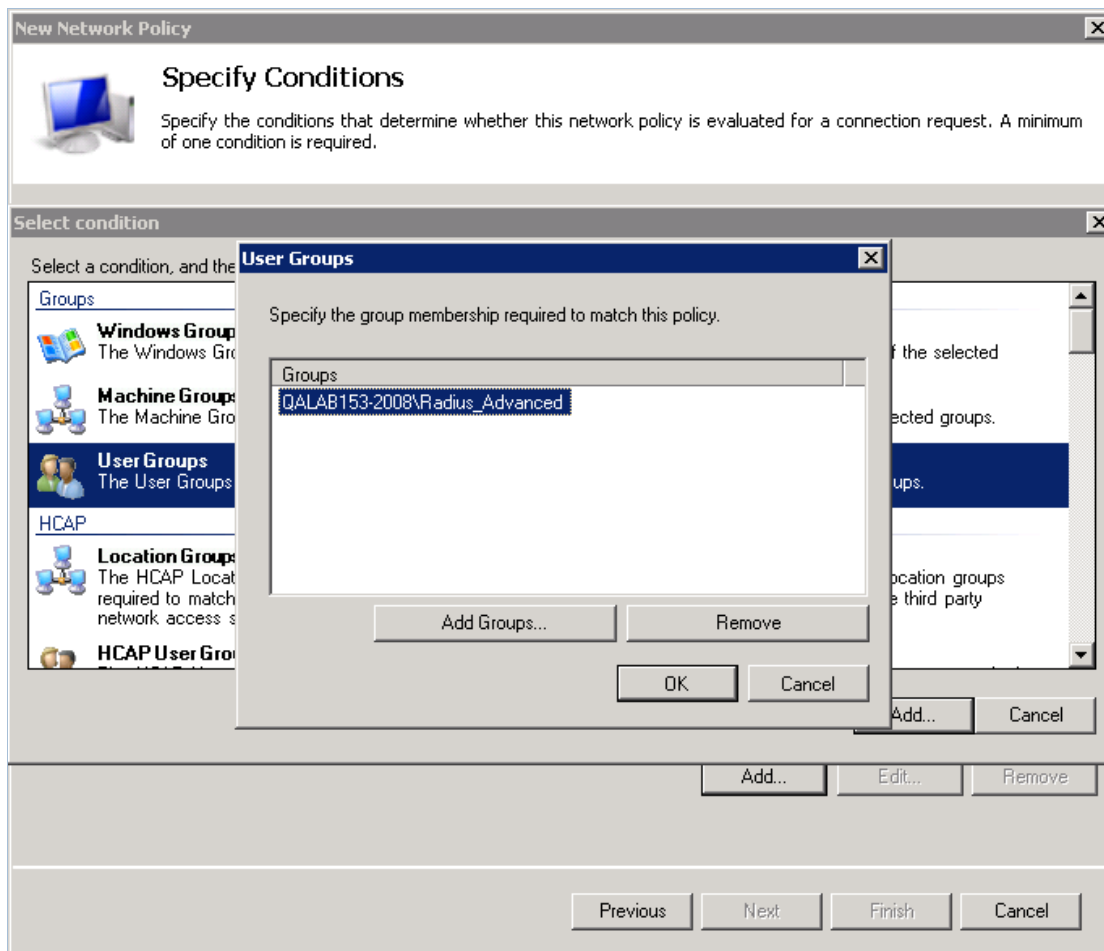
- 1 In the Server Manager, navigate to **Roles > Network Policy and Access Service > NPS (Local) > Policies > Network Policies**.
- 2 Right-click **Network Policies**, and select **New**. The New Network Policy wizard appears.
- 3 In the specify Network Policy Name and Connection Type, give the policy a descriptive name, indicating whether it is a policy for the Advanced, the Normal or the Viewer group.

Figure 262 Create Network Policy – Specify Name and Connection Type

- 4 Click **Next**.
- 5 In the Specify Conditions window, click **Add**.
- 6 In the Select Condition window that appears, select the **User Groups** condition and click **Add**.

Figure 263 Create Network Policy – Select Condition

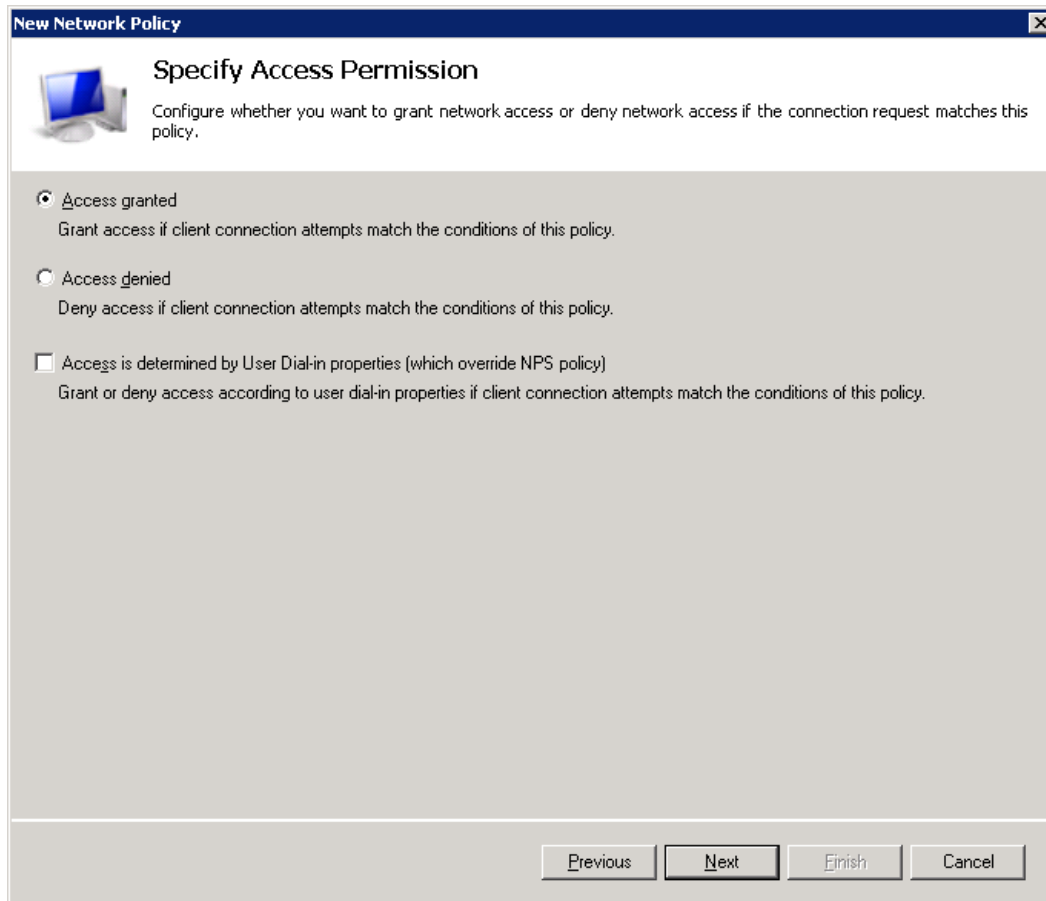
- 7 In the User Groups window that appears, click **Add Groups**.
- 8 In the Select Group window that appears, click **Advanced**.
- 9 In the Select Group window that appears, click **Find Now** to list all groups, and then select the appropriate group from the list: Radius_Advanced, Radius_Normal, or Radius_Viewer.
- 10 Click **OK**.

Figure 264 Create Network Policy – User Group added to Policy's Conditions

- 11 Click **OK** to save settings.
- 12 Click **Next**.

- 13 In the Specify Access Permission window that appears, select the **Access Granted** option.

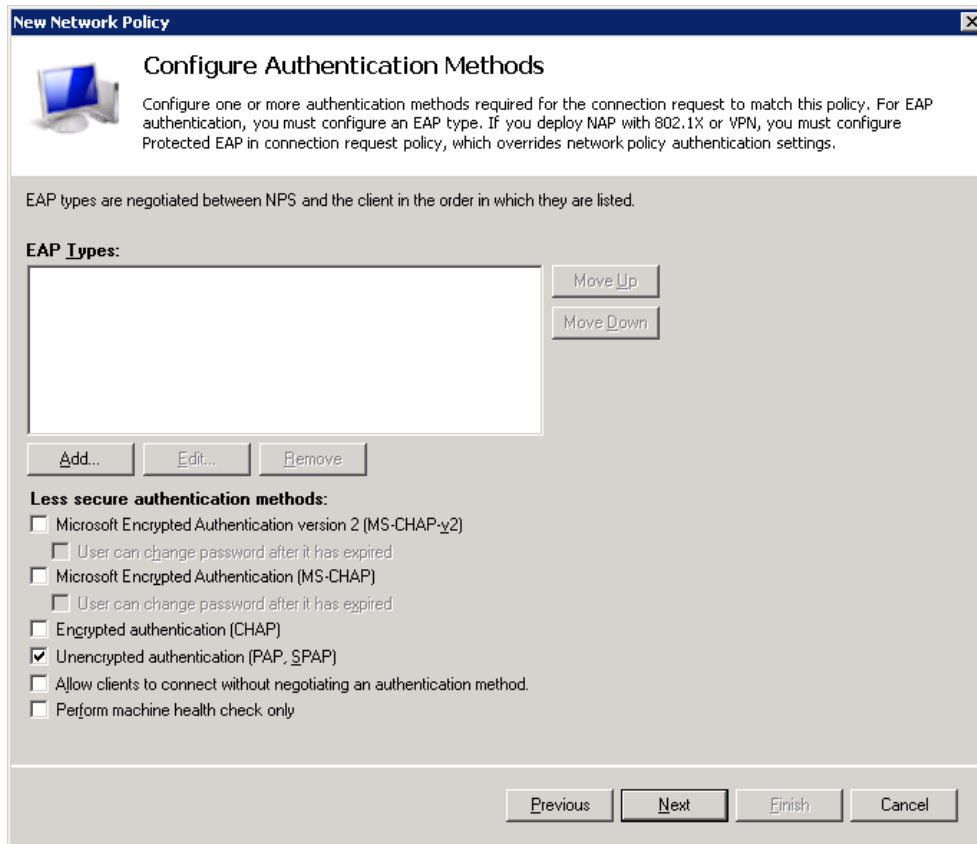
Figure 265 Create Network Policy – Specifying Access Permission



- 14 Click **Next**.

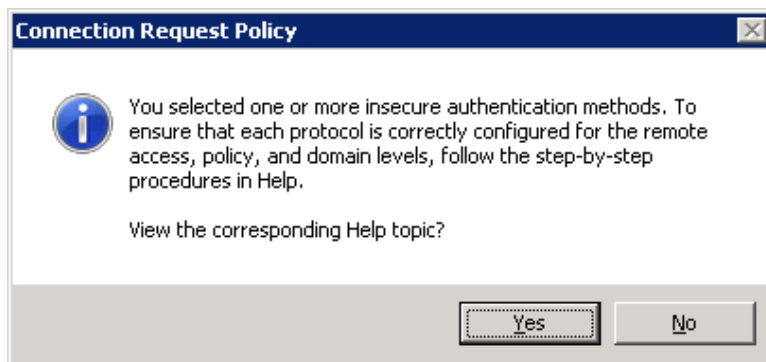
- 15 In the Configure Authentication Methods window that appears, make sure only the **Unencrypted Authentication (PAP, SPAP)** option is selected.

Figure 266 Create Network Policy – Configuring Authentication Methods



- 16 In the query window that appears, click **No**.

Figure 267 Create Network Policy – Insecure Authentication Method Query



17 In the Configure Constraints window that appears, click **Next**.

Figure 268 Create Network Policy – Configuring Constraints

New Network Policy

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

- Constraints**
- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

☐ Disconnect after the maximum idle time

1

Previous Next Finish Cancel

18 In the Configure Settings window that appears:

- i Remove all **Standard** RADIUS attributes. Make sure the Attributes table is empty.

Figure 269 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:

RADIUS Attributes

- ☒ Standard
- ☐ Vendor Specific

Network Access Protection

- ☐ NAP Enforcement
- ☐ Extended State

Routing and Remote Access

- ☐ Multilink and Bandwidth Allocation Protocol (BAP)
- ☐ IP Filters
- ☐ Encryption
- ☒ IP 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

Add... Edit... Remove

Previous Next Finish Cancel

- 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 270 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

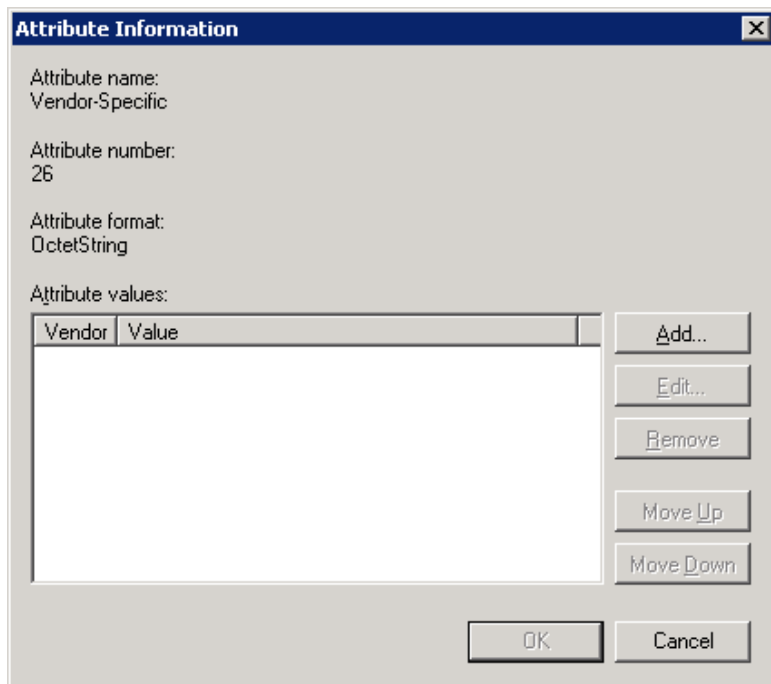
Description:

Specifies the support of proprietary NAS features.

Add... Close

20 In the Attribute Information window that appears, click **Add**.

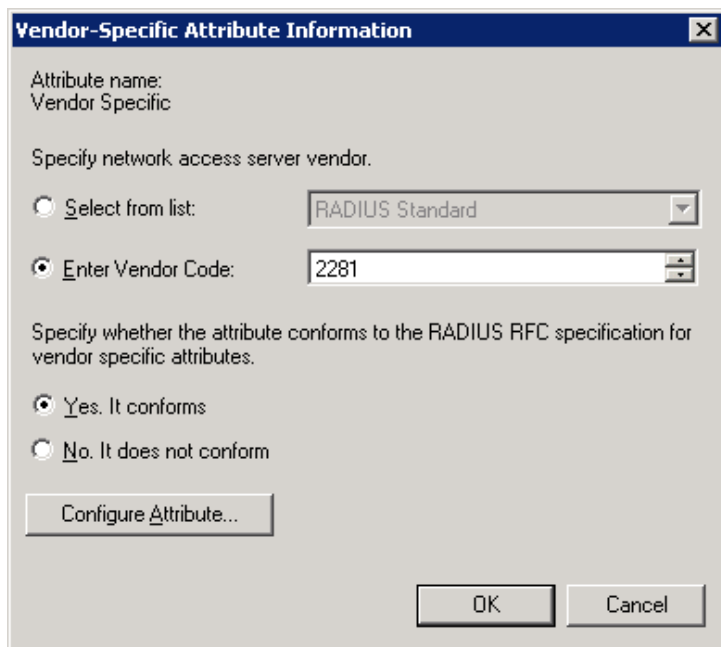
Figure 271 Create Network Policy – Selecting to Add Attribute Information



21 In the Vendor-Specific Attribute Information window that appears:

- i Select **Enter Vendor Code**.
- ii Enter **2281** in the **Enter Vendor Code** field.
- iii Select the option **Yes. It conforms**.
- iv Click **Configure Attribute**.

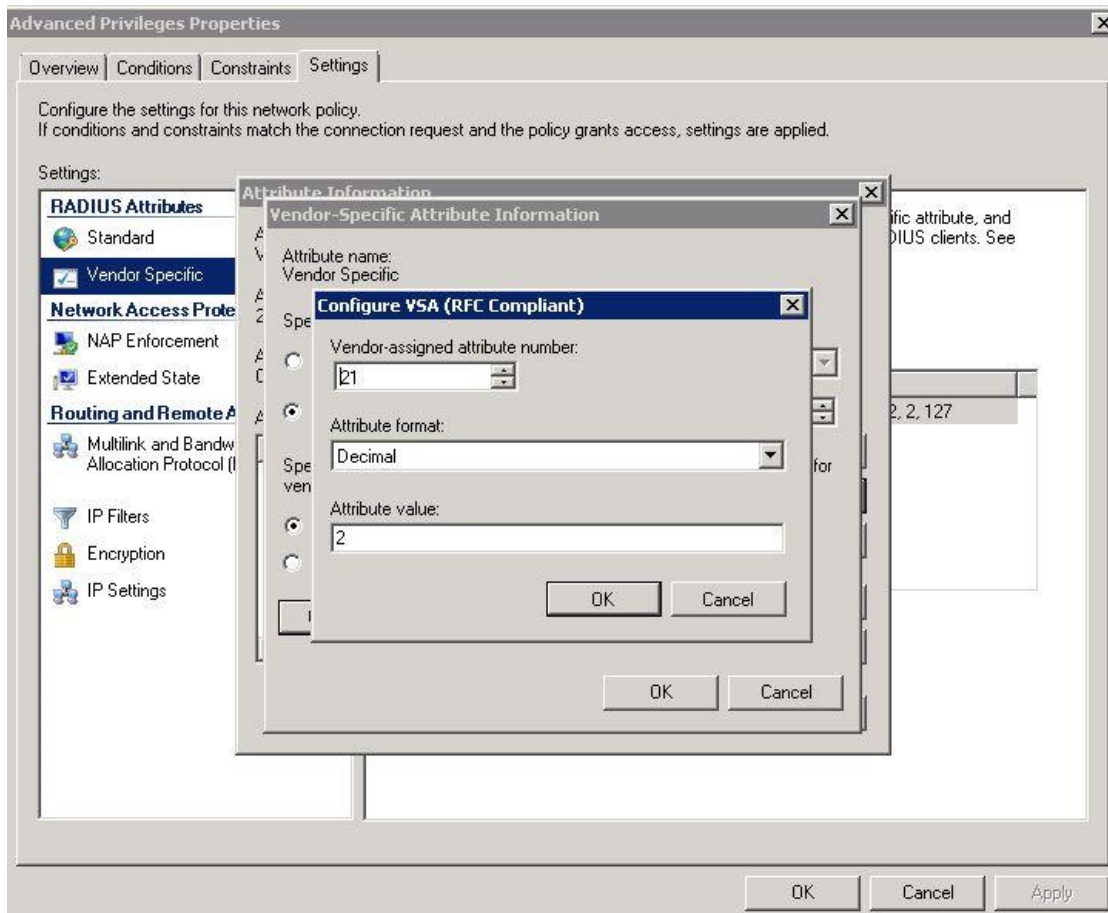
Figure 272 Create Network Policy – Specifying the Vendor



- 22 In the Configure VSA (RFC Compliant) window that appears, configure 13 attributes as follows:
- For **Vendor-assigned attribute number** from 21 till 32, select **Decimal** in the **Attribute format** field. These twelve attributes define the Read access level (None, Regular, or Advanced), and the Write access level (None, Regular, or Advanced) for each of the six functional groups (Ethernet, Management, Radio, Security, Sync, TDM). Therefore, in the **Attribute value** field enter the value corresponding to the access level you wish to permit to members of the group whose policy you are configuring, where:
 - 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 273 Create Network Policy – Configuring Vendor-Specific Attribute Information



- 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;

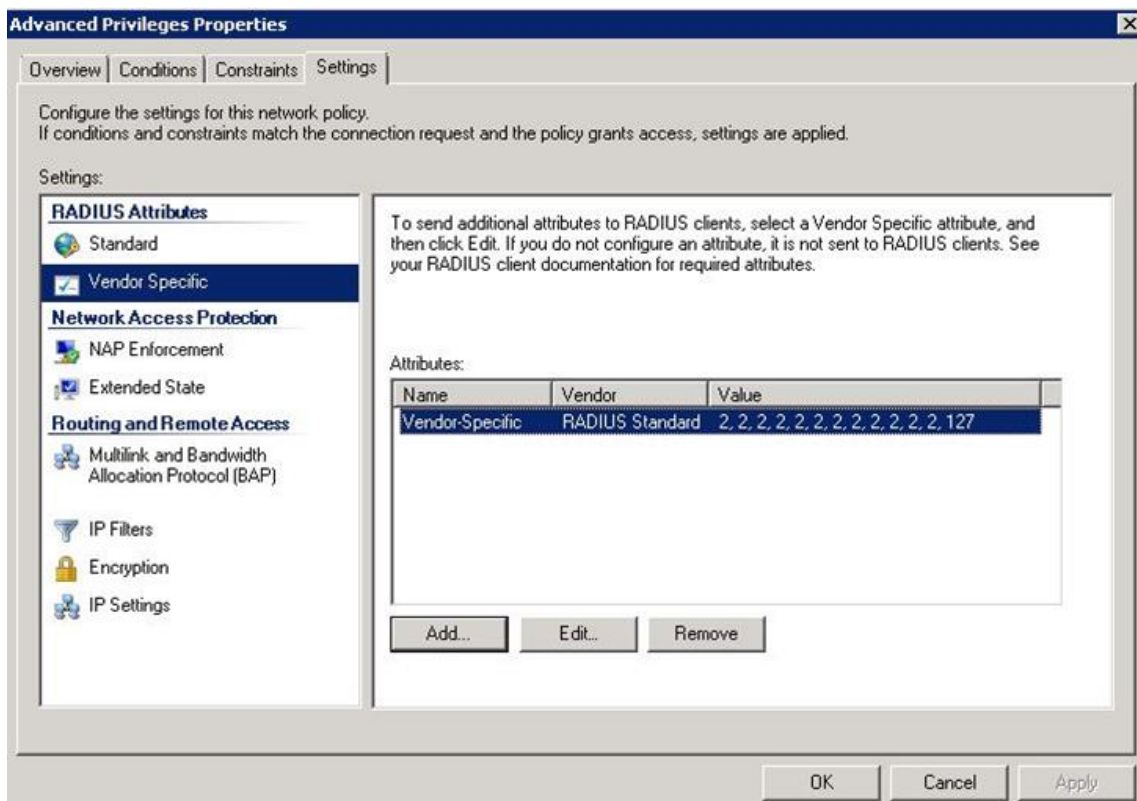
Or enter **24** to allow access only from NMS + SNMP channels.

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 274 Create Network Policy – Example of Vendor-Specific Attribute Configuration

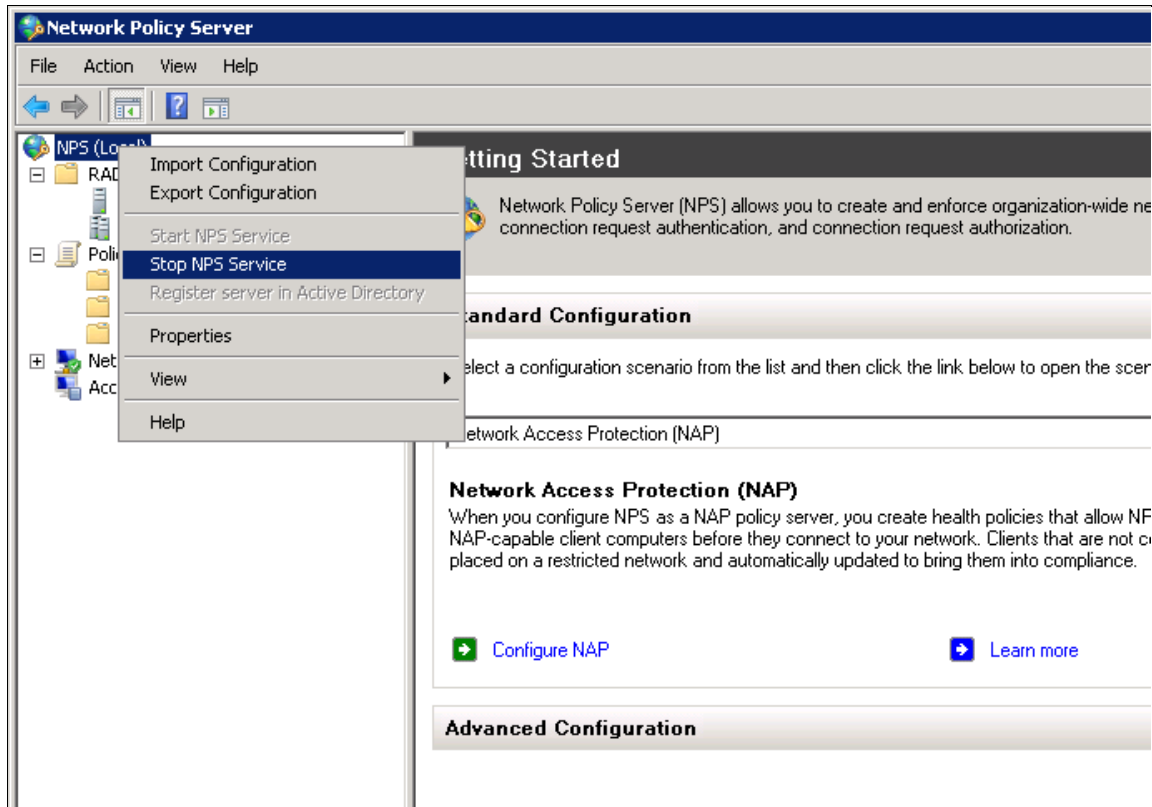


24 Close all opened windows and click **Next**.

25 In the Completing New Network Policy window, click **Finish**.

- 26 Reset the Network Policy Server (NPS) by stopping and starting the NPS service as follows:
- Right click the **NPS (Local)** node, and select **Stop NPS Service**.
 - Right click the **NPS (Local)** node, and select **Start NPS Service**.

Figure 275 Create Network Policy – Stopping/Starting NPS Services



Configuring a Linux FreeRADIUS Server

The following sub-sections describe how to configure a Linux FreeRADIUS server to work with a PTP 820 device.

To so do, you will need to modify the following three files:

- `/etc/raddb/users`
- `/etc/raddb/clients.conf`
- `/usr/share/freeradius/dictionary.cambium`

Step 1 – Creating Users

This step describes how to create the following three users:

- u1 – with advanced read/write privileges, password 1111
- u2 – with normal read/write privileges, password 2222
- u3 – with no read/write privileges, password 3333

To create these RADIUS users:

- 1 Add the users in the `/etc/raddb/users` file, using any editor you like, according to the following example:

```
# user1 - advanced privileges
u1    auth-type := local, Cleartext-Password := "1111"
      security-ro = advanced,
      security-wo = advanced,
      mng-ro = advanced,
      mng-wo = advanced,
      radio-ro = advanced,
      radio-wo = advanced,
      tdm-ro = advanced,
      tdm-wo = advanced,
      eth-ro = advanced,
      eth-wo = advanced,
      sync-ro = advanced,
      sync-wo = advanced,
      access_channel = u1accesschannel,
      fall-through = yes

# user2 - regular privileges
u2    auth-type := local, Cleartext-Password := "2222"
      security-ro = regular,
      security-wo = regular,
      mng-ro = regular,
      mng-wo = regular,
      radio-ro = regular,
      radio-wo = regular,
      tdm-ro = regular,
      tdm-wo = regular,
      eth-ro = regular,
      eth-wo = regular,
      sync-ro = regular,
      sync-wo = regular,
      access_channel = u2accesschannel,
      fall-through = yes
```

```
# user3 - no privilege (viewer)
u3      auth-type := local, Cleartext-Password := "3333"
        security-ro = none,
        security-wo = none,
        mng-ro = none,
        mng-wo = none,
        radio-ro = none,
        radio-wo = none,
        tdm-ro = none,
        tdm-wo = none,
        eth-ro = none,
        eth-wo = none,
        sync-ro = none,
        sync-wo = none,
        access_channel = u3accesschannel,
        fall-through = yes
```

2 Save the changes in the `/etc/raddb/users` file.

Step 2 – Defining the Permitted Access Channels

The `access_channel` of each user we configured in the `/etc/raddb/users` file, defines the channels through which that user is allowed to access the unit.

This is done by summing the values corresponding to the allowed channels, where the values are:

###	none	0
###	serial	1
###	telnet	2
###	ssh	4
###	web	8
###	nms	16
###	snmp	32
###	snmpV3	64

For example:

- The value `127` denotes permission to access the device from all channels:
Serial + Telnet + SSH + Web + NMS + SNMP +SNMPv3
- The value `24` indicates permission to access the device only from the Web + NMS channels.

To define each user's access channels:

- 1 In the `usr/share/freeradius/dictionary.cambium` file, configure the values of the access channels according to the following example:

```
### access channel for u1 user:serial+telnet+ssh+web+nms+snmp+snmpV4
VALUE ACCESS_CHANNEL u1accesschannel 127
```

- 2 Save the changes to the `usr/share/freeradius/dictionary.cambium` file.

Step 3 – Specifying the RADIUS client

This step describes how to define a device as a RADIUS client. The RADIUS server accepts attempts to connect to a device only if that 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 a PTP 820G device with IP address 192.168.1.118:

```
# PTP 820C
client 192.168.1.118 {
    secret          = default_not_applicable
    shortname       = cambium-ptp 820G
}
```

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 (Figure 256).
- 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 – Restarting the RADIUS client

After configuring all of the above, restart the RADIUS process.

To restart the RADIUS process:

- 1 Stop the process by entering:

```
killall -9 radiusd
```

- 2 Start the process running in the background by entering:

```
radius -X &
```



Note

To check the logs each time a user connects to the server, enter:
`radius -X &`

Configuring X.509 CSR Certificates and HTTPS

The web interface protocol for accessing PTP 820 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 820 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 820 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

To generate a Certificate Signing Request (CSR) file:

1. Select **Platform > Security > X.509 Certificate > CSR**. The Security Certificate Request page opens.

Figure 276 Security Certificate Request Page

Logout Connection Admin

▼ Filter

[Unit & Radio Summary](#)

- Platform
 - Management
 - Software
 - Configuration
 - Activation Key
- Security
 - General
 - X.509 Certificate
 - [CSR](#)
 - [Download & Install](#)
 - Access Control
 - [Protocols Control](#)
- Faults
- Radio
- Ethernet
- Sync
- Quick Configuration
- Utilities

Microwave radio: Security Certificate Request

Certificate Attributes

Common Name (domain)

Organization

Organization Unit

Locality (City)

State

Country

Email

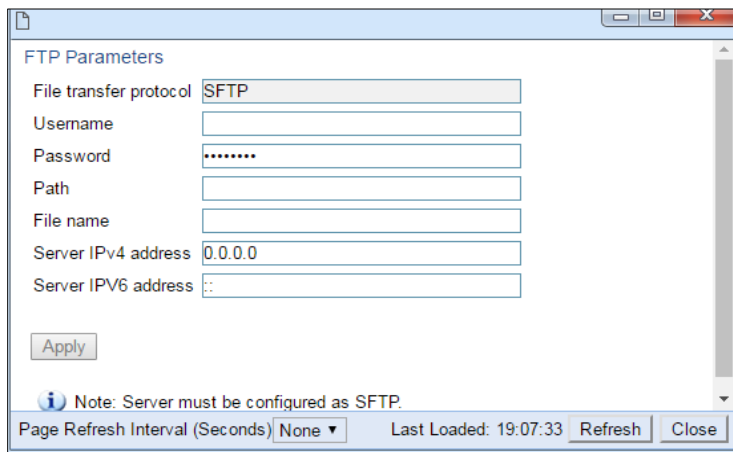
File Format

Generate/Upload Certification Status

Creation/Upload status

Creation/Upload progress

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.
10. Click **Apply** to save your settings.
11. Click **FTP Parameters** to display the FTP Parameters page.

Figure 277 FTP Parameters Page (Security Certificate Request)


12. In the **Username** field, enter the user name you configured in the SFTP server.
13. In the **Password** field, enter the password you configured in the SFTP server. If you did not configure a password for your SFTP user, simply leave this field blank.
14. In the **Path** field, enter the directory path to which you are uploading the CSR. Enter the path relative to the SFTP user's home directory, not the absolute path. If the location is the home directory, it should be left empty. If the location is a sub-folder under the home directory, specify the folder name. If the shared folder is "C:\", this parameter can be left empty or populated with "/".
15. In the **File name** field, enter the name you want to give to the exported CSR.
16. If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the SFTP server in the **Server IPv4 address** field. See [Defining the IP Protocol Version for Initiating Communications](#).
17. If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the SFTP server in the **Server IPv6 address** field. See [Defining the IP Protocol Version for Initiating Communications](#).
18. Click **Apply**, then **Close**, to save the FTP parameters and return to the Security Log Upload page.
19. Click **Generate & Upload**. The file is generated and uploaded.

The **CSR Status** field displays the status of any pending CSR generation and upload. Possible values are:

- **Ready** – The default value, which appears when CSR generation and upload is in progress.
- **File-in-transfer** – The upload operation is in progress.
- **Success** – The file has been successfully uploaded.
- **Failure** – The file was not successfully uploaded.

The **CSR Percentage** field displays the progress of any current CSR upload operation.

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 278 Security Certification Download and Install Page

Logout Connection Admin

▼ Filter

Unit & Radio Summary

Platform

- Management
- Software
- Configuration
- Activation Key
- Security
 - General
 - X.509 Certificate
 - CSR
 - Download & Install**
 - Access Control
 - Protocols Control
- Faults
- Radio
- Ethernet
- Sync
- Quick Configuration
- Utilities

Microwave radio: Security Certification Download & Install

Download Certification Status

Download status Ready

Download progress 0

Download Install FTP Parameters FTP Port

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

Figure 279 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 ::

Apply

Note: Server must be configured as SFTP.

Page Refresh Interval (Seconds) None Last Loaded: 19:07:33 Refresh Close

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 820.

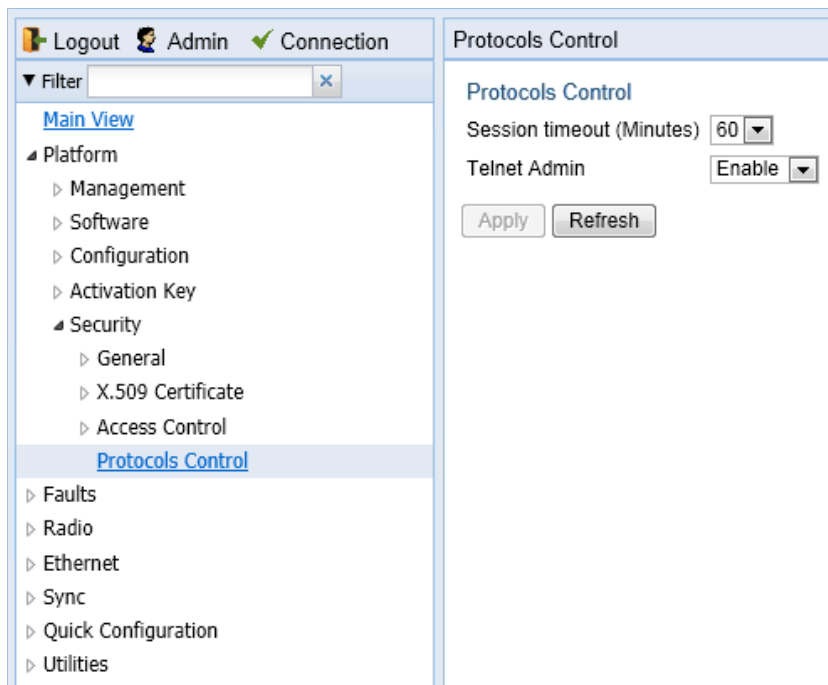
Blocking Telnet Access

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 280 Protocols Control Page



- 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 820 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 281 Security Log Upload Page

The screenshot shows the 'Microwave radio: Security Log Upload' page. On the left, a navigation tree includes 'Unit & Radio Summary', 'Platform' (with sub-items like Management, Software, Configuration, Activation Key, Security, and General), 'Security Log Upload' (highlighted), 'Configuration Log Upload', 'X.509 Certificate', 'Access Control', 'Protocols Control', 'Faults', 'Radio', 'Ethernet', 'Sync', 'Quick Configuration', and 'Utilities'. The main panel on the right is titled 'Security Log Upload' and contains two input fields: 'File transfer status' with the value 'Ready' and 'File transfer progress' with the value '0'. At the bottom of this panel are three buttons: 'Upload', 'FTP Parameters', and 'FTP Port'.

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

Figure 282 FTP Parameters Page (Security Log Upload)

4. In the **Username** field, enter the user name you configured in the FTP server.
5. 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.
6. 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](#).
7. 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](#).
8. 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 "/".
9. In the **File name** field, enter the name you want to give to the exported security log.
10. Click **Apply**, then **Close** to save the FTP parameters and return to the Security Log Upload page.
11. 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 **Process percentage** field displays the progress of any current security log upload operation.

Uploading the Configuration Log

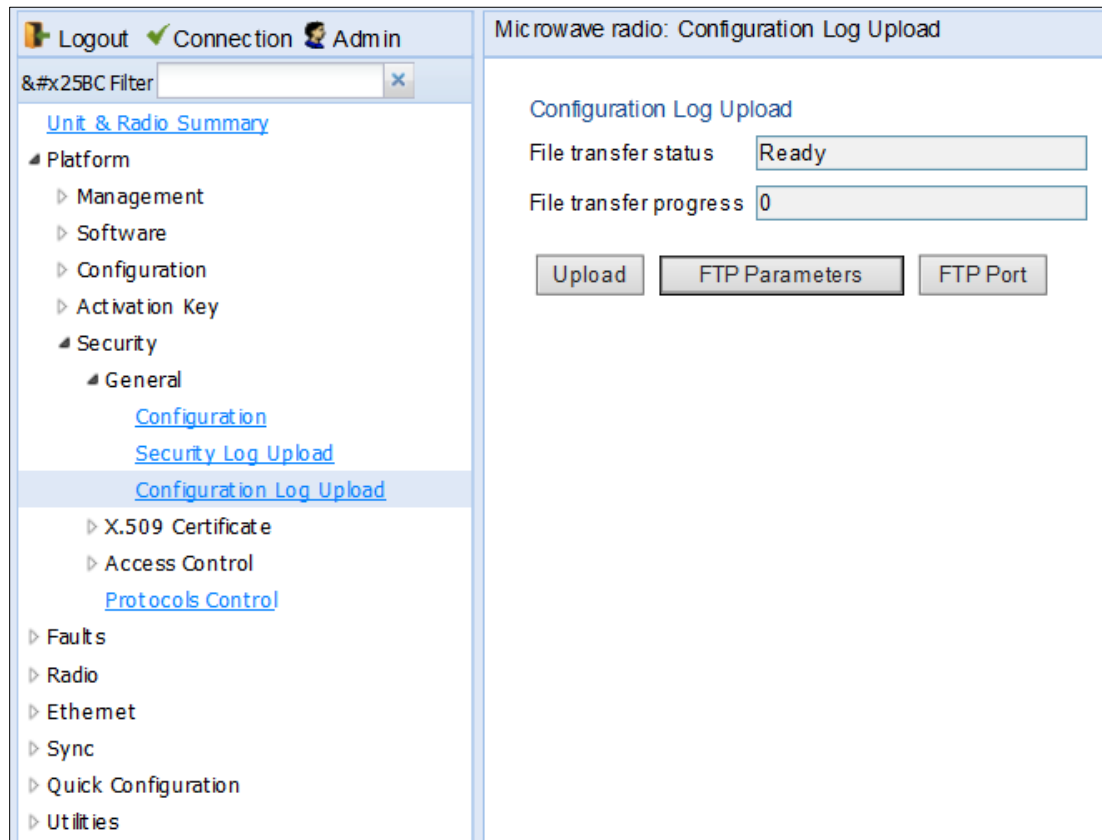
The configuration log lists actions performed by users to configure the system. This file is mostly used for security, to identify suspicious user actions. It can also be used for troubleshooting.

When uploading the configuration log, the PTP 820 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 283 Configuration Log Upload Page



3. Click FTP Parameters to display the FTP Parameters page.

Figure 284 Configuration Log Upload Page

The screenshot shows a web-based configuration window titled "Configuration Log Upload Page". It features a section for "FTP Parameters" with the following fields:

- Username:** Text box containing "anonymous".
- Password:** Text box with masked characters (dots).
- Server IP address:** Text box containing "0.0.0.0".
- Server IPv6 address:** Text box containing "::".
- Path:** Empty text box.
- File name:** Empty text box.

Below the fields is an "Apply" button. At the bottom of the window, there is a status bar containing:

- "Page Refresh Interval (Seconds)" with a dropdown menu set to "None".
- "Last Loaded: 15:38:38".
- "Refresh" and "Close" buttons.
- A zoom level indicator showing "110%".

4. In the **Username** field, enter the user name you configured in the FTP server.
5. 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.
6. 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](#).
7. 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](#).
8. 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 "/".
9. In the **File Name** field, enter the name you want to give to the exported configuration log.

**Note**

The directory path and file 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

10. Click **Apply**, and **Close** to save the FTP parameters and return to the Configuration Log Upload page.
11. 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 **Process percentage** field displays the progress of any current configuration log upload operation.

Chapter 11: Alarm Management and Troubleshooting

This section includes:

- [Viewing Current Alarms](#)
- [Viewing Alarm Statistics](#)
- [Viewing Alarm Statistics](#)
- [Viewing the Event Log](#)
- [Editing Alarm Text and Severity](#)
- [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 30-second wait time 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 60](#).

Figure 285 Current Alarms Page

#	Time	Severity	Description	User Text	Origin	Alarm id
1	20-09-2015 12:59:24	Red Triangle	Multi Carrier ABC LOF		Slot 0	2200
2	17-09-2015 10:22:52	Red Triangle	Radio loss of frame		Radio: Slot 2, port 1	603
3	17-09-2015 10:22:51	Red Triangle	Radio loss of frame		Radio: Slot 2, port 2	603
4	17-09-2015 10:22:18	Red Triangle	Loss of Carrier		Ethernet: Slot 1, port	401
5	17-09-2015 10:24:46	Yellow Triangle	Demo mode is active		Slot 1	901
6	17-09-2015 10:22:51	Yellow Triangle	RFU RX level out of range		Radio: Slot 2, port 1	1727
7	17-09-2015 10:22:51	Yellow Triangle	RFU TX Mute		Radio: Slot 2, port 1	1735
8	17-09-2015 10:22:51	Yellow Triangle	RFU RX level out of range		Radio: Slot 2, port 2	1727
9	17-09-2015 10:22:51	Yellow Triangle	RFU TX Mute		Radio: Slot 2, port 2	1735

2. To view more detailed information about an alarm, click + at the beginning of the row or select the alarm and click **View**.

Figure 286 Current Alarms - View Page

Active, Current Alarms - View

Sequence Number

Time

Severity

Description

User Text

Origin

Probable Cause

Corrective Actions

Alarm id

Table 60 Alarm Information

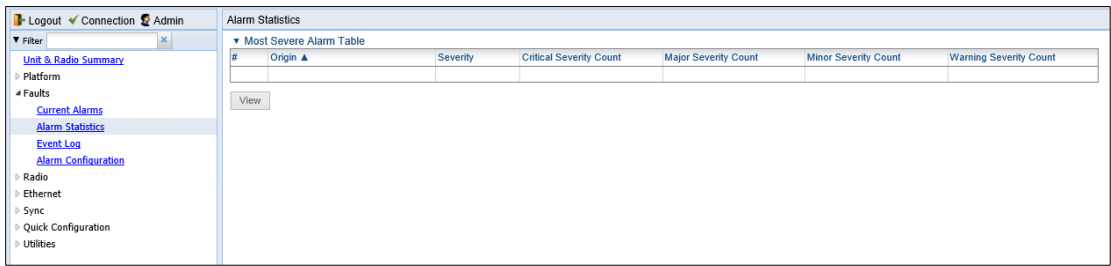
Parameter	Definition
Sequence Number (#)	A unique sequence number assigned to the alarm by the system.
Time	The date and time the alarm was triggered.
Severity	<p>The severity of the alarm. In the Current Alarms table, the severity is indicated by a symbol. You can display a textual description of the severity by holding the cursor over the symbol.</p> <p>Note: You can edit the severity of alarm types in the Alarm Configuration page. See Editing Alarm Text and Severity.</p>
Description	A system-defined description of the alarm.
User Text	<p>Additional text that has been added to the system-defined description of the alarm by users.</p> <p>Note: You can add user text to alarms in the Alarm Configuration page. See Editing Alarm Text and Severity.</p>
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 287 Alarm Statistics Page



The Alarm Statistics page displays the number of current alarms per severity level for each module, interface, and virtual interface (such as Multi-Carrier ABC groups) in the unit. Only modules and interfaces for which one or more alarms are currently raised are listed in the Alarm Statistics page.

Viewing 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 61 Event Log Information](#).

Figure 288 Event Log

#	Time	Sequence Number	Severity	State	Description	User Text	Origin
1	04-10-2015 20:23:44	11	Event	Event	Demo mode is started		Slot 1
2	04-10-2015 20:23:44	10	Raised	Raised	Demo mode is active		Slot 1
3	04-10-2015 20:23:44	9	Cleared	Cleared	Activation key violation		Slot 1
4	04-10-2015 20:18:36	8	Raised	Raised	Activation key violation		Slot 1
5	04-10-2015 20:17:23	7	Raised	Raised	RFU RX level out of range		Radio: Slot 2, port 1
6	04-10-2015 20:17:23	6	Raised	Raised	Radio loss of frame		Radio: Slot 2, port 1
7	04-10-2015 20:17:22	5	Raised	Raised	RFU TX Mute		Radio: Slot 2, port 1
8	04-10-2015 20:17:19	4	Event	Event	Change in system reference clock quality level; new quality: g.813		Slot 0
9	04-10-2015 20:16:33	3	Raised	Raised	Loss of Carrier		Ethernet: Slot 1, port 2
10	04-10-2015 20:16:32	2	Raised	Raised	Loss of Carrier		Ethernet: Slot 1, port 1
11	04-10-2015 20:15:32	1	Event	Event	Unit Perform Power up		Slot 1

Table 61 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	<p>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.</p> <p>Note: You can edit the severity of event types in the Alarm Configuration page. See Editing Alarm Text and Severity.</p>
State	Indicates whether the event is currently raised or has been cleared.
Description	A system-defined description of the event.
User Text	<p>Additional text that has been added to the system-defined description of the event by users.</p> <p>Note: You can add user text to events in the Alarm Configuration page. See Editing Alarm Text and Severity.</p>
Origin	The module that generated the event.

Editing Alarm Text and Severity

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](#)
- [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 62 Alarm Configuration Page Parameters](#).

Figure 289 Alarm Configuration Page

#	Alarm ID	Severity	Description	Additional Text	Service Affecting
1	10	Warning	Framer digital loopback		off
2	25	Warning	Unit Temperature is out of system specified limits		off
3	26	Warning	Unit input voltage is too low		off
4	27	Warning	Unit input voltage is too high		off
5	28	Warning	Unit warm Reset		off
6	29	Warning	Unit Reset		off
7	31	Error	Protection switchover due to remote request		on
8	32	Error	Change Remote request was sent		on
9	33	Error	Unit Redundancy and MIMO 4x4 can not operate simultaneously		on
10	100	Error	LAG is not fully functional - LAG Degraded		off
11	101	Error	LAG operational state is down		off
12	102	Error	Loopback is active		on
13	103	Warning	Slot X port XX is mirrored to slot Y port YY		on
14	150	Error	Interface is down due to auto state propagation		on
15	200	Error	Protection communication is down		on
16	201	Error	Protection in Lockout State		off
17	202	Error	Protection switchover due to local failure		off
18	203	Error	Mate does not exist		on
19	307	Warning	TDM interface is up		on
20	308	Warning	TDM interface is down		on

Table 62 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.

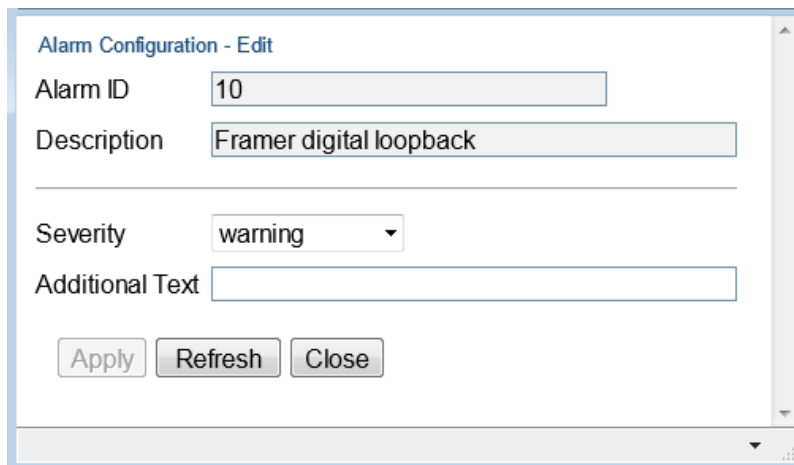
Figure 290 Alarm Configuration Page – Expanded

Alarm Configuration					
#	Alarm ID	Severity	Description	Additional Text	Service Affecting
1	10		Framer digital loopback		off
<div> <div>Probable Cause</div> <div>User enabled framer digital loopback</div> </div> <div> <div>Corrective Actions</div> <div>Disable framer digital loopback</div> </div>					
2	25		Unit Temperature is out of system specified limits		off

Editing an Alarm Type

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 289](#)).
2. Click **Edit**. The Alarm Configuration - Edit page opens.

Figure 291 Alarm Configuration - Edit Page

Alarm Configuration - Edit

Alarm ID

Description

Severity

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 289](#)).

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 820 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 292 Unit Info Page

The screenshot shows the 'Unit Info' page in the PTP 820 web interface. The left sidebar contains a navigation menu with the following items: Logout, Admin, Connection, Filter, Main View, Platform, Management (expanded), Unit Parameters, NTP Configuration, Time Services, Interface Manager, Inventory, Unit Info (selected), Reset, Set to Factory Default, Unit Redundancy, Networking, SNMP, Software, Configuration, Activation Key, Security, Faults, Radio, Ethernet, Sync, Quick Configuration, and Utilities. The main content area is titled 'Unit Info' and contains the following fields and buttons:

- Unit Info section:
 - File creation status: Ready
 - File creation progress: 0
 - File transfer status: Ready
 - File transfer progress: 0
- File transfer protocol: FTP (dropdown menu)
- Username: anonymous
- Password: [masked with dots]
- Server IPv4 address: 0.0.0.0
- Path: [empty field]
- File name: [empty field]
- Server IPv6 address: :: [empty field]
- Buttons: Apply, Create, Export, Refresh

3. In the **File transfer protocol** field, select the file transfer protocol you want to use (**FTP** or **SFTP**).
4. In the **Username in server** field, enter the user name you configured in the FTP server.

5. 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.
6. 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](#).
7. 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](#).
8. 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 "/".
9. In the **File Name** field, enter the name you want to give to the exported Unit Information file.
10. Click **Apply** to save your settings.
11. 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.
12. 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

To perform loopback on a radio:

1. Select **Radio > Diagnostics > Loopback**. The Radio Loopbacks page opens.

Figure 293 Radio Loopbacks Page

The screenshot shows the 'Radio Loopbacks' page. On the left, a navigation pane has 'Radio' expanded, showing sub-items like 'Radio Parameters', 'Remote Radio Parameters', 'Radio Thresholds', 'ATPC', 'Ethernet Interface', 'MRMC', 'PM & Statistics', 'Diagnostics', and 'Loopback' (which is selected). The main content area is titled 'Radio Loopbacks' and contains a table with the following data:

Radio location ▲	Loopback timeout (minutes)	RF Loopback
Radio: Slot 2, port 1	1	Off
Radio: Slot 2, port 2	1	Off

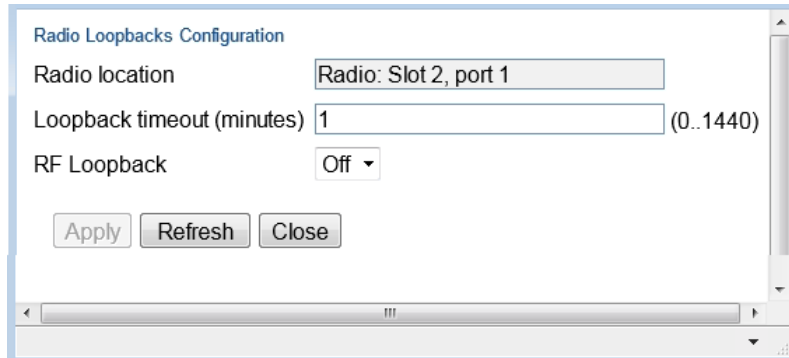
Below the table are 'Edit' and 'Refresh' buttons.

2. Select the slot on which you want to perform loopback and click **Edit**. The Radio Loopbacks – Edit page opens.



Note

You cannot perform loopback directly on a Multi-Carrier ABC group. To perform traffic-level diagnostics on a Multi-Carrier ABC group, the loopback must be activated for all members of the group. Radio-level diagnostics can still be performed on individual members of the group.

Figure 294 Radio Loopbacks – Edit Page

3. 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.
4. In the **RF loopback** field, select **On**.
5. 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 182](#)).
2. Select an interface in the Ethernet Logical Port Configuration table and click **Loopback**. The Logical Interfaces – Loopback page opens.

Figure 295 Logical Interfaces – Loopback Page

The screenshot shows a web-based configuration interface. On the left is a navigation pane with a tree structure. The 'Logical Interfaces' link is highlighted. The main content area is titled 'Logical Interfaces' and contains a sub-header 'Ethernet Logical Port Configuration Table - Edit'. Below this are four configuration fields: 'Interface location' with a text box containing 'Ethernet: Slot 1, port 1'; 'Ethernet loopback admin' with a dropdown menu set to 'Disable'; 'Ethernet loopback duration (sec)' with a text box containing '1' and a range '(1..900)' to its right; and 'Swap MAC address admin' with a dropdown menu set to 'Enable'. At the bottom of the configuration area are two buttons: 'Apply' and 'Refresh'.

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](#)

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 820 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.

**Note**

MIP – (MEG Intermediate Points) Similar to MEPs, but located inside the MEG and can only respond to, not initiate, CMM message.

- 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 296 SOAM MD Page

Logout Admin Connection

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
 - General Configuration
 - Services
 - Interfaces
 - PM & Statistics
 - QOS
 - Protocols
 - Adaptive Bandwidth Notification
 - LLDP
 - SOAM
 - MD
 - MA/MEG
 - MEP
 - Sync
 - Quick Configuration
 - Utilities

SOAM MD

SOAM MD Table

<input checked="" type="checkbox"/>	MD ID ▲	MD Name	MD Format	MD Level	MHF (MIP) Creation	Sender TLV content
<input checked="" type="checkbox"/>	1	MD1	None	0	MHF default	Send Id Chassis

Add Delete Refresh

- Click **Add**. The SOAM MD – Add page opens.

Figure 297 SOAM MD Page

SOAM MD

SOAM MD Table - Add

MD Name

MD Format None

MD Level 0

MHF (MIP) Creation MHF default

Sender TLV content Send Id Chassis

Apply Refresh Close

- 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.
- 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.

- 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.
- 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 1024 Slow MEPs and up to 256 Fast MEPs per network element. You can configure up to 348 Slow Local MEPs (a local MEP in a Slow MEG) and up to 64 Fast Local MEPs (a local MEP in a Fast MEG) per network element.

To add a MEG:

- Select **Ethernet > Protocols > SOAM > MA/MEG**. The SOAM MA/MEG page opens.

Figure 298 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	

Add MEG Edit Delete MEG MEP List

- Click **Add MEG**. The SOAM MA/MEG – Add page opens.

Figure 299 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

Apply

Last Loaded: 11:06:07

Refresh

Close

3. Configure the fields described in *Table 63*.

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

[Table 64](#) describes the status (read-only) fields in the SOAM MA/MEG Component table.

Table 63 SOAM MA/MEG Configuration Parameters

Parameter	Definition
MD (ID, Name)	Select the MD to which you are assigning the MEP.
MA/MEG short name	Enter a name for the MEG (up to 44 alphanumeric characters).

Parameter	Definition
MEG Level	<p>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.</p> <p>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.</p> <p>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:</p> <p>The customer role is assigned MEG levels 6 and 7.</p> <p>The provider role is assigned MEG levels 3 through 5.</p> <p>The operator role is assigned MEG levels: 0 through 2.</p> <p>The default MEG level assignment can be changed via a mutual agreement among customer, provider, and/or operator roles.</p> <p>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.</p>
CCM Interval	<p>The interval at which CCM messages are sent within the MEG. Options are:</p> <ul style="list-style-type: none"> 1 second (default) 10 seconds 1 minute 10 minutes <p>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.</p>
Service ID	<p>Select an Ethernet service to which the MEG belongs. You must define the service and add service points before you configure the MEG.</p>

Table 64 SOAM MA/MEG Status Parameters

Parameter	Definition
MIP Creation	<p>Determines whether MIPs are created on the MEG. Options are:</p> <ul style="list-style-type: none"> • 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. <p>MHF defer – No MIPs are created. Not used in the current release.</p>
MA/MEG ID	Automatically generated by the system.
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 [1. 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 [2. Configuring the Local MEPs](#).
3. Enable the Local MEPs. See [3. Enabling Local MEPs](#).

1. 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 300 MEP List Page

Logout Admin Connection

Filter

Main View

- Platform
- Faults
- Radio
- Ethernet
 - General Configuration
 - Services
 - Interfaces
 - PM & Statistics
 - QOS
 - Protocols
 - Adaptive Bandwidth Notification
 - LLDP
 - SOAM
 - MD
 - MA/MEG**
 - MEP
 - Sync
 - Quick Configuration
 - Utilities

Microwave radio: - MD ID: 1 (TR_998) MA/MEG ID: 1 (56)

<< Back to MA/MEG

MD ID 1

MD Name TR_998

MA/MEG ID 1

MA/MEG short name 56

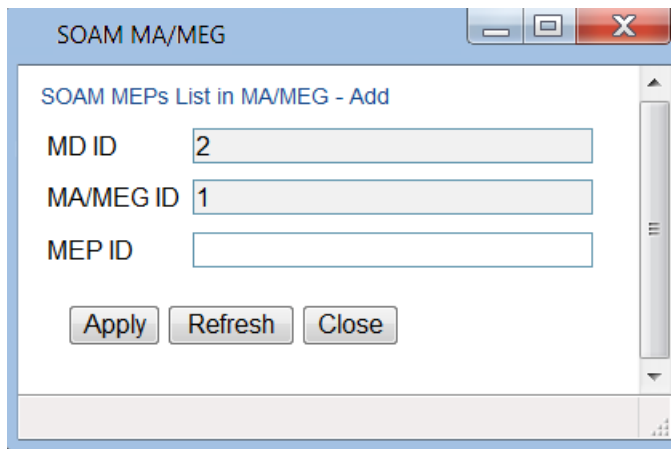
SOAM MA/MEG

<input type="checkbox"/>	MEP ID ▲
<input type="checkbox"/>	25
<input type="checkbox"/>	35

Add Delete Refresh

2. Click **Add**. The Add MEP page opens.

Figure 301 Add MEP Page



The screenshot shows a web-based form titled "SOAM MA/MEG". Inside the form, there is a section "SOAM MEPs List in MA/MEG - Add". It contains three input fields: "MD ID" with the value "2", "MA/MEG ID" with the value "1", and "MEP ID" which is empty. Below these fields are three buttons: "Apply", "Refresh", and "Close".

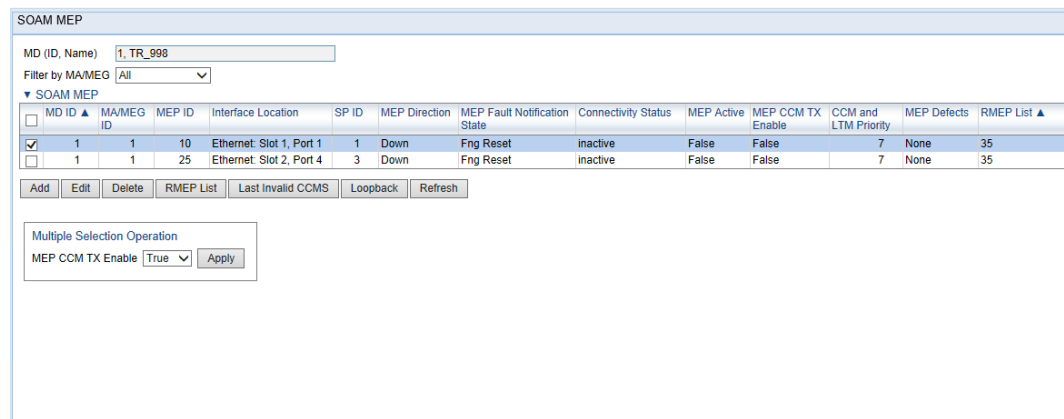
3. In the **MEP ID** field, enter a MEP ID (1-8191).
4. Click **Apply**, then **Close**.

2. 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 65](#) lists and describes the parameters displayed in the SOAM MEP page.

Figure 302 SOAM MEP Page



The screenshot shows the "SOAM MEP" page. At the top, there is a field "MD (ID, Name)" with the value "1_TR_998" and a "Filter by MA/MEG" dropdown menu set to "All". Below this is a table with the following columns: 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, and RMEP List. The table contains two rows of data. Below the table are buttons for "Add", "Edit", "Delete", "RMEP List", "Last Invalid CCMS", "Loopback", and "Refresh". At the bottom, there is a "Multiple Selection Operation" section with a "MEP CCM TX Enable" dropdown set to "True" and an "Apply" button.

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

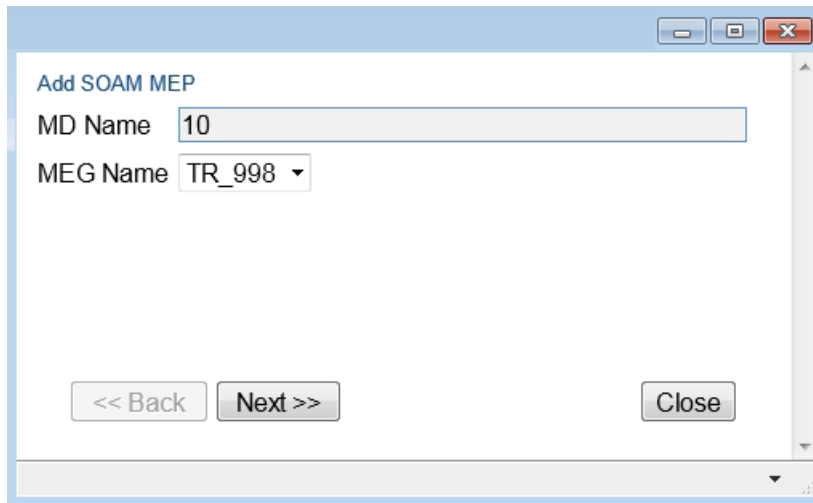


Note

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 303 Add SOAM MEP Wizard – Page 1



Add SOAM MEP

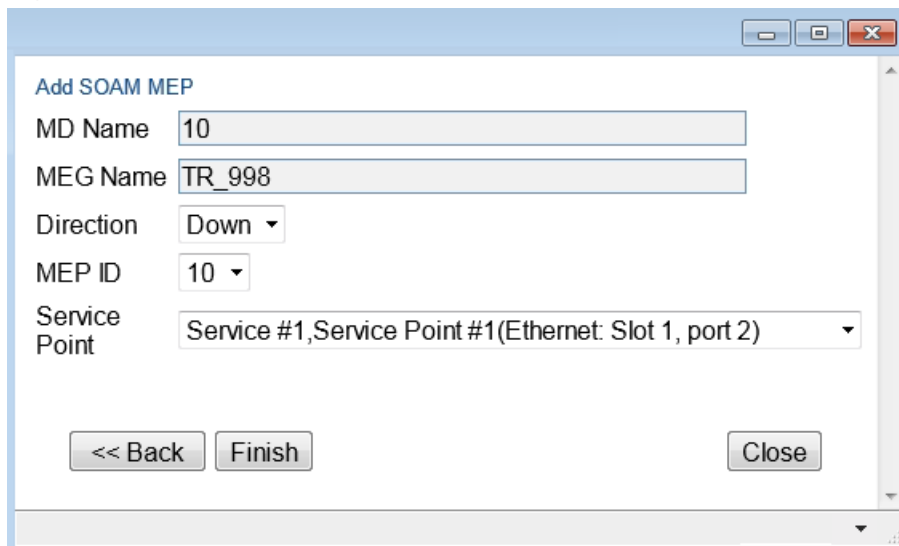
MD Name

MEG Name

<< Back Next >> Close

3. In the **MEG Name** field, select an MA/MEG.
4. Click **Next**. Page 2 of the Add SOAM MEP wizard opens.

Figure 304 Add SOAM MEP Wizard – Page 2



Add SOAM MEP

MD Name

MEG Name

Direction

MEP ID

Service Point

<< Back Finish Close

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 305 Add SOAM MEP Wizard –Summary Page

9. Verify that you want to submit the displayed parameters and click **Submit**.

Table 65 SOAM MEP Parameters

Parameter	Definition
MD (ID, Name)	AnThe MD ID and name are automatically generated by the system.
MA/MEG (ID, Name)	AnThe 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	In this release, only Up or Down is supported.
MEP Fault Notification State	<p>The initial Indicates the status of the defect SOAM state machine. Possible values are:</p> <ul style="list-style-type: none"> • 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. <p>Fng Defect Cleared – The defect has been cleared (Transient state).</p>

Parameter	Definition
MEP ActiveConnectivity 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: <ul style="list-style-type: none"> inactive – At least one of the MEPreremote 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	Reserved for future use.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.

3. 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 302](#)), select the MEP you want to enable.
2. Click **Edit**. The SOAM MEP - Edit page opens.

Figure 306 SOAM MEP - Edit Page

SOAM MEP - Edit

MD ID	1
MD Name	TR_998
MA/MEG ID	1
MA/MEG Name	56
MEP ID	25
MEG Level	1
<hr/>	
Interface Location	Ethernet: Slot 1, Port 1
Service ID	10
Service point ID	1
MEP Direction	Down
<hr/>	
MEP Fault Notification State	Eng 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
<hr/>	
MEP Active	True
MEP CCM TX Enabled	True
CCM and LTM Priority	7
<hr/>	
<input type="button" value="Apply"/>	
<hr/>	
Page Refresh Interval (Seconds)	None
Last Loaded:	11:55:18
<input type="button" value="Refresh"/>	<input type="button" value="Close"/>

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 302](#)).
2. Select a MEP and click **RMEP List**. The SOAM MEP DB table is displayed.

Figure 307 SOAM MEP DB Table

Microwave radio - MD ID: 1 (TR_998) MA/MEG ID: 1 (56) MEP ID: 10

Back to MEP

MD ID: 1
MD Name: TR_998
MA/MEG ID: 1
MA/MEG short name: 56
MEP ID: 10

SOAM MA/MEG

RMEP ID ▲	RMEP Operational State	RMEP Last rx CCM MAC Address	RMEP Last CCM OK or Fail Timestamp	RMEP Last rx CCM RDI Indication	RMEP Last rx CCM Port status TLV	RMEP Last rx CCM Interface Status TLV	RMEP Last rx CCM chassis ID format	RMEP Last rx CCM Chassis ID
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	

View Refresh

Table 66 lists and describes the parameters displayed in the SOAM MEP DB table. To return to the SOAM MEP page, click **Back to MEP**.

Table 66 SOAM MEP DB Table Parameters

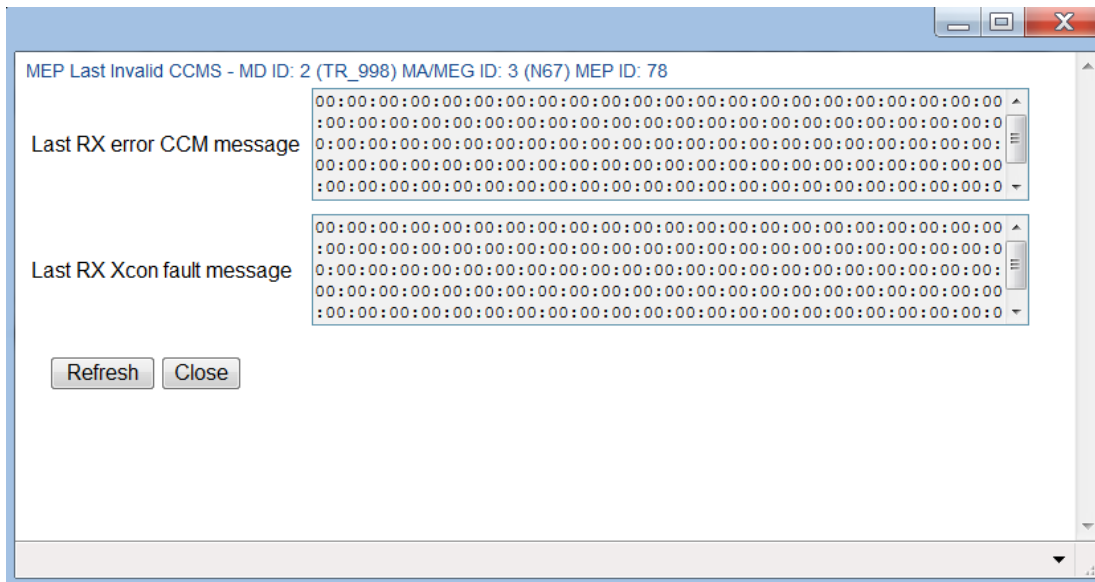
Parameter	Definition
RMEP ID	The remote MEP ID.
RMEP Operational State	The operational state of the remote MEP.
RMEP Last rx CCM MAC Address	The MAC Address of the interface on which the remote MEP is located.
RMEP Last CCM OK or Fail Timestamp	The timestamp marked by the remote MEP indicated the most 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. If none, displays False .
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 MAC addressformat of the remote unit.chassis (always the MAC address).
RMEP Last rx CCM Chassis ID	Reserved for future use.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 302).
2. Select a MEP and click **Last Invalid CCMS**. The MEP Last Invalid CCMS page opens.

Figure 308 MEP Last Invalid CCMS Page



The **Last RX error CCM message** field displays the frame of the last CCM that contains an error message received by the MEP.

The **Last RX Xcon fault message** field displays the frame of the last CCM that contains a cross-connect error message received by the MEP.



Note

A cross-connect error occurs when a CCM is received from a remote MEP that has not been defined locally.

Configuring MIPs with MHF Default

If you configure a MEG with the MHF default option, MIPS are created automatically on all service points of the service to which the MEG is attached. These MIPS cannot be displayed in the Web EMS, but can be displayed via CLI. 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 than 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 302](#)), select the MEP on which you want to perform the loopback.
- 2 Click **Loopback**. The SOAM MEP – Loopback page opens.

Figure 309 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

Apply Refresh Close

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 12: Web EMS Utilities

This section includes:

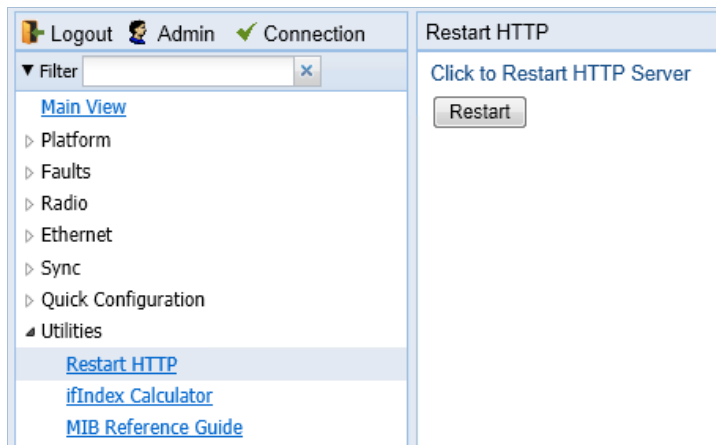
- [Restarting the HTTP Server](#)
- [Calculating an ifIndex](#)
- [Displaying, Searching, and Saving a list of MIB Entities](#)

Restarting the HTTP Server

To restart the unit's HTTP server:

- 1 Select **Utilities > Restart HTTP**. The Restart HTTP page opens.

Figure 310 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 311 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 820 private MIB:

- 1 Select **Utilities > ifCalculator**. The ifIndex Calculator page opens.

Figure 312 MIB Reference Table Page

#	MIB OID	MIB Name	Type	MIB Type	MIB Access	Description
1	1.3.6.1.2.1.1.1	sysDescr	Scalar	OCTET STRING	read-only	A short description of the system
2	1.3.6.1.2.1.1.2	sysObjectID	Scalar	OCTET STRING	read-only	System object ID
3	1.3.6.1.2.1.1.3	sysUpTime	Scalar	INTEGER	read-only	The time (in hundredths of a second) since the system was last re-initialized
4	1.3.6.1.2.1.1.4	sysContact	Scalar	OCTET STRING	read-write	The required contact person for the system
5	1.3.6.1.2.1.1.5	sysName	Scalar	OCTET STRING	read-write	The name of the system
6	1.3.6.1.2.1.1.6	sysLocation	Scalar	OCTET STRING	read-write	The location of the system
7	1.3.6.1.2.1.2.1	ifNumber	Scalar	INTEGER	read-only	The number of managed network interfaces as they appear in the IF-Manager table or ifTable
8	1.3.6.1.2.1.2.2	ifTable	Table		not-accessible	This table contains a list of configuration information about the user managed interfaces
9	1.3.6.1.2.1.2.2.1	ifIndex	Column	INTEGER	read-only	Interface location
10	1.3.6.1.2.1.2.2.1	ifDescr	Column	OCTET STRING	read-only	A textual string containing information about the interface
11	1.3.6.1.2.1.2.2.1	ifType	Column	INTEGER (1..1)	read-only	The type of the interface
12	1.3.6.1.2.1.2.2.1	ifMtu	Column	INTEGER (1..10000)	read-only	Maximum Transmission Unit, "The size of the largest datagram which can be sent/receive on the interface, specified in octets"
13	1.3.6.1.2.1.2.2.1	ifSpeed	Column	INTEGER	read-only	An estimate of the interface's bandwidth in bits per second
14	1.3.6.1.2.1.2.2.1	ifPhysAddress	Column	OCTET STRING	read-only	The MAC (Media Access Control) address of the interface
15	1.3.6.1.2.1.2.2.1	ifAdminStatus	Column	INTEGER (1..2)	read-write	The desired state of the interface
16	1.3.6.1.2.1.2.2.1	ifOperStatus	Column	INTEGER (1..7)	read-only	The current operational state of the interface
17	1.3.6.1.2.1.2.2.1	ifLastChange	Column	INTEGER (1..1)	read-only	The value of system up time at the time the interface has entered its current operational-state

The MIB Reference Table is customized to the type of PTP 820 product you are using. There are three separate versions of the MIB Reference Table:

- PTP 820G
- PTP 20C/S



Note

Even though the MIB Reference Table is customized to these three product groups, some of the entities listed in the Table may not be relevant to the particular unit you are using. This may occur because of activation key restrictions, minor differences between product 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 13: Getting Started (CLI)

This section includes:

- [General \(CLI\)](#)
- [Establishing a Connection \(CLI\)](#)
- [Logging On \(CLI\)](#)
- [General CLI Commands](#)
- [Changing Your Password \(CLI\)](#)
- [Mate Management Access \(IP Forwarding\) \(CLI\)](#)
- [Mate Management Access \(IP Forwarding\) \(CLI\)](#)

Mate Management Access enables the use of in-band management for nodes that use two PTP 820C units (4x4 MIMO, 2+2 XPIC, and 4+0 Multi-Carrier ABC), where traffic comes from an external switch operating in LAG mode. When Mate Management Access is enabled, the two units exchange incoming management packets, ensuring that all management data is received by both units.



Note

Mate Management Access can be used regardless of whether the unit's IP address is in IPv4 or IPv6 format.

Mate Management Access should only be enabled for nodes receiving traffic from a LAG, where in-band management is to be used. If either of these conditions is not present, Mate Management Access should be disabled. By default, the feature is disabled.

The following are the requirements for using Mate Management Access:

- The management ports of both PTP 820C units must be connected by a protection cable (PTP 820_MIMO_Prot_mng_cbl_1m).
- To ensure proper convergence after failure events, Automatic State Propagation must be enabled on both units at the local node and both units at the remote node. See [Configuring Automatic State Propagation \(CLI\)](#).
- Mate Management Access must be enabled on both units at the local node and both units at the remote node. On each unit, Mate Management Access must be enabled before configuring in-band management.

To enable Mate Management Access, enter the following command:

```
root> platform management mate-access admin enable
```

Note: When you enable or disable Mate Management Access, the unit is reset.

To disable Mate Management Access, enter the following command:

```
root> platform management mate-access admin disable
```

To display whether Mate Management Access is enabled, enter the following command:

```
root> platform management mate-access show
```

**Note**

Mate Management Access can only be configured via CLI.

Upon recovery from a failure event, management may be lost for up to 40 seconds.

- [Configuring In-Band Management \(CLI\)](#)
- [Changing the Management IP Address \(CLI\)](#)
- [Configuring the Activation Key \(CLI\)](#)
- [Setting the Time and Date \(Optional\) \(CLI\)](#)
- [Enabling the Interfaces \(CLI\)](#)
- [Configuring the Radio Parameters \(CLI\)](#)
- [Configuring the Radio \(MRMC\) Script\(s\) \(CLI\)](#)
- [Enabling ACM with Adaptive Transmit Power \(CLI\)](#)
- [Configuring the RSL Threshold Alarm \(CLI\)](#)
- [Operating in FIPS Mode \(CLI\)](#)
- [Configuring Grouping \(Optional\) \(CLI\)](#)
- [Creating Service\(s\) for Traffic \(CLI\)](#)

General (CLI)

Before connection over the radio hop is established, it is of high importance that you assign to the PTP 820 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 820 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 820 unit to a PC by means of a Twisted Pair cable. The cable is connected to the MGT port on the PTP 820 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 820 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 820 unit, it is necessary to have an IP address on the PC within the same subnet as the PTP 820 unit. The default PTP 820 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 820 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 820 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: admin
Password:
Wind River Linux glibc_cg1 (cg1) 4.1 CE.1.0
Last login: Mon Apr 13 11:27:02 on console
Wind River Linux glibc_cg1 (cg1) 4.1 CE.1.0
PTP 820C
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`.

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 \(CLI\)](#).

Mate Management Access (IP Forwarding) (CLI)

Mate Management Access enables the use of in-band management for nodes that use two PTP 820C units (4x4 MIMO, 2+2 XPIC, and 4+0 Multi-Carrier ABC), where traffic comes from an external switch operating in LAG mode. When Mate Management Access is enabled, the two units exchange incoming management packets, ensuring that all management data is received by both units.



Note
Mate Management Access can be used regardless of whether the unit’s IP address is in IPv4 or IPv6 format.

Mate Management Access should only be enabled for nodes receiving traffic from a LAG, where in-band management is to be used. If either of these conditions is not present, Mate Management Access should be disabled. By default, the feature is disabled.

The following are the requirements for using Mate Management Access:

- The management ports of both PTP 820 units must be connected by a protection cable. The cable can be ordered in a variety of sizes, depending on the distance between the two PTP 820 units. See the following Table.
- To ensure proper convergence after failure events, Automatic State Propagation must be enabled on both units at the local node and both units at the remote node. See [Configuring Automatic State Propagation and Link Loss Forwarding \(CLI\)](#).
- Mate Management Access must be enabled on both units at the local node and both units at the remote node. On each unit, Mate Management Access must be enabled before configuring in-band management.

Table 67 MIMO Protection Cables.

Marketing Model	Description
PTP 820_MIMO_Prot_mng_cbl_1m	PTP 820 MIMO or Prot management cable 1m
PTP 820_MIMO_Prot_mng_cbl_5m	PTP 820C MIMO or Prot management cable 5m
PTP 820_MIMO_Prot_mng_cbl_10m	PTP 820C MIMO or Prot management cable 10m
PTP 820_MIMO_Prot_mng_cbl_20m	PTP 820C MIMO or Prot management cable 20m
PTP 820_MIMO_Prot_mng_cbl_30m	PTP 820C MIMO or Prot management cable 30m

To enable Mate Management Access, enter the following command:

```
root> platform management mate-access admin enable
```

Note: When you enable or disable Mate Management Access, the unit is reset.

To disable Mate Management Access, enter the following command:

```
root> platform management mate-access admin disable
```

To display whether Mate Management Access is enabled, enter the following command:

```
root> platform management mate-access show
```

**Note**

Mate Management Access can only be configured via CLI.

Upon recovery from a failure event, management may be lost for up to 40 seconds.

Configuring In-Band Management (CLI)

**Note**

To use in-band management for nodes that utilize two PTP 820C units (4x4 MIMO, 2x2 XPIC, and 4+0 Multi-Carrier ABC), you must first configure Mate Management Access (IP Forwarding). See [Mate Management Access \(IP Forwarding\) \(CLI\)](#).

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

Each PTP 820 unit includes a pre-defined management service with Service ID 257. The management service is a multipoint service that connects the two local management ports and the network element host CPU in a single service. In order to enable in-band management, you must add at least one service point to the management service, in the direction of the remote site or sites from which you want to access the unit for management. For instructions on adding service points, see [Configuring Service Points \(CLI\)](#).

**Note**

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

Changing the Management IP Address (CLI)

Related Topics:

- [Defining the IP Protocol Version for Initiating Communications \(CLI\)](#)
- [Configuring the Remote Unit's IP Address \(CLI\)](#)

You can enter the unit's address in IPv4 format and/or in IPv6 format. The unit will receive communications whether they were sent to its IPv4 address or its IPv6 address.

To set the unit's IP address in IPv4 format, enter the following command in root view to configure the IP address, subnet mask, and default gateway:

```
root> platform management ip set ipv4-address <ipv4-address> subnet
<subnet> gateway <gateway> name <name> description <name>
```

Table 68 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 69 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 820 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 820 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 820 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.

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
```

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 \(CLI\)](#)



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 70 Local Time Configuration CLI Parameters

Parameter	Input Type	Permitted Values	Description
date-and-time	Number	dd-mm-yyyy, hh:mm:ss where: dd = date mm = month yyyy= year hh = hour mm = minutes ss = seconds	Sets the UTC time.
hours-offset	Number	-12 – 13	The required hours offset (positive or negative) relative to GMT. This is used to offset the clock relative to GMT, according to the global meridian location.
minutes-offset	Number	0 – 59	The required minutes relative to GMT. This is used to offset the clock relative to GMT, according to the global meridian location.

Examples

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 71: 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.

Examples

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

PTP 820S unit has a single radio interface.

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 72 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 in PTP 820C or PTP 820S: 2	The slot on which the interface is located.
port	Number	GbE 1: 1 GbE 2: 2 GbE 3: 3 Radio Carrier 1: 1 Radio Carrier 2 (PTP 820C only): 2	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.

Examples

The following command enables Ethernet port 2:

```
root> platform if-manager set interface-type ethernet slot 1 port 2 admin up
```

The following command enables radio interface 1 in a PTP 820C or PTP 820S unit:

```
root> platform if-manager set interface-type radio slot 2 port 1 admin up
```

The following command disables Ethernet port 3:

```
root> platform if-manager set interface-type ethernet slot 1 port 3 admin down
```

Configuring the Radio Parameters (CLI)

In order to establish a radio link, you must:

- Enter radio view.
- Unmute the radio carrier.
- Configure the radio frequencies.
- Configure the TX level.

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>
```

Table 73 Entering Radio View CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	2	
port	Number	Radio Carrier 1: 1 Radio Carrier 2 (PTP 820C only): 2	The specific radio carrier you want to access.

Examples

The following command enters radio view for radio carrier 1:

```
root> radio slot 2 port 1
```

The following prompt appears:

```
radio[2/1]>
```



Note

For convenience, this User Guide generally shows the radio prompt as `radio[2/1]>`.

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 display the mute status of a radio, enter the following command:

```
radio[x/x]>rf mute show status
```

Table 74 Radio Mute/Unmute CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin	Variable	on off	Mutes (on) or unmutes (off) the radio.

Examples

The following command mutes radio carrier 1:

```
radio[2/1]>rf mute set admin on
```

The following command unmutes radio carrier 2 in a PTP 820C unit:

```
radio[2/2]>rf mute set admin off
```

Configuring the Transmit (TX) Level (CLI)

To set the transmit (TX) level of a radio, enter the following command:

```
radio[x/x]>rf set tx-level <tx-level>
```

To display the maximum transmit (TX) level of a radio, enter the following command:

```
radio[x/x]>rf show max-tx-level
```

Table 75 Radio Transmit (TX) Level CLI Parameters

Parameter	Input Type	Permitted Values	Description
tx-level	Number	PTP 820C and PTP 820S units: -1 to 22 (Hardware model dependent)	The desired TX signal level (TSL), in dBm.

Examples

The following command sets the TX level of radio carrier 1 to 10 dBm:

```
radio[2/1]>rf set tx-level 10
```

Configuring the Transmit (TX) Frequency (CLI)

To set the transmit (TX) frequency of a radio, enter the following command. This command includes an option to set the remote RX frequency in parallel:

```
radio[x/x]>rf set tx-frequency <tx-frequency> local-remote <local-remote>
```


Table 76 Radio Transmit (TX) Frequency CLI Parameters

Parameter	Input Type	Permitted Values	Description
tx-frequency	Number	Depends on the MRMC script and the unit type.	The desired TX frequency (in KHz) and, if <local-remote> is set to enable, the desired RX frequency of the remote unit.
local-remote	Variable	enable disable	Optional. Determines whether to apply the configured TX frequency value to the RX frequency of the remote unit.

Examples

The following command sets the TX frequency of radio carrier 1 in a PTP 820C or PTP 820S unit to 12900000 KHz, and sets the RX frequency of the remote unit to the same value.

```
radio[2/1]>rf set tx-frequency 12900000 local-remote enable
```

The following command sets the TX frequency of radio carrier 1 in a PTP 820C or PTP 820S unit to 12900000 KHz, but does not set the RX frequency of the remote unit.

```
radio[2/1]>rf set rx-frequency 12900000 local-remote disable
```

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, enter the following command in radio view:

```
radio[x/x]>mrmc script show script-type <script-type> acm-support <acm-support>
```



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

Table 77 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.

Parameter	Input Type	Permitted Values	Description
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.

Examples

The following command displays available symmetrical (normal) scripts with ACM support for radio carrier 2 in a PTP 820C unit:

```
radio[2/2]>mrmc script show script-type normal acm-support yes
```

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.

To assign a script with ACM enabled, enter the following command:

```
radio[x/x]> mrmc set acm-support script-id <script-id> modulation  
adaptive max-profile <profile>
```

To assign a script without ACM enabled, enter the following command:

```
radio[x/x]> mrmc set acm-support script-id <script-id> modulation fixed  
profile <profile>
```

To display the current MRMC script configuration, enter the following command:

```
radio[x/x]>mrmc show script-configuration
```

Table 78 MRMC Script Assignment to Radio Carrier CLI Parameters

Parameter	Input Type	Permitted Values	Description
script-id	Number	Depends on available scripts.	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	Depends on the unit type. See Configuring the Radio (MRMC) Scripts (CLI) .	Adaptive ACM mode only: The maximum profile for the script. For example, if you select a maximum profile of 5, the system will not climb above profile 5, even if channel fading conditions allow it.
min-profile	Number	Depends on the unit type. See Configuring the Radio (MRMC) Scripts (CLI) .	Adaptive ACM mode only: The minimum profile for the script. For example, if you select a minimum profile of 3, the system will not go below profile 3 regardless of the channel fading conditions. The minimum profile cannot be greater than the maximum profile, but it can be equal to it. If you do not include this parameter in the command, the minimum profile is set at the default value of 0.
profile	Number	Depends on the unit type. See Configuring the Radio (MRMC) Scripts (CLI) .	Fixed ACM mode only: The profile in which the system will operate

Examples

The following command assigns MRMC script ID 1503, with ACM enabled, a minimum profile of 3, and a maximum profile of 9, to radio carrier 1 in a PTP 820C or PTP 820S unit:

```
radio[2/1]>mrnc set acm-support script-id 13 modulation adaptive max-profile 9 min-profile 3
```

The following command assigns MRMC script ID 1502, with ACM disabled and a profile of 5, to radio carrier 2 in a PTP 820C unit:

```
radio[2/2]>mrnc set acm-support script-id 13 modulation fixed profile 5
```

Enabling ACM with Adaptive Transmit Power (CLI)

When planning ACM-based radio links, the radio planner attempts to apply the lowest transmit power that will perform satisfactorily at the highest level of modulation. During fade conditions requiring a modulation drop, most radio systems cannot increase transmit power to compensate for the signal degradation, resulting in a deeper reduction in capacity. The PTP 820 is capable of adjusting power on the fly, and optimizing the available capacity at every modulation point.

To enable Adaptive TX Power for a radio, enter the following command:

```
radio[x/x]>rf adaptive-power set admin enable
```

To disable Adaptive TX Power for a radio, enter the following command:

```
radio[x/x]>rf adaptive-power set admin disable
```

To display whether Adaptive TX Power is enabled, enter the following command:

```
radio[x/x]>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 that the feature is configured and operates independently for each radio link.

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.

Operating in FIPS Mode (CLI)

**Note**

This feature is only relevant for PTP 820C and PTP 820S units. FIPS 140-2 compliance is only available with the PTP 820 Assured platform.¹The PTP 820 Assured Platform is not supported by System release 10.0..

From release 9.0, PTP 820C and PTP 820S can be configured to be FIPS 140-2-compliant in specific hardware and software configurations, as described in this section.

Requirements for FIPS Compliance (CLI)

For details on hardware requirements for operating in FIPS mode, see [Requirements for FIPS Compliance](#).

Enabling FIPS Mode (CLI)

To set the unit to operate in FIPS mode, enter the following command in root view:

```
root> platform security fips-mode set admin enable
```

To disable FIPS mode, enter the following command in root view:

```
root> platform security fips-mode set admin disable
```

**Note**

Changing the FIPS configuration causes a unit reset.

To display the unit's current FIPS setting, enter the following command in root view:

```
root> platform security fips-mode show
```

Status values are:

- **enable** – FIPS mode is enabled.
- **disable** – FIPS mode is disabled.

After enabling FIPS:

- The MD5 option for SNMPv3 is blocked.
- After any system reset, the length of time before users can log back into the system is longer than usual due to FIPS-related self-testing.

¹ The PTP 820 Assured platform is supported with Release 8.3. It is not supported with Release 9.0.

Configuring Grouping (Optional) (CLI)

At this point in the configuration process, you should configure any interface groups that need to be set up according to your network plan. For details on available grouping and other configuration options, as well as configuration instructions, see [System Configurations \(CLI\)](#).

Creating Service(s) for Traffic (CLI)

In order to pass traffic through the PTP 820, you must configure Ethernet traffic services. For configuration instructions, see [Configuring Ethernet Services \(CLI\)](#).

Chapter 14: Configuration Guide (CLI)

This section includes:

- [System Configurations \(CLI\)](#)
- [Configuring Multi-Carrier ABC \(CLI\)](#)
- [Configuring Link Aggregation \(LAG\) and LACP \(Optional\) \(CLI\)](#)
- [Configuring XPIC \(CLI\)](#)
- [Configuring Unit Protection with HSB Radio Protection \(External Protection\) \(CLI\)](#)
- [Configuring MIMO and Space Diversity \(CLI\)](#)
- [Operating a PTP 820C in Single Radio Carrier Mode \(CLI\)](#)

System Configurations (CLI)

This section lists the basic system configurations and the PTP 820 product types that support them, as well as links to configuration instructions.

Table 79 System Configurations (CLI)

Configuration	Supported Products	Link to Configuration Instructions
Multi-Carrier ABC (Multi-Radio)	PTP 820C	Configuring Multi-Carrier ABC (CLI)
Link Aggregation (LAG)	PTP 820C/S	Configuring Link Aggregation (LAG) and LACP (Optional) (CLI)
XPIC	PTP 820C	Configuring XPIC (CLI)
HSB Radio Protection	PTP 820C/S	Configuring Unit Protection with HSB Radio Protection (External Protection) (CLI)
MIMO and Space Diversity	PTP 820C	Configuring MIMO and Space Diversity (CLI)
1+1 HSB with Space Diversity	PTP 820C	Configuring 1+1 HSB with Space Diversity (CLI)
AFR+1	PTP 820C (hub site or tail site) PTP 820S (tail site only)	Configuring Advanced Frequency Reuse (AFR) (CLI)
PTP 820C in Single Radio Carrier Mode	PTP 820C	Operating a PTP 820C in Single Radio Carrier Mode (CLI)

Configuring Multi-Carrier ABC (CLI)

**Note**

This option is only relevant for PTP 820C units.

This section includes:

- [Multi-Carrier ABC Overview \(CLI\)](#)
- [Configuring a Multi-Carrier ABC Group \(CLI\)](#)
- [Configuring the Multi-Carrier ABC Minimum Bandwidth Override Option \(CLI\)](#)
- [Configuring the Multi-Carrier ABC Minimum Bandwidth Override Option \(CLI\)](#)

A multi-carrier ABC group can be configured to be placed in Down state if the group's capacity falls beneath a user-defined threshold.

By default, the Multi-Carrier ABC minimum bandwidth override option is disabled. When enabled, the Multi-Carrier ABC group is automatically placed in a Down state in the event that the group's aggregated capacity falls beneath the user-configured threshold. The group is returned to an Up state when its aggregated capacity goes above the threshold. An alarm is also raised:

- Alarm ID – 2201
- Alarm Description – Multi Carrier ABC bandwidth is below the threshold

This option is used in conjunction with the LAG group shutdown in case of degradation event option ([see Enabling and Disabling the LAG Group Shutdown in Case of Degradation Event Option \(CLI\)](#)) in cases where the operator wants to re-route traffic from an upstream switch connected to an another PTP 820 unit whenever the link is providing less than a certain capacity. To set up a configuration in which a drop in the capacity of the Multi-Carrier ABC group closes the Ethernet port in the upstream PTP 820 unit, you must perform all of the following steps:

- Enable the Multi-Carrier ABC minimum bandwidth option and set a threshold on the PTP 820C unit, as described below.
- Enable an ASP group on the PTP 820C unit, where the Monitored Interface is the Multi-Carrier ABC group and the Controlled Interface is the Ethernet interface that faces the upstream PTP 820 unit. See [Configuring Automatic State Propagation \(CLI\)](#).
- Enable the LAG group shutdown in case of degradation event option on the upstream PTP 820 unit.

Notes:**Note**

When using in-band management, management is lost in the event of radio failure and returns when the radio link is restored.

The minimum bandwidth threshold is based on the capacity of the Multi-Carrier ABC group, not the combined capacities of the group's members. The group's aggregated capacity is displayed in the Multi-Carrier ABC Group – Edit Group page ([Figure 57](#))..

To enable Multi-Carrier ABC Minimum Bandwidth Override, enter the following command in root view:

```
root> platform if-manager set group-type abc group-number <1-4> minimum-bw-admin enable
```

To disable Multi-Carrier ABC Minimum Bandwidth Override, enter the following command in root view:

```
root> platform if-manager set group-type abc group-number <1-4> minimum-bw-admin disable
```

To set the Multi-Carrier ABC Minimum Bandwidth Override threshold (in Mbps), enter the following command in root view:

```
root> platform if-manager set group-type abc group-number <1-4> minimum-bw-threshold <0-20000>
```

The threshold can be between 0 – 20000 Mbps, with a resolution of 1 Mbps.

The following commands enable Multi-Carrier ABC Minimum Bandwidth Override threshold for Multi-Carrier ABC group 1, and set a threshold of 12000 Mbps.

```
root> platform if-manager set group-type abc group-number 1 minimum-bw-admin enable
root> platform if-manager set group-type abc group-number 1 minimum-bw-threshold 12000
```

To view the status and the threshold use the following command:

```
root> platform if-manager show interfaces
```

- [Removing Members from a Multi-Carrier ABC Group \(CLI\)](#)
- [Deleting a Multi-Carrier ABC Group \(CLI\)](#)

Multi-Carrier ABC Overview (CLI)

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 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.

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
multi-carrier-abc group-id [1]>
```

- 2 Enter Multi-Carrier ABC Group view by entering the following command in root view:

```
root> multi-carrier-abc group-id [1]
```

- 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.

```
multi-carrier-abc group-id [1]> attach-member slot 2 port <port> 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.

```
root> multi-carrier-abc create group group_id 1
multi-carrier-abc group-id[1]> attach-member slot 2 port 1 channel-id 1
multi-carrier-abc group-id[1]> attach-member slot 2 port 2 channel-id 2
multi-carrier-abc group-id[1]> exit
```

Configuring the Multi-Carrier ABC Minimum Bandwidth Override Option (CLI)

A multi-carrier ABC group can be configured to be placed in Down state if the group's capacity falls beneath a user-defined threshold.

By default, the Multi-Carrier ABC minimum bandwidth override option is disabled. When enabled, the Multi-Carrier ABC group is automatically placed in a Down state in the event that the group's aggregated capacity falls beneath the user-configured threshold. The group is returned to an Up state when its aggregated capacity goes above the threshold. An alarm is also raised:

- Alarm ID – 2201
- Alarm Description – Multi Carrier ABC bandwidth is below the threshold

This option is used in conjunction with the LAG group shutdown in case of degradation event option (see [Enabling and Disabling the LAG Group Shutdown in Case of Degradation Event Option \(CLI\)](#)) in cases where the operator wants to re-route traffic from an upstream switch connected to an another PTP 820 unit whenever the link is providing less than a certain capacity. To set up a configuration in which a drop in the capacity of the Multi-Carrier ABC group closes the Ethernet port in the upstream PTP 820 unit, you must perform all of the following steps:

- Enable the Multi-Carrier ABC minimum bandwidth option and set a threshold on the PTP 820C unit, as described below.
- Enable an ASP group on the PTP 820C unit, where the Monitored Interface is the Multi-Carrier ABC group and the Controlled Interface is the Ethernet interface that faces the upstream PTP 820 unit. See [Configuring Automatic State Propagation and Link Loss Forwarding \(CLI\)](#).
- Enable the LAG group shutdown in case of degradation event option on the upstream PTP 820C unit.

Notes:**Note**

When using in-band management, management is lost in the event of radio failure and returns when the radio link is restored.

The minimum bandwidth threshold is based on the capacity of the Multi-Carrier ABC group, not the combined capacities of the group's members. The group's aggregated capacity is displayed in the Multi-Carrier ABC Group – Edit Group page ([Figure 57](#)).

To enable Multi-Carrier ABC Minimum Bandwidth Override, enter the following command in root view:

```
root> platform if-manager set group-type abc group-number <1-4> minimum-
bw-admin enable
```

To disable Multi-Carrier ABC Minimum Bandwidth Override, enter the following command in root view:

```
root> platform if-manager set group-type abc group-number <1-4> minimum-
bw-admin disable
```

To set the Multi-Carrier ABC Minimum Bandwidth Override threshold (in Mbps), enter the following command in root view:

```
root> platform if-manager set group-type abc group-number <1-4> minimum-
bw-threshold <0-20000>
```

The threshold can be between 0 – 20000 Mbps, with a resolution of 1 Mbps.

The following commands enable Multi-Carrier ABC Minimum Bandwidth Override threshold for Multi-Carrier ABC group 1, and set a threshold of 12000 Mbps.

```
root> platform if-manager set group-type abc group-number 1 minimum-bw-
admin enable
root> platform if-manager set group-type abc group-number 1 minimum-bw-
threshold 12000
```

To view the status and the threshold use the following command:

```
root> platform if-manager show interfaces
```

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 group-id[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 [Configuring the Multi-Carrier ABC Minimum Bandwidth Override Option \(CLI\)](#).

A multi-carrier ABC group can be configured to be placed in Down state if the group's capacity falls beneath a user-defined threshold.

By default, the Multi-Carrier ABC minimum bandwidth override option is disabled. When enabled, the Multi-Carrier ABC group is automatically placed in a Down state in the event that the group's aggregated capacity falls beneath the user-configured threshold. The group is returned to an Up state when its aggregated capacity goes above the threshold. An alarm is also raised:

- Alarm ID – 2201
- Alarm Description – Multi Carrier ABC bandwidth is below the threshold

This option is used in conjunction with the LAG group shutdown in case of degradation event option (see [Enabling and Disabling the LAG Group Shutdown in Case of Degradation Event Option \(CLI\)](#)) in cases where the operator wants to re-route traffic from an upstream switch connected to an another PTP 820 unit whenever the link is providing less than a certain capacity. To set up a configuration in which a drop in the capacity of the Multi-Carrier ABC group closes the Ethernet port in the upstream PTP 820 unit, you must perform all of the following steps:

- Enable the Multi-Carrier ABC minimum bandwidth option and set a threshold on the PTP 820C unit, as described below.
- Enable an ASP group on the PTP 820C unit, where the Monitored Interface is the Multi-Carrier ABC group and the Controlled Interface is the Ethernet interface that faces the upstream PTP 820 unit. See [Configuring Automatic State Propagation \(CLI\)](#).
- Enable the LAG group shutdown in case of degradation event option on the upstream PTP 820 unit.

Notes:



Note

When using in-band management, management is lost in the event of radio failure and returns when the radio link is restored.

The minimum bandwidth threshold is based on the capacity of the Multi-Carrier ABC group, not the combined capacities of the group's members. The group's aggregated capacity is displayed in the Multi-Carrier ABC Group – Edit Group page ([Figure 57](#)).

To enable Multi-Carrier ABC Minimum Bandwidth Override, enter the following command in root view:


```
root> platform if-manager set group-type abc group-number <1-4> minimum-  
bw-admin enable
```

To disable Multi-Carrier ABC Minimum Bandwidth Override, enter the following command in root view:

```
root> platform if-manager set group-type abc group-number <1-4> minimum-  
bw-admin disable
```

To set the Multi-Carrier ABC Minimum Bandwidth Override threshold (in Mbps), enter the following command in root view:

```
root> platform if-manager set group-type abc group-number <1-4> minimum-  
bw-threshold <0-20000>
```

The threshold can be between 0 – 20000 Mbps, with a resolution of 1 Mbps.

The following commands enable Multi-Carrier ABC Minimum Bandwidth Override threshold for Multi-Carrier ABC group 1, and set a threshold of 12000 Mbps.

```
root> platform if-manager set group-type abc group-number 1 minimum-bw-  
admin enable  
root> platform if-manager set group-type abc group-number 1 minimum-bw-  
threshold 12000
```

To view the status and the threshold use the following command:

```
root> platform if-manager show interfaces
```

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
```

Configuring Link Aggregation (LAG) and LACP (Optional) (CLI)

Link aggregation (LAG) enables you to group several physical Ethernet or radio interfaces into a single logical interface bound to a single MAC address. This logical interface is known as a LAG group. Traffic sent to the interfaces in a LAG group is distributed by means of a load balancing function. PTP 820 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 function. PTP 820 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 820 supports LACP, which expands the capabilities of static LAG and provides interoperability with third-party equipment that uses LACP. LACP improves the communication between LAG members. This improves error detection capabilities in situations such as improper LAG configuration or improper cabling. It also enables the LAG to detect uni-directional failure and remove the link from the LAG, preventing packet loss.

LACP is enabled as part of the LAG configuration process. It should only be used if the LAG is in a link with another LACP-enabled LAG.

**Note**

LACP is not supported with unit protection. For unit protection, a special, limited implementation is configured on the logical interface level. See [Configuring Line Protection Mode \(CLI\)](#).

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 80 LAG Group CLI Parameters

Parameter	Input Type	Permitted Values	Description
lagid	Variable	lag1 lag2 lag3 lag4	The ID for the LAG.
slot	Number	Ethernet: 1 Radio: 2	Depends on the interface and unit type.
port	Number	GbE 1: 1 GbE 2: 2 GbE 3: 3 Radio Carrier 1: 1 Radio Carrier 2 (PTP 820C only): 2	The port number of the interface.

Examples

The following commands create a LAG with the ID lag2. The LAG includes the Ethernet interfaces 1 and 2 and radio interface 1:

```

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 1 admin
up
root> platform if-manager set interface-type ethernet slot 1 port 2 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)         2/1
eth group [lag2]> operational state show
Port operational state: up.
eth group [lag2]>
```

The following commands remove port 2 on slot 1 from the LAG:

```
root> platform if-manager set interface-type ethernet slot 1 port 2 admin
down
root> ethernet interfaces group lag2
eth group [lag2]>
eth group [lag2]> port static-lag remove member interface eth slot 1 port
2
```

Enabling and Disabling the LAG Group Shutdown in Case of Degradation Event Option (CLI)

**Note**

LAG Group Shutdown in Case of Degradation Event cannot be used with LACP.

A LAG group can be configured to be automatically closed in the event of LAG degradation. This option is used if you want traffic from the switch to be re-routed during such time as the link is providing less than a certain capacity.

By default, the LAG group shutdown in case of degradation event option is disabled. When enabled, the LAG is automatically closed in the event that any one or more ports in the LAG fail. When all ports in the LAG are again operational, the LAG is automatically re-opened.

**Note**

Failure of a port in the LAG also triggers a lag-degraded alarm, Alarm ID 100.

To enable the LAG group shutdown in case of degradation event option, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> static-lag set lag-degrade-admin admin enable
```

To disable the LAG group shutdown in case of degradation event option, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> static-lag set lag-degrade-admin admin disable
```

To display the current LAG group shutdown in case of degradation event option setting, go to interface view for the LAG and enter the following command:

```
eth group [lagx]> static-lag show lag-degrade-admin
```

The following commands enable the LAG group shutdown in case of degradation event option for LAG group 1:

```
root> ethernet interfaces group lag1  
eth group [lag1]>static-lag set lag-degrade-admin admin enable  
eth group [lag1]>
```

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 820 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 81 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

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 82 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.

Parameter	Definition
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: <ul style="list-style-type: none"> • 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 83 LACP Port Statistics (CLI)

Parameter	Definition
LACPDU RX	The number of LACPDU s that this port has received.
LACPDU TX	The number of LACPDU s 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.

Configuring XPIC (CLI)

**Note**

This option is only relevant for PTP 820C units.

This section explains how to configure XPIC and includes the following topics:

- [XPIC Overview \(CLI\)](#)
- [Configuring the Radio Carriers for XPIC \(CLI\)](#)
- [Creating an XPIC Group \(CLI\)](#)
- [Performing Antenna Alignment for XPIC \(CLI\)](#)

XPIC Overview (CLI)

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.

In addition, XPIC includes an automatic recovery mechanism that ensures that if one carrier fails, or a false signal is received, the mate carrier will not be affected. This mechanism also ensures that both carriers will be operational, after the failure is cleared.

To configure and enable XPIC, first configure the Carriers and then perform antenna alignment, as described below.

For 2+2 XPIC using an external switch operating in LAG mode, Mate Management Access enables users to manage both units via in-band management. See [Mate Management Access \(IP Forwarding\) \(CLI\)](#).

Configuring the Radio Carriers for XPIC (CLI)

To configure the radio carriers:

1. Configure the carriers on both ends of the link to the desired frequency channel. Both carriers must be configured to the same frequency channel.
2. Assign XPIC (CCDP operational mode) support-enabled script to both RMCs on both ends of the link. Each RMC must be assigned the same script. See [Configuring the Radio \(MRMC\) Script\(s\) \(CLI\)](#).

**Note**

XPIC support is indicated by an X in the script name. For example, mdN_A2828X_111_1205 is an XPIC-enabled script. mdN_A2828N_130_100 is not an XPIC-enabled script. For a list of XPIC support-enabled scripts, refer to the most recent PTP 820C/S Release Notes.

3. Create an XPIC group. See [Creating an XPIC Group \(CLI\)](#).

Creating an XPIC Group (CLI)

To create an XPIC group, enter the following commands:

```
root> radio-groups
radio-groups>
radio-groups> xpik set admin enable
```

To disable XPIC, enter the following commands:

```
root> radio-groups
radio-groups>
radio-groups> xpik set admin disable
```

Performing Antenna Alignment for XPIC (CLI)

To configure the antennas:

1. Align the antennas for the first carrier. For a 2+2 XPIC configuration (or a 4x4 MIMO configuration), align the antennas for the first carrier on the upper PTP 820C unit. While you are aligning these antennas, mute the second carrier. See ***Error! Reference source not found..*** For a 2+2 XPIC configuration (or a 4x4 MIMO configuration), mute all the carriers except the first carrier on the upper PTP 820C unit.
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}".

**Note**

To measure the second carrier, leave the Voltmeter connected to the BNC connector. In the Radio Parameters page of the Web EMS, change the **RSL Connector Source** field from **PHYS1** to **PHYS2** (or vice versa). The BNC connector will now measure RSL from the other carrier.

4. Determine the XPI, using either of the following two methods:
 - To calculate the XPI, subtract RSL_{unwanted} from the RSL_{wanted}.
 - Read the XPI by going to radio view and entering one of the following commands:

```
radio [x/x]>modem pm-xpi show interval 15min
```

```
radio [x/x]>modem pm-xpi show interval 24hr
```

5. The XPI should be between 25dB and 30 dB. 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 XPI, 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 XPI.



Note

As an extra step, to check the veracity of the initial measurements, you can mute the first carrier and unmute the second carrier on the upper PTP 820C units on both sides of the link. Then measure the RSL of the second carrier link (the "RSL_{wanted}"), measure the RSL of the first carrier (the "RSL_{unwanted}") and determine the XPI. The XPI should match the XPI with the second carriers muted.

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 ± 2 dB. The RSL of the vertical carrier of the local unit should match the RSL of the horizontal carrier of the remote unit, within ± 2 dB.
7. For a 2x2 configuration, repeat Steps **Error! Reference source not found.** through **Error! Reference source not found.** for the lower PTP 820C unit.
8. Check the XPI levels of all the carriers at both sides of the link by going to radio view and entering one of the following commands:

```
radio [x/x]>modem pm-xpi show interval 15min
```

```
radio [x/x]>modem pm-xpi show interval 24hr
```

All four 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.

Displaying XPIC Status (CLI)

To display the status of an XPIC group, enter the following command in radio-groups view:

```
radio-groups> xpig show status
```

The following is a typical command output:

```
XPIC:
Carrier 1: Radio #[2/1]      ;   Carrier 2: Radio #[2/2]
Admin mode: enable
XPIC state: XPIC-Idle
```

Configuring Unit Protection with HSB Radio Protection (External Protection) (CLI)

This section explains how to configure HSB radio protection and includes the following topics:

- [Unit Protection Overview \(CLI\)](#)
- [Configuring HSB Radio Protection \(CLI\)](#)
- [Configuring 2+2 HSB Protection on a PTP 820C Unit \(CLI\)](#)
- [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 \(CLI\)](#)

Unit Protection Overview (CLI)

PTP 820C and PTP 820S support 1+1 HSB radio protection. PTP 820C also supports 2+2 HSB radio protection. In HSB radio protection, one PTP 820 operates in active mode and the other operates in standby mode. If a protection switchover occurs, the Active unit goes into standby mode and the Standby unit goes into active mode.

- For a full explanation of 1+1 HSB radio protection and 2+2 HSB radio protection support in PTP 820C, refer to the PTP 820C Technical Description.
- For a full explanation of 1+1 HSB radio protection support in PTP 820S, refer to the PTP 820S Technical Description.

To configure unit protection, you must perform the following steps:

- 1 Configure Ethernet interface protection – See [Configuring Ethernet Interface Protection \(CLI\)](#).
- 2 Configure HSB radio protection – See [Configuring HSB Radio Protection \(CLI\)](#).
- 3 For 2+2 HSB configurations (PTP 820C only), perform the additional steps described in [Configuring 2+2 HSB Protection on a PTP 820C Unit \(CLI\)](#).

Configuring Ethernet Interface Protection (CLI)

There are two modes for Ethernet interface protection in an HSB radio protection configuration:

Line Protection Mode – Traffic is routed to the Ethernet ports via two ports on an external switch.

Split Protection Mode – Only available for optical Ethernet ports. An optical splitter cable is used to connect to both the active and the standby optical Ethernet ports.

Configuring Line Protection Mode (CLI)

To configure line protection mode:

- 1 Configure the GE ports on the external switch in LACP mode. The external switch must support LACP.



Note

PTP 820 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 Connect one port on the external switch to an Ethernet port on the active PTP 820, and the other port on the external switch to an Ethernet port on the standby PTP 820.
- 3 Enable LACP on the Ethernet interface connected to the external switch on the active PTP 820:
 - i Go to interface view for the Ethernet interface connected to the external switch on the active PTP 820.
 - 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 Split Ethernet Interface Protection Mode (CLI)

To configure split Ethernet interface protection mode:

- 1 Use an optical splitter to route traffic to an optical Ethernet port on each PTP 820 unit.
- 2 Proceed to [Configuring HSB Radio Protection \(CLI\)](#).

Configuring HSB Radio Protection (CLI)

You must perform the initial configuration of a 1+1 or 2+2 HSB system using a splitter cable for each unit to provide a management connection to each unit. For instructions on preparing and connecting the splitter cables, refer to the Installation Guide for PTP 820C or PTP 820S.

To configure HSB radio protection:

1. Before enabling protection, you must:

- i. Verify that both units have the same hardware part number (see [Displaying Unit Inventory \(CLI\)](#)) and the same software version (see [Viewing Current Software Versions \(CLI\)](#)). If the units do not have the same software version, upgrade each unit to the most recent software release (see [Configuring a Software Download \(CLI\)](#)).
 - ii. Assign an IP address to each unit. For instructions, see [Changing the Management IP Address \(CLI\)](#).
 - iii. Establish a management connection to one of the units. You can select either unit; once you enable Protection Administration, the system will determine which unit becomes the Active unit.
2. To enable protection, enter the following command in root view:

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

The system configures itself for HSB protection:

- o The system determines which unit is the Active unit based on a number of pre-defined criteria.
 - o When the system returns online, all management must be performed via the Active unit using the IP address you defined for that unit.
 - o 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.
 - o Management of the Standby unit is performed via the Active unit, via the cable between the two MIMO/Prot ports on the splitters connecting the two units.
 - o HSB protection is enabled on both units.
3. Once you have enabled Protection Admin:
 - i. Perform all necessary radio configurations on the Active unit, such as setting the frequency, assigning MRMC scripts, unmuting the radio, and setting up radio groups such as XPIC or Multi-Carrier ABC (Multi-Radio).
 - ii. Perform all necessary Ethernet configurations on the Active unit, such as defining Ethernet services.
 - iii. Enter the following command in root view to copy the configuration of the Active unit to the Standby unit:

```
root> platform management protection copy-to-mate
```

**Note**

While the system is performing the copy-to-mate operation, a temporary loss of management connection will occur.

To keep the Standby unit up-to-date, after any change to the configuration of the Active unit enter the `copy-to-mate` command to copy the configuration to the Standby unit.

If you are unsure whether the Standby unit's configuration matches that of the Active unit, enter the following command in root view. The command output displays the list of mismatched parameters.

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

Configuring 2+2 HSB Protection on a PTP 820C Unit (CLI)

In order to configure 2+2 HSB unit protection on a PTP 820C unit, you must simply enable the second radio carrier on both units on both sides of the link. No other configuration is necessary other than the configuration described above.

To enable the second radio carrier on both units using the CLI, enter the following commands in root view:

```
root> platform if-manager set interface-type radio slot 2 port 2 admin up
root> platform management protection copy-to-mate
```

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:

- Setting the Unit Name. Refer to the description of `platform management system-name set name` in [Configuring Unit Parameters \(CLI\)](#).
- Disabling/enabling Radio TX-mute. Refer to the description of `rf mute set admin` in [Muting and Unmuting a Radio \(CLI\)](#).
- Clearing the Radio and RMON counters. Refer to the description of `modem clear counters` in [Displaying General Modem Status and Defective Block PMs \(CLI\)](#).
- Setting the activation key configuration. Refer to [Mate Management Access \(IP Forwarding\) \(CLI\)](#) and [Activating a Demo Activation Key \(CLI\)](#).
- Defining user accounts. Refer to [Configuring User Accounts \(CLI\)](#).
- Setting synchronization settings. Refer to [Activating a Demo Activation Key \(CLI\)](#).

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
```

- To view the current lockout status, enter the following command in root view:

```
root> platform management protection show lockout status
```

Manually Switching to the Standby Unit (CLI)

The following events trigger switchover for HSB radio protection according to their priority, with the highest priority triggers listed first.

- 1 Loss of active unit
- 2 Lockout

- 3 Radio/Ethernet interface failure
- 4 Manual switch

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 command 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 1+1 HSB with Space Diversity (CLI)



Note

This feature is only relevant for PTP 820C. It can be used with all PTP 820C hardware versions.

A 1+1 HSB-SD configuration utilizes two PTP 820C units on each side of the link, with both radio carriers activated. The PTP 820C units are combined and connected to the primary and diversity antennas via a dual coupler and two flexible waveguides.

Radio carrier 2 is muted on each unit. On the receiving side, the signals are combined in the active unit to produce a single, optimized signal. The link is protected via external protection, so that if a protection switchover occurs, the standby unit becomes the active unit, and the link continues to function with full space diversity.

To configure a 1+1 HSB link with Space Diversity:

1. For one PTP 820C unit, enter the following command in root view to create a Space Diversity group:

```
root> radio mimo create group 1 mimo-type 1-plus-0-sd radio 2 port 1  
radio 2 port 2
```

2. Enter the following command in root view to enable the Space Diversity group:

```
root> radio mimo set-admin group 1 admin enable
```

3. Repeat Steps **Error! Reference source not found.** and **Error! Reference source not found.** for the second unit.

**Note**

The identity of the active and standby units is not determined until unit protection is configured.

4. Configure Unit Protection, according to the instructions in [Configuring Unit Protection with HSB Radio Protection \(External Protection\) \(CLI\)](#)
5. on the active PTP 8200 unit, mute the transmitter of radio carrier2. For instructions, see [Muting and Unmuting a Radio \(CLI\)](#).
6. Perform Copy to Mate. See Step 3 in [Configuring HSB Radio Protection \(CLI\)](#)

**Note**

It is crucial to ensure that the port connected to the Diversity antenna is muted in each PTP 820 unit. If you perform Copy to Mate after configuring unit protection, as indicated above, the mute configuration will be copied to the standby unit. If you mute the interface before configuring unit protection, you must make sure to manually mute the interface on both PTP 820 units. Otherwise, configuring unit protection will override the mute configuration.

Configuring MIMO and Space Diversity (CLI)

**Note**

This feature is only relevant for PTP 820C units.

This section describes how to configure MIMO and space diversity, and include the following topics:

- [MIMO and Space Diversity Overview \(CLI\)](#)
- [Configuring a MIMO Link \(CLI\)](#)
- [Creating a MIMO or Space Diversity Group \(CLI\)](#)
- [Enabling/Disabling a MIMO or Space Diversity Group \(CLI\)](#)
- [Setting the Role of a MIMO or Space Diversity Group \(CLI\)](#)
- [Resetting MIMO \(CLI\)](#)
- [Viewing MMI and XPI Levels \(CLI\)](#)
- [Deleting a MIMO or Space Diversity Group \(CLI\)](#)

MIMO and Space Diversity Overview (CLI)

Line-of-Sight (LoS) Multiple Input Multiple Output (MIMO) achieves spatial multiplexing by creating an artificial phase de-correlation by deliberate antenna distance at each site in deterministic constant distance. At each site in a LoS MIMO configuration, data to be transmitted over the radio link is split into two bit streams (MIMO 2x2) or four bit streams (MIMO 4x4). These bit streams are transmitted via two antennas. In MIMO 2x2, the antennas use a single polarization. In MIMO 4x4, each antenna uses dual polarization. The phase difference caused by the antenna separation enables the receiver to distinguish between the streams.

PTP 820C supports both MIMO 2x2 and MIMO 4x4. For a full explanation of MIMO support in PTP 820C, refer to the PTP 820C Technical Description.

The same hardware configurations can also be used to implement BBS Space Diversity. PTP 820C supports 1+0, 2+0 and 2+2 Space Diversity.

**Note**

Only one MIMO or Space Diversity group can be created per PTP 820C unit.

For 4x4 MIMO using an external switch operating in LAG mode, Mate Management Access enables users to manage both units via in-band management. See [Mate Management Access \(IP Forwarding\) \(CLI\)](#).

2+2 Space Diversity (CLI)

2+2 HSB Space Diversity provides both equipment protection and signal protection. If one unit goes out of service, the other unit takes over and maintains the link until the other unit is restored to service and Space Diversity operation resumes.

2+2 HSB Space Diversity utilizes two PTP 820C units operating in dual core mode. In each PTP 820C unit, both radio carriers are connected to a single antenna. One optical GbE port on each PTP 820C is connected to an optical splitter. Traffic must be routed to an optical GbE port on each PTP 820C unit.

In effect, a 2+2 HSB configuration is a protected 2+0 Space Diversity configuration. Each PTP 820C monitors both of its cores. If the active PTP 820C detects a radio failure in either of its cores, it initiates a switchover to the standby PTP 820C.

Configuring a MIMO Link (CLI)

To configure a MIMO link, you must perform the following steps:

1. If you are configuring a 4x4 MIMO link, verify that the following three cables are connected between the Master and Slave PTP 820C units on each side of the link. For details, refer to the PTP 820C Installation Guide:
 - Source sharing cable between both EXT REF PTP 820C radio connectors.
 - MIMO data sharing cable between both PTP 820C ETH3/EXT ports.
 - MIMO signaling cable between both PTP 820C MGT/PROT ports.
2. If you are configuring a 4x4 MIMO link, you must initially configure the PTP 820C carriers as XPIC links, using XPIC scripts, and configuring the carriers as XPIC groups. [See Configuring XPIC \(CLI\)](#).
3. Perform antenna alignment for XPIC. [See Performing Antenna alignment for XPIC \(CLI\)](#).
4. Configure MIMO groups on each PTP 820C unit. [See Creating a MIMO or Space Diversity Group \(CLI\)](#).

If you are configuring a 4x4 MIMO link, configure the groups in the following order:

- i Upper unit (Master) on the local side of the link.
 - ii Upper unit (Master) on the remote side of the link.
 - iii Lower unit (Slave) on the local side of the link.
 - iv Lower unit (Slave) on the remote side of the link.
5. After enabling the MIMO groups and setting their roles on the Master units on both sides of the link, reset the MIMO state machine. [See Resetting MIMO \(CLI\)](#).
 6. Verify that the MMI and XPIC levels are appropriate. [See Viewing MMI and XPI levels \(CLI\)](#)
 7. For a 4x4 MIMO link, configure LAG on the two Ethernet ports of the external switches connected to the PTP 820C units on both sides of the link.
 8. For a 4x4 MIMO link, configure Automatic State Propagation with **ASP trigger by remote fault** enabled on the MIMO group in all four PTP 820C units that make up the link. [See Configuring Automatic State Propagation and Link Loss Forwarding \(CLI\)](#)

**Note**

The last two steps are crucial to ensure that the link continues to function via the MIMO resiliency mechanism in the event of a hardware failure scenario. See [Resetting MIMO \(CLI\)](#).

Creating a MIMO or Space Diversity Group (CLI)

**Note**

Only one MIMO or Space Diversity group can be created per PTP 820C unit.

1. To create a MIMO or Space Diversity group, enter the following command:

```
root> radio mimo create group 1 mimo-type <mimo-type> radio 2 port <first
radio carrier in the group: either 1 or 2> radio 2 port <second radio
carrier in the group: either 2 or 1 >
```

where **<mimo-type>** defines the MIMO or Space Diversity configuration. The options are:

- **mimo-2x2** – 2x2 MIMO.
- **mimo-4x4** – 4x4 MIMO.
- **1-plus-0-sd** – 1+0 Space Diversity.
- **2-plus-0-sd** – 2+0 Space Diversity.

**Note**

To enable 2+2 Space Diversity, specify **2-plus-0-sd** after setting up the hardware configuration for 2+2 Space Diversity. See [2+2 Space Diversity \(CLI\)](#).

2. After creating the group, you must enable the group. See [Enabling/Disabling a MIMO or Space Diversity Group \(CLI\)](#).
3. For 4x4 MIMO configurations, and 2+2 Space Diversity configurations, you must set the role of the group to **Master** or **Slave**. See [Setting the Role of a MIMO or Space Diversity Group \(CLI\)](#).

Enabling/Disabling a MIMO or Space Diversity Group (CLI)

To set the admin state of a MIMO or Space Diversity group, enter the following command in root view:

```
root> radio mimo set-admin group <group_id> admin <enable | disable>
```

Setting the Role of a MIMO or Space Diversity Group (CLI)

For 4x4 MIMO configurations and 2+2 Space Diversity configurations, you must set the role of the group to Master or Slave. This determines the role of the PTP 820C unit in the overall MIMO or Space Diversity configuration.

To set the role of a MIMO or Space Diversity group, enter the following command in root view:

```
root> radio mimo set-role group 1 mimo-role <slave|master>
```

Resetting MIMO (CLI)

In hardware failure scenarios, MIMO 4x4 provides a resiliency mechanism that enables the link to continue functioning as a 2+0 XPIC link.

To restore full MIMO operation, the faulty equipment must be replaced. The replacement equipment must be pre-configured to the same configuration as the equipment being replaced. Once the new equipment has been properly installed and, if necessary, powered up, you must reset MIMO.



Note

MIMO reset causes a traffic interruption. It is recommended to reset MIMO on the remote side of the link first, then on the local side.

To reset MIMO, enter the following command in root view:

```
root> radio mimo reset group 1
```

Viewing MMI and XPI Levels (CLI)

You can view MMI and XPI levels for the individual radio carriers in a MIMO group.

Note that the MMI value can also be calculated manually. To calculate it manually, you must measure the following RSL levels per receiver:

1. Mute all remote transmitters except the transmitter for the link you want to measure, and measure the local RSL level (RSL_Wanted).
2. Mute all remote transmitters except the same polarization interferer and measure the local RSL2 (RSL_Int).
3. The MMI is equal to $RSL_Wanted - RSL_Int$.

To show the status of a MIMO group, as well as the MMI and XPI levels for the individual radio carriers, enter the following command:

```
root> radio mimo show status group 1
```

The following is a sample output from this command:

```
root> radio mimo show status group 1

MIMO group type:          mimo-4x4.
MIMO group 1st member:    slot 2 port 1.
MIMO group 2nd member:    slot 2 port 2.
MIMO group admin status:  disable.
MIMO state:               MIMO-Disabled.
MIMO advanced state:      disabled.
MIMO RFU role:            slave.
MIMO 1st carrier MMI:     -0.0
MIMO 2nd carrier MMI:     -0.0
MIMO 1st carrier XPI:     99.0
MIMO 2nd carrier XPI:     99.0
```

Table 84 MMI and XPI Levels CLI Parameters

Parameter	Input Type
MIMO group type	The MIMO or Space Diversity configuration: mimo-2x2 – 2x2 MIMO. mimo-4x4 – 4x4 MIMO. 1-plus-0-sd – 1+0 BBS Space Diversity. 2-plus-0-sd – 2+0 XPIC with BBS Space Diversity.
MIMO group 1st member	The first radio carrier in the group.
MIMO group 2nd member	The second radio carrier in the group.
MIMO group admin status	Indicates whether the MIMO group is enabled or disabled.
MIMO state	Indicates whether MIMO is enabled or disabled.
MIMO advanced state	A detailed description of the MIMO state.
MIMO RFU role	Indicates the role of the unit in the MIMO configuration (Master or Slave).
MIMO 1st carrier MMI	MIMO Mate Interference for the first group member. MMI represents the difference between the RSL1 and the RSL2 of the remote Master and Slave transmitters with the same polarization. The nominal range is 0. The range should be from -3 dB to +3 dB. MMI is not relevant for 1+0 Space Diversity.
MIMO 2nd carrier MMI	MMI for the second group member.
MIMO 1st carrier XPI	Cross Polarization Interference for the first group member. This is only relevant in 4x4 MIMO configurations, where each unit operates in dual polarization (XPIC) mode. The XPI value should be at least 25 dB. For further information, refer to Configuring XPIC (CLI) .
MIMO 2nd carrier XPI	XPI for the second group member.

Deleting a MIMO or Space Diversity Group (CLI)

You can delete a MIMO or Space Diversity Group.

To delete a MIMO or Space Diversity Group:

1. Before deleting a MIMO or Space Diversity group, you must first disable the group using the following command in root view:

```
root> radio mimo set-admin group 1 admin disable
```

**Note**

When the MIMO or Space Diversity group is disabled, the system is automatically reset.

2. Delete the MIMO or Space Diversity group by entering the following command in root view:

```
root> radio mimo delete group 1
```

Configuring Advanced Frequency Reuse (AFR) (CLI)

For a general description of AFR, see AFR Overview.

Initial Link Configuration and Alignment for AFR (CLI)

Before performing the software configuration for AFR, you must set up and align the two links as individual 1+0 links. For instructions, see [Initial Link Configuration and Alignment for AFR](#).

Software Configuration for AFR (CLI)



Note

AFR is not supported with ATPC. ATPC should be disabled before configuring AFR. See [Configuring ATPC and ATPC Override Timer \(CLI\)](#).

Perform the following steps for each site in the AFR configuration.

- If you are performing the configuration locally at the Hub site and each Tail site, the order in which you configure the sites does not matter.
- If you are performing the configuration for all three sites remotely from the Hub Site, you must configure the sites in the following order:
 - Tail Site 1
 - Tail Site 2
 - Hub Site

After you configure AFR on the Tails Sites, the link between the Hub Site and the Tail Sites will be lost. The links will be restored after you configure AFR on the Hub site and the Hub site comes back up after unit reset.

1. Create an AFR group by entering one of the following commands in root view:

If you are configuring the Hub site, enter the following command:

```
root> amcc create group group_id 1 group_type afr-agg group_sub_type internal
```

If you are configuring a Tail site, enter the following command:

```
root> amcc create group group_id 1 group_type afr-tail group_sub_type internal
```

2. Enter AMCC Group view by entering the following command in root view:

```
root> amcc group group_id 1  
group [1]>
```

3. Assign a role to each radio interface, as follows:

If you are configuring the Hub site, enter the following command in group view for each radio interface:

```
group [1]> amcc attach slot 2 port <1|2> role <agg-1|agg-2>
```

If you are configuring a Tail site, enter the following command in group view:

```
group [1]> amcc attach slot 2 port <1|2> role <tail-1|tail-2>
```

Make sure the interface you configure as agg-1 is part of the link with tail-1 and that the interface you configure as agg-2 is part of the link with tail-2.

4. Enter the following command to enable the group. When you execute the command, the unit is automatically reset.

```
group [1]> amcc set enable
```

Once AFR has been configured on the Hub site and both Tail sites, the configuration is complete.

To display the current AFR configuration, enter the following command in root view:

```
root> amcc show
```

The following sequence of commands enables AFR at the Hub site, in a configuration where radio interface 1 is Aggregator 1, connected to Tail Site 1, and radio interface 2 is Aggregator 2, connected to Tail Site 2:

```
root> amcc create group group_id 1 group_type afr-agg group_sub_type
internal
root> amcc group group_id 1
group[1]> amcc attach slot 2 port 1 role agg-1
group [1]> amcc set enable
```

The following sequence of commands enables AFR at Tail Site 1:

```
root> amcc create group group_id 1 group_type afr-tail group_sub_type
internal
root> amcc group group_id 1
group[1]> amcc attach slot 2 port 1 role tail-1
group [1]> amcc set enable
```

The following sequence of commands enables AFR at Tail Site 2:

```
root> amcc create group group_id 1 group_type afr-tail group_sub_type
internal
root> amcc group group_id 1
group[1]> amcc attach slot 2 port 1 role tail-2
group [1]> amcc set enable
```

Deleting an AFR Group (CLI)

If you want to disable AFR and convert the two links into non-AFR links, you must perform the following steps for each site in the AFR configuration. If you are managing the links by in-band management from the hub site, you must disable AFR at the tail sites first, then disable AFR at the hub site. Once AFR has been disabled at all of the sites, you can delete the AFR groups in any order.

1. Enter AMCC Group view by entering the following command in root view:

```
root> amcc group group_id 1
group [1]>
```

2. Enter the following command to disable the group. When you execute the command, the unit is automatically reset.

```
group [1]> amcc set disable
```

3. Detach the radio interface from the group. If you are disabling AFR at the Hub site, detach both interfaces. To detach an interface from the group, enter the following command in root view for each interface:

```
group [1]> amcc detach slot 2 port <port>
```

4. Exit group view and enter the following command in root view to delete the group:

```
root> amcc delete group group_id 1
```

Once you have performed this procedure for the Hub site and both Tail sites, you can reconfigure the links according to the new network plan.

The following sequence of commands disables AFR at the Hub site:

```
root> amcc group group_id 1
group[1]> amcc set disable
group[1]> amcc detach slot 2 port 1
slot 2 port 1 detached from group_id 1
group[1]> amcc detach slot 2 port 2
slot 2 port 2 detached from group_id 1
group[1]> exit
root> amcc delete group group_id 1
group_id 1 deleted
```


Operating a PTP 820C in Single Radio Carrier Mode (CLI)

If you wish to operate a PTP 820C unit in single radio carrier mode, you must perform the following steps:

1. Verify that XPIC is disabled. See [Configuring XPIC \(CLI\)](#)
2. Disable Multi-Carrier ABC, as described in [Deleting a Multi-Carrier ABC Group \(CLI\)](#)
3. Disable one of the two radio interfaces, as described in [Enabling the Interfaces \(CLI\)](#)
4. Mute the disabled radio interface, as described in [Muting and Unmuting a Radio \(CLI\)](#)

Chapter 15: 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 \(CLI\)](#)

Related topics:

- [Setting the Time and Date \(Optional\) \(CLI\)](#)
- [Uploading Unit Info \(CLI\)](#)
- [Changing the Management IP Address \(CLI\)](#)

Defining the IP Protocol Version for Initiating Communications (CLI)

You can specify which IP protocol the unit will use when initiating communications, such as downloading software, sending traps, pinging, or exporting configurations. The options are IPv4 or IPv6.

To define which IP protocol the unit will use when initiating communications, enter the following command in root view:

```
root> platform management ip set ip-address-family <ipv4|ipv6>
```

To show the IP protocol version the unit will use when initiating communications, enter the following command in root view:

```
root> platform management ip show ip-address-family
```

Configuring the Remote Unit's IP Address (CLI)

You can configure the remote unit's IP address, subnet mask and default gateway in IPv4 format and/or in IPv6 format. The remote unit will receive communications whether they were sent to its IPv4 address or its IPv6 address.

Configuring the Remote Radio's IP Address in IPv4 format (CLI)

To set the remote radio's IP Address, enter the following command in radio view:

```
radio[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 85 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.

Examples

The following command sets the default gateway of the remote radio as 192.168.1.20:

```
radio[2/1]>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[2/2]>remote-unit set ip-address 192.168.1.1
radio[2/2]>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 86 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.

Examples

The following command sets the default gateway of the remote radio as FE80:0000:0000:0000:0202:B3FF:FE1E:8329 :

```
radio[2/1]>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[2/2]>remote-unit set ip-address-ipv6  
FE80:0000:0000:0000:0202:B3FF:FE1E:8329  
radio[2/2]>remote-unit set prefix-length 64
```

Configuring SNMP (CLI)

PTP 820 supports SNMP v1, V2c, and v3. You can set community strings for access to PTP 820 units.

PTP 820 supports the following MIBs:

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

Access to the unit is provided by making use of the community and context fields in SNMPv1 and SNMPv2c/SNMPv3, respectively.

This section includes:

- [Configuring Basic SNMP Settings \(CLI\)](#)
- [Configuring SNMPv3 \(CLI\)](#)
- [Displaying the SNMP Settings \(CLI\)](#)
- [Configuring Trap Managers \(CLI\)](#)

Configuring Basic SNMP Settings (CLI)

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 87 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.

Parameter	Input Type	Permitted Values	Description
write-community	Text String	Any valid SNMP write community.	The community string for the SNMP write community.

Example

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 88 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.

Parameter	Input Type	Permitted Values	Description
v3-user-password	Text String	Must be at least eight characters.	An SNMPv3 user password.
v3-security-mode	Variable	authNoPriv authPriv noAuthNoPriv	Defines the security mode to be used for this user.
v3-encryption-mode	Variable	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.

Example

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 manager, 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 manager 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 89 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.

Parameter	Input Type	Permitted Values	Description
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.
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.

Examples

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 820 ports are used for FTP and SFTP when the PTP 820 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 820 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 820 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 820 that are currently running an older version.
3. **Reset** – The PTP 820 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 820 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 820 functions as the server, and you can download the software directly to the PTP 820 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 90 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.

Parameter	Input Type	Permitted Values	Description
server-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The IPv6 address of the PC or laptop you are using as the FTP server.
directory	Text String.		The directory path from which you are downloading the files. Enter the path relative to the FTP user's home directory, not the absolute path. 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
```

Important Note – If upgrading from version 7.9 or earlier:

- Before you proceed to install the software, repeat the download process even if the `platform software download status show` command produced a `download success` message, until the unit displays the message `all components exist`.
- In case of failure, wait at least 30 minutes and repeat the software download.

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 820 configuration files. This enables you to copy the system configuration to multiple PTP 820 units. You can also backup and save configuration files.

Configuration files can only be copied between units of the same type, i.e., PTP 820C to PTP 820C and PTP 820S to PTP 820S.

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 820 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 91 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.

Examples

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 92 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.

Examples

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 93 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.

Examples

The following commands import a configuration file from an external PC or laptop to Restore Point 2 on the PTP 820, and restore the file to be the system configuration file for the PTP 820:

```
root> platform configuration configuration-file import restore-point-2
root> platform configuration configuration-file restore restore-point-2
```

Editing CLI Scripts (CLI)

The configuration file package includes a text file that enables you to write CLI scripts in a backed-up configuration that are executed after restoring the configuration.

To edit a CLI script:

1. Back up the current configuration to one of the restore points. See [Backing up and Exporting a Configuration File \(CLI\)](#).
2. Export the configuration from the restore point to a PC or laptop. See [Backing up and Exporting a Configuration File \(CLI\)](#).
3. On the PC or laptop, unzip the file *Configuration_files.zip*.
4. Edit the *cli_script.txt* file using clish commands, one per line.
5. Save and close the *cli_script.txt* file, and add it back into the *Configuration_files.zip* file.
6. Import the updated *Configuration_files.zip* file back into the unit. See [Importing and Restoring a Configuration File \(CLI\)](#).
7. Restore the imported configuration file. See [Importing and Restoring a Configuration File \(CLI\)](#). The unit is automatically reset. During initialization, the CLI script is executed, line by line.



Note

If any specific command in the CLI script requires reset, the unit is reset when that command is executed. During initialization following the reset, execution of the CLI script continues from the following command.

Setting the Unit to the Factory Default Configuration (CLI)

To restore the unit to its factory default configuration, while retaining the unit's IP address settings and logs, enter the following commands in root view:

```
root> platform management set-to-default
```

The following prompt appears:

```
WARNING: All database and configuration will be lost, unit will be  
restart.  
Are you sure? (yes/no):yes
```

At the prompt, type **yes**.

**Note**

This does not change the unit's IP address or FIPS configuration.

Performing a 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.

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 94 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.

Examples

The following commands configure a name, location, contact person, latitude coordinates, longitude coordinates, and units of measurements for the PTP 820:

```
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 820 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.

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 95 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.

Example

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 820
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>
```

Chapter 16: Radio Configuration (CLI)

This section includes:

- [Viewing and Configuring the Remote Radio Parameters \(CLI\)](#)
- [Configuring ATPC and ATPC Override Timer \(CLI\)](#)
- [Configuring Header De-Duplication \(CLI\)](#)
- [Configuring Frame Cut-Through \(CLI\)](#)
- [Configuring AES-256 Payload Encryption \(CLI\)](#)
- [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 Multi-Carrier ABC \(CLI\)](#)
- [Configuring Link Aggregation \(LAG\) and LACP \(Optional\) \(CLI\)](#)
- [Configuring XPIC \(CLI\)](#)
- [Configuring Unit Protection with HSB Radio Protection \(External Protection\) \(CLI\)](#)
- [Configuring MIMO and Space Diversity \(CLI\)](#)
- [Operating a PTP 820C in Single Radio Carrier Mode \(CLI\)](#)



Note

For convenience, this User Guide generally shows the radio prompt as `radio[2/1]>`.

To view and configure radio parameters, you must first enter the radio's view level in the CLI. For details, refer to [Entering Radio View \(CLI\)](#)

Viewing and Configuring the Remote Radio Parameters (CLI)

This section includes:

- [Displaying Communication Status with the Remote Radio \(CLI\)](#)
- [Displaying the Remote Radio's Link ID \(CLI\)](#)
- [Muting and Unmuting the Remote Radio \(CLI\)](#)
- [Displaying the Remote Radio's RX Level \(CLI\)](#)
- [Configuring the Remote Radio's TX Level \(CLI\)](#)
- [Configuring Remote ATPC \(CLI\)](#)

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 the Remote Radio's Link ID (CLI)

To display the remote radio's Link ID, enter the following command:

```
radio[x/x]>remote-unit show link-id
```

Muting and Unmuting the Remote Radio (CLI)

To mute or unmute the remote radio, enter the following command:

```
radio[x/x]>remote-unit mute set admin <admin>
```

To display the mute status of the remote radio, enter the following command:

```
radio[x/x]>remote-unit mute show status
```

Table 96 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:

```
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:

```
radio[x/x]>remote-unit set tx-level <tx-level>
```

To display the transmit (TX) level of the remote radio, enter the following command:

```
radio[x/x]>remote-unit show tx-level
```

Table 97 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:

```
radio[x/x]>remote-unit atpc set ref-level <ref-level>
```

To display the RX reference level for ATPC on the remote radio, enter the following command:

```
radio[x/x]>remote-unit atpc show ref-level
```

Table 98 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
```


Configuring ATPC and ATPC Override Timer (CLI)

ATPC is a closed-loop mechanism by which each carrier changes the TX power according to the indication received across the link, in order to achieve a desired RSL on the other side of the link. With ATPC, if the radio increases its TX power up to the configured TX power, it can lead to a period of sustained transmission at maximum power, resulting in unacceptable interference with other systems.

In order to minimize interference, PTP 820 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. You cannot use ATPC in MIMO mode. See [Configuring MIMO and Space Diversity \(CLI\)](#).

To enable or disable ATPC, enter the following command:

```
radio[x/x]>atpc set admin <admin>
```

To display whether or not ATPC is enabled, enter the following command:

```
radio[x/x]>atpc show admin
```

To set the RX reference level for ATPC, enter the following command

```
radio[x/x]>atpc set rx-level atpc_ref_rx_level <rx-level>
```

To display the RX reference level for ATPC, enter the following command:

```
radio[x/x]>atpc show rx-level
```

To set an ATPC override timer, enter the following command in radio view:

```
radio[x/x]>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/x]>atpc override set admin <override admin>
```

To display whether or not ATPC override is enabled, enter the following command in radio view:

```
radio[x/x]>atpc override show admin
```

To display the ATPC override timeout, enter the following command in radio view:

```
radio[x/x]>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/x]>atpc set override-tx-level <override-tx-level>
```

To display the ATPC override TX power, enter the following command in radio view:

```
radio[x/x]>atpc show override tx-level
```

To display the current ATPC override state, enter the following command in radio view:

```
radio[x/x]>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 99 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 RX reference level for the ATPC mechanism.
timeout	Number	0-1800	The amount of time, in seconds, the timer counts from the moment the radio reaches its maximum configured TX power until ATPC override goes into effect.
override admin	Variable	Enable disable	Enables or disables ATPC override.

Parameter	Input Type	Permitted Values	Description
override-tx-level	Number	-50 - 50	The TX power, in dBm, to be used when the unit is in an ATPC override state. The range of values depends on the frequency, MRMC script, and radio type.

The following commands enable ATPC mode and ATPC override for radio carrier 1, 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)

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:

```
radio[2/1]> compression header-compression set <mode>
```

**Note**

In this release, if two radio carriers in a PTP 820C unit are activated, the Header De-Duplication configuration for radio carrier 1 are applied to both carriers. You must enter radio view for radio interface 1.

To clear Ethernet port counters, including both Frame Cut-Through and Header De-Duplication counters, enter the following command:

```
radio[x/x]>clear-ethernet-port-counters
```

Table 100 Header De-Duplication CLI Parameters

Parameter	Input Type	Permitted Values	Description
mode	Variable	Disabled	Disabled - Header De-Duplication is disabled.
		Layer2	Layer2 - Header De-Duplication operates on the Ethernet level.
		MPLS	MPLS - Header De-Duplication operates on the Ethernet and MPLS levels.
		Layer3	Layer3 - Header De-Duplication operates on the Ethernet and IP levels.
		Layer4	Layer4 - Header De-Duplication operates on all supported layers up to Layer 4.
		Tunnel	Tunnel - Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel layer for packets carrying GTP or GRE frames.
		Tunnel-Layer3	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	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 radio carrier 1:

```
root> radio slot 2 port 1
radio[2/1]> compression header-compression set mode Layer2
radio[2/1]> compression header-compression set flow-type 0x00
```

Displaying Header De-Duplication Information (CLI)

To display the current Header De-Duplication configuration, enter the following command:

```
radio[2/1]> compression show-configuration
```

To display counters for Header De-Duplication, enter the following command:

```
radio[2/1]> 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)

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**

The 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.

To enable Frame Cut-Through, enter the following command in radio view:

```
radio[2/1]> cut-through mode yes
```

To disable Frame Cut-Through, enter the following command in radio view:

```
radio[2/1]> cut-through mode no
```

To display whether Frame Cut-Through is currently enabled or disabled, enter the following command in radio view:

```
radio[2/1]> 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[2/1]> cut-through show-counters
```

Displaying Frame Cut-Through Information (CLI)

To display the current Frame Cut-Through mode for carrier, enter the following command:

```
radio[x/x]>cut-through show-mode
```

To display counters for Frame Cut-Through for a carrier, enter the following command:

```
radio[x/x]>cut-through show-counters
```

The command output displays the number of frames, bytes, good frames, and good bytes that have been transmitted via Frame Cut-Through since the last time the counters were cleared.

The following is a sample output of the command:

```
radio [2/1]>cut-through show-counters  
Total frame count = 0  
Total byte count = 0  
Total good frame count = 0  
Total good byte count = 0  
Radio [2/1]>
```


Configuring AES-256 Payload Encryption (CLI)

**Note**

This feature is only relevant for PTP 820C and PTP 820S units.
This feature is not supported with MIMO or Space Diversity links.

This feature requires:

- Requires an activation key per radio. 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 820C and PTP 820S support AES-256 payload encryption. The purpose of payload encryption is to secure the radio link and provide protection against eavesdropping and/or personification (“man-in-the-middle”) attacks.

AES is enabled and configured separately for each radio carrier.

PTP 820 uses a dual-key encryption mechanism for AES:

- 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.

AES key generation is completely hitless, and has no effect on ACM operation.

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 on radio interface 1, and disabled on radio interface 2.

```
root> payload encryption status show
```

Traffic Crypto configuration table:

Interface slot	Interface port	Admin mode	Master Key	Session Key Period
2	1	AES-256	5QV_{Fm`v1iKgaQhnP#09As6&QA.#dH^	00:00
2	2	Disable		00:00

Interface slot	Interface port	Crypto Validation State
2	1	not-valid
2	2	not-valid

```
root> _
```

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 In a protected link, enable protection lockout, first on the remote and then on the local unit. See [Disabling Automatic Switchover to the Standby Unit \(CLI\)](#).
- 4 To configure AES on a radio carrier, you must first enter traffic encryption view for the specific radio. To enter Payload Encryption view, enter the following command in root view:

```
root> payload encryption slot 2 port <port>
```

For example, to configure AES on radio interface 1, enter the following command in root view:

```
root> payload encryption slot 2 port 1
```

Payload Encryption [1/1]>To display the payload encryption mode of the radio interface, enter the following command in PayloadEncryption view:

```
PayloadEncryption [2/x]> payload encryption mode show
```

The following display indicates that payload encryption is enabled on radio interface 1:

```
PayloadEncryption [2/1]> payload encryption mode show
```

```
Admin Mode: AES-256
```

The following display indicates that payload encryption is disabled on radio interface 1:

```
PayloadEncryption [2/1]> payload encryption mode show
```

```
Admin Mode: Disable
```

- 5 Configure the master key by doing one of the following:
 - o Enter a master key manually.
 - o 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 PayloadEncryption view:

```
PayloadEncryption [2/x]> 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 PayloadEncryption view:

```
PayloadEncryption [2/x]> 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.

- 6 On the local unit, follow the procedure described in Step 5 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 Enter the following command in Payload Encryption view:

```
Payload Encryption [2/x]> 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 [2/x]> 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  
<00:00-00:00>
```

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 [2/1]> 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 [2/x]> payload encryption session-key period show
```



Note

The session key regeneration interval must be the same on both sides of the link.

- 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 In a protected link, perform copy-to-mate, first on the remote and then on the local unit. See Step 3 in [Configuring HSB Radio Protection \(CLI\)](#). After the copy-to-mate operation, wait for both standby units to re-boot and verify that there are no alarms.



Note

The standby unit may have a *payload encryption failure* alarm for up to about one minute after the unit is up and running.

- 4 In a protected link, remove the protection lockout, first on the remote and then on the local unit. See [Disabling Automatic Switchover to the Standby Unit \(CLI\)](#).
- 5 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
```



Warning

Executing this command on a FIPS-enabled unit formats the unit's disk, and renders the unit non-operational. If it is necessary to use this command, contact Cambium Networks Technical Support for instructions how to re-configure the unit.

This command has no effect on units that are not enabled for FIPS



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 \(CLI\)](#)
- [Displaying ACM PMs \(CLI\)](#)

Displaying General Modem Status and Defective Block PMs (CLI)

To display the general status of the modem, enter the following command:

```
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:

```
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:

```
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 101 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 102 Excessive BER CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin	Variable	enable disable	Enables or disables propagation of excessive BER as a fault.

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 103 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 104 TSL Thresholds CLI Parameters

Parameter	Input Type	Permitted Values	Description
threshold1	Number	-75 - -15	The first RSL threshold (dBm).
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 [2/1]>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         -90           -33            15            15            0           18           18
1          0         -90           -33            15            15            0           39           39
2          0         -90           -33            15            15            0            8            8
3          0         -90           -33            15            15            0           15           15
4          0         -90           -33            15            15            0            7            7
5          0         -90           -33            15            15            0           15           15
6          0         -90           -33            15            15            0           49           49
7          0         -90           -33            15            15            0           28           28
8          0         -90           -33            15            15            0           31           30
9          0         -90           -33            15            15            0           40           40
10         0         -90           -33            15            15            0           41           41
11         0         -90           -33            15            15            0          165          165
12         0         -90           -33            15            15            0           14           14
13         0         -90           -33            15            15            0           71           71
14         0         -90           -33            15            15            0            4            4
15         0         -36           -36            15            15            0            0            0
16         0         -90           -33            15            15            0           65           65
17         0         -90           -33            15            15            0          461          461
18         0         -90           -33            15            15            0          391          391
19         0         -90           -33            15            15            0          509          509
20         0         -90           -33            15            15            0          168          168
```

Table 105 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 106 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 107 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 108 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)

To configure the modem XPI threshold for calculating XPI Exceed Threshold seconds, enter the following command:

```
radio[x/x]>modem set threshold-xpi-exceed threshold <threshold>
```

To display the currently configured XPI threshold, enter the following command:

```
radio[x/x]>modem show threshold-xpi-below
```

Table 109 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:

```
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 [2/1]>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 [2/1]>
```

To display XPI PMs in daily intervals, enter the following command:

```
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 [2/1]>modem pm-xpi show interval 24hr

Modem XPI PM Table:
=====

Interval    Integrity    Min XPI (dB)    Max XPI (dB)    XPI below
                                     threshold
                                     seconds
=====
1            1            55.00           0.00            0
2            1            55.00           0.00            0
3            1            55.00           0.00            0
4            1            55.00           0.00            0
5            1            55.00           0.00            0
6            1            55.00           0.00            0
7            1            55.00           0.00            0
8            1            55.00           0.00            0
9            1            55.00           0.00            0
10           1            55.00           0.00            0
11           1            55.00           0.00            0
12           1            55.00           0.00            0
13           1            55.00           0.00            0
14           1            55.00           0.00            0
15           1            55.00           0.00            0
16           1            55.00           0.00            0
17           1            55.00           0.00            0
18           1            55.00           0.00            0
19           1            55.00           0.00            0
20           1            55.00           0.00            0

radio [2/1]>

```

Table 110 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 for radio carrier 2 to 15:

```
radio[2/1]>modem set threshold-xpi-below threshold 15
```

Displaying ACM PMs (CLI)

To display ACM PMs in 15-minute intervals, enter the following command:

```
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 [2/1]>mrmc pm-acm show interval 15min
```

MPMC PM Table:

```
=====
```

Interval	Integrity	Min profile	Max profile	Min bitrate	Max bitrate
0	1	0	0	43389	43389
1	1	0	0	43389	43389
2	1	0	0	43389	43389
3	1	0	0	43389	43389
4	1	0	0	43389	43389
5	1	0	0	43389	43389
6	1	0	0	43389	43389
7	1	0	0	43389	43389
8	1	0	0	43389	43389
9	1	0	0	43389	43389
10	1	0	0	43389	43389

```
radio [2/1]>
```

To display ACM PMs in daily intervals, enter the following command:

```
radio [x/x]>mrmc pm-acm show interval 24hr
```

The following is sample output of the `modem pm-acm show interval 24hr` command:

```
radio [2/1]>mrmc pm-acm show interval 24hr
```

MPMC PM Table:

```
=====
```


Interval	Integrity	Min profile	Max profile	Min bitrate	Max bitrate
0	1	0	0	43389	43389
4	1	0	0	43389	43389
5	1	0	0	43389	43389
6	1	0	0	43389	43389
8	1	0	0	43389	43389
11	1	0	0	43389	43389
15	1	0	0	43389	43389
17	1	0	0	43389	43389

radio [2/1]>

Table 111 ACM 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 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 17: 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 \(Optional\) \(CLI\)](#)
- [Quality of Service \(QoS\) \(CLI\)](#)
- [Ethernet Protocols \(CLI\)](#)
- [Performing Ethernet Loopback \(CLI\)](#)

Configuring Ethernet Services (CLI)

This section includes:

- [Ethernet Services Overview \(CLI\)](#)
- [General Guidelines for Provisioning Ethernet Services \(CLI\)](#)
- [Defining Services \(CLI\)](#)
- [Configuring Service Points \(CLI\)](#)
- [Defining the MAC Address Forwarding Table for a Service \(CLI\)](#)

Ethernet Services Overview (CLI)

Users can define up to 64 Ethernet services. Each service constitutes a virtual bridge that defines the connectivity between logical ports in the PTP 820 network element.

This version of PTP 820 supports the following service types:

- Multipoint (MP)
- Point-to-Point (P2P)
- Management (MNG)

In addition to user-defined services, PTP 820 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 \(IP Forwarding\) \(CLI\)](#)

Mate Management Access enables the use of in-band management for nodes that use two PTP 820C units (4x4 MIMO, 2+2 XPIC, and 4+0 Multi-Carrier ABC), where traffic comes from an external switch operating in LAG mode. When Mate Management Access is enabled, the two units exchange incoming management packets, ensuring that all management data is received by both units.



Note

Mate Management Access can be used regardless of whether the unit's IP address is in IPv4 or IPv6 format.

Mate Management Access should only be enabled for nodes receiving traffic from a LAG, where in-band management is to be used. If either of these conditions is not present, Mate Management Access should be disabled. By default, the feature is disabled.

The following are the requirements for using Mate Management Access:

- The management ports of both PTP 820C units must be connected by a protection cable (PTP 820_MIMO_Prot_mng_cbl_1m).

- To ensure proper convergence after failure events, Automatic State Propagation must be enabled on both units at the local node and both units at the remote node. See [Configuring Automatic State Propagation \(CLI\)](#).
- Mate Management Access must be enabled on both units at the local node and both units at the remote node. On each unit, Mate Management Access must be enabled before configuring in-band management.

To enable Mate Management Access, enter the following command:

```
root> platform management mate-access admin enable
```

Note: When you enable or disable Mate Management Access, the unit is reset.

To disable Mate Management Access, enter the following command:

```
root> platform management mate-access admin disable
```

To display whether Mate Management Access is enabled, enter the following command:

```
root> platform management mate-access show
```

**Note**

Mate Management Access can only be configured via CLI.

Upon recovery from a failure event, management may be lost for up to 40 seconds.

Configuring In-Band Management (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 to 30 service points.

For a more detailed overview of the PTP 820 service-oriented Ethernet switching engine, refer to the Technical Description for the PTP 820 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 820 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 112 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	Any unused value from 1-256	A unique ID for the service. Once you have added the service, you cannot change the Service ID. Service ID 257 is reserved for a pre-defined management service.
service admin mode	Variable	Operational reserved	The administrative state of the service: operational - The service is functional. reserved - The service is disabled until this parameter is changed to operational. In this mode, the service occupies system resources but is unable to receive and transmit data.
evc-id	Text String	Up to 20 characters.	Defines an Ethernet Virtual Connection (EVC) ID. This parameter does not affect the network element's behavior, but is used by the NMS for topology management.
evc-description	Text String	Up to 64 characters.	A text description of the service. This parameter does not affect the network element's behavior, but is used by the NMS for topology management.

Example

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 113 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.

Example

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 114 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 115 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.

Example

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 116 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.

Examples

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 117 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.

Examples

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 118 Deleting Ethernet Service CLI Parameters

Parameter	Input Type	Permitted Values	Description
sid	Number	Any defined Service ID.	The Service ID.

Examples

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 119](#) summarizes the service point types available per service type.

Table 119 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 120](#) shows which service point types can co-exist on the same interface.

Table 120 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
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 121](#) and [Table 122](#) show which service point – Interface Type combinations can co-exist on the same interface.

Table 121 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 122 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 123 Add Service Point CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-type	Variable	sap	SAP - Service Access Point
		snp	SNP - Service Network Point
		pipe	PIPE - Pipe service point
		mng	MNG - Management service point
int-type	Variable	all-to-one	<p>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.</p> <p>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.</p> <p>dot1q - A single C-VLAN is classified to the service point. Valid for all service point types.</p> <p>s-tag - A single S- VLAN is classified to the service point. Valid for SNP and MNG service point types.</p> <p>bundle-c-tag - A set of multiple C-VLANs is classified to the service point. Only valid for SAP service point types.</p> <p>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.</p> <p>qinq - A single S-VLAN and C-VLAN combination is classified to the service point. Valid for SAP and MNG service point types.</p>
		dot1q	
		s-tag	
		bundle-c-tag	
		bundle-s-tag	
		qinq	
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 820C units.
slot	Number	Ethernet: 1 Radio: 2	
port	Number	For an Ethernet interface: 1-3 For a radio interface in PTP 820C units: 1-2 For a radio interface in PTP 820S: 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	<p>Defines the VLAN classified to the service point.</p> <p>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).</p> <p>This parameter is also not relevant for:</p> <p>Service points with an interface type of qinq and all-to-one.</p> <p>Pipe service points.</p>
outer-vlan	Number	1-4094 (except 4092, which is reserved for the default management service), or Untagged	<p>Defines the S-VLAN classified to the service point.</p> <p>This parameter is only relevant for service points with the interface type bundle-s-tag or qinq.</p>
inner-vlan	Number	1-4094 (except 4092, which is reserved for the default management service), or Untagged	<p>Defines the C-VLAN classified to the service point.</p> <p>This parameter is only relevant for service points with the interface type qinq.</p>
sp-name	Text string	Up to 20 characters.	A descriptive name for the service point (optional).

Examples

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 820C 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 820C 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 124 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.

Examples

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 125 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.

Examples

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 126 Service Point Enable/Disable Flooding CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
state	Variable	Allow disable	Determines whether incoming frames with unknown MAC addresses are forwarded to other service points via flooding.

Examples

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 \(CLI\)](#)

Appendix A: 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 127 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)).

Examples

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
```

Appendix B: 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 128 C-VLAN Preservation CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
c-vlan preservation mode	Variable	enable disable	Determines whether the original C-VLAN ID is preserved or restored for frames egressing from the service point. enable - The C-VLAN ID of frames egressing the service point is the same as the C-VLAN ID when the frame entered the service. disable - The C-VLAN ID of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking (see Configuring Marking (CLI)).

Examples

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
```

Appendix C: 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 129 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)).

Examples

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 130 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.

Examples

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 131 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.

Examples

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 132 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.

Example

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 133 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.

Example

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 820 performs MAC address learning per service. PTP 820 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 134 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.

Example

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 135 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.

Example

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 136 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.

Examples

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 137 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.

Parameter	Input Type	Permitted Values	Description
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.

Examples

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 820 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 820 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 138 Configure S-VLAN Ethertype CLI Parameters

Parameter	Input Type	Permitted Values	Description
ethertype	Hexadecimal	0x8100	Defines the ethertype recognized by the system as the S-VLAN ethertype.
		0x88a8	
		0x9100	
		0x9200	

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 139 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 \(CLI\)](#)
- [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 \(CLI\)](#)
- [Displaying Interface Statistics \(RMON\) \(CLI\)](#)

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 140 Entering Interface View 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.
slot	Number	Ethernet: 1 Radio in PTP 820C or PTP 820S: 2	Depends on the interface and unit type.

Parameter	Input Type	Permitted Values	Description
port	Number	GbE 1: 1 GbE 2: 2 GbE 3: 3 Radio Carrier 1: 1 Radio Carrier 2 (PTP 820C only): 2	The port number of the interface.
group	Variable	rp1 rp2 rp3 rp4 lag1 lag2 lag3 lag4 mc-abc1 mc-abc2 mc-abc3 mc-abc4	To enter interface view for a group, enter the group ID for one of the following types of group: HSB group (rp1 - rp-4) LAG (lag1 - lag4) Multi-Carrier ABC group (mc-abc1 - mc-abc4) Note: HSB and Multi-Carrier ABC groups are only relevant for PTP 820C.

Example

The following command enters interface view for Ethernet port 3:

```
root> ethernet interfaces eth slot 1 port 3
```

The following prompt appears:

```
eth type eth [1/3]>
```

The following command enters interface view for radio interface 2 in a PTP 820C unit:

```
root> ethernet interfaces radio slot 2 port 2
```

The following prompt appears:

```
radio [2/2]>
```

The following command enters interface view for the radio interface in a PTP 820S unit:

```
root> ethernet interfaces radio slot 2 port 1
```

The following prompt appears:

```
radio [2/1]>
```

The following prompt appears:

```
radio [16/1]>
```

The following command enters interface view for LAG 1:

```
root> ethernet interfaces group lag1
```

The following prompt appears:

```
eth type group [64/1]>
```

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 | slot | port | Type | Description | Admin | Operational | Secondary | Last change | Connector | Speed | MTU | MAC |
| type     |      |      |      |             | status | status      | operational-status |              | Present   |        |     |     |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| ethernet | 1    | 1    | 6    | Ethernet    | up     | down        | 0X1        | 01-01-1970,00:00:01 | false    | 10000000 | 1632 | 0:0:0:0:0:0 |
| ethernet | 1    | 2    | 6    | Ethernet    | up     | down        | 0X1        | 01-01-1970,00:00:01 | false    | 10000000 | 1632 | 0:0:0:0:0:0 |
| radio    | 2    | 1    | 1    | Radio       | up     | down        | 0X82       | 01-01-1970,00:00:01 | false    | 40978000 | 2000 | 0:0:0:0:0:0 |
| radio    | 2    | 2    | 1    | Radio       | up     | down        | 0X82       | 01-01-1970,00:00:01 | false    | 40978000 | 2000 | 0:0:0:0:0:0 |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
root> _
```

Viewing Interface Attributes (CLI)

To display an interface's attributes, go to interface view for the interface and enter the following command:

```
eth type eth [x/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 [x/x]>operational state show
```

Examples

The following command shows the attributes of GbE 1:

```
eth type eth [1/1]>summary show
```

The following command shows the operational state of GbE 1:

```
eth type eth [1/1]>operational state show
```

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.

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 141 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.

Example

The following command sets GbE 1 to RJ-45 (electrical):

```
eth type eth [1/2]>media-type state set rj45
```

The following command sets GbE 2 to SFP:

```
eth type eth [1/2]>media-type state set sfp
```

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 142 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**

10HD is not supported in the current release.

Examples

The following command sets GbE 1 to 100 Mbps, full duplex:


```
eth type eth [1/1]>speed-and-duplex state set '100fd'
```

**Note**

Before performing this command, you must verify that the media-type attribute is set to RJ45.

The following command sets GbE 1 to 1000 Mbps, full duplex:

```
eth type eth [1/1]>speed-and-duplex state set '1000fd'
```

Configuring an Interface's Auto Negotiation State (CLI)

To configure an Ethernet interface's auto-negotiation state, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>autoneg state set <autoneg state>
```

Table 143 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.

Example

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 144 Interface IFG CLI Parameters

Parameter	Input Type	Permitted Values	Description
ifg	Number	6 - 15	Sets the interface's IFG (in bytes).

Example

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 145 Interface Preamble CLI Parameters

Parameter	Input Type	Permitted Values	Description
preamble	Number	6 - 15	Sets the interface’s preamble (in bytes).

Example

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 146 Interface Description CLI Parameters

Parameter	Input Type	Permitted Values	Description
description	Text String	Up to 40 characters	Adds a text description to the interface.

Example

The following command adds the description “Line” to GbE 1:

```
eth type eth [1/1]>description set Line
```

Displaying Interface Statistics (RMON) (CLI)

PTP 820 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:

```
eth type eth [x/x]>rmon statistics show clear-on-read <clear-on-read>
layer-1 <layer-1>
```

Table 147 Interface Statistics (RMON) CLI Parameters

Parameter	Input Type	Permitted Values	Description
clear-on-read	Boolean	yes no	If you enter yes, the statistics are cleared once you display them.
layer-1	Boolean	yes no	yes – Statistics are represented as Layer 1 statistics, including preamble and IFG. no – Statistics are represented as Layer 2 statistics.

Example

The following commands enter interface view for GbE 1, and clear 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 enter interface view for radio carrier 1 in a PTP 820C or PTP 820S unit, and display statistics for the interface, without clearing the statistics.

```
root> ethernet interfaces radio slot 2 port 1
eth type radio[2/1]>rmon statistics show clear-on-read no layer-1 no
```

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
- Remote Radio LOF
- Remote Excessive BER
- Remove 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 <eth-slot>  
eth-port <eth-port> radio-slot <radio-slot> radio-port <radio-port> llf-id  
<llf-id>
```

To configure propagation of a Multi-Carrier ABC group failure to an Ethernet port, use the following command:

```
root> auto-state-propagation add eth-port-to-multi-radio-group eth-slot  
<eth-slot> eth-port <eth-port> multi-radio-group <multi-radio-group> slot  
1 type TCC llf-id <llf-id>
```

To configure propagation of an HSB-SD protection group failure to an Ethernet port, use the following command:

```
root> auto-state-propagation add eth-port-to-protection-group eth-slot  
<eth-slot> eth-port <eth-port> protection-group <protection-group> llf-id  
<llf-id>
```

To enable automatic state propagation on an Ethernet port, determine whether remote interface failures are also propagated, enable CSF mode (optional), and set a trigger delay (optional), use the following command:

```
root> auto-state-propagation configure eth-port eth-slot <eth-slot> 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 <eth-slot> 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 148: Automatic State Propagation to an Ethernet Port CLI Parameters

Parameter	Input Type	Permitted Values	Description
eth-slot	Number	1	Always enter 1.
eth-port	Number	1-3	The interface to which you want to propagate faults from the selected radio or group.
radio-slot	Number	2	
radio-port	Number	Radio Carrier 1: 1 Radio Carrier 2 (PTP 820C): 2	The radio interface.
multi-radio-group	Number	1-4	The Multi-Carrier ABC group failure of which is propagated to the defined interface. Note: Only relevant for PTP 820C units.
protection-group	Number	1-4	The HSB-SD protection group failure of which is propagated to the defined interface. Note: Only relevant for PTP 820C units.

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 <i>can</i> 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 Client Signal Failure (CSF) mode. In CSF 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 (a CSF message). The CSF message is used to propagate the failure indication to external equipment.
trigger-delay	Number	0-10000	Sets a trigger delay time, in milliseconds. When a triggering event takes place, the ASP mechanism does not propagate the event until this delay time has elapsed. By default, the trigger-delay is 0 (no delay time). 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 with radio interface 1 is propagated to any of local Ethernet ports 1 or 2 that share an LLF ID with an Ethernet interface in an ASP pair with the remote radio.
- A failure on the remote side of the link with radio interface 2 is propagated to Ethernet port 3 if it shares an LLF ID with an Ethernet interface in an ASP pair with the remote radio.
- The trigger delay for Ethernet port 1 is 100 ms. The trigger delay for Ethernet port 2 is 5000 ms. There is no trigger delay for Ethernet port 3.

```
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
```

The following commands configure and enable automatic state propagation to propagate faults from Multi-Carrier ABC group 1 to Ethernet port 1. Faults on the remote carrier are also propagated to Ethernet port 1 if the LLF ID of an Ethernet port paired with the remote carrier is 4. CSF mode is disabled and the trigger delay is 300 ms.

```
root> auto-state-propagation add eth-port-to-multi-radio-group eth-slot 1
eth-port 1 multi-radio-group 1 llf-id 4

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 300
```

The following commands configure and enable automatic state propagation to propagate faults from 1+1 HSB protection group 1 to Ethernet port 2. Faults on the remote carrier are not propagated to Ethernet port 2. CSF mode is disabled and there is no trigger delay.

```
root> auto-state-propagation add eth-port-to-protection-group eth-slot 1
eth-port 2 protection-group 1 llf-id 1

root> auto-state-propagation configure eth-port eth-slot 1 eth-port 2
asp-admin enable remote-fault-trigger-admin disable csf-mode-admin
disable
```


Viewing Ethernet PMs and Statistics (CLI)

PTP 820 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 RMON Statistics \(CLI\)](#)
- [Configuring Ethernet Port PMs and PM Thresholds \(CLI\)](#)
- [Displaying Ethernet Port PMs \(CLI\)](#)
- [Clearing Ethernet Port PMs \(CLI\)](#)

Displaying RMON Statistics (CLI)

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 149 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 150 Port PM Thresholds CLI Parameters

Parameter	Input Type	Permitted Values	Description
rx-layer1-rate-threshold	Number	0-4294967295	The exceed threshold for port RX PMs, in bytes per second.
tx-layer1-rate-threshold	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 151 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 18: 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 Egress 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 802.1p Classification \(CLI\)](#)
- [Configuring DSCP Classification \(CLI\)](#)
- [Configuring MPLS Classification \(CLI\)](#)
- [Configuring a Default CoS \(CLI\)](#)
- [Configuring Ingress Path Classification on a Service Point \(CLI\)](#)
- [Configuring Ingress Path Classification on a Service \(CLI\)](#)

Classification Overview (CLI)

PTP 820 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 together, 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
- 802.1p bits.
- DSCP values.
- MPLS EXP field.
- Default CoS

PTP 820 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.

For example, if the frame is an untagged IP Ethernet frame, a match will not be found until the third priority level (DSCP). The CoS and Color values defined for the frame's DSCP value will be applied to the frame.

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.

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 152 VLAN Classification and Override CLI Parameters

Parameter	Input Type	Permitted Values	Description
outer-vlan-id	Number	1 – 4094 (except 4092, which is reserved for the default management service)	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.

Parameter	Input Type	Permitted Values	Description
inner-vlan-id	Number	1 – 4094 (except 4092, which is reserved for the default management service)	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 <code>outer-vlan-id</code> and <code>inner-vlan-id</code> values, respectively, in order for the defined CoS and Color values to be applied to the frame.
use-cos	Number	0 – 7	The CoS value applied to matching frames.
use-color	Variable	green yellow	The Color applied to matching frames.

Examples

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 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 [x/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 [x/x]>classification show 802.1p state
```

Table 153 802.1p 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). VLAN UP bit classification has priority over DSCP and MPLS classification, so that if a match is found with the UP bit of the ingress frame, DSCP values and MPLS bits are not considered. un-trust – The interface does not consider 802.1 UP bits during classification.

Examples

The following command enables 802.1p trust mode for GbE 1:

```
eth type eth [1/1]>classification set 802.1p trust
```

The following command disables 802.1p trust mode for GbE 1:

```
eth type eth [1/1]>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 154 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 155 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.

Examples

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 156 S-VLAN 802.1 UP and DEI 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

802.1 UP	CFI	CoS (configurable)	Color (configurable)
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 157 S-VLAN 802.1 UP and DEI Bit Classification Table CLI Parameters

Parameter	Input Type	Permitted Values	Description
802.1p	Number	0 – 7	The User Priority (UP) bit to be mapped.
dei	Number	0 - 1	The DEI bit to be mapped.
cos	Number	0 – 7	The CoS assigned to frames with the designated UP and CFI.
color	Variable	green yellow	The Color assigned to frames with the designated UP and CFI.

Example

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 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 158 Trust Mode for DSCP CLI Parameters

Parameter	Input Type	Permitted Values	Description
ip-dscp	Variable	trust un-trust	<p>Select the interface's trust mode for DSCP classification:</p> <p>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.</p> <p>un-trust – The interface does not consider DSCP during classification.</p>

Examples

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)

The following table shows the default values for the DSCP classification table.

Table 159 DSCP Classification Table Default Values

DSCP	DSCP (bin)	Description	CoS (Configurable)	Color (Configurable)
0 (default)	000000	BE (CS0)	0	Green
10	001010	AF11	1	Green
12	001100	AF12	1	Yellow
14	001110	AF13	1	Yellow
18	010010	AF21	2	Green
20	010100	AF22	2	Yellow
22	010110	AF23	2	Yellow
26	011010	AF31	3	Green
28	011100	AF32	3	Yellow

DSCP	DSCP (bin)	Description	CoS (Configurable)	Color (Configurable)
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 160 Modify DSCP Classification Table CLI Parameters

Parameter	Input Type	Permitted Values	Description
dscp	Number	Valid DSCP values. Refer to the DSCP column in the table above.	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>
```

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 161 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.

Examples

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 162 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 163 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.

Example

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 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 164 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.

Example

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 \(CLI\)](#)
- [Configuring the Line Compensation Value for a Rate Meter \(Policer\) \(CLI\)](#)
- [Displaying Rate Meter Statistics for an Interface \(CLI\)](#)

Overview of Rate Metering (Policing) (CLI)

The PTP 820 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 820'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 165 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 - 128	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 - 128	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.

Examples

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
- 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
```

Example

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>
```

Example

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 Multicast Traffic \(CLI\)](#)
- [Assigning a Rate Meter \(Policer\) for Broadcast 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 166 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.

Examples

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 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 167 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.

Examples

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 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 168 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.

Examples

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 169 Assigning Rate Meter per Ethertype CLI Parameters

Parameter	Input Type	Permitted Values	Description
ethertype#	Variable	ethertype1 ethertype2 ethertype3	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) .

Examples

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
```

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 170 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.

Example

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)

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 171 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.

Example

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 820'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 172 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	<p>Determines whether re-marking of the outer VLAN (C-VLAN or S-VLAN) of tagged frames that pass through the service point is enabled.</p> <p>If <code>mode</code> is set to <code>enable</code>, and CoS preservation for the relevant outer VLAN is set to <code>disable</code>, 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.</p> <p>If <code>mode</code> is set to <code>enable</code> and CoS preservation for the relevant outer VLAN is also set to <code>enable</code>, re-marking is not performed.</p> <p>If <code>mode</code> is set to <code>disable</code> and CoS preservation for the relevant outer VLAN is also set to <code>disable</code>, re-marking is applied, but only according to the values defined for Green frames in the 802.1Q and 802.1AD marking tables.</p> <p>For information about configuring CoS Preservation, refer to <i>CoS Preservation and Modification on a Service Point (CLI)</i>.</p>

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 173 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 174 802.1q 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 175 802.1ad 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

CoS	Color	802.1ad UP (Configurable)	DEI Color (Configurable)
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 176 802.1ad UP Marking Table (S-VLAN) CLI Parameters

Parameter	Input Type	Permitted Values	Description
cos	Number	0 – 7	The CoS value to be mapped.
color	Variable	green yellow	The Color to be mapped.
802.1p	Number	0 – 7	The UP bit value assigned to matching frames.
dei	Number	0 – 1	The DEI bit value assigned to matching frames.

Example

The following command marks CoS 5, Yellow, to 802.1p UP bit 5, and DEI bit 1:

```
root> ethernet qos 802.1ad-up-bits-marking-tbl set cos 5 color yellow
802.1p 5 dei 1
```

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 177 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	0 - 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	0 - 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	0 - 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.

Parameter	Input Type	Permitted Values	Description
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 178 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)

This section includes:

- [Overview of Egress Shaping \(CLI\)](#)
- [Configuring Shapers \(CLI\)](#)
- [Configuring Service Bundle Shapers \(CLI\)](#)
- [Configuring Egress Line Compensation for Shaping \(CLI\)](#)

Overview of Egress Shaping (CLI)

Egress shaping determines the traffic profile for each queue. PTP 820 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.

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 \(CLI\)](#)
- [Attaching a Shaper Profile to a Queue \(CLI\)](#)

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 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 179 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.

Examples

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 (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 180 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.

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 – 32	Enter the ID of one of the configured queue shaper profiles.

Examples

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 (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 \(CLI\)](#)
- [Attaching a Shaper Profile to a Service Bundle \(CLI\)](#)

Configuring Service Bundle Shaper Profiles (CLI)

To configure a service bundle shaper profile, enter the following command in root view:

```
root> ethernet qos service-bundle-shaper-profile-tbl 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 181 Service Bundle Shaper Profiles CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 - 256	A unique ID that identifies the profile.
cir	Number	1 - 1000000000	The Committed Information Rate (CIR) assigned to the profile (in bps).
pir	Number	16000 - 1000000000	The Peak Information Rate (PIR) assigned to the profile (in bps).
shaper-profile-name	Text String	Up to 20 characters.	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 (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 182 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.

Examples

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 (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 183 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.

Example

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 \(CLI\)](#)
- [Configuring Queue Priority \(CLI\)](#)
- [Configuring Interface Priority Profiles \(CLI\)](#)
- [Attaching a Priority Profile to an Interface \(CLI\)](#)
- [Configuring Weighted Fair Queuing \(WFQ\) \(CLI\)](#)

Overview of Egress Scheduling (CLI)

Egress scheduling is responsible for transmission from the priority queues. PTP 820 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 184 Interface Priority Profile Example

Profile ID (1-9)			
CoS	Green Priority (user defined)	Yellow Priority (read only)	Description
0	1	1	Best Effort
1	2	1	Data Service 4
2	2	1	Data Service 3
3	2	1	Data Service 2
4	2	1	Data Service 1
5	3	1	Real Time 2 (Video with large buffer)
6	3	1	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 185 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.

Parameter	Input Type	Permitted Values	Description
cos4-priority	Number	1 – 4	The Green priority for the CoS 4 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 4 egressing the service bundle to which the profile is assigned.
cos5-priority	Number	1 – 4	The Green priority for the CoS 5 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 5 egressing the service bundle to which the profile is assigned.
cos6-priority	Number	1 – 4	The Green priority for the CoS 6 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 6 egressing the service bundle to which the profile is assigned.
cos7-priority	Number	1 – 4	The Green priority for the CoS 7 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 7 egressing the service bundle to which the profile is assigned.

Example

The following command configures a priority profile with Profile ID 1.

```
root> ethernet qos port-priority-profile-tbl add profile-id 1 cos0-
priority 1 description c0_p1 cos1-priority 1 description c1_p1 cos2-
priority 1 description c2_p1 cos3-priority 2 description c3_p2 cos4-
priority 2 description c4_p2 cos5-priority 3 description c5_p3 cos6-
priority 4 description c6_p4 cos7-priority 4 description c7_p4
```

This profile has the parameters listed in the following table.

Table 186 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

CoS	Green Priority (user defined)	Yellow Priority (read only)	Description
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 187 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 \(CLI\)](#)
- [Configuring a WFQ Profile \(CLI\)](#)
- [Attaching a WFQ Profile to an Interface \(CLI\)](#)

Overview of WFQ (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.

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 188 WFQ Profile Example

Profile ID (1-7)		
CoS	Queue Weight (Green)	Queue Weight (Yellow – not visible to users, and cannot be edited)
0	20	20
1	20	20
2	20	20
3	20	20
4	20	20

Profile ID (1-7)		
CoS	Queue Weight (Green)	Queue Weight (Yellow – not visible to users, and cannot be edited)
5	20	20
6	20	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 (CLI)

To define a WFQ profile, enter the following command in root view:

```
root> ethernet qos wfq-weight-profile-tbl add 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 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 189 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.

Parameter	Input Type	Permitted Values	Description
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 190 WFQ Sample Profile Parameters

CoS	Queue Weight (Green)	Queue Weight (Yellow – not visible to users, and cannot be edited)
0	15	20
1	20	20
2	20	20
3	20	20
4	20	20
5	20	20
6	20	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 191 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 Egress Statistics (CLI)

PTP 820 collects egress PMs at the queue level and the service bundle level.

Displaying Queue-Level PMs (CLI)

PTP 820 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 192 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.

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 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
```

Displaying Service Bundle-Level PMs (CLI)

PTP 820 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 193 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 19: Ethernet Protocols (CLI)

This section includes:

- [Configuring Adaptive Bandwidth Notification \(ABN\) \(CLI\)](#)
- [Configuring LLDP \(CLI\)](#)

Related Topics:

- [Configuring Service OAM \(SOAM\) Fault Management \(FM\)](#)

Configuring Adaptive Bandwidth Notification (ABN) (CLI)

This section includes:

- [Adaptive Bandwidth Notification Overview \(CLI\)](#)
- [Configuring an ABN Entity \(CLI\)](#)

Adaptive Bandwidth Notification Overview (CLI)

Adaptive Bandwidth Notification (ABN), also known as Ethernet Operation and Maintenance (EOAM), enables third party applications to learn about bandwidth changes in a radio link when ACM is active. Once ABN is enabled, the radio unit reports bandwidth information to upstream third-party switches.

The ABN entity creates a logical relationship between a radio interface or a logical group of radio interfaces, called the Monitored Interface, and an Ethernet interface or a logical group of Ethernet interfaces, called the Control Interface. When bandwidth degrades from the nominal value in the monitored interface, messages relaying the actual bandwidth values are periodically sent over the Control Interface. A termination message is sent once the bandwidth returns to its nominal level.

Configuring an ABN Entity (CLI)

You must first create an ABN 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 relating to the bandwidth sampling and the transmitted bandwidth messages.

To create an ABN entity consisting of a physical radio interface as the monitored interface and a physical Ethernet interface as the control interface, enter the following command in root view:

```
root> ethernet abn abn-entity-create abn-name <ab-name> monitored-  
interface <monitored-interface> monitored-slot <monitored-slot>  
monitored-port <monitored-port> control-interface <control-interface>  
control-slot <control-slot> control-port <control-port> vlan <vlan>
```

To create an ABN entity consisting of a physical radio interface as the monitored interface and an interface group as the control interface, enter the following command in root view:

```
root> ethernet abn abn-entity-create abn-name <abn-name> monitored-  
interface <monitored-interface> monitored-slot <monitored-slot>  
monitored-port <monitored-port> control-group <control-group> vlan <vlan>
```

To create an ABN entity consisting of an interface group as the monitored interface and a physical Ethernet interface as the control interface, enter the following command in root view:

```
root> ethernet abn abn-entity-create abn-name <abn-name> monitored-group
<monitored-group> control-interface <control-interface> control-slot
<control-slot> control-port <control-port> vlan <vlan>
```

To create an ABN entity consisting of an interface group as the monitored interface and an interface group as the control interface, enter the following command in root view:

```
root> ethernet abn abn-entity-create abn-name <abn-name> monitored-group
<monitored-group> control-group <control-group> vlan <vlan>
```

To set the Admin status of an ABN entity, enter the following command in root view:

```
root> ethernet abn abn-admin-set abn-name <abn-name> admin <admin-state>
```

To delete an ABN entity, enter the following command in root view:

```
root> ethernet abn abn-entity-delete abn-name <abn-name>
```

To show a summary of all ABN entities defined, enter the following command in root view:

```
root> ethernet abn abn-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 abn abn-entity-show abn-name <abn-name>
```

To set the monitoring interval for which a weighted average of the bandwidth readings is calculated, enter the following command in root view:

```
root> ethernet abn abn-monitoring-interval-set abn-name <abn-name> period
<monitoring-interval>
```

To set how often messages are transmitted when bandwidth is below the nominal value, enter the following command in root view:

```
root> ethernet abn abn-period-set abn-name <abn-name> period <message-
frequency>
```

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 abn abn-holdoff-set abn-name <abn-name> holdoff <holdoff-
time>
```

To clear the messages counter, enter the following command in root view:

```
root> ethernet abn abn-entity-counter-reset abn-name <abn-name>
```

Table 194 ABN Entity CLI Parameters

Parameter	Input Type	Permitted Values	Description
pipe-id	Number	1	The pipe ID. Only one pipe is supported in the current release.
abn-name	Text String		The name of the ABN entity.
monitored-interface	Variable	radio	This parameter is always set to radio.

Parameter	Input Type	Permitted Values	Description
monitored-slot	Number	2	
monitored-port	Number	Radio Carrier 1: 1 Radio Carrier 2 (PTP 820C only): 2	
monitored-group	Variable	rp1 rp2 rp3 rp4 lag1 lag2 lag3 lag4 mc-abc1 mc-abc2 mc-abc3 mc-abc4	When the monitored group is an HSB protection group (rp1 - rp-4), a LAG (lag1 - lag4), or a Multi-Carrier ABC group (mc-abc1 - mc-abc4), use this parameter instead of the monitored-interface parameter to identify the group. The group must be defined before you create the ABN entity. Note: Multi-Carrier ABC and HSP protection are only relevant for PTP 820C units.
control-interface	Variable	eth	This parameter is always set to ethernet.
control-slot	Number	1	This parameter is always set to 1.
control-port	Number	1-3	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
control-group	Variable	rp1 rp2 rp3 rp4 lag1 lag2 lag3 lag4 mc-abc1 mc-abc2 mc-abc3 mc-abc4	When the control group is an HSB protection group (rp1 - rp4), a LAG (lag1 - lag4), or a Multi-Carrier ABC group (mc-abc1 - mc-abc4), use this parameter instead of the control-interface parameter to identify the group. The group must be defined before you create the ABN entity. Note: Multi-Carrier ABC and HSP protection are only relevant for PTP 820C units.
vlan	Variable	untag 1 - 4094, except 4092 (reserved for the default management service)	The VLAN on which messages are transmitted (optional).
admin-state	Variable	isUp isDown	Enter isUp to enable ABN monitoring on the interface, or isDown to disable ABN monitoring on the interface.
monitoring-interval	Number	1 - 20	The interval (in seconds) for which a weighted average of the bandwidth readings is calculated.
message-frequency	Variable	4-one-second - sets message frequency to 1 second 5-ten-seconds - sets message frequency to 10 seconds 6-one-minute - sets message frequency to 1 minute	How often messages are transmitted when bandwidth is below the nominal value.
holdoff-time	Number	10 - 29	The amount of time the system waits when bandwidth degradation occurs, before transmitting a message.

Examples

The following command creates an ABN entity with radio interface 1 as the monitored interface and Ethernet port 1 as the control interface. It also specifies to transmit bandwidth messages on VLAN 1:

```
root> ethernet abn abn-entity-create abn-name ABN-1 monitored-interface  
radio monitored-slot 1 monitored-port 1 control-interface ethernet  
control-slot 1 control-port 1 vlan 1
```

The following command creates an ABN entity in a PTP 820C unit with radio interface 2 as the monitored interface and LAG group lag1 as the control interface. It also specifies to transmit bandwidth messages on VLAN 55:

```
root> ethernet abn abn-entity-create abn-name ABN-3 monitored-interface  
radio monitored-slot 1 monitored-port 2 control-group lag1 vlan 55
```

The following command creates an ABN entity in a PTP 820C unit with HSB protection group rp1 as the monitored interface and Ethernet port 2 as the control interface. It also specifies to transmit bandwidth messages on VLAN 200:

```
root> ethernet abn abn-entity-create abn-name ABN-4 monitored-group rp1  
control-interface ethernet control-slot 1 control-port 2 vlan 200
```

The following command creates an ABN entity in a PTP 820C unit with HSB protection group rp1 as the monitored interface and LAG group lag1 as the control interface. It also specifies to transmit bandwidth messages on VLAN 300:

```
root> ethernet abn abn-entity-create abn-name ABN-5 monitored-group rp1  
control-group lag1 vlan 300
```

The following command deletes ABN-1:

```
root> ethernet abn abn-entity-delete abn-name ABN-1
```

The following command sets the monitoring interval of ABN-1 to 1 second:

```
root> ethernet abn abn-monitoring-interval-set abn-name ABN-1 period 1
```

The following command sets the frequency of bandwidth messages regarding ABN-1 to 10 seconds:

```
root> ethernet abn abn-period-set abn-name ABN-1 period 5-ten-seconds
```

The following command sets the Holdoff time of ABN-1 to 15 seconds:

```
root> ethernet abn abn-holdoff-set abn-name ABN-1 holdoff 15
```

The following command clears the messages counter for ABN-1:

```
root> ethernet abn abn-entity-counter-reset abn-name ABN-1
```

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 transmissions 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 195 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.

Examples

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 196 LLDP Port CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	1	The slot in which the card resides.
port	Number	1-3	The port for which you want to configure LLDP.

Parameter	Input Type	Permitted Values	Description
agent-admin	Variable	txOnly rxOnly txAndRx disabled	<p>Defines how the LLDP protocol operates for this port:</p> <p>txOnly - The LLDP agent transmits LLDP frames on this port but does not update information about its peer.</p> <p>rxOnly - The LLDP agent receives but does not transmit LLDP frames on this port.</p> <p>txAndRx - The LLDP agent transmits and receives LLDP frames on this port (default value).</p> <p>disabled - The LLDP agent does not transmit or receive LLDP frames on this port.</p>
agent-notif-enable	Variable	true false	<p>true - The agent sends a Topology Change trap to the NMS whenever the system information received from its peer changes.</p> <p>false - Notifications to the NMS are disabled (default value).</p>

Example

The following commands configure Ethernet port 2 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 2 agent-
admin txAndRx
root> ethernet lldp agent-notif-enable interface eth slot 1 port 2 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 type	slot	port	Mac DA Identifier	Admin Status	Notification Enable	TLV TX
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 197 LLDP Remote Unit CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	1	The slot in which the card resides.
port	Number	1-3	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's chassis.
- **Remote Chassis ID** – An octet string used to identify the peer's chassis.
- **Rem Port ID subType** – The type of port identifier encoding used in the peer's Port ID.
- **Rem Port ID** – An octet string used to identify the port component associated with the peer.
- **Rem Port Description** – A description of the peer's port.
- **Rem System Name** – The peer's system name.
- **Rem System Description** – The peer's system description.



Note

The Rem Port Description, Rem System Name, and Rem System Description fields are not used in the current version.

- **Rem System Cap Supported** - The bitmap value used to identify which system capabilities are supported on the peer. The bitmap is defined by the following parameters:
 - 0 - other
 - 1 - repeater
 - 2 - bridge
 - 3 - wlanAccessPoint
 - 4 - router
 - 5 - telephone
 - 6 - docsisCableDevice
 - 7 - stationOnly
 - 8 - cVLANComponent
 - 9 - sVLANComponent

- 10 - twoPortMACRelay
- **Rem System Cap Enabled** - The bitmap value used to identify which system capabilities are enabled on the peer. The bitmap is defined by the following parameters:
 - 0 - other
 - 1 - repeater
 - 2 - bridge
 - 3 - wlanAccessPoint
 - 4 - router
 - 5 - telephone
 - 6 - docsisCableDevice
 - 7 - stationOnly
 - 8 - cVLANComponent
 - 9 - sVLANComponent
 - 10 - twoPortMACRelay
- **Remote Changes** - Indicates whether there are changes in the peer's MIB, as determined by the variable **remoteChanges**. Possible values are:
 - **True** - Changes have taken place in the peer's MIB since the defined agent-start-time.
 - **False** - No changes have taken place in the peer's MIB since the defined agent-start-time.

Displaying the LLDP Remote Management Data per Port (CLI)

To display remote LLDP management data from a specific port, starting from a specific time, enter the following command in root view. If no time is specified, all data is displayed.

```
root> ethernet lldp agent-remote-mng-show agent-start-time <agent-start-time> interface eth slot <slot> port <port>
```

Table 198 LLDP Remote Management Data Per Port CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	1	
port	Number	1-3	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 20: Synchronization (CLI)

This section includes:

- [Configuring SyncE Regenerator \(CLI\)](#)
- [Changing the ETSI/ANSI Mode \(CLI\)](#)
- [Configuring the Sync Source \(CLI\)](#)
- [Configuring the Outgoing Clock \(CLI\)](#)
- [Configuring SSM Messages \(CLI\)](#)
- [Configuring the Revertive Timer \(CLI\)](#)
- [Displaying Synchronization Status and Parameters \(CLI\)](#)
- [Configuring 1588 Transparent Clock \(CLI\)](#)

Configuring SyncE Regenerator (CLI)

In SyncE PRC pipe regenerator mode, frequency is transported between two interfaces through the radio link.

With the system acting as a simple link, no distribution mechanism is necessary, resulting in improved frequency distribution performance with PRC quality and a simplified configuration.



Note

SyncE Regenerator currently supports only a single pipe configuration.

Before adding a pipe configuration, you must set the Sync mode to Pipe. Enter the following command in root view:

```
root> platform sync mode set pipe
```

By default, the Sync mode is set to **Automatic**. To display the current Sync mode, enter the following command in root view:

```
root> platform sync mode show
```

To add a pipe configuration, enter the following command in root view:

```
root> platform sync pipe add pipe-id <pipe-id> interface-1-type
<interface-1-type> slot <slot> port <port> interface-2-type <interface-2-
type> slot <slot> port <port>
```

To change the first interface in a SyncE pipe, enter the following command in root view:

```
root> platform sync pipe edit interface-1 pipe-id <pipe-id> interface-1-
type <interface-1-type> slot <slot> port <port>
```

To change the second interface in a SyncE pipe, enter the following command in root view:

```
root> platform sync pipe edit interface-1 pipe-id <pipe-id> interface-2-
type <interface-2-type> slot <slot> port <port>
```

To remove a SyncE pipe, enter the following command in root view:

```
root> platform sync pipe remove pipe-id <pipe-id>
```

To remove all SyncE Regenerators (pipes), enter the following command in root view:

```
root> platform sync pipe remove all
```

To view the configured SyncE pipes, enter the following command in root view:

```
root> platform sync pipe show
```

Table 199 SyncE Regenerator CLI Parameters

Parameter	Input Type	Permitted Values	Description
pipe-id	Number	1	The pipe ID. Only one pipe is supported in the current release.

Parameter	Input Type	Permitted Values	Description
interface-1-type	Variable	ethernet radio	The interface type for the first interface in the pipe.
slot	Number	Ethernet: 1 Radio: 2	
port	Number	GbE 1: 1 GbE 2: 2 GbE 3: 3 Radio Carrier 1: 1 Radio Carrier 2 (PTP 820C only): 2	
interface-2-type	Variable	ethernet radio	The interface type for the second interface in the pipe. If the first interface type is ethernet, the second must be radio, and vice versa.

Examples

The following command configures a SyncE pipe between Ethernet port 1 and radio interface 1:

```
root> platform sync pipe add pipe-id 1 interface-1-type ethernet slot 1
port 1 interface-2-type radio slot 2 port 1
```

The following command changes the first interface in the pipe from ethernet port 1 to Ethernet port 2:

```
root> platform sync pipe edit interface-1 pipe-id 1 interface-1-type
ethernet slot 1 port 2
```

The following command changes the second interface in the pipe from radio interface 1 to radio interface 2:

```
root> platform sync pipe edit interface-2 pipe-id 1 interface-2-type
radio slot 2 port 2
```

The following command removes SyncE pipe 1:

```
root> platform sync pipe remove pipe-id 1
```

Changing the ETSI/ANSI Mode (CLI)

By default, PTP 820 units are set to ETSI mode. No mode change is necessary to configure an MPMC 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 \(CLI\)](#)
- [Clearing All Sync Sources \(CLI\)](#)

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 200 Sync Source Ethernet CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	1	
port	Number	1-3	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: <ul style="list-style-type: none"> • automatic • prc • ssu-a • ssu-b • g813.8262 For ANSI (FCC) systems: <ul style="list-style-type: none"> • 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 201 Sync Source Radio CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	2	
port	Number	1-2	
radio-channel	Number	0 – 85	Must be set to 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: <ul style="list-style-type: none"> • automatic • prc • ssu-a • ssu-b • g813.8262 For ANSI (FCC) systems: <ul style="list-style-type: none"> • 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 radio interface 1 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
```

Clearing All Sync Sources (CLI)

To clear all synchronization sources that have been configured in the system, enter the following command in root view:

```
root> platform sync source remove all
```

Configuring the Outgoing Clock (CLI)

For each interface, you can choose between using the system clock or the interface's internal clock as its synchronization source. By default, interfaces use the system clock.

When configuring the outgoing clock, the Sync mode must be set to its default setting of automatic. To display the current Sync mode, enter the following command in root view:

```
root> platform sync mode show
```

If the Sync mode is set to pipe, you must set it to automatic by entering the following command in root view:

```
root> platform sync mode set automatic
```

;

To set the interface clock for a radio interface, enter the following command in root view:

```
root> platform sync interface-clock set radio-interface slot <slot> port
<port> radio-channel <radio-channel> source <source>
```

To set the interface clock for an Ethernet interface, enter the following command in root view:

```
root> platform sync interface-clock set eth-interface slot <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 Ethernet Interfaces \(CLI\)](#).

Table 202 Outgoing Clock CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	ethernet: 1 radio: 2	
port	Number	ethernet: 1-3 radio: 1-2	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 radio interface 2 to its internal clock:

```
root> platform sync interface-clock set radio-interface slot 2 port 2  
radio-channel 0 source local-clock
```

The following command sets the clock source for Ethernet port 2 to the system clock:

```
root> platform sync interface-clock set eth-interface slot 1 port 2  
source system-clock
```

Configuring SSM Messages (CLI)

In order to provide topological resiliency for synchronization transfer, PTP 820C implements the passing of SSM messages over the Ethernet and radio interfaces. SSM timing in PTP 820C 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
```

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 203 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
```

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 | 1 | Ethernet | 11 | automatic |
-----|
| 1 | 2 | Ethernet | 3 | automatic |
-----|
| 2 | 1 | Radio | 5 | automatic |
-----|
| 2 | 2 | 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:

```
number of configured sources = 4
=====|
| Slot | Port | Type | Instance | Active-Src | Act. Quality | Received
SSM | revert-time |
=====|
| 1 | 1 | ethernet | false | PRC | do-not-use | 0 |
-----|
| 1 | 2 | ethernet | false | do-not-use | do-not-use | 0 |
-----|
| 2 | 1 | radio | false | failure | do-not-use | 0 |
-----|
| 2 | 2 | radio | true | failure | g.813 | 0 |
=====|
```

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:

```

number of configured clock-interfaces = 14
=====|
| Slot | Port | Type | Trail Radio | Source-Type | SSM-Admin |
=====|
| 1 | 1 | Ethernet | | System Clock | off |
| 1 | 2 | Ethernet | | System Clock | off |
| 1 | 3 | Ethernet | | System Clock | off |
| 2 | 1 | Radio    | | System Clock | on  |
| 2 | 2 | Radio    | | System Clock | on  |
=====|

```

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)

**Note**

1588 Transparent Clock is supported with PTP 820C and PTP 820S.

PTP 820 uses 1588v2-compliant Transparent Clock to counter the effects of delay variation. Transparent Clock measures and adjusts for delay variation, enabling the PTP 820 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 10.0:

- 1588 TC Transparent Clock is not supported when Master-Slave communication is using the UDP/IPv6 transport layer.
 - 1588 TC cannot be used on 1+1 HSB links.
 - If 1588 TC is not supported with Frame Cut-Through.
-

**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. See [Configuring an Ethernet Interface as a Synchronization Source \(CLI\)](#).
2. Add a radio interface as a Sync source, with lower priority than the port receiving synchronization from the customer side. See [Configuring a Radio Interface as a Synchronization Source \(CLI\)](#).
3. On the remote side of the radio link, add the radio interface facing the local device as a Sync source, with Sync Interface Priority 1. See [Configuring a Radio Interface as a Synchronization Source \(CLI\)](#).
4. Add the port receiving synchronization from the customer side as a Sync source, with Sync Interface Priority 1. See [Configuring an Ethernet Interface as a Synchronization Source \(CLI\)](#).
5. Verify that the Sync Interface Quality Status of the first Sync source is not Failure. See [Displaying Synchronization Status and Parameters \(CLI\)](#).
6. Enter the following command in root view to enable Transparent Clock:

```
root> platform sync ptp-tc set admin enable
```

**Note**

To disable Transparent Clock, enter the following command in root view:

```
root> platform sync ptp-tc set admin disable
```

**Note**

Disabling 1588 PTP can drastically affect time synchronization performance in the entire network.

7. Enter one of the following commands in root view to assign the radio or Multi-Carrier ABC group that will carry the PTP packets and determine the direction of the PTP packet flow:

For an individual radio, enter the following command:

```
root> platform sync ptp-tc set radio slot <slot> port <port> direction
<upstream|downstream>
```

For a Multi-Carrier ABC group, enter the following command:

```
root> platform sync ptp-tc set group id <group> 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 on radio carrier 1 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 2 port 1 direction upstream
```

The following commands enable Transparent Clock on Multi-Carrier ABC group 1 and configure the radio to send PTP packets upstream:

```
root> platform sync ptp-tc set group id mc-abc1 direction upstream
```

Table 204 1588 Transparent Clock CLI Parameters

Parameter	Input Type	Permitted Values	Description
slot	Number	2	
port	Number	1-2	
group	Variable	mc-abc1	

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.

Chapter 21: Access Management and Security (CLI)

This section includes:

- [Configuring the General Access Control Parameters \(CLI\)](#)
- [Configuring the Password Security Parameters \(CLI\)](#)
- [Configuring Users \(CLI\)](#)
- [Configuring RADIUS \(CLI\)](#)
- [Configuring X.509 CSR Certificates and HTTPS \(CLI\)](#)
- [Uploading the Security Log \(CLI\)](#)
- [Uploading the Configuration Log \(CLI\)](#)

Related Topics:

- [Logging On \(CLI\)](#)
- [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.

- [Operating in FIPS Mode \(CLI\)](#)
- [Configuring AES-256 Payload Encryption](#)

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 205 Inactivity Timeout Period CLI Parameters

Parameter	Input Type	Permitted Values	Description
inactivity-timeout	Number	1 - 60	The session inactivity timeout period (in minutes).

Example

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 206 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.

Example

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 207 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.

Examples

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 208 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 209 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 210 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 820 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 211 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 212 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 213 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 \(CLI\)](#)
- [Viewing RADIUS Access Control and Server Attributes \(CLI\)](#)
- [Viewing RADIUS User Permissions and Connectivity \(CLI\)](#)

RADIUS Overview (CLI)

The RADIUS protocol provides centralized user management services. PTP 820 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 820 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 214 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 215 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 during 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.

Example

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
```

Viewing RADIUS Access Control and Server Attributes (CLI)

To display the Radius access control status, enter the following command:

```
root> platform security radius-admin show
```

To display Radius server attributes, enter the following command:

```
root> platform security radius-server-communication show
```

Viewing RADIUS User Permissions and Connectivity (CLI)

You can view Radius user connectivity and permissions information for all Radius users currently connected. To do so, enter the following command:

```
root> platform security radius-server-privileges show
```

The following user information is displayed, for each currently connected Radius user:

- **User ID** - The user name
- **Access Channels** - The permitted access channels.
- **User Instances** - 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 and HTTPS (CLI)

The web interface protocol for accessing PTP 820 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 820 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 820 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)

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 216 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 217 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 820 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 820 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
```

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 820 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 218 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 820 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 219 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		<p>The name you want to give the file you are exporting.</p> <p>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</p> <p>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</p>
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 file 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
```

Chapter 22: Alarm Management and Troubleshooting (CLI)

This section includes:

- [Viewing Current Alarms \(CLI\)](#)
- [Viewing the Event Log \(CLI\)](#)
- [Editing Alarm Text and Severity \(CLI\)](#)
- [Uploading Unit Info \(CLI\)](#)
- [Performing Diagnostics \(CLI\)](#)
- [Working in CW Mode \(Single or Dual Tone\) \(CLI\)](#)

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 \(CLI\)](#)
- [Editing an Alarm Type \(CLI\)](#)
- [Setting Alarms to their Default Values \(CLI\)](#)

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 220 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 221 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
```

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 820 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 222 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
```

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 223 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 224 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 \(CLI\)](#)
- [Configuring MDs \(CLI\)](#)
- [Configuring MA/MEGs \(CLI\)](#)
- [Configuring MEPs \(CLI\)](#)
- [Displaying MEP and Remote MEP Attributes \(CLI\)](#)
- [Displaying Detailed MEP Error Information \(CLI\)](#)
- [Performing Loopback \(CLI\)](#)

SOAM Overview (CLI)

The Y.1731 standard and the MEF-30 specifications define Service OAM (SOAM). SOAM is concerned with detecting, isolating, and reporting connectivity faults spanning networks comprising multiple LANs, including LANs other than IEEE 802.3 media.

Y.1731 Ethernet FM (Fault Management) consists of three protocols that operate together to aid in fault management:

- Continuity check
- Link trace
- Loopback



Note

Link trace is planned for future release.

PTP 820 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 225 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	<p>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.</p> <p>Note: In the current release, the maintenance level is not relevant to the SOAM functionality.</p>

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 226](#)):

- 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 intervals
```

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 226 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	<p>The MEG level must be the same for MEGs on both sides of the link. Higher levels take priority over lower levels.</p> <p>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.</p> <p>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:</p> <p>The customer role is assigned MEG levels 6 and 7</p> <p>The provider role is assigned MEG levels 3 through 5</p> <p>The operator role is assigned MEG levels: 0 through 2</p> <p>The default MEG level assignment can be changed via a mutual agreement among customer, provider, and/or operator roles.</p> <p>The number of MEG levels used depends on the number of nested MEGs for which the OAM flows are not distinguishable based on the Ethernet layer encapsulation.</p>
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 227 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> 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       Priority  Address      priority    on time    Clear Time
=====
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> 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      |intervals  |4            |2                    |0              |
=====

SOAM MEP Table:
=====
MEP ID      Interface Location  MEP Direction  MEP Active  MEP CCM TX Enable  CCM and 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      |intervals  |4            |2                    |0              |
=====

SOAM MEP Table:
=====
MEP ID      Interface Location  MEP Direction  MEP Active  MEP CCM TX Enable  CCM and LTM Priority  MEP MAC Address  MEP Lowest priority fault alarm  MEP Alarm on time  MEP Alarm Clear Time  Sequence Errors CCM Frames TX  CCM Messages
=====
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 228 MEP and Remote MEP Status Parameters (CLI)

Parameter	Description
MD Parameters	
MD ID	The MD ID.
MD Name	The MD name (44 characters).

Parameter	Description
MD Format	The MD format (None).
MD Level	The maintenance level of the MD (0-7).
MEG Parameters	
MA ID	The MA/MEG ID.
Format	charString in the current release.
Name	The MA/MEG name (43 characters).
Level	The MEG Level (0-7).
Service	The Service ID of the Ethernet service to which the MEG belongs.
CCM Interval	The interval at which CCM messages are sent within the MEG.
Number of MEPs	The number of MEPs that belong to the MEG.
Number of Local MEPs	The number of local MEPs that belong to the MEG.
Number of MIPs	The number of MIPs that belong to the MEG.
SOAM MEP Table Parameters	
MEP ID	The MEP ID.
Interface Location	The interface on which the service point associated with the MEP is located.
MEP Direction	Up or Down.
MEP Active	Indicates whether the MEP is enabled (true) or disabled (false).
MEP CCM TX Enable	Indicates whether the MEP is configured to send CCMs (true or false).
CCM and LTM Priority	The p-bit included in CCMs sent by the MEP (0-7).
MEP MAC Address	The MAC address of the service point associated with the MEP.
MEP Lowest priority fault alarm	The lowest defect priority that can trigger alarm generation. Defects with a lower priority will not trigger alarms.
MEP Alarm on time	The amount of time that defects must be present before an alarm is generated, in msec intervals (250-1000).
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.

Parameter	Description
RMEP Parameters	
MepId	The MEP ID of the local MEP paired with the remote MEP.
Rmep Id	The remote MEP ID.
operState	The operational state of the remote MEP.
OKorFail Time	The timestamp marked by the remote MEP indicating the most recent CCM OK or failure it recorded. If none, this field indicates the amount of time, in msec intervals, since SOAM was activated.
MAC	The MAC Address of the interface on which the remote MEP is located.
Rdi	Displays the state of the RDI (Remote Defect Indicator) bit in the most recent CCM received by the remote MEP: <ul style="list-style-type: none"> 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:

[illegible]

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 Messages Loopback Messages Loopback Messages Drop Loopback Loopback Loopback Loopback
to be Messages Messages Messages Enable Messages Messages Messages Replies
transmitt Destination Priority MAC Address Interval Frame Size Data Pattern Age-out
ed MAC Address Priority 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 229 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.

Parameter	Input Type	Permitted Values	Description
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 <code>platform if-manager show interfaces</code> command in root view.
dest-mep-id	Number	1-8191	The MEP ID of the interface to which you want to send the loopback.
tx-num	Number	0-1024	The number of loopback messages to transmit. If you enter 0, loopback will not be performed.

To display loopback results, enter the following command in root view:
`root> ethernet soam loopback status show meg-id <meg-id> mep-id <mep-id>`

The following is a sample output for this command on MEG ID 127, MEP ID 1.

```
root> ethernet soam loopback status show meg-id 127 mep-id 1
```

SOAM MEP LBM Attributes Table:
=====

Loopback messages transmitted in session	Loopback messages left to transmit in session	Loopback replies received in session	Transaction ID of loopback message	Loopback session state	Next transaction ID	Loopback messages transmitted	Loopback messages received	Valid in-order loopback replies received	Loopback replies transmitted	Valid out-of-order loopback replies received	Bad MSDU Loopback Replies	Loopback messages received with bad sender id	Loopback replies received with bad sender id
9	114	9	1	soamLbmActive	10	9	0	9	0	0	0	0	0

```
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 230 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 23: Maintenance

This section includes:

- [Temperature Ranges](#)
- [Troubleshooting Tips](#)
- [PTP 820C Connector Pin-outs](#)
- [PTP 820C LEDs](#)
- [PTP 820S Connector Pin-outs](#)
- [PTP 820S LEDs](#)

Temperature Ranges

The following are the permissible unit temperature ranges for PTP 820C and PTP 820S.

- **-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.

To display the current unit temperature, see [Configuring Unit Parameters](#).

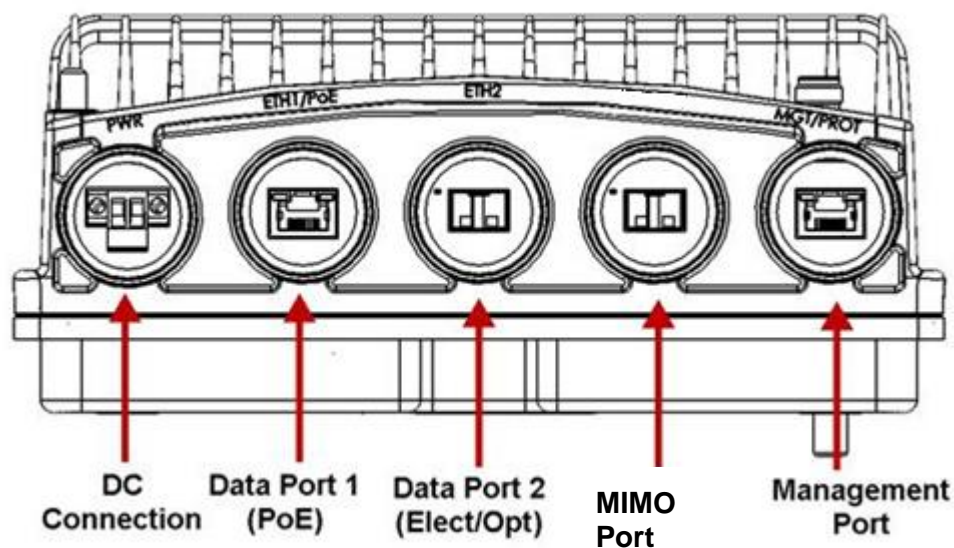
- The permissible IDU humidity range is 5%RH to 100%RH

Troubleshooting Tips

- For dual-polarization and 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 dual-polarization and XPIC links, the RSL should be similar for both polarizations. For XPIC links, 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 820C Connector Pin-outs

Figure 313 PTP 820C Interfaces



Eth1/PoE - GbE Electrical+PoE/Optical

Table 231: PTP 820C Eth1/PoE Interface- RJ-45/SFP 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)

Eth2 - GbE Electrical/Optical

Table 232 PTP 820C Eth2 Interface - RJ-45/SFP 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)

MIMO Port

Table 233 PTP 820C MIMO Port - RJ-45/SFP 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)

MGT/PROT - Management (FE-Standard) and Protection (FE-Non-Standard)

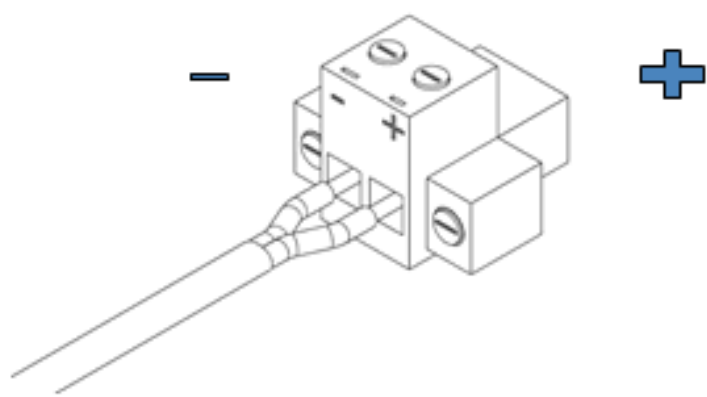
Table 234 PTP 820C MGT/PROT Interface - RJ-45 Pinouts

Pin no.	Description
Protection - Non-Standard 100Base-T 4 Wire	
1	TX+
2	TX-
3	RX+
6	RX-
Protection - Non-Standard 100Base-T 4 Wire	
4	TX+
5	TX-
7	RX+
8	RX-

DC

The DC port is UL-60950 compliant, with a 2-pin connector.

Figure 314 PTP 820C DC Port Connector



RSL Interface

PTP 820C uses a weather-proof BNC connector.

**Note**

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

Source Sharing

PTP 820C uses a TNC connector for source sharing. This connector is marked EXT/REF.

PTP 820C LEDs

The PTP 820C provides the following LEDs to indicate the status of the unit's interfaces, and the unit as a whole:

- [Electrical GbE Interface \(RJ-45\) LEDs](#)
- [Optical GbE Interface \(SFP\) LEDs](#)
- [Management FE Interface \(RJ-45\) LEDs](#)
- [Radio LED](#)
- [Status LED](#)
- [Protection LED](#)

Electrical GbE Interface (RJ-45) LEDs

There are two LEDs next to each electrical (RJ-45) 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 port's Admin state:

- **Off** - Admin is Disabled.
- **Green** – Admin is Enabled.

The Orange LED indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

- **Off – Off** - Admin is Disabled *or* no cable is connected to the interface.
- **Orange** – Admin is Enabled and a cable is connected to the interface.
- **Blinking Orange** – Admin is Enabled and a cable is connected to the interface, *and* there is traffic on the interface.

Optical GbE Interface (SFP) LEDs

There is one Green LED next to each optical (SFP) GbE 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 FE Interface (RJ-45) LEDs

There are two LEDs next to the MGT (management) 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 port's Admin state :

- **Off** - Admin is Disabled .
- **Green** - Admin is Enabled .

If the MGT interface is being used for protection, the Orange LED indicates the status of the mate unit.:

- **Off** – The interface is not in an operational state (down).
- **Orange** – The interface is operational (up).
- **Blinking Orange** –Management traffic is passing through the interface.

The Link LED is a three-color LED that 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.

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.
- **Red** - The power is on, and one or more major or critical alarms are raised on the motherboard.

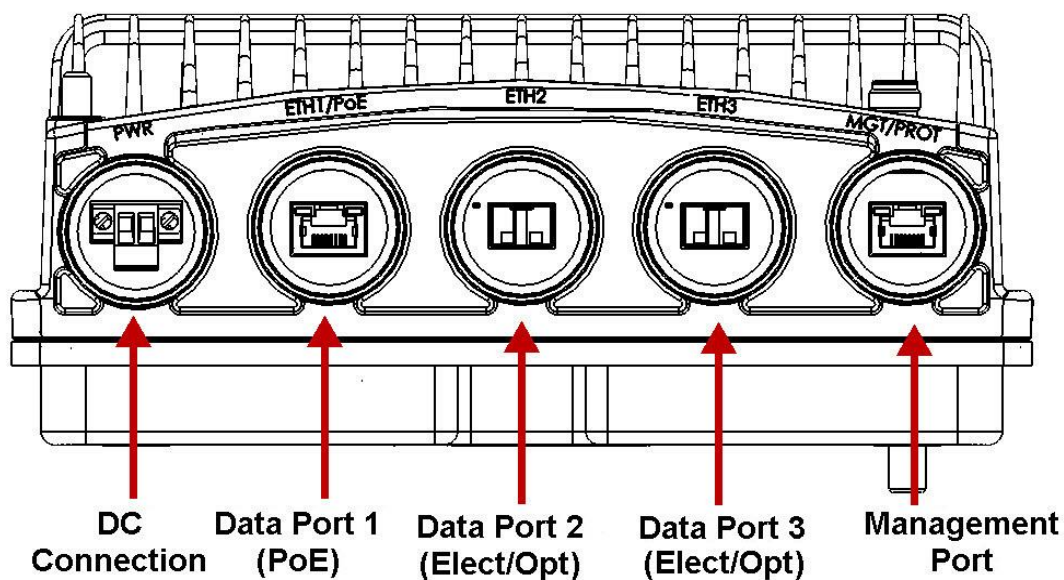
Protection LED

The Protection LED operates in a protected configuration to indicate the protection status:

- **Orange** - Protection is enabled, and the unit is in standby mode.
- **Green** - Protection is disabled or protection is enabled, and the unit is in active mode.

PTP 820S Connector Pin-outs

Figure 315 PTP 820S Interfaces



Eth1/PoE - GbE Electrical+PoE/Optical

Table 235 PTP 820S Eth1/PoE Interface- RJ-45/SFP 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)

Eth2 - GbE Electrical/Optical

Table 236 PTP 820S Eth2 Interface - RJ-45/SFP 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)

Eth3 - GbE Electrical/Optical

Table 237 PTP 820S Eth3/EXP Interface - RJ-45/SFP 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)

MGT/PROT - Management (FE-Standard) and Protection (FE-Non-Standard)

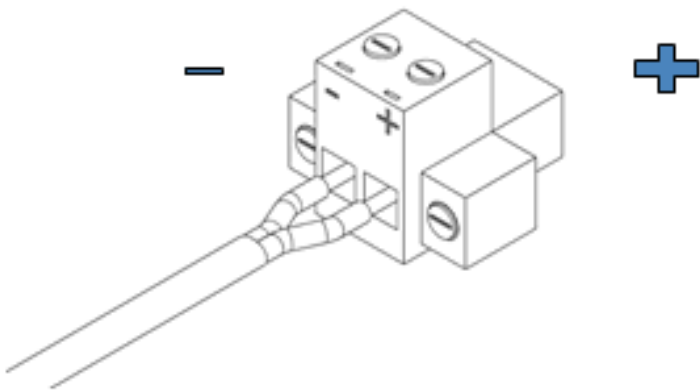
Table 238 PTP 820S MGT/PROT Interface - RJ-45 Pinouts

Pin no.	Description
Management - Standard 100Base-T 4 Wire	
1	TX+
2	TX-
3	RX+
6	RX-
Protection - Non-Standard 100Base-T 4 Wire	
4	TX+
5	TX-
7	RX+
8	RX-

DC

The DC port is UL-60950 compliant, with a 2-pin connector.

Figure 316 PTP 820S DC Connector



RSL Interface

PTP 820S uses a weather-proof BNC connector.

**Note**

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

PTP 820S LEDs

The PTP 820S provides the following LEDs to indicate the status of the unit's interfaces, and the unit as a whole:

- [Electrical GbE Interface \(RJ-45\) LEDs](#)
- [Optical GbE Interface \(SFP\) LEDs](#)
- [Management FE Interface \(RJ-45\) LEDs](#)
- [Radio LED](#)
- [Status LED](#)
- [Protection LED](#)

Electrical GbE Interface (RJ-45) LEDs

There are two LEDs next to each electrical (RJ-45) 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 port's Admin state :

- **Off** - Admin is Disabled .
- **Green** - Admin is Enabled .

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.
- **Orange** – Admin is Enabled and a cable is connected to the interface.
- **Blinking Orange** – Admin is Enabled and a cable is connected to the interface, *and* there is traffic on the interface..

Optical GbE Interface (SFP) LEDs

There is one Green LED next to each optical (SFP) GbE 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 FE Interface (RJ-45) LEDs

There are two LEDs next to the MGT (management) 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 port's Admin state :

- **Off** - Admin is Disabled.
- **Green** - Admin is Enabled .
- **Blinking Green** – Management traffic is passing through the interface.

If the MGT interface is being used for protection, the Orange LED indicates the status of the mate unit:

- **Off** – Admin is Disabled *or* no cable is connected to the interface..
- **Orange** – Admin is Enabled and a cable is connected to the interface .
- **Blinking Orange** – Admin is Enabled and a cable is connected to the interface, *and* there is traffic on the interface .

Radio LED

The RadioLED indicates the status of the radio link:

- **Green** - The power is on, and all carriers are operational (up).
- **Red** - A Loss of Frame (LOF) condition exists in at least one 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.
- **Red** - The power is on, and one or more major or critical alarms are raised on the motherboard.

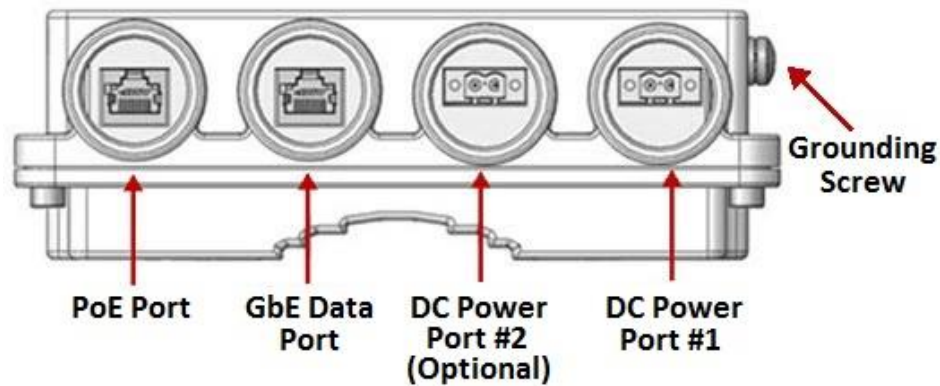
Protection LED

The Protection LED operates in a protected configuration to indicate the protection status:

- **Yellow** - Protection is enabled, and the unit is in standby mode.
- **Green** - Protection is disabled, or protection is enabled, and the unit is in active mode.

PoE Injector Pin-outs

Figure 317: PoE Injector Connectors



PoE Port

Table 239 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 240 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)

Pin no.	Description
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:

The available PoE Injector model is:

- PTP 820 PoE Injector all outdoor, redundant DC input, +24VDC support (part number: N000082L022A) – PoE_Inj_AO_2DC_24V_48V – Includes two DC power ports with power input ranges of $\pm(18-60)V$ each.

These ports are UL-60950 compliant, with a 2-pin connector.

PoE Injector LEDs

- 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.

Chapter 24: Alarms List

The following table lists all alarms used in the PTP 820C/S products.

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
10	Alarm	Framer digital loopback	Warning	User enabled framer digital loopback.	Disable framer digital loopback.	
25	Alarm	Unit Temperature is out of system specified limits.	Warning			
26	Alarm	Unit input voltage is too low.	Warning			
27	Alarm	Unit input voltage is too high.	Warning			
28	Event	Unit warm reset.	Indeterminate			
29	Event	Unit reset.	Warning			
30	Alarm	POE input voltage is too low	Warning			
31	Event	Change Remote request was sent	Major			(1)
32	Event	Protection switchover due to remote request	Major			(1)
33	Alarm	Protection-MIMO-misconfiguration- alarm	Major	Unit redundancy and MIMO 4X4 can not operate simultaneously		

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
100	Alarm	LAG is not fully functional - LAG Degraded.	Major			
101	Alarm	LAG operational state is down	Critical			
102	Alarm	Loopback is active	Major	Ethernet loopback is active.	Wait till loopback timeout expires or disable loopback.	
103	Alarm	Slot X port XX is mirrored to slot Y port YY	Minor	Mirroring is enabled by user configuration.	Disable mirroring.	
120	Alarm	Port speed mismatch	Major	System reset is required after the port speed was changed		
150	Alarm	Interface is down due to automatic state propagation.	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	Alarm	Protection communication is down	Major	Mate unit is absent/failure. Protection cable is disconnected. Unit failure.	1. Check existence of mate unit. 2. Check protection cable connection between units. 3. Reset mate unit. 4. Replace mate unit.	
201	Alarm	Protection in Lockout State	Major			
202	Event	Protection switchover due to local failure	Major			
203	Alarm	Mate does not exist	Major	Mate does not exist or cable unplugged.		

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
204	Alarm	HSB insufficient configuration	Critical	External Protection configured both with HSB.	Remove External Protection and HSB configuration.	
307	Event	TDM interface is up	Warning			
308	Event	TDM interface is up	Warning			
401	Alarm	Ethernet Loss of Carrier	Major	Cable disconnected. Defective cable.	1. Check connection of cable 2. Replace cable.	
407	Event	Ethernet interface is up	Warning			
408	Event	Ethernet interface is down	Warning			
601	Alarm	Radio excessive BER	Major	1. Fade in the link. 2. Defective IF cable. 3. Fault in RFU. 4. Fault in RMC (Radio Modem Card).	1. Check link performance. 2. Check IF cable and replace if required. 3. Replace RFU. 4. Replace RMC (Radio Modem Card).	
602	Alarm	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	Alarm	Radio loss of frame	Critical	1. Fade in the link. 2. Defective IF cable. 3. Fault in RFU. 4. Fault in RMC (Radio Modem Card). 5. Different radio scripts at both ends of the link.	1. Check link performance. 2. Check IF cable and replace if required. 3. Replace RFU. 4. Replace RMC (Radio Modem Card). 5. Make sure same script is loaded at both ends of the link.	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
604	Alarm	Radio signal degrade	Minor	<ol style="list-style-type: none"> 1. Fade in the link. 2. Defective IF cable. 3. Fault in RFU. 4. Fault in RMC (Radio Modem Card). 	<ol style="list-style-type: none"> 1. Check link performance. 2. Check IF cable and replace if required. 3. Replace RFU. 4. Replace RMC (Radio Modem Card). 	
605	Event	Radio interface is up	Warning			
606	Event	Radio interface is down	Warning			
801	Alarm	Corrupted inventory file	Warning	The inventory file is corrupted	<ol style="list-style-type: none"> 1. Reset the system. 2. Reinstall the software. 	
802	Alarm	Inventory file not found	Warning	The inventory file is missing	<ol style="list-style-type: none"> 1. Reset the system. 2. Reinstall the software. 	
901	Alarm	Demo license is active	Warning	Demo license has been activated by the user	Disable the demo license	
902	Event	Demo license is expired	Warning			
903	Event	Demo license is started	Warning			
904	Event	Demo license is stopped	Warning			
905	Event	License key loading failure	Major			
906	Event	License key loaded successfully	Warning			

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
907	Alarm	License violation	Critical	The current configuration does not match the licensed feature set. 48 hours after a "license violation" alarm is raised, sanction mode is activated in which all alarms except the license violation alarm are cleared and no new alarms are raised.	<ol style="list-style-type: none"> 1. Get the list of features' configurations that are violated via the "license information report". 2. Install a new license that allows the use of all required features. 	
908	Alarm	Demo license is about to expire	Major	Demo license allowed period is about to end within 10 days	Disable the demo license and install a new valid one	
910	Alarm	License signature failure	Major	License key validation has failed due to invalid product serial number	Replace the IDU	
911	Event	License violation sanction is enforced	Major			
913	Alarm	License components are missing or corrupted	Major	Essential internal license components are missing or corrupted.	Reinstall software	
1002	Alarm	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	Event	Radio protection switchover - reason	Warning	Protection decision machine initiated switchover due to local failure or user command	Check the system for local failures	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1007	Alarm	Radio protection no mate	Major	Radio protection function is missing radio module, module defected or disabled	<ol style="list-style-type: none"> 1. Add radio module. 2. Replace a defective existing radio module. 3. Make sure all radio interfaces are enabled. 	
1008	Event	Remote switchover request was sent - reason	Warning			
1009	Alarm	Rdadio protection lockout command is on.	Major	The user has issued a lockout command	Clear the lockout command	
1010	Event	Ethernet interface Group protection switchover	Warning	<ol style="list-style-type: none"> 1. LOC event on an Ethernet interface. 2. Protection group member was disabled or pulled out of the shelf. 	<ol style="list-style-type: none"> 1. Check the system for local failures. 2. Check external equipment. 	
1011	Alarm	Interface protection lockout is on	Major	<ol style="list-style-type: none"> 1. The user has issued a lockout command 	<ol style="list-style-type: none"> 1. Clear the lockout command 	
1012	Alarm	Interface protection no mate: mate interface is missing or disabled	Major	Interface protection function is missing interface module, module defected or disabled	<ol style="list-style-type: none"> 1. Add interface module. 2. Replace a defective existing interface module. 3. Make sure all interface interfaces are enabled. 	
1102	Event	Software installation status:	Warning			
1105	Event	New version installed	Warning	A software version has been installed but system has not been reset.		

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1111	Event	User approved download of software version file	Warning			
1112	Event	Software download status:	Warning			
1113	Event	Missing components:	Warning			
1114	Event	Incomplete file set; missing components	Warning	Software bundle is missing components.	Get a complete software bundle	
1150	Event	Configuration file backup generation started	Warning	User command		
1151	Event	Configuration file backup created	Warning	Backup file creation finished successfully		
1152	Event	Failure in configuration file backup generation	Warning	System failed in attempt to create backup configuration file		
1153	Event	Configuration successfully restored from file backup	Warning	Configuration restore finished successfully		
1154	Event	Failure in configuration restoring from backup file	Warning	System failed in attempt to restore configuration from backup file	1. Configuration file system type mismatch 2. Invalid or corrupted configuration file	
1155	Event	Configuration restore operation cancelled	Warning	Restore operation cancelled because of user command or execution of another configuration management operation	Try again	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1156	Event	User issued command for transfer of configuration file	Warning	User command		
1157	Event	Configuration file transfer successful	Warning	Configuration file transfer successful		
1158	Event	Configuration file transfer failure	Warning	1. Communications failure. 2. File not found in server	1. Mark sure protocol details are properly configured. 2. Make sure file exists.	
1159	Event	Configuration file transfer in progress	Warning	File transfer started		
1163	Event	CLI configuration script activation started	Warning	User command		
1164	Event	CLI Configuration script executed successfully	Warning			
1165	Event	CLI Configuration script failed	Warning	1. Syntax Error. 2. Error returned by system during runtime	Verify script in the relevant line, and run again. Note that script may assume pre-existing configuration.	
1166	Event	Unit info file transfer status:	Warning			
1167	Event	Unit info file creation status:	Warning			
1169	Event	Configuration restore operation started	Warning	Restore operation started because of user command		

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1201	Alarm	Modem firmware file not found	Critical	Modem file is missing	1. Download software package. 2. Reset the system.	
1202	Alarm	Modem firmware was not loaded successfully	Critical	1. Modem firmware file is corrupted. 2. System failure.	1. Download software package. 2. Reset the system.	
1203	Event	Modem watch-dog reset event	Warning			
1301	Alarm	Radio MRMC script LUT file is corrupted	Critical	Damaged radio MRMC script LUT file	Download the specific radio MRMC script LUT file	
1302	Alarm	Radio MRMC script LUT file is not found	Critical	Missing radio MRMC script LUT file	Download the specific radio MRMC script LUT file	
1304	Alarm	Radio MRMC script modem file is corrupted	Critical	Damaged radio MRMC script modem file	Download the specific radio MRMC script LUT file	
1305	Alarm	Radio MRMC script modem file is not found	Critical	Missing radio MRMC script modem file	Download the specific radio MRMC script LUT file	
1308	Alarm	Radio MRMC file is corrupted	Critical	Damaged radio MRMC script LUT file	Download the specific radio MRMC script LUT file	
1309	Alarm	Radio MRMC RFU file is not found	Major	Missing radio MRMC RFU file	Download the specific radio MRMC script LUT file	
1312	Alarm	Radio MRMC script loading failed	Major	Damaged hardware module	Replace the radio hardware module	
1401	Alarm	Incompatible RFU TX calibration	Major	RFU calibration tables require SW upgrade	Upgrade IDU SW	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1501	Alarm	Remote communication failure	Critical	Fade in the link	Check the link performance	
1601	Alarm	IF loopback	Warning	User enabled IF loopback	Disable IF loopback	
1602	Alarm	IF synthesizer is unlocked.	Critical	<ol style="list-style-type: none"> 1. Extreme temperature condition. 2. HW failure. 	<ol style="list-style-type: none"> 1. Check installation. 2. Reset the RMC (Radio Modem Card) module. 3. Replace the RMC (Radio Modem Card). 	
1610	Alarm	Radio Receive Signal Level is below the configured threshold	Warning	<p>RSL is very low due to:</p> <ol style="list-style-type: none"> 1. Weather conditions, obstruction in antenna line of sight, antennae alignment. 2. Configured threshold needs to be adjusted.2. 	<ol style="list-style-type: none"> 1. Check for obstruction in link path. 2. Check the antennae alignment and link planning. 3. Recalculate the Path Loss and set the threshold accordingly. 4. Check link settings - Tx Power and Tx Frequency. 5. Hardware problem. 	
1651	Alarm	ATPC overridden: Tx level has been equal to the Max Tx level for a longer time than allowed	Warning	<p>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.</p>	<p>Correct the transmission levels. The alarm will be cleared only upon manual clearing.</p>	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1697	Alarm	Radio Unit extreme temperature	Warning	<ol style="list-style-type: none"> 1. Installation conditions 2. Defective RFU 	<ol style="list-style-type: none"> 1. Check installation conditions 2. Verify operation as per products specs 3. Replace RFU 	
1698	Alarm	Radio unit input voltage is too low	Warning	<ol style="list-style-type: none"> 1. Power supply output too low. 2. Power cable to RFU 	<ol style="list-style-type: none"> 1. Check power supply 2. Replace cable. 	
1699	Alarm	Radio unit input voltage is too high	Warning	Power supply output too high	<ol style="list-style-type: none"> 1. Check power supply 	
1700	Alarm	Radio unit not aligned to IDU	Critical	<ol style="list-style-type: none"> 1. FW alignment interrupted, power disruption, ODU cable malfunction. 2. Damaged ODU. 	<ol style="list-style-type: none"> 1. Reinitiate FW download by disable/ enable the corresponding port. 2. Replace RFU 	
1701	Alarm	Cable open	Major	Cable is not connected to RMC (Radio Modem Card) or RFU	<ol style="list-style-type: none"> 1. Check IF cable and connectors. 2. Verify that the N-Type connector inner pin is not spliced. 3. Replace RMC (Radio Modem Card). 4. Replace RFU. 	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1702	Alarm	Cable short	Major	Physical short at the IF cable	<ol style="list-style-type: none"> 1. Check IF cable and connectors. 2. Verify that the N-Type connector inner pin is not spliced. 3. Replace RMC (Radio Modem Card). 4. Replace RFU. 	
1703	Alarm	RFU communication failure	Warning	<ol style="list-style-type: none"> 1. Defective IF cable. 2. IF cable not connected properly. 3. Defective RMC (Radio Modem Card). 4. Defective RFU. 5. RFU software download in progress. 	<ol style="list-style-type: none"> 1. Check IF cable and connectors. 2. Verify that N-Type connector inner pin is not spliced. 3. Replace RMC (Radio Modem Card). 4. Replace RFU. <p>For a high power RF Unit:</p> <ol style="list-style-type: none"> 1. Check BMA connector on OCB 2. Check BMA connector on RFU. 	
1704	Alarm	RFU delay calibration failure 1	Warning	Defective RFU	<ol style="list-style-type: none"> 1. Reset the RMC (Radio Modem Card) / RFU. 2. Replace RFU. 	
1705	Alarm	RFU delay calibration failure 2	Warning	Calibration cannot be completed due to notch detection	Enter delay calibration value manually.	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1706	Alarm	RFU extreme temperature	Warning	<ol style="list-style-type: none"> 1. Installation conditions. 2. Defective RFU. 	<ol style="list-style-type: none"> 1. Check installation conditions. 2. Verify operation as per product's specs. 3. Replace RFU. 	
1707	Alarm	RFU is incompatible with ABC configuration	Warning	<ol style="list-style-type: none"> 1. The RFU type does not support the type of multi-carrier ABC the user has configured 	Replace the RFU with an RFU type that supports the configured Multi-Carrier ABC type.	
1708	Event	RFU frequency was set automatically	Warning	Defective RFU	<ol style="list-style-type: none"> 1. Check if problem repeats and if errors/alarms reported. 2. Replace RFU. 	
1709	Alarm	RFU hardware failure 1	Critical	Defective RFU.	Replace RFU.	
1710	Alarm	RFU hardware failure 2	Critical	Defective RFU.	Replace RFU.	
1711	Alarm	Low IF signal to RFU	Major	IF cable connection. Defective RFU. Defective RMC (Radio Modem Card).	<ol style="list-style-type: none"> 1. Check IF cable connectors. 2. Verify that N-Type connector inner pin is not spliced. 3. Replace RMC (Radio Modem Card). 4. Replace RFU. 	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1712	Alarm	Low IF signal from RFU	Warning	Low RX IF signal (140 MHz) from RFU.	<ol style="list-style-type: none"> 1. Check IF cable and connectors. 2. Verify that N-Type connector inner pin is not spliced. 3. Replace RMC (Radio Modem Card). 4. Replace RFU. 	
1713	Alarm	RFU PA extreme temperature	Warning	<ol style="list-style-type: none"> 1. Installation conditions. 2. Defective RFU. 	<ol style="list-style-type: none"> 1. Check installation conditions. 2. Replace RFU. 	
1721	Event	RFU reset	Major			
1722	Alarm	RFU loopback is active	Major	User has activated RFU loopback.	Disable RFU loopback.	
1723	Event	RFU mode changed to Combined	Indeterminate			
1724	Event	RFU mode changed to Diversity	Indeterminate			
1725	Event	RFU mode changed to Main	Indeterminate			
1726	Alarm	RFU power supply failure	Major	At least one of the RFU's power supply voltages is too low.	Replace RFU.	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1727	Alarm	RFU RX level out of range	Warning	RSL is very low, link is down.	<ol style="list-style-type: none"> 1. Check antenna alignment & link planning. 2. Check link settings (TX power, TX frequency). 3. Check antenna connections. 4. Replace local/remote RFU. 	
1728	Alarm	RFU RX level path1 out of range	Warning	<ol style="list-style-type: none"> 1. Improper installation. 2. Fading event. 3. Defective RFU. 	<ol style="list-style-type: none"> 1. Check that the fault is not due to rain/multi-path fading or lack of LOS. 2. Check link settings (TX power, TX frequency). 3. Check antenna alignment. 4. Check antenna connections. 5. Replace local/remote RFU. 	
1729	Alarm	RFU RX level path2 out of range	Warning	<ol style="list-style-type: none"> 1. Improper installation. 2. Fading event. 3. Defective RFU. 	<p>Check that the fault is not due to rain/multi-path fading or lack of LOS.</p> <p>Check link settings (TX power, TX frequency).</p> <p>Check antenna alignment.</p> <p>Check antenna connections.</p> <p>Replace local/remote RFU.</p>	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1730	Alarm	Radio unit communication failure	Critical	<ol style="list-style-type: none"> 1. Defective RFU cable 2. RFU cable not connected properly 3. Defective RIC (Radio Interface card.) 4. Defective RFU. 5. RFU initialization in progress. 6. RFU powered off. 	<ol style="list-style-type: none"> 1. Check RFU power supply. 2. Check RFU cable and connectors 3. Replace RIC (Radio Interface card) 4. Replace RFU 	
1731	Alarm	Power supply cable open	Major	Power is enabled but consumption is lower than threshold	<ol style="list-style-type: none"> 1. Check ETH cable and connectors 2. Verify RFU is connected 3. If RFU is connected with an optical cable, disable power interface. 	
1732	Alarm	Power supply cable short	Major	<ol style="list-style-type: none"> 1. Power is enabled but consumption reached the threshold. 2. Physical short at the ETH cable. 	<ol style="list-style-type: none"> 1. Check ETH cable and connectors 2. Replace RIC (Radio Interface Card) 3. Replace RFU 4. If RFU is connected with an optical cable, disable power interface. 	
1733	Alarm	RFU synthesizer unlocked	Major	At least one of the RFU synthesizers is unlocked	<p>Replace RFU.</p> <p>In XPIC mode, replace mate RFU as well.</p>	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1734	Alarm	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	Alarm	RFU TX Mute	Warning	RFU Transmitter muted by user	Unmute the RFU transmitter	
1736	Alarm	IDU SW does not support this type of RFU	Major	IDC SW does not support the RFU	Upgrade IDC SW	
1737	Event	Card was extracted from slot	Warning	Card was extracted from slot	NA	
1738	Alarm	Card is in Failure state	Major	Card is down as a result of card failure	1. Reset Card. Check if slot was disabled.	
1739	Alarm	FPGA Firmware file not found	Critical	There is no FPGA file found on the Main Board for the card on the slot	NA	
1740	Alarm	Download card firmware has failed	Major	Firmware download was unsuccessful.	1. Reset Card. 2. Download software package. Try to insert another Card.	
1741	Event	Card was inserted to slot	Warning	Card was inserted to slot	NA	
1742	Alarm	Card is in interconnection failure state	Major	Card is down as a result of card interconnection failure	1. Reset Card. Check if the slot was disabled.	
1743	Alarm	Expected Card is missing in slot	Major	1. Card is missing. Expected Card Type configured on empty slot.	1. Insert Expected Card. Clear Expected Card Type.	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1744	Alarm	This Card type is not supported in this slot	Major	The card is not on the Allowed Card Types list for this slot.	1. Reset. Insert Card belongs to Allowed Card Types list.	
1745	Event	Card operational state is Down	Indeterminate	Card state was change to Down state	NA	
1746	Event	Card operational state is Up	Indeterminate	Card state was change to Up state	NA	
1747	Event	Card operational state is Up with Alarms	Indeterminate	Card state was change to Up state but with Alarms indication	NA	
1748	Alarm	Unexpected Card Type in slot	Minor	Expected card type is different than the actual card type	1. Insert Expected Card. Change Expected Card Type.	
1749	Event	Slot was Disabled	Indeterminate	The user Disabled slot	NA	
1750	Event	Slot was Enabled	Indeterminate	The user Enabled slot	NA	
1751	Event	Card on slot was Reset	Indeterminate	The user Reset slot	NA	
1752	Event	FAN Card was extracted from slot	Warning	FAN Card was extracted from slot		
1753	Event	FAN failure	Major			
1754	Event	FAN Card was inserted to slot	Warning	FAN Card was inserted to slot		
1755	Alarm	FAN Card is missing in slot	Critical	1. FAN Card is missing. Slot enabled when empty.	1. Insert FAN Card. Disable slot.	
1756	Alarm	Extreme Temperature	Major	System Temperature not in allowed range.	NA	
1757	Alarm	FAN Card is in Failure state	Major	FAN Card is in Failure state	Change FAN Card	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1758	Event	Power Supply was extracted from slot	Warning	Power Supply was extracted from slot		
1759	Event	Power Supply was inserted to slot	Warning	Power Supply was inserted to slot.		
1760	Alarm	Power Supply is missing in slot	Major	1. Power Supply is missing. Slot enabled when empty.	1. Insert Power Supply. Disable slot.	
1761	Alarm	Over voltage	Major	System Power Voltage higher than allowed.	NA	
1762	Alarm	Under voltage	Major	System Power Voltage Lower than allowed.	NA	
1763	Alarm	The Main board firmware is not found	Warning			
1764	Alarm	Download Main Board firmware has failed	Major	Firmware download was unsuccessful.	1. Reset board. 2. Download software package. Try to insert another board.	
1765	Event	Main Board was reset	Warning			
1766	Event	RFU installation failure	Warning	1. Unsupported RFU type. 2. IDU-RFU communications problem. RFU failure.	1. Make sure RFU is supported by SW version. 2. Check IDU-RFU cable. Replace RFU.	
1767	Event	RFU installation in progress	Warning	User command		
1768	Event	RFU installation successfully completed	Warning	User command		

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1769	Event	Unit Perform Power up	Warning			
1770	Event	Unit performing power-up.	Major			
1771	Alarm	RFU cable error.	Major	Errors in signal from IDU to XCVR.	<ol style="list-style-type: none"> 1. Check the IF cable and connectors. 2. Verify that the N-Type/TNC connector inner pin is not spliced. 3. Replace RMC. 4. Replace XCVR. 	
1772	Alarm	Radio XPIC sync loss	Major	Signaling between RMCs (Radio Modem Cards) for XPIC functionality has failed	<ol style="list-style-type: none"> 1. Check that the RMCs are in allowed slots. 2. Populate the RMCs in different allowed location in the chassis. 3. Replace RMC/s. 4. Replace chassis. 	
1773	Alarm	Radio early warning.	Warning	The estimated radio BER (Bit Error Rate) is above 10E-12.	<ol style="list-style-type: none"> 1. Check link performance. 2. Check IF cable, and replace if required. 3. Replace XCVR. 4. Replace RMC. 	
1774	Alarm	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	Alarm	RFU software download is not possible.	Critical	Wrong type of XCVR, the XCVR hardware is METRO.	Replace the XCVR	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1776	Alarm	RMC hardware failure.	Major	RMC hardware failure of the clock distributor.	Replace the RMC.	
1780	Event	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	Event	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	Alarm	2.5Gbps mismatch configuration	Warning	The card can not function outside of an ABC group in 2.5Gbps mode.	Add the card to an ABC group, or change the Slot Section to 1Gbps.	
1783	Alarm	Radio remote fault indication (RFI)	Minor			
1790	Alarm	Hardware failure	Critical	An internal hardware failure has been detected by the system.	Replace the card or unit reporting the hardware failure.	
1800	Alarm	T3 sync interface Loss of Carrier	Major	1. Cable disconnected. Defective cable.	1. Check connection of the cable. Replace the cable.	
2001	Alarm	TDM-LIC has rebooted and is not in service now	Major	1. Recent TDM-LIC card reset; System malfunction.	1. Wait for card to reboot. Reset the TDM-LIC card.	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2002	Alarm	TDM-LIC configuration mismatch	Major	1. Recent warm reset of TDM-LIC; System malfunction.	Power cycle the TDM-LIC.	
2003	Alarm	Loss of Signal (LOS) on TDM-LIC's front panel clock port	Major	1. Line is not properly connected. External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment. Power cycle the TDM-LIC.	
2004	Alarm	Communication with TDM-LIC is disrupted in Host-Card direction	Minor	System malfunction	Reset the TDM-LIC.	
2005	Alarm	TDM-LIC hardware failure	Major	System malfunction	Reset the TDM-LIC.	
2006	Alarm	No communication with TDM-LIC	Major	System malfunction	Reset the TDM-LIC.	
2007	Alarm	Jitter-buffer-overflow alarm on TDM service	Major	Something wrong on TDM service synchronization	Check TDM service configuration	
2008	Alarm	Late-frame alarm on TDM service	Warning	Something wrong on TDM service	Check TDM service configuration	
2009	Alarm	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	Alarm	Malformed-frames alarm on TDM service	Major	1. Payload size does not correspond to the defined value. Mismatch in PT value in RTP header (if used)	Check TDM service configuration	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2011	Alarm	Misconnection alarm on TDM service	Major	Stray packets with wrong RTP configurations are received and dropped.	Check TDM service configuration	
2012	Alarm	Alarm Indication Signal (AIS) on TDM-LIC TDM port	Major	1. Line is not properly connected. External equipment is faulty.	1. Reconnect line. 2. Check line cables. Check external equipment.	
2013	Alarm	Loss Of Frame (LOF) on TDM-LIC TDM port	Major	1. Line is not properly connected. External equipment is faulty.		
2014	Alarm	Loss Of Multi-Frame (LOMF) on TDM-LIC TDM port	Major	1. Line is not properly connected. External equipment is faulty.	1. Reconnect line. 2. Check line cables. Check external equipment.	
2015	Alarm	Loopback on TDM-LIC TDM port	Warning	1. Line is not properly connected. External equipment is faulty.	1. Reconnect line. 2. Check line cables. Check external equipment.	
2016	Alarm	Loss Of Signal (LOS) on TDM-LIC TDM port	Major	1. Line is not properly connected. 2. Cable is faulty. 3. External equipment is faulty. Defective TDM-LIC.	1. Reconnect line. 2. Check line cables. Check external equipment.	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2017	Alarm	Remote Alarm Indication (RAI) on TDM-LIC TDM port	Minor	1. Line is not properly connected. External equipment is faulty.	1. Reconnect line. 2. Check line cables. Check external equipment.	
2018	Alarm	E1/DS1 Unexpected signal on TDM-LIC TDM port	Warning	1. Port is disabled. Line is connected to a disabled port.	1. Enable relevant port. Disconnect cable from relevant port.	
2021	Event	SSM received pattern change was discovered	Warning		No action is required.	
2022	Alarm	Excessive BER on TDM-LIC STM1/OC3 port	Major	1. Line is not properly connected. External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment. Power cycle the TDM-LIC.	
2023	Alarm	Loss Of Frame (LOF) on TDM-LIC STM1/OC3 port	Major	1. Line is not properly connected. External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment. Power cycle the TDM-LIC.	
2024	Alarm	Loopback on TDM-LIC STM1/OC3 port	Warning	1. Line is not properly connected. External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment. Power cycle the TDM-LIC.	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2025	Alarm	Loss Of Signal (LOS) on TDM-LIC STM1/OC3 port	Critical	1. Line is not properly connected. External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment. Power cycle the TDM-LIC.	
2026	Alarm	SFP is muted on TDM-LIC STM1/OC3 port	Warning			
2027	Alarm	SFP absent in TDM-LIC STM1/OC3 port	Critical	1. SFP is not properly installed. SFP is faulty.	1. Install SFP properly. Replace the card.	
2028	Alarm	SFP failure on TDM-LIC STM1/OC3 port	Critical	1. SFP is not properly installed. SFP is faulty.	1. Install SFP properly. Replace the card.	
2029	Alarm	SFP transmit failure on TDM-LIC STM1/OC3 port	Critical	1. SFP is not properly installed. SFP is faulty.	1. Install SFP properly. Replace the card.	
2030	Alarm	Signal Degrade on TDM-LIC STM1/OC3 port	Minor	1. Line is not properly connected. 2. SFP is not properly installed. 3. SFP is faulty. External equipment is faulty	1. Install SFP properly. 2. Reconnect line. 3. Check line cables. 4. Check external equipment. Power cycle the TDM-LIC.	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2031	Alarm	J0 Trace Identifier Mismatch on TDM-LIC STM1/OC3 port	Minor	<ol style="list-style-type: none"> 1. J0 misconfiguration. 2. Line is not properly connected. 3. SFP is not properly installed. External equipment is faulty.	<ol style="list-style-type: none"> 1. Make sure expected and received J0 match. 2. Install SFP properly. 3. Reconnect line. 4. Check line cables. 5. Check external equipment. Power cycle the TDM-LIC.	
2032	Event	SSM pattern received on TDM-LIC STM1/OC3 port changed	Warning			
2033	Alarm	Alarm Indication Signal (AIS) on TDM-LIC VC12/VT1.5	Minor	<ol style="list-style-type: none"> 1. Line is not properly connected. External equipment is faulty.	<ol style="list-style-type: none"> 1. Reconnect line. 2. Check line cables. 3. Check external equipment. Power cycle the TDM-LIC.	
2034	Alarm	Excessive BER on TDM-LIC VC12/VT1.5	Minor	<ol style="list-style-type: none"> 1. Line is not properly connected. External equipment is faulty.	<ol style="list-style-type: none"> 1. Reconnect line. 2. Check line cables. 3. Check external equipment. Power cycle the TDM-LIC.	
2035	Alarm	Loopback on TDM-LIC VC12/VT1.5	Warning	<ol style="list-style-type: none"> 1. Line is not properly connected. External equipment is faulty.	<ol style="list-style-type: none"> 1. Reconnect line. 2. Check line cables. 3. Check external equipment. Power cycle the TDM-LIC.	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2036	Alarm	Payload Mismatch Path (PLM) received on TDM-LIC VC12/VT1.5	Minor	1. Line is not properly connected. External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment. Power cycle the TDM-LIC.	
2037	Alarm	Remote Defect Indication (RDI) received on TDM-LIC VC12/VT1.5	Minor	1. Line is not properly connected. External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment. Power cycle the TDM-LIC.	
2038	Alarm	Signal Label Mismatch (SLM) received on TDM-LIC VC12/VT1.5	Minor	1. J2 misconfiguration. 2. Line is not properly connected. External equipment is faulty.	1. Make sure expected and receive J2 match. 2. Reconnect line. 3. Check line cables. 4. Check external equipment. Power cycle the TDM-LIC.	
2039	Alarm	Signal Degrade on TDM-LIC VC12/VT1.5	Minor	1. Line is not properly connected. External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment. Power cycle the TDM-LIC.	
2040	Alarm	Unequipped on TDM-LIC VC12/VT1.5	Minor	1. Line is not properly connected. External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment. Power cycle the TDM-LIC.	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2041	Alarm	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	Alarm	TDM-LIC card protection group lockout command is on	Minor	The user has issued a lockout command	Clear the lockout command	
2043	Alarm	A member of TDM-LIC card protection group is missing	Minor	TDM-LIC card is not installed in the shelf	Install the missing TDM-LIC card	
2044	Event	TDM-LIC card protection switch over, priority	Warning	1. 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	1. Check line cables. Check external equipment.	
2045	Alarm	Loss Of Pointer (LOP) received on TDM-LIC VC12/VT1.5	Minor	1. Line is not properly connected. External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment. Power cycle the TDM-LIC.	
2046	Event	Path protection switch on TDM service	Minor	1. Failure along service primary path. User command.	1. Check errors along primary path Check local service configuration.	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2047	Event	Path protection revertive switch on TDM service	Minor	Primary path has been operational for the duration of the defined WTR time	-	
2100	Alarm	Loss of Signal on Line Interface (LOS) on STM-1/OC-3 port.	Critical	<ol style="list-style-type: none"> 1. Line is not properly connected. 2. External equipment is faulty. 	<ol style="list-style-type: none"> 1. Reconnect line. 2. Check line cables. 3. Check external equipment. 	
2101	Alarm	Loss of Frame on Line Interface (LOF) on STM-1/OC-3 port.	Major	<ol style="list-style-type: none"> 1. Line is not properly connected. 2. External equipment is faulty. 	<ol style="list-style-type: none"> 1. Reconnect line. 2. Check line cables. 3. Check external equipment. 	
2102	Alarm	Alarm Indication Signal on Line Interface (MS-AIS/AIS-L) received.	Minor	<ol style="list-style-type: none"> 1. Line is not properly connected. 2. External equipment is faulty. 	<ol style="list-style-type: none"> 1. Reconnect line. 2. Check line cables. 3. Check external equipment. 	
2103	Alarm	Remote Defect Indication on Line Interface (MS-RDI/RDI-L) received.	Minor	External equipment is faulty.	Check external equipment.	
2104	Alarm	Loss of STM-1/OC-3 Frame on Radio Interface.	Major	<ol style="list-style-type: none"> 1. All channels in Multi Carrier ABC group are down. 2. Incorrect configuration on remote side. 	<ol style="list-style-type: none"> 1. Check link performance. 2. Check radio alarms for channel. 3. Check configuration. 	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2105	Alarm	MS-AIS/AIS-L on Radio Interface detected.	Minor	<ol style="list-style-type: none"> 1. Remote STM-1/OC-3 signal is missing (LOS/LOF/MS-AIS/AIS-L on remote STM-1/OC-3 interface). 2. STM-1/OC-3 Channel removed due to reduced radio capacity on remote side. 	Check remote equipment.	
2106	Alarm	MS-RDI/RDI-L on Radio Interface detected.	Minor	External equipment is faulty.	Check remote equipment.	
2107	Alarm	Loopback	Warning	Looping.	Remove looping.	
2108	Alarm	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	<ol style="list-style-type: none"> 1. Reduced capacity. 2. Fading 	<ol style="list-style-type: none"> 1. Check link performance. 2. Check radio alarms for channel. 	
2109	Alarm	PBRs insertion.	Warning	PRBS insertion on STM-1/OC-3 card.	Remove PRBS insertion.	
2110	Alarm	SFP absent on STM-1/OC-3 port.	Critical	<ol style="list-style-type: none"> 1. SFP is not properly installed. 2. SFP is faulty. 	<ol style="list-style-type: none"> 1. Install SFP properly. 2. Replace the card. 	
2111	Alarm	SFP Transmit Failure on STM-1/OC-3 port.	Critical	SFP is faulty.	<ol style="list-style-type: none"> 1. Replace SFP or insert SFP if it is not inserted correctly. 2. Replace the card. 	
2112	Alarm	SFP is muted on STM-1/OC-3 port.	Warning	SFP is muted by configuration.	Remove muting.	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2113	Alarm	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for channel.	
2114	Alarm	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for channel.	
2115	Alarm	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for channel.	
2116	Alarm	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for channel.	
2117	Alarm	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for channel.	
2118	Alarm	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for channel.	
2119	Alarm	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for channel.	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2200	Alarm	Multi Carrier ABC LOF.	Critical	All channels in Multi Carrier ABC group are down.	<ol style="list-style-type: none"> 1. Check link performance on all radio channels in Multi Carrier ABC group. 2. Check radio alarms for channels in Multi Carrier ABC group. 3. Check configuration of Multi Carrier ABC group. 	
2201	Alarm	Multi Carrier ABC bandwidth is below the threshold	Major	<ol style="list-style-type: none"> 1. One of the radio channels in the Multi Carrier ABC group has a lower capacity than expected 2. Minimum bandwidth threshold configuration is wrong 	<ol style="list-style-type: none"> 1. Check link performance on all radio channels in Multi Carrier ABC group 2. Check radio alarms for channels in Multi Carrier ABC group 3. Check configuration of Multi Carrier ABC group Minimum bandwidth threshold 	
2203	Alarm	LVDS RX Error Slot 2.	Major	Hardware failure between RMC and TCC cards.	<ol style="list-style-type: none"> 1. Replace RMC. 2. Replace TCC. 3. Replace chassis. 	
2204	Alarm	LVDS RX Error Slot 3.	Major	Hardware failure between RMC and TCC cards.	<ol style="list-style-type: none"> 1. Replace RMC. 2. Replace TCC. 3. Replace chassis. 	
2205	Alarm	LVDS RX Error Slot 4.	Major	Hardware failure between RMC and TCC cards.	<ol style="list-style-type: none"> 1. Replace RMC. 2. Replace TCC. 3. Replace chassis. 	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2206	Alarm	LVDS RX Error Slot 5.	Major	Hardware failure between RMC and TCC cards.	1. Replace RMC. 2. Replace TCC. 3. Replace chassis.	
2207	Alarm	LVDS RX Error Slot 6.	Major	Hardware failure between RMC and TCC cards.	1. Replace RMC. 2. Replace TCC. 3. Replace chassis.	
2208	Alarm	LVDS RX Error Slot 7.	Major	Hardware failure between RMC and TCC cards.	1. Replace RMC. 2. Replace TCC. 3. Replace chassis.	
2209	Alarm	LVDS RX Error Slot 8.	Major	Hardware failure between RMC and TCC cards.	1. Replace RMC. 2. Replace TCC. 3. Replace chassis.	
2210	Alarm	LVDS RX Error Slot 9.	Major	Hardware failure between RMC and TCC cards.	1. Replace RMC. 2. Replace TCC. 3. Replace chassis.	
2211	Alarm	LVDS RX Error Slot 10.	Major	Hardware failure between RMC and TCC cards.	1. Replace RMC. 2. Replace TCC. 3. Replace chassis.	
2212	Alarm	LVDS RX Error Slot 12.	Major	Hardware failure between RMC and TCC cards.	1. Replace RMC. 2. Replace TCC. 3. Replace chassis.	
2219	Alarm	Multi Carrier ABC Channel Id Mismatch Ch1.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2220	Alarm	Multi Carrier ABC Channel Id Mismatch Ch2.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.	
2221	Alarm	Multi Carrier ABC Channel Id Mismatch Ch3.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.	
2222	Alarm	Multi Carrier ABC Channel Id Mismatch Ch4.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.	
2223	Alarm	Multi Carrier ABC Channel Id Mismatch Ch5.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.	
2224	Alarm	Multi Carrier ABC Channel Id Mismatch Ch6.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.	
2225	Alarm	Multi Carrier ABC Channel Id Mismatch Ch7.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.	
2226	Alarm	Multi Carrier ABC Channel Id Mismatch Ch8.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.	
2235	Alarm	Multi Carrier ABC Channel Id Manual Disabled Ch1.	Warning	Admin state for channel is down.	Enable admin state for channel.	
2236	Alarm	Multi Carrier ABC Channel Id Manual Disabled Ch2.	Warning	Admin state for channel is down.	Enable admin state for channel.	
2237	Alarm	Multi Carrier ABC Channel Id Manual Disabled Ch3.	Warning	Admin state for channel is down.	Enable admin state for channel.	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2238	Alarm	Multi Carrier ABC Channel Id Manual Disabled Ch4.	Warning	Admin state for channel is down.	Enable admin state for channel.	
2239	Alarm	Multi Carrier ABC Channel Id Manual Disabled Ch5.	Warning	Admin state for channel is down.	Enable admin state for channel.	
2240	Alarm	Multi Carrier ABC Channel Id Manual Disabled Ch6.	Warning	Admin state for channel is down.	Enable admin state for channel.	
2241	Alarm	Multi Carrier ABC Channel Id Manual Disabled Ch7.	Warning	Admin state for channel is down.	Enable admin state for channel.	
2242	Alarm	Multi Carrier ABC Channel Id Manual Disabled Ch8.	Warning	Admin state for channel is down.	Enable admin state for channel.	
2300	Alarm	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.	All
2301	Event	Copy to mate started	Indeterminate	The copy-to-mate command has just begun!	This is a notification	All
2302	Event	Copy to mate completed	Indeterminate	The copy-to-mate command was completed.	This is a notification	All
3000	Event	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	Alarm	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.	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
3002	Alarm	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	Alarm	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	Alarm	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	Alarm	Card has one or more HW failures	Critical	One or more HW faults.	Replace card.	
4001	Alarm	Card can not function in 2.5Gbps mode.	Warning	The user set an expected card that does not support 2.5Gbps.	Change the Slot Section to 1Gbps.	
4002	Alarm	Card is not functional until chassis is reset	Warning	Slot is not in 10Gbps mode.	Reset chassis.	
5000	Event	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	Alarm	ERPI is either in protection state or forced protection state	Minor	Either user "force switch" command or one of the ring links has failed	Either clear force command or recover the link	
5002	Alarm	More than a single RPL is configured in a ring	Warning	User configuration	Reconfigure the RPL	
5003	Event	LLDP topology change	Warning	New neighbor	None	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
5004	Event	Security log upload started	Indeterminate	Security log upload started		
5005	Event	Security log upload failed	Indeterminate	Security log upload failed		
5006	Event	Security log upload succeeded	Indeterminate	Security log upload succeeded		
5010	Alarm	System is in sync force mode state	Warning			
5011	Event	The sync-source quality level was changed	Major			
5012	Alarm	System Synchronization Reference in Holdover Mode	Critical			
5013	Event	System Sync reference-to quality has change changed	Major			
5014	Alarm	The pipe interface clock-source in signal-interface table is not system-clock	Major			
5015	Alarm	The pipe is missing an edge interface	Major			
5016	Alarm	Pipe interface operational state is down	Major			
5017	Alarm	Pipe is invalid	Major			
5018	Alarm	1588TC is not operational	Major	System Failure	Reboot the unit	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
5030	soam-connectivity-failure	A connectivity failure in MA/MEG	Minor	Specific defect dependent: User configuration , connectivity loss.	Reconfigure the RPL.	
5031	soam-def-error-failure	Error CCM received	Major	Invalid CCMs has been received	Check the link in the traffic path	(1)
5032	soam-def-mac-failure	Remote mep MAC status not up	Minor	Remote MEP's associated MAC is reporting an error status	Check remote MEP's MAC status	(1)
5033	soam-def-rdi-failure	Mep Rdi received	Minor	Remote Defect indication has been received from remote MEP	Check the SOAM configurations	(1)
5034	soam-remote-ccm-failure	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 enbaled	(1)
5035	soam-def-xcon-failure	Cross Connect CCM received	Major	CCM from another MAID or lower MEG level have been received	Check MA/MEG and MEP configurations	(1)
5036	Event	1588-BC port state changed	Warning			
5037	Event	1588-BC BMCA has been updated.	Warning			

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
5038	Event	1588-BC outputs are squelched.	Warning			
5039	Event	1588-BC parent dataset has changed.	Warning			
5040	Event	1588-BC UTC offset value changed.	Warning			
5041	Event	1588-BC one of the leap seconds flags have changed.	Warning			
5042	Event	1588-BC message interval change detected.	Warning			
5043	Alarm	1588-BC announce message rate is below expected.	Major	Misconfiguration of the peer system.	Check the configuration of the peer system.	
5044	Alarm	1588-BC sync message rate is below expected.	Major	Misconfiguration of the peer system.	Check the configuration of the peer system.	
5045	Alarm	1588-BC delay request message rate is below expected.	Major	Misconfiguration of the peer system.	Check the configuration of the peer system.	
5046	Alarm	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.	
5100	Alarm	Master key mismatch cross over the link	Critical	Master Key was not set correctly.	Verify the Master Key.	(1)

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
5101	Alarm	No Master Key set, default value used	Warning	Crypto module has been enabled, but no Master Key has been loaded.	Set the Master Key.	(1)
5102	Alarm	Payload Encryption failure	Critical	<ol style="list-style-type: none"> 1. Radio LOF on Tx/Rx direction. 2. The session key does not match across the link. 3. The AES admin setting does not match across the link. 	<ol style="list-style-type: none"> 1. Validate the MSE on both sides of the link. 2. Validate the session key on both sides of the link. 3. Validate the AES admin setting on both sides of the link. 	(1)
5104	Event	Key Exchange Protocol progress, Traffic has been blocked	Indeterminate			(1)
5105	Event	Key Exchange Protocol initiated by remote side	Indeterminate			(1)
5106	Event	Key Zeroization command executed	Indeterminate			(1)
5107	Alarm	FIPS Bypass Self-Test failed	Critical	Disk failure		(1)
5108	Alarm	Power On Self-Test Failed	Critical	System failure	Reboot the unit.	(1)
5109	Alarm	Main board is not FIPS certified	Critical	Main Board used is not FIPS certified	Use a FIPS-certified TCC.	
5110	Alarm	Radio card is not FIPS certified	Major	Radio Card used is not FIPS certified	Use a FIPS-certified RMC.	
5111	Alarm	Radio crypto module fail	Critical	FIPS Radio Encryption Self-Test failed	Use different FIPS supported radio card	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
5112	Alarm	Radio encryption not supported	Major	No Payload Encryption Activation Key inserted	Insert suitable Activation Key and reboot the unit	
5030	Alarm	A connectivity failure in MA/MEG	Minor	Specific defect dependent: User configuration , connectivity loss.	Reconfigure the RPL.	
30007	Event	Clock source sharing failure	Critical	<ol style="list-style-type: none"> 1. Faulty coaxial cable between master and slave RFUs. 2. Hardware failure in Master RFU. 3. Hardware failure in Slave RFU. 	<ol style="list-style-type: none"> 1. Try re-initiation of MIMO. If still fails: 2. Replace faulty coaxial cable and reset Master RFU. 3. Replace faulty RFU. 	(2)
31000	Alarm	Insufficient conditions for MIMO	Critical	<ol style="list-style-type: none"> 1. Insufficient conditions for MIMO. 2. Hardware failure. 	<ol style="list-style-type: none"> 1. Make sure all cables between master and slave are connected (MIMO 4x4 only). 2. Replace faulty units and check that cables are plugged. 	(2)
31003	Alarm	Unsuitable hardware for MIMO	Critical	<ol style="list-style-type: none"> 1. Unsuitable hardware for MIMO operation requirements. 2. Dual carrier RFUs (MIMO 2x2 and 4x4). 3. RFUs with MIMO bus interface (MIMO 4x4). 4. Clock source sharing capability (MIMO 4x4). 	Make sure both RFUs are compatible for MIMO operation.	(2)

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
31004	Alarm	Unsuitable software configuration for MIMO	Critical	<ol style="list-style-type: none"> 1. Not all MIMO carriers are set to same radio script or script is not compatible for MIMO. 2. Radio TX and RX frequency is not identical on all MIMO carriers. 3. XPIC or Multi radio or ATPC features are enabled. 	<ol style="list-style-type: none"> 1. Load same MIMO compatible radio script to all MIMO carriers. 2. Set same TX and RX frequency on all MIMO carriers. 3. Disable XPIC, Multi radio and ATPC on all MIMO carriers. 	(2)
31005	Alarm	Clock source sharing cable unplugged	Critical	<ol style="list-style-type: none"> 1. Faulty coaxial cable between master and slave RFUs 2. Mate does not exist 	<ol style="list-style-type: none"> 1. Replace faulty coaxial cable and reset Master RFU. 2. Replace faulty RFU. 	(2)
31100	Alarm	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	Alarm	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	Alarm	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	Alarm	Agg 1 failed Bring-up procedure	Critical	Agg1 did not complete Bring-up successfully	Drop both Agg1 & Agg2 into single carrier mode (Pre-Init)	
31104	Alarm	Invalid ACM configuration	Critical	AMCC member have been set to fixed profile	Set AMCC member to adaptive ACM profiles	

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
5100	Alarm	Master key mismatch cross over the link	Critical	Master Key was not set correctly.	Verify the Master Key.	(1)
5101	Alarm	No Master Key set, default value used	Warning	Crypto module has been enabled, but no Master Key has been loaded.	Set the Master Key.	(1)
5102	Alarm	Payload REncryption failure	Critical	<ol style="list-style-type: none"> 1. Radio LOF on Tx/Rx direction. 2. The session key does not match across the link. 3. The AES admin setting does not match across the link. 	<ol style="list-style-type: none"> 1. Validate the MSE on both sides of the link. 2. Validate the session key on both sides of the link. 3. Validate the AES admin setting on both sides of the link. 	(1)
5103	Event	Key Exchange Protocol successfully finished	Indeterminate			(1)
5104	Event	Key Exchange Protocol initiated	Indeterminate			(1)
5105	Event	Key Exchange Protocol initiated by remote side	Indeterminate			(1)
5106	Event	Key Zeroization command executed	Indeterminate			(1)
5107	Alarm	FIPS Bypass Self-Test failed	Critical	Disk failure		(1)
5108	Alarm	Power On Self-Test Failed	Critical	System failure	Reboot the unit.	(1)
5033	Alarm	Communications	Critical	Radio script is incompatible to AMCC	Set AFR Script in both Agg1 & Agg2 carriers	(1)
5034	Alarm	Communications	Critical	Inconsistent MPMC script between members	Set the members to the appropriate MPMC script	(1)

Alarm ID	Type	Description	Severity	Probable Cause	Corrective Action	Notes
5035	Alarm	Communications	Critical	Inconsistent radio frequency	Set same radio TX/RX frequency on all AMCC carriers	(1)
5100	Alarm	Communications	Critical	Agg 1 failed Bring-up procedure	Drop both Agg1 & Agg2 into single carrier mode (Pre-Init)	(1)
5101	Alarm	Communications	Critical	Invalid ACM configuration	Set AMCC member to adaptive ACM profiles	(1)

(1) Supported by PTP 820C and PTP 820S

(2) Supported by PTP 820C only

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	

Term	Definition
CBS	Committed Burst Size
CCDP	Co-Channel Dual Polarization
CCITT	Comité Consultatif International de Télégraph et des Télécommunications (ITU)
CET	Carrier-Ethernet Transport
CFM	Connectivity Fault Management
CIR	Committed Information Rate
CLI	Command Line Interface
Clk	Clock
CODEC	Coder/Decoder
CoS	Class of Service
D	
DA	Destination Address
DC	Direct Current
DCB	Diversity Circulator Block
DCC	Data Communication Channel
DXC	Digital Cross Connect
DSCP	Differentiated Services Code Point
E	
EBS	Excess Burst Size
EIR	Excess Information Rate
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	

Term	Definition
FCC	Federal Communications Commission
FCS	Frame Check Sequence
FTP	File Transfer Protocol
G	
GbE	Gigabit Ethernet
GFP	Generic Framing Procedure (Procedure for mapping of Ethernet traffic over a transport network)
GND	Ground
GRE	Generic Routing Encapsulation
GTP	GPRS Tunneling Protocol
H	
HBER	High Bit Error Rate
HDLC	High-level Data Link Control
HF	High Frequency (3-30 MHz)
HSB	Hot-Standby
HTTP	Hypertext Transfer Protocol
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

Term	Definition
LBER	Low Bit Error Rate
LCAS	Link Capacity Adjustment Scheme
LED	Light Emitting Diode
LIU	Line Interface Unit
LLDP	Link Layer Discovery Protocol
LLF	Link Loss Forwarding
LMS	License Management System
LO	Local Oscillator
LOC	Loss of Carrier
LOF	Loss of Frame
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	

Term	Definition
PBB-TE	Provider Backbone Bridge Traffic Engineering
PBS	Peak Burst Rate
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

Term	Definition
SDWRR	Shaped Deficit Weighted Round Robin
SETS	Synchronous Equipment Timing Source
SFTP	Secure FTP
SLA	Service Level Agreements
SNCP	Simple Network Connection Protection
SNMP	Simple Network Management Protocol
SNP	Service Network Point
SNR	Signal to Noise Ratio
SNTP	Simple Network Time Protocol
SOH	Section OverHead (ETSI)
SONET	Synchronous Optical NETwork
SP	Service Point
SSH	Secured Shell (Protocol)
SSM	Synchronization Status Message
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

Term	Definition
WFQ	Weighted Fair Queue
WG	Waveguide
WRED	Weighted Random Early Detection
WRR	Weighted Round Robin
X	
XCVR	Transceiver (Transmitter/Receiver)
XMTR	Transmitter
XO	Crystal Oscillator
XPD	Cross Polar Differentiation
XPI	Cross Polarization Isolation
XPIC	Cross Polarization Interference Cancellation