Netronics

NetStream Diplo / Primo

System Manual

Revision: 2.01
Update: August 2016

This document contains information that is proprietary to Netronics Technologies Inc.

No part of this publication may be reproduced, modified, or distributed without prior written authorization of Netronics Networks.
This document is provided as is, without warranty of any kind.

Statement of Conditions

The information contained in this document is subject to change without notice.

Netronics shall not be liable for errors contained herein or for incidental or consequential damage in connection with the furnishing, performance, or use of this document or equipment supplied with it.

Information to User

Any changes or modifications of equipment not expressly approved by the manufacturer could void the user's authority to operate the equipment and the warranty for such equipment.

Regulatory Compliance

General Note

This system has achieved Type Approval in various countries around the world. This means that the system has been tested against various local technical regulations and found to comply. The frequency bands in which the system operates may be “unlicensed” and in these bands, the system can be used provided it does not cause interference.

FCC - Compliance

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generate, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications to this equipment not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

⚠ *Warning*

It is the responsibility of the installer to ensure that when using the outdoor antenna kits in the United States (or where **FCC** rules apply), only those antennas certified with the product are used. The use of any antenna other than those certified with the product is expressly forbidden by **FCC** rules 47 CFR part 15.204.

⚠ *Warning*

It is the responsibility of the installer to ensure that when configuring the radio in the United States (or where **FCC** rules apply), the Tx power is set according to the values for which the product is certified. The use of Tx power values other than those, for which the product is certified, is expressly forbidden by **FCC** rules 47 CFR part 15.204.

Caution

Outdoor units and antennas should be installed ONLY by experienced installation professionals who are familiar with local building and safety codes and, wherever applicable, are licensed by the appropriate government regulatory authorities. Failure to do so may void the product warranty and may expose the end user or the service provider to legal and financial liabilities. Resellers or distributors of this equipment are not liable for injury, damage or violation of regulations associated with the installation of outdoor units or antennas. The installer should configure the output power level of - antennas according to country regulations and antenna type.

Warning

Where Outdoor units are configurable by software to Tx power values other than those for which the product is certified, it is the responsibility of the Professional Installer to restrict the Tx power to the certified limits.

This product was tested with special accessories - indoor unit (IDU or PoE), FTP CAT 5e shielded cable with sealing gasket, 12 AWG grounding cable - which must be used with the unit to insure compliance.

Indoor Units comply with part 15 of the FCC rules. Operation is subject to the following two conditions:

- These devices may not cause harmful interference.
- These devices must accept any interference received, including interference that may cause undesired operation.

Canadian Emission Requirements for Indoor Units

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numẻrique de la classe B est conforme ả la norme NMB-003 du Canada.

China MII

Operation of the equipment is only allowed under China MII 5.8 GHz band regulation configuration with EIRP limited to 33 dBm (2 Watt).

India WPC

Operation of the equipment is only allowed under India WPC GSR-38 for 5.8GHz band regulation configuration.

Unregulated

In countries where the radio is not regulated the equipment can be operated in any regulation configuration, best results will be obtained using Universal regulation configuration.

Safety Practices

Applicable requirements of National Electrical Code (NEC), NFPA 70; and the National Electrical Safety Code, ANSI/IEEE C2, must be considered during installation.

Note

A Primary Protector is not required to protect the exposed wiring as long as the exposed wiring length is limited to less than or equal to 140 feet, and instructions are provided to avoid exposure of wiring to accidental contact with lightning and power conductors in accordance with NEC Sections 725-54 (c) and 800-30.

In all other cases, an appropriate Listed Primary Protector must be provided. Refer to Articles 800 and 810 of the NEC for details.

For protection of ODU against direct lightning strikes, appropriate requirements of NFPA 780 should be considered in addition to NEC.

For Canada, appropriate requirements of the CEC 22.1 including Section 60 and additional requirements of CAN/CSA-B72 must be considered as applicable.

Table of Contents

Safety Precautions & Declared Material

General Equipment Precautions

⚠ *Warning*

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

When working with a NS Diplo/Primo IDU, note the following risk of electric shock and energy hazard: Disconnecting one power supply disconnects only one power supply module. To isolate the unit completely, disconnect all power sources.

Machine noise information order - 3. GPSGV, the highest sound pressure level amounts to 70 dB (A) or less, in accordance with ISO EN 7779.
Static electricity may cause body harm, as well as harm to electronic components inside the device.
To prevent damage, before touching components inside the device, all electrostatic charge must be discharged from both personnel and tools.

High Frequency Electromagnetic Fields!

⚠ *Warning*

Exposure to strong high frequency electromagnetic fields may cause thermal damage to personnel. The eye (cornea and lens) is easily exposed.
Any unnecessary exposure is undesirable and should be avoided.
In radio-relay communication installations, ordinary setup for normal operation, the general RF radiation level will be well below the safety limit.
In the antennas and directly in front of them the RF intensity normally will exceed the danger level, within limited portions of space.
Dangerous radiation may be found in the neighborhood of open waveguide flanges or horns where the power is radiated into space.

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

ESD

⚠ *Caution*

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

Anyone responsible for the installation or maintenance of the NS Diplo/Primo IDU must use an ESD Wrist Strap.

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

Laser

⚠ *Caution*

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

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

When handling laser products the following precautions must be taken:

Never look directly into an open connector or optical cable.

Before disconnecting an optical cable from the optical transmitter, the power should be switched off. If this is not possible, the cable must be disconnected from the transmitter before it is disconnected from the receiver.

When the cable is reconnected it must be connected to the receiver before it is connected to the transmitter.

Special Requirements for North America

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

Note

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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

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

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

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

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

Warning

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

Special Requirements for Norway and Sweden:

Warning

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

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

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

Précautions générales relatives à l'équipement

Warning

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

L'usage de NS Diplo/Primo IDU s'accompagne du risque suivant d'électrocution et de danger électrique : le débranchement d'une alimentation électrique ne déconnecte qu'un module d'alimentation électrique. Pour isoler complètement l'unité, il faut débrancher toutes les alimentations électriques.

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

Allgemeine Vorsichtsmaßnahmen für die Anlage

Warning

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

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

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

RoHS Compliance Declaration

Electronic Information Products Declaration of Hazardous/Toxic Substances

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

About This Guide

This document explains how to configure and operate a NetStream Diplo/S/E system. This document applies to software version C8.0.7.

Note

The term **NS Primo/Diplo** in this document refers to all three products: the NetStream Diplo, NetStream Primo and NS Primo/DiploE.

The NS Primo/Diplo system is a modular system with a wide variety of configuration options. Not all configurations are described in this manual.

This document applies to NetStream OS version 8.3.

What You Should Know

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

Target Audience

This manual is intended for use by individuals responsible for configuration and administration of an NS Primo/Diplo system or network.

Related Documents

- NetStream Diplo Technical Description
- NetStream Diplo Installation Guide
- NetStream Primo Technical Description

- NetStream Primo Installation Guide
- NetStream Primo/DiploE Technical Description
- NetStream Primo/DiploE Installation Guide
- NetStream Primoeries MIB Reference
- NetStream Diplo/S/E Release Notes

Section I

Introduction

1. Introduction

This section includes:

- *NetStream Diplo System Overview*
- *NetStream Primo System Overview*
- ***Error! Reference source not found.***
- *PoE Injector Overview*
- *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:

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

Each of these systems can be used with a PoE Injector.

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

1.1. NetStream Diplo System Overview

NetStream Diplo represents a new generation of radio technology, capable of high bit rates and longer reach, and suitable for more diverse deployment scenarios. NetStream Diplo 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.

NetStream Diplo offers the convenience of an easy installation procedure, and full compatibility with NetStream Primo/Diplo ODU antennas. It is designed for use in network configurations which require high capacity solutions. NetStream Diplo covers the entire licensed frequency spectrum (6-42GHz) and offers a wide capacity range, including Header De-Duplication.

1.2. NetStream Primo System Overview

NetStream Primo is an all-outdoor solution for backhaul sites. It runs under NetStream OS, the high-performance, internetworking operating system, and supports all common features of the NS Primo/Diplo platform in a compact, environmentally friendly architecture.

NetStream Primo supports cutting edge capacity-boosting techniques, such as QPSK to 2048 QAM and Header De-Duplication, to offer a high capacity solution for every network topology and every site configuration. Its green, compact, all-outdoor configuration makes NetStream Primo ideal for any location.

1.3. PoE Injector Overview

The PoE injector box is designed to offer a single cable solution for connecting both data and the DC power supply to the NetStream Diplo, NetStream Primo, or NS Primo/DiploE system. To do so, the PoE injector combines 48VDC input and GbE signals via a standard CAT5E cable using a proprietary Netronics 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.

1.4. The Web-Based Element Management System

1.4.1. Introduction to the Web EMS

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

- **Configuration Management** – Enables you to view and define configuration data.
- **Fault Monitoring** – Enables you to view active alarms.
- **Performance Monitoring** – Enables you to view and clear performance monitoring values and counters.
- **Diagnostics and Maintenance** – Enables you to define and perform loop back tests and software updates.
- **Security Configuration** – Enables you to configure security features.
- **User Management** – Enables you to define users and user groups.

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

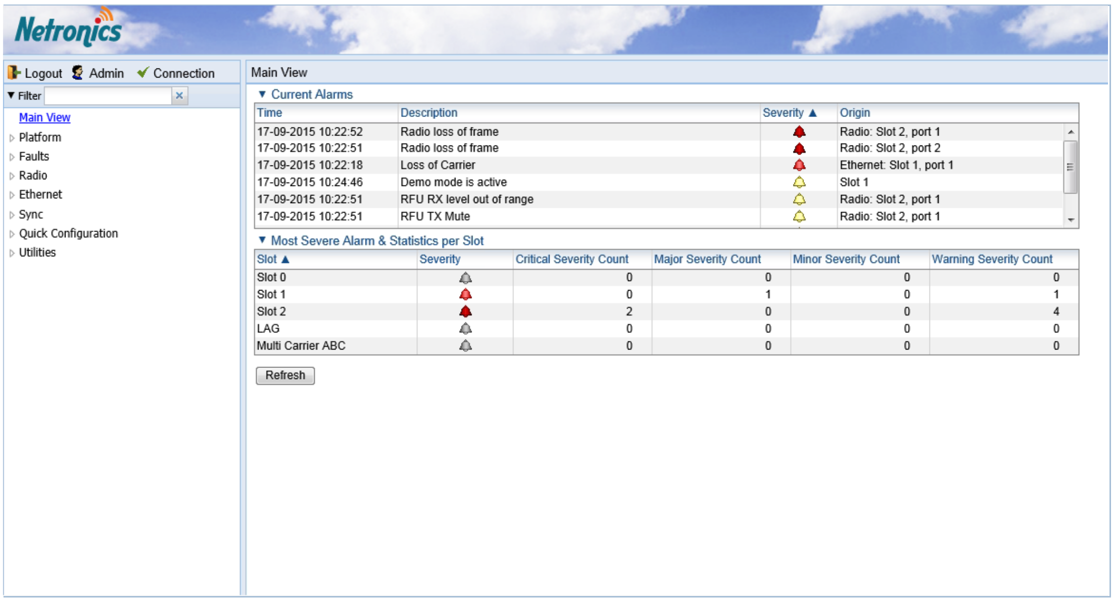
The alarms and system configuration details shown in this manual do not necessarily represent actual parameters and values on a fully operating NS Primo/Diplo system. Some of the pages and tasks described in this Manual may not be available to all users, based on the actual system configuration, activation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

1.4.2. Web EMS Page Layout

Each Web EMS page includes the following sections:

- The left section of the page displays the Web EMS menu tree:
  - Click ⊞ to display the sub-options under a menu item.
  - Click ⊟ to hide the sub-options under a menu item.
- The main section of the page provides the page's basic functionality.

Figure 1: Main Web EMS Page



Current Alarms

Time	Description	Severity ▲	Origin
17-09-2015 10:22:52	Radio loss of frame	🔴	Radio: Slot 2, port 1
17-09-2015 10:22:51	Radio loss of frame	🔴	Radio: Slot 2, port 2
17-09-2015 10:22:18	Loss of Carrier	🔴	Ethernet: Slot 1, port 1
17-09-2015 10:24:46	Demo mode is active	🟡	Slot 1
17-09-2015 10:22:51	RFU RX level out of range	🟡	Radio: Slot 2, port 1
17-09-2015 10:22:51	RFU TX Mute	🟡	Radio: Slot 2, port 1

Most Severe Alarm & Statistics per Slot

Slot ▲	Severity	Critical Severity Count	Major Severity Count	Minor Severity Count	Warning Severity Count
Slot 0	⚪	0	0	0	0
Slot 1	🔴	0	1	0	1
Slot 2	🔴	2	0	0	4
LAG	⚪	0	0	0	0
Multi Carrier ABC	⚪	0	0	0	0

Optionally, you can display a representation of the NS Primo/Diplo front panel by clicking either the arrow in the center or the arrow at the right of the bottom toolbar.

Figure 1: Displaying a Representation of the Front Panel

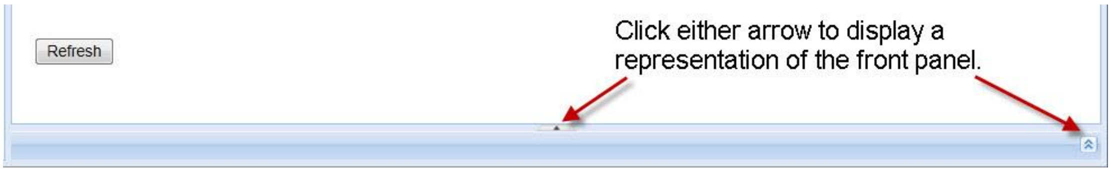
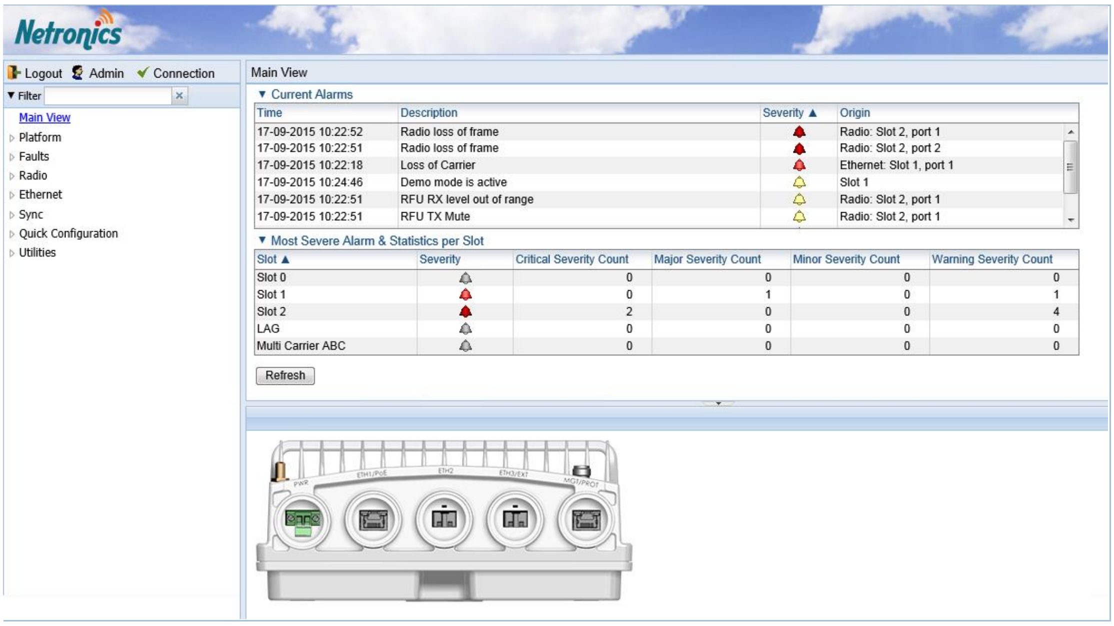

Refresh
Click either arrow to display a representation of the front panel.

Figure 2: Main Web EMS Page with Representation of Front Panel – NetStream Diplo/S



Main View

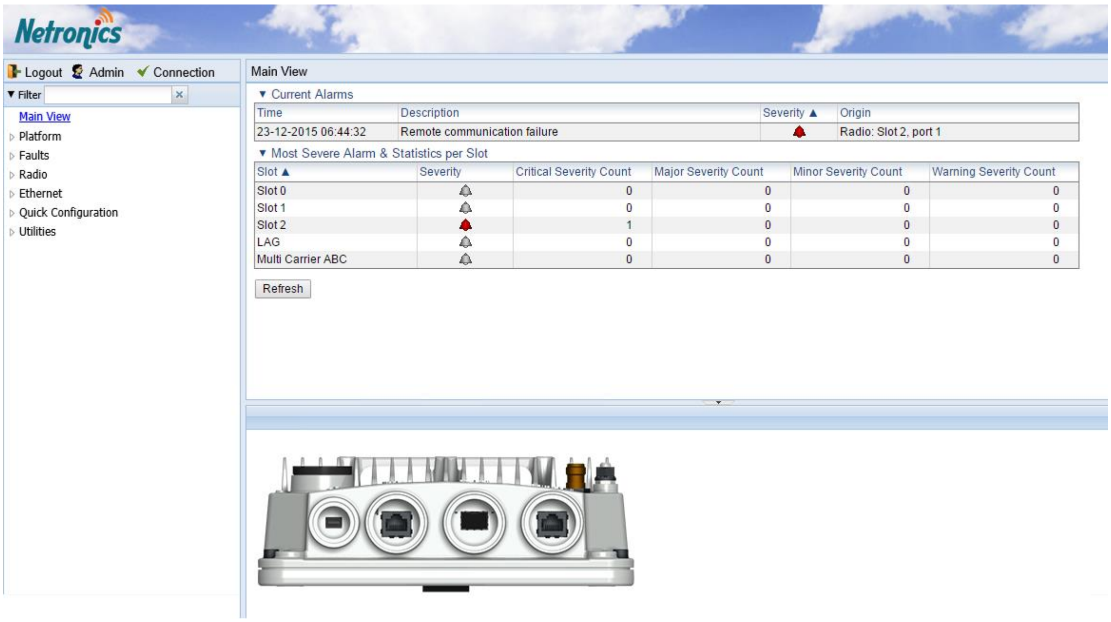
▼ Current Alarms

Time	Description	Severity ▲	Origin
17-09-2015 10:22:52	Radio loss of frame	🔴	Radio: Slot 2, port 1
17-09-2015 10:22:51	Radio loss of frame	🔴	Radio: Slot 2, port 2
17-09-2015 10:22:18	Loss of Carrier	🔴	Ethernet: Slot 1, port 1
17-09-2015 10:24:46	Demo mode is active	🟡	Slot 1
17-09-2015 10:22:51	RFU RX level out of range	🟡	Radio: Slot 2, port 1
17-09-2015 10:22:51	RFU TX Mute	🟡	Radio: Slot 2, port 1

▼ Most Severe Alarm & Statistics per Slot

Slot ▲	Severity	Critical Severity Count	Major Severity Count	Minor Severity Count	Warning Severity Count
Slot 0	⚪	0	0	0	0
Slot 1	🔴	0	1	0	1
Slot 2	🔴	2	0	0	4
LAG	⚪	0	0	0	0
Multi Carrier ABC	⚪	0	0	0	0

Figure 3: Main Web EMS Page with Representation of Front Panel – NS Primo/DiploE



Main View

▼ Current Alarms

Time	Description	Severity ▲	Origin
23-12-2015 06:44:32	Remote communication failure	🔴	Radio: Slot 2, port 1

▼ Most Severe Alarm & Statistics per Slot

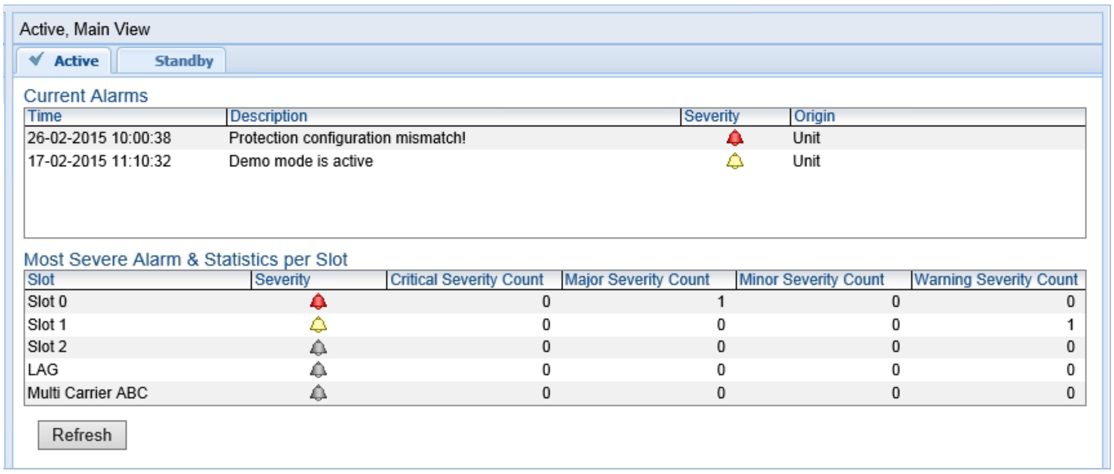
Slot ▲	Severity	Critical Severity Count	Major Severity Count	Minor Severity Count	Warning Severity Count
Slot 0	⚪	0	0	0	0
Slot 1	⚪	0	0	0	0
Slot 2	🔴	1	0	0	0
LAG	⚪	0	0	0	0
Multi Carrier ABC	⚪	0	0	0	0

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 HSB Radio Protection*.

Note

HSB protection is only available for NetStream Diplo and NetStream Primo.

Figure 4: Main Web EMS Page with Active and Standby Tabs



Active, Main View

Current Alarms

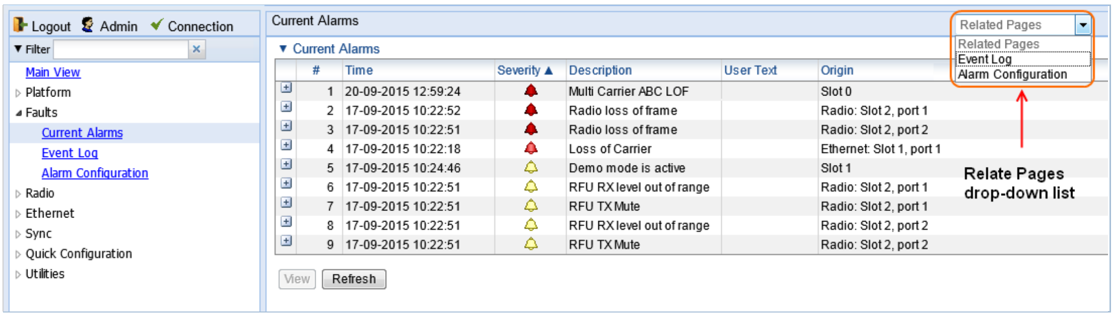
Time	Description	Severity	Origin
26-02-2015 10:00:38	Protection configuration mismatch!	🔔	Unit
17-02-2015 11:10:32	Demo mode is active	🔔	Unit

Most Severe Alarm & Statistics per Slot

Slot	Severity	Critical Severity Count	Major Severity Count	Minor Severity Count	Warning Severity Count
Slot 0	🔔	0	1	0	0
Slot 1	🔔	0	0	0	1
Slot 2	🔔	0	0	0	0
LAG	🔔	0	0	0	0
Multi Carrier ABC	🔔	0	0	0	0

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 5: Related Pages Drop-Down List



▼ Current Alarms

	#	Time	Severity ▲	Description	User Text	Origin
⊞	1	20-09-2015 12:59:24	🔔	Multi Carrier ABC LOF		Slot 0
⊞	2	17-09-2015 10:22:52	🔔	Radio loss of frame		Radio: Slot 2, port 1
⊞	3	17-09-2015 10:22:51	🔔	Radio loss of frame		Radio: Slot 2, port 2
⊞	4	17-09-2015 10:22:18	🔔	Loss of Carrier		Ethernet: Slot 1, port 1
⊞	5	17-09-2015 10:24:46	🔔	Demo mode is active		Slot 1
⊞	6	17-09-2015 10:22:51	🔔	RFU RX level out of range		Radio: Slot 2, port 1
⊞	7	17-09-2015 10:22:51	🔔	RFU TX Mute		Radio: Slot 2, port 1
⊞	8	17-09-2015 10:22:51	🔔	RFU RX level out of range		Radio: Slot 2, port 2
⊞	9	17-09-2015 10:22:51	🔔	RFU TX Mute		Radio: Slot 2, port 2

1.5. 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: NS Primo/Diplo Web EMS Menu Hierarchy – Platform Menu

Sub-Menus	For Further Information
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 HSB Radio Protection*
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	*Configuring SNMP*
Management > SNMP > Trap Managers	*Configuring Trap Managers*
Management > SNMP > V3 Users	*Configuring SNMP*
Software > Timer Parameters	*Configuring a Timed Installation*
Software > Versions	*Viewing Current Software Versions*
Software > Download & Install	*Downloading and Installing Software*
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*
Activation Key > Activation Key Overview	*Displaying a List of Activation-Key-Enabled Features*
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* *Blocking Telnet Access*

Table 2: NS Primo/Diplo Web EMS Menu Hierarchy – Faults Menu

Sub-Menus	For Further Information
Current alarms	*Viewing Current Alarms*
Event Log	*Viewing the Event Log*
Alarm Configuration	*Editing Alarm Text and Severity*

Table 3: NS Primo/Diplo Web EMS Menu Hierarchy – Radio Menu

Sub-Menus	For Further Information
Radio Parameters	*Configuring the Radio Parameters*
Remote Radio Parameters	*Configuring the Remote Radio Parameters*
Radio Thresholds	*Configuring Radio Thresholds*
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	Reserved for future use
PM & Statistics > Combined	Reserved for future use
PM & Statistics > Aggregate	*Displaying Modem BER (Aggregate) PMs*
PM & Statistics > MSE	*Displaying Modem MSE PMs*
PM & Statistics > XPI	*Displaying XPI PMs*
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*
Groups > XPIC	*Configuring XPIC*
Groups > Multi Radio	*Configuring Multi-Carrier ABC*
Groups > MIMO	*Configuring MIMO and Space Diversity*

Table 4: NS Primo/Diplo Web EMS Menu Hierarchy – Ethernet Menu

Sub-Menus	For Further Information
General Configuration	*Setting the MRU Size and the S-VLAN Ethertype*
Services	*Configuring Ethernet Service(s)*
Interfaces > Physical Interfaces	*Configuring Ethernet Interfaces*
Interfaces > Logical Interfaces	*Configuring Ingress Path Classification on a Logical Interface* *Assigning Policers to Interfaces* *Configuring the Ingress and Egress Byte Compensation* *Assigning WRED Profiles to Queues* *Assigning a Queue Shaper Profile to a Queue* *Assigning a 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 > Automatic State Propagation	*Configuring Automatic State Propagation*
Interfaces > Groups > LAG	*Configuring Link Aggregation (LAG)*
PM & Statistics > RMON	*RMON 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*
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*
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)*

Table 5: NS Primo/Diplo Web EMS Menu Hierarchy – Sync Menu

Note

For NS Primo/DiploE, synchronization is planned for future release and the Sync menu does not appear.

Sub-Menus	For Further Information
SyncE Regenerator	*Configuring SyncE Regenerator*
Sync Source	Reserved for future use
Outgoing Clock	Reserved for future use
1588-TC	Reserved for future use

Table 6: NS Primo/Diplo Web EMS Menu Hierarchy – Quick Configuration Menu

Sub-Menus	For Further Information
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*
Link Setup (PIPE) > Multi Carrier ABC > 2 + 0	*Configuring a 2+0 Multi-Carrier ABC Link Using the Quick Configuration Wizard*

Table 7: NS Primo/Diplo Web EMS Menu Hierarchy – Utilities Menu

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

Section II

Web EMS Configuration

2. Getting Started

This section includes:

- *Assigning IP Addresses in the Network*
- *Establishing a Connection*
- *Logging on*
- *Changing Your Password*
- *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*

2.1. Assigning IP Addresses in the Network

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

By default, a new NS Primo/Diplo unit has the following IP settings:

- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0

Note

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

2.2. Establishing a Connection

Connect the NS Primo/Diplo unit to a PC by means of a TP cable. The cable is connected to the MGT port on the NS Primo/Diplo 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.

2.2.1. PC Setup

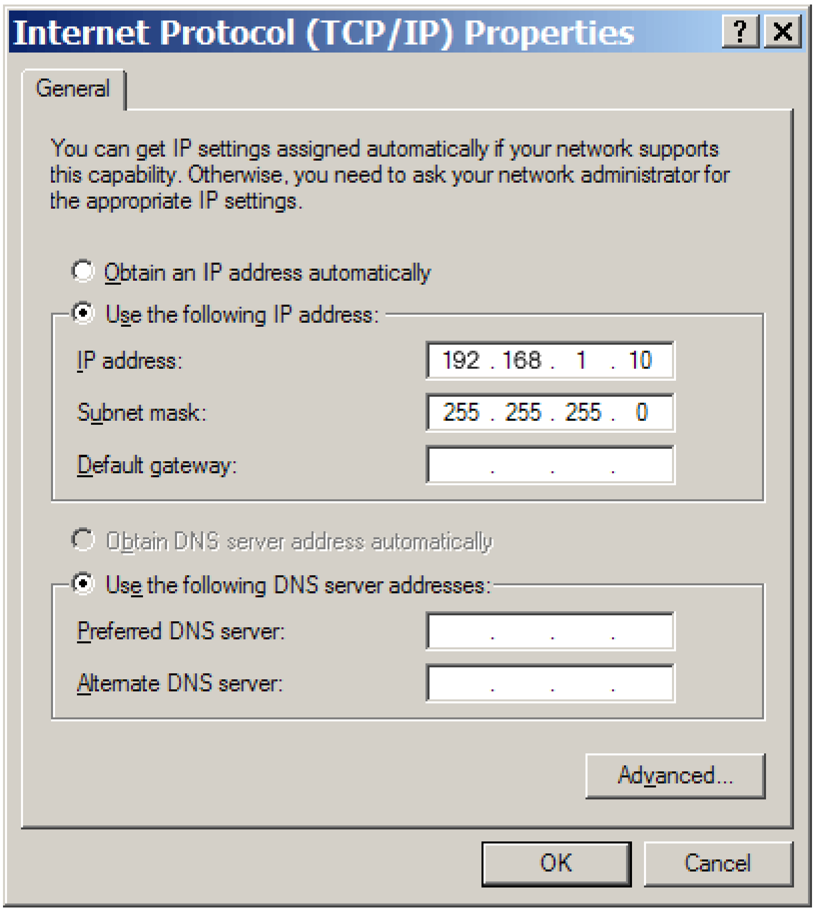
To obtain contact between the PC and the NS Primo/Diplo unit, it is necessary to configure an IP address on the PC within the same subnet as the NS Primo/Diplo unit. The default NS Primo/Diplo IP address is 192.168.1.1. Set the PC address to e.g. 192.168.1.10 and subnet mask to 255.255.255.0. Note the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

Note

The NS Primo/Diplo 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 6: Internet Protocol Properties Window



Internet Protocol (TCP/IP) Properties

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

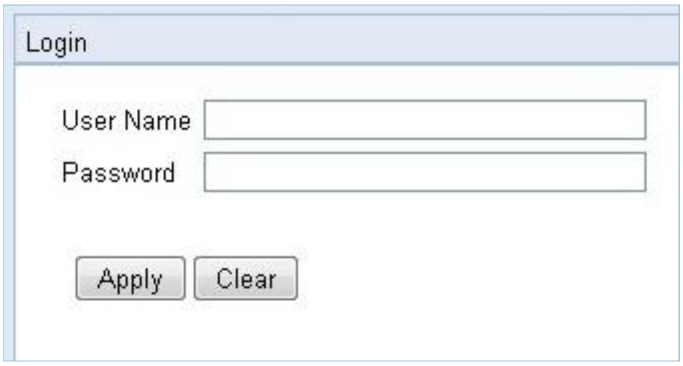
Alternate DNS server: . . .

2.3. 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 7: Login Page



3 In the Login window, enter the following:

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

4 Click **Apply**.

2.3.1. 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 Netronics Networks proprietary Ethernet cable. This cable should be ordered from Netronics Networks, according to the following table.

Cables for Direct CPU Connection

Product	Cable Marketing Model	Cable Description
NetStream Diplo and NetStream Primo	NS Primo/Diplo_MIMO_Prot_mng_spltr	CABLE,RJ45M TO 2xRJ45F, 1.0M, WITH GLANDS, UV PROTECTED
NS Primo/DiploE	NS Primo/Diplo_Mini-MNG-CBL	CABLE,MiniDP TO RJ45F,0.2M,FOR FIELD DEBUG

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:

- NetStream Diplo and NetStream Primo: The MGT port on the NS Primo/Diplo unit.
- NS Primo/DiploE: The EXT port on the NS Primo/Diplo unit.

3 Connect the single end of the cable to the LAN port on the PC.
4 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.)

Note

For NS Primo/DiploE, there is no LED to indicate whether the connection has been established.

5 The system will prompt you for a user name and password (see *Figure 7*).
6 Enter the default user name and password:

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

7 Click **Apply**.
8 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*.

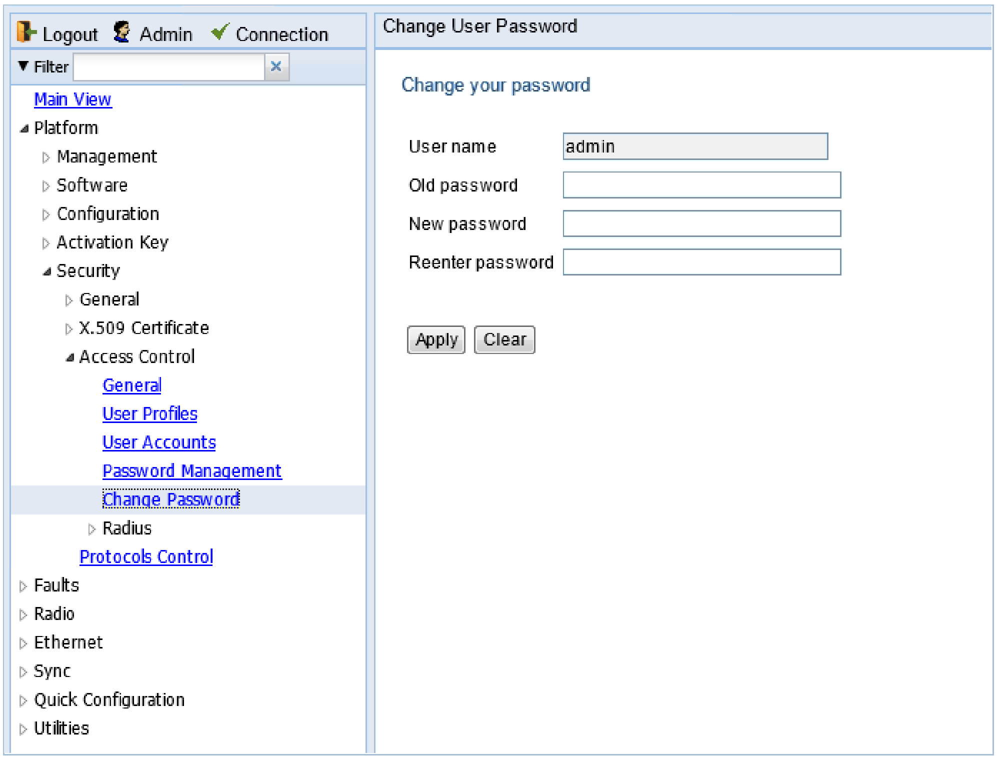
2.4. Changing Your Password

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

To change your password:

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

Figure 8: Change User Password Page



Change User Password

Change your password

User name: admin

Old password:

New password:

Reenter password:

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

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

- Password length must be at least eight characters.
- Password must include characters of at least three of the following character types: lower case letters, upper case letters, digits, and special characters. 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 Netronics Customer Support. It is strongly recommended to change this password.

2.5. Configuring In-Band Management

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

Each NetStream Diplo 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*.

2.6. Changing the Management IP Address

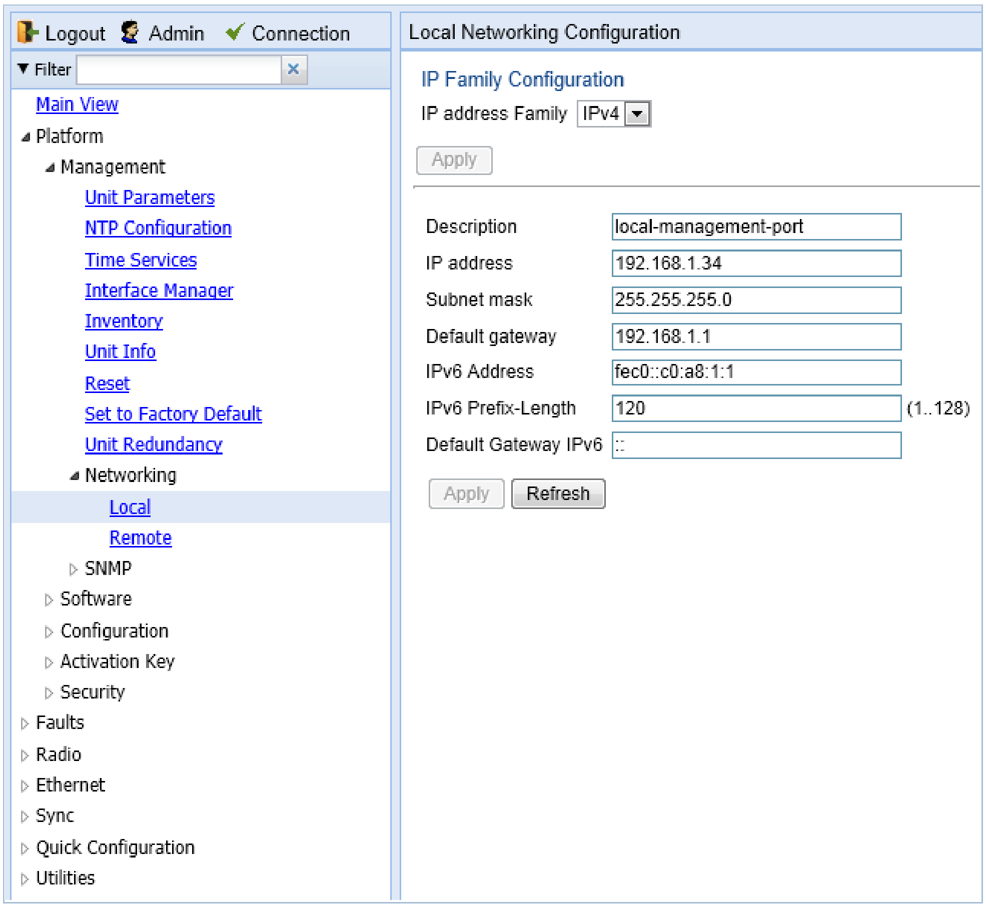
Related Topics:

- *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 9: Local Networking Configuration Page



Local Networking Configuration

IP Family Configuration

IP address Family: IPv4

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	::

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**.

2.7. Configuring the Activation Key

This section includes:

- *Activation Key Overview*
- *Viewing the Activation Key Status Parameters*
- *Entering the Activation Key*
- *Activating Demo Mode*
- *Displaying a List of Activation-Key-Enabled Features*

2.7.1. Activation Key Overview

NS Primo/Diplo 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 NS Primo/Diplo 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.

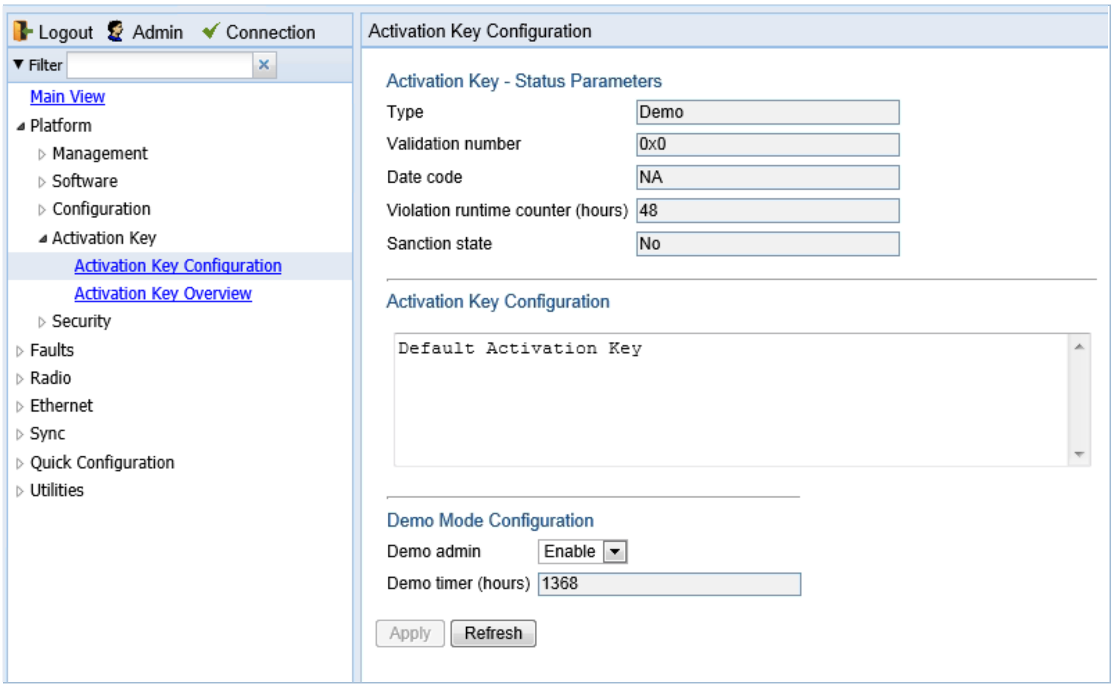
Demo mode is available, which enables all features for 60 days. When demo mode expires, the most recent valid activation key goes into effect. The 60-day period is only counted when the system is powered up. 10 days before demo mode expires, an alarm is raised indicating that demo mode is about to expire.

2.7.2. Viewing the Activation Key Status Parameters

To display the current activation key status parameters:

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

Figure 10: Activation Key Configuration Page



Activation Key Configuration

Activation Key - Status Parameters

Type: Demo

Validation number: 0x0

Date code: NA

Violation runtime counter (hours): 48

Sanction state: No

Activation Key Configuration

```
Default Activation Key
```

Demo Mode Configuration

Demo admin: Enable

Demo timer (hours): 1368

Table 8: Activation Key Status Parameters

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

2.7.3. Entering the Activation Key

To enter a new activation key:

1 Select **Platform > Activation Key > Activation Key Configuration**. The Activation Key Configuration page opens (*Figure 10)*.

2 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.

3 Click **Apply**.

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

2.7.4. Activating Demo Mode

To activate demo mode:

1 Select **Platform > Activation Key > Activation Key Configuration**. The Activation Key Configuration page opens (*Figure 10*).
2 In the **Demo admin** field, select **Enable**.
3 Click **Apply**.

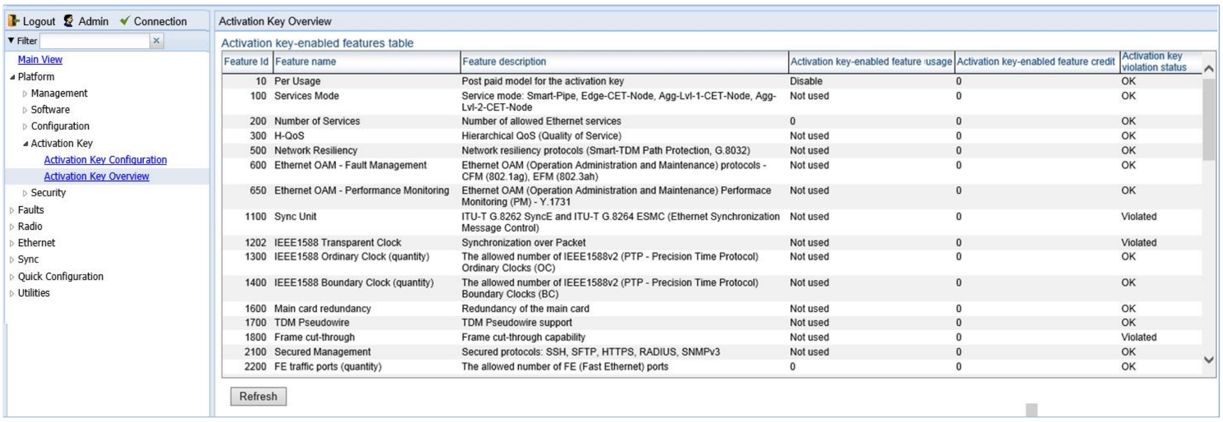
The **Demo timer** field displays the number of hours that remain before demo mode expires.

2.7.5. Displaying a List of Activation-Key-Enabled Features

To display the status of activation key coverage for features and capacities in the NS Primo/Diplo:

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

Figure 11: Activation Key Overview Page



Activation key-enabled features table

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) Performace 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 NS Primo/Diplo, and indicates the activation key status of each feature according to the activation key currently implemented in the unit.

Note

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

Table 9: Activation Key-Enabled-Features Table Parameters

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

2.8. Setting the Time and Date (Optional)

Related Topics:

- *Configuring NTP*

NS Primo/Diplo 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 NS Primo/Diplo unit holds the UTC offset and daylight savings time information for the location of the unit. Each management unit presenting the information uses its own UTC offset to present the information with the correct time.

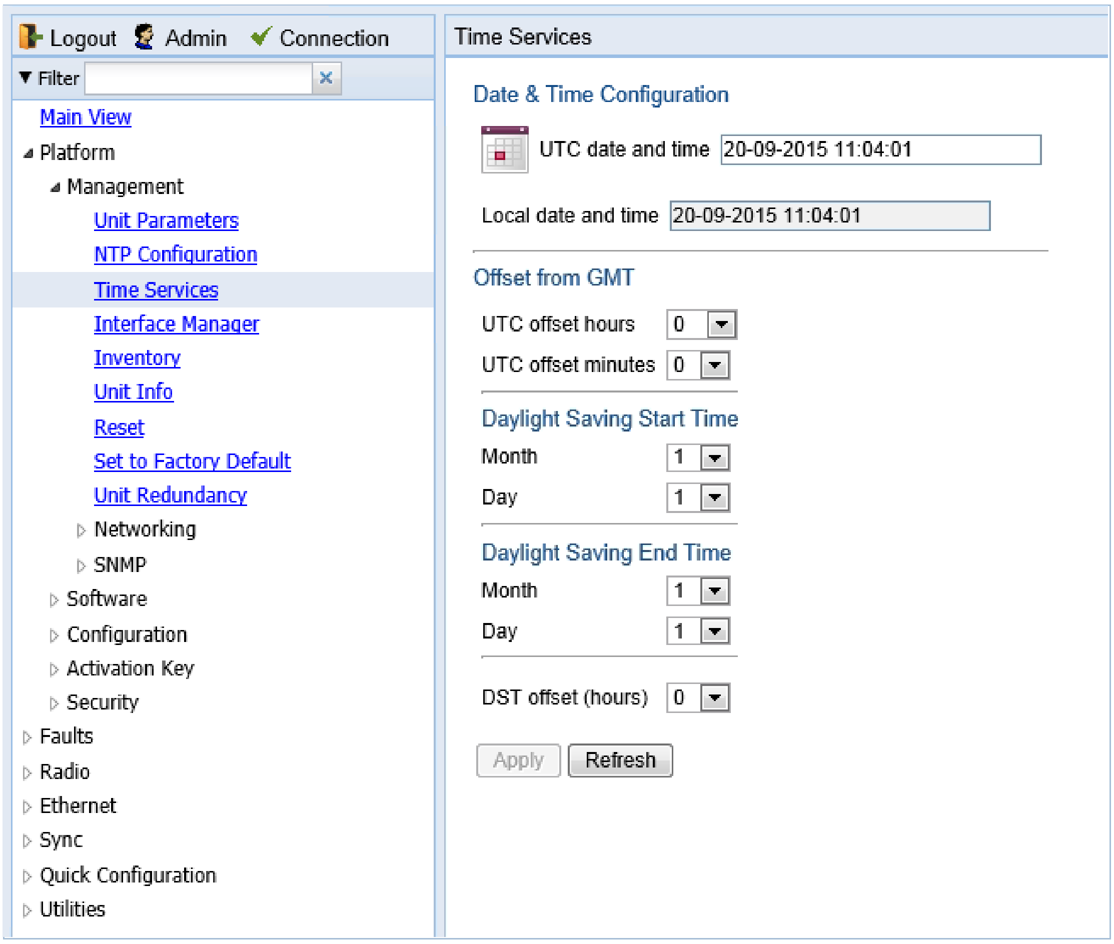
Note

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

To display and configure the UTC parameters:

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

Figure 12: Time Services Page



Date & Time Configuration

UTC date and time 20-09-2015 11:04:01

Local date and time 20-09-2015 11:04:01

Offset from GMT

UTC offset hours 0

UTC offset minutes 0

Daylight Saving Start Time

Month 1

Day 1

Daylight Saving End Time

Month 1

Day 1

DST offset (hours) 0

2 Configure the fields listed in *Table 10*.

3 Click **Apply**.

Table 10: Time Services Parameters

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

2.9. Enabling the Interfaces (Interface Manager)

By default:

- Ethernet traffic interfaces are disabled and must be manually enabled.
- The Ethernet management interface is enabled.
- Radio interfaces are enabled.

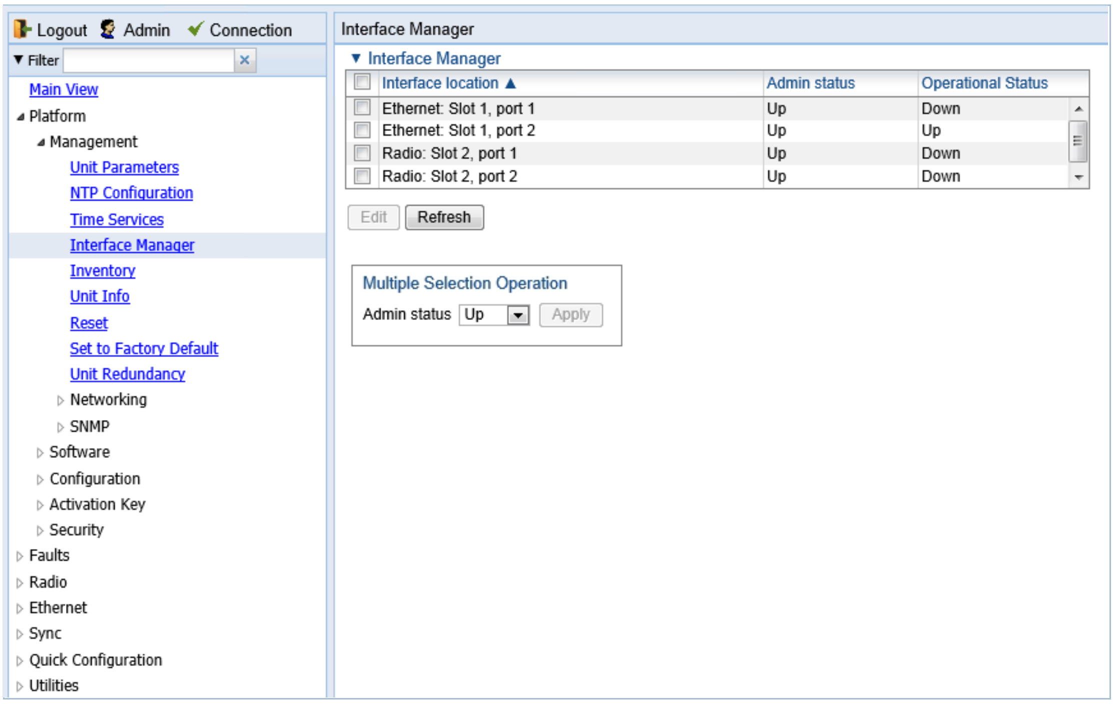
Note

NetStream Primo and NS Primo/DiploE 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 13: Interface Manager Page



□	Interface location ▲	Admin status	Operational Status
□	Ethernet: Slot 1, port 1	Up	Down
□	Ethernet: Slot 1, port 2	Up	Up
□	Radio: Slot 2, port 1	Up	Down
□	Radio: Slot 2, port 2	Up	Down

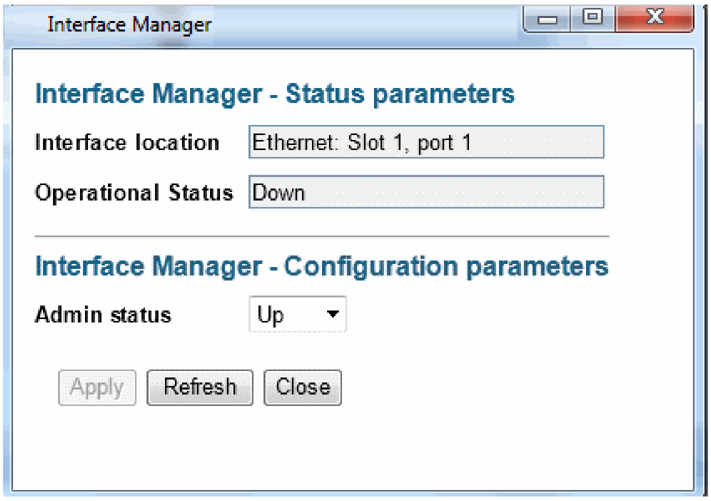
Admin status Up

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 14: Interface Manager – Edit Page



Interface Manager - Status parameters

Interface location: Ethernet: Slot 1, port 1

Operational Status: Down

Interface Manager - Configuration parameters

Admin status: Up

3 In the **Admin status** field, select **Up** to enable the interface or **Down** to disable the interface.

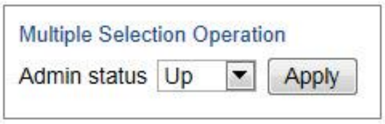
4 Click **Apply**, then **Close**.

To enable or disable multiple interfaces:

1 Select the interfaces in the Interface Manager table or select all the interfaces by selecting the check box in the top row.

2 In the **Multiple Selection Operation** section underneath the Interface Manager Table, select **Admin status – Up** or **Admin status – Down**.

Figure 15: Multiple Selection Operation Section (Interface Manager Page)



Multiple Selection Operation

Admin status: Up

3 Click **Apply**.

Note

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

2.10. 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.

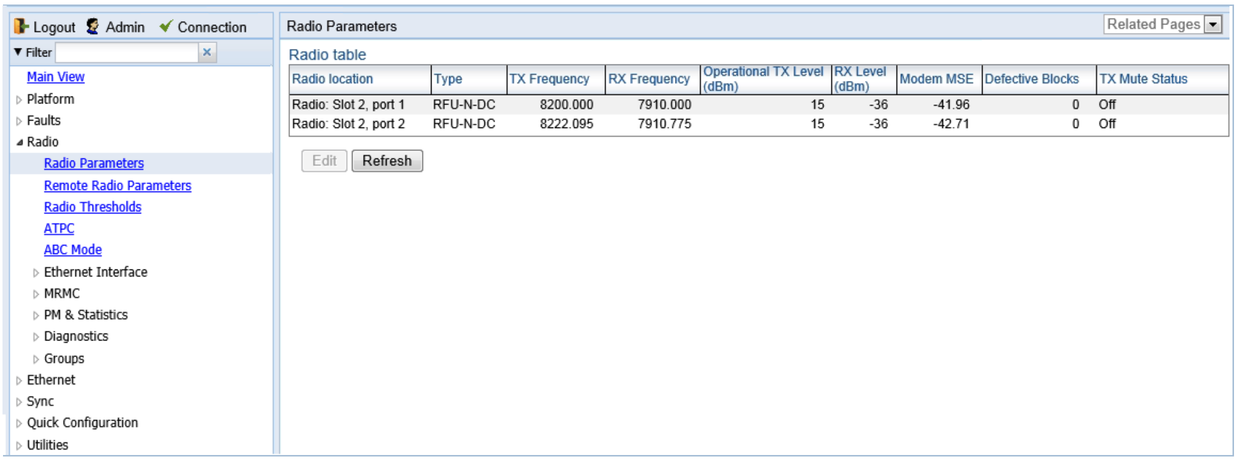
You can do these tasks, perform other radio configuration tasks, and display the radio parameters in the Radio Parameters page.

To configure the radio parameters:

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

   - For NetStream Diplo units, the Radio Parameters page initially displays a table as shown in *Figure 16*.
   - For NetStream Primo units and NS Primo/DiploE units, a page appears, similar to *Figure 17* (which shows an NetStream Diplo page).

Figure 16: Radio Parameters Page – NetStream Diplo

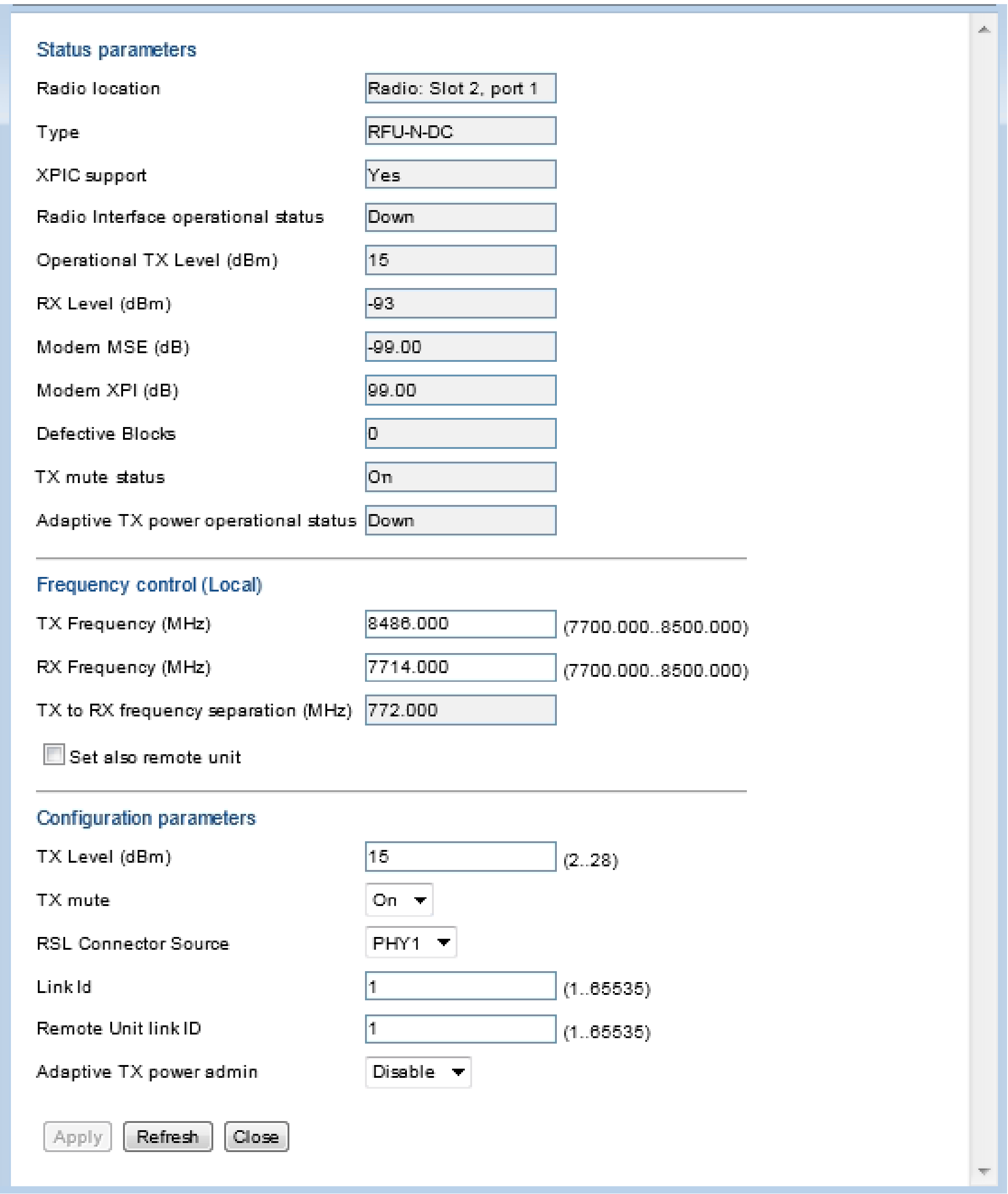


Radio table

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

2 For NetStream Diplo units, select the carrier in the Radio table (see *Figure 16*) and click **Edit**. A separate Radio Parameters page opens. The page is essentially identical to the NS Primo/DiploE and NetStream Primo page, except for the addition of a **Radio location** parameter.

Figure 17: Radio Parameters Page Per Carrier – NetStream Diplo



Status parameters

Radio location	Radio: Slot 2, port 1
Type	RFU-N-DC
XPIC support	Yes
Radio Interface operational status	Down
Operational TX Level (dBm)	15
RX Level (dBm)	-93
Modem MSE (dB)	-99.00
Modem XPI (dB)	99.00
Defective Blocks	0
TX mute status	On
Adaptive TX power operational status	Down

Frequency control (Local)

TX Frequency (MHz)	8486.000	(7700.000..8500.000)
RX Frequency (MHz)	7714.000	(7700.000..8500.000)
TX to RX frequency separation (MHz)	772.000	

□ Set also remote unit

Configuration parameters

TX Level (dBm)	15	(2..28)
TX mute	On	
RSL Connector Source	PHY1	
Link Id	1	(1..65535)
Remote Unit link ID	1	(1..65535)
Adaptive TX power admin	Disable	

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.

iv In the **Remote Unit Link ID** field, enter the same link identifier you entered in the **Link ID** field. This ensures that the Link ID is configured identically on both sides of the link.

v In the **Adaptive TX power admin** field, select **Enable** if you wish the NS Primo/Diplo 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*.

2.11. 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**.

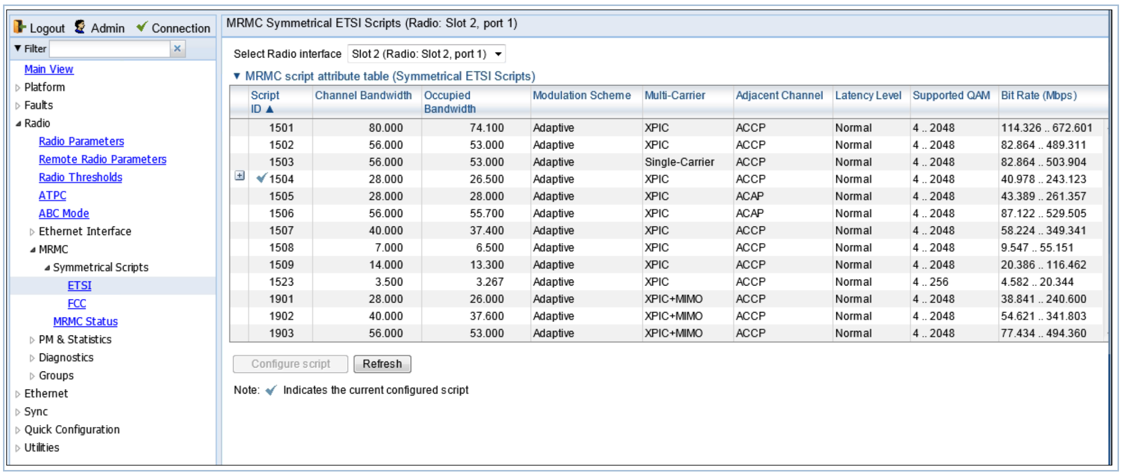
The MRMC Symmetrical Scripts page opens. For a description of the parameters displayed in the MRMC Symmetrical Scripts page, see *Table 11: MRMC Symmetrical Scripts Page Parameters*.

Note

NetStream Primo and NS Primo/DiploE units do not support XPIC or MIMO. For NS Primo/DiploE units, only Profile 0 through Profile 6 are available, and only ETSI scripts are available.

The following figures show scripts supported by the NetStream Diplo and NS Primo/DiploE. For an up-to-date list of scripts supported by the NetStream Diplo, NetStream Primo, and NS Primo/DiploE in this release, see the NetStream Diplo, NetStream Primo, and the NS Primo/DiploE Release Notes.

Figure 18: MRMC Symmetrical Scripts Page (NetStream Diplo) (ETSI)



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

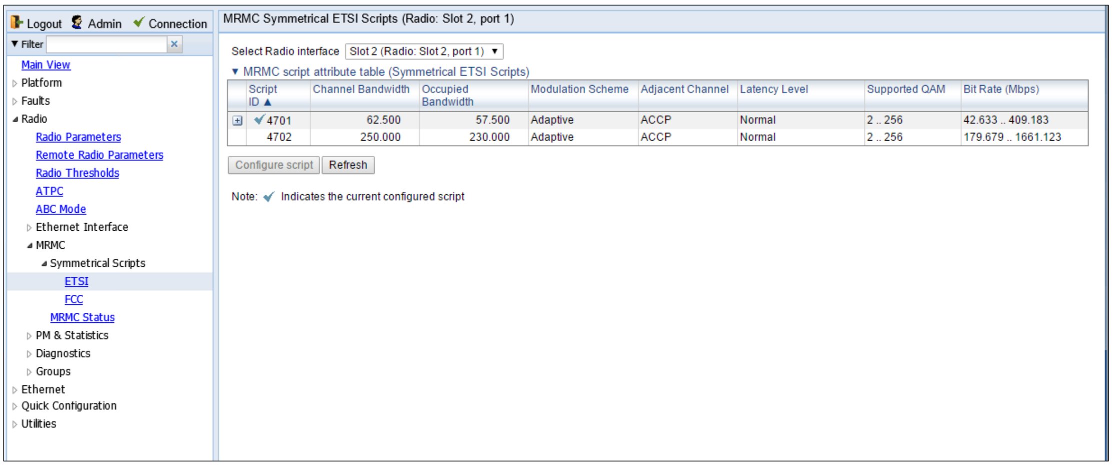
Select Radio interface: Slot 2 (Radio: Slot 2, port 1)

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

Note: ✓ Indicates the current configured script

Figure 19: MRMC Symmetrical Scripts Page (NS Primo/DiploE) (ETSI)



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

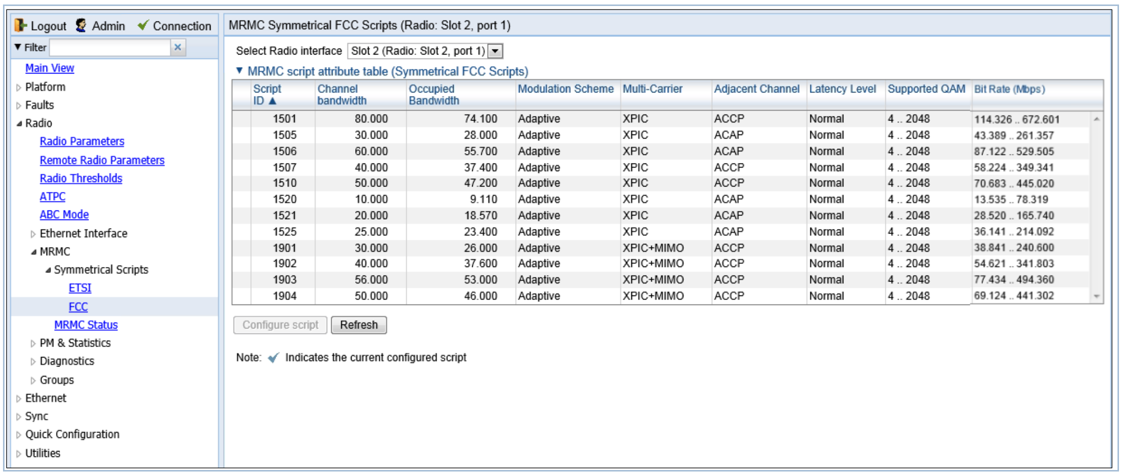
Select Radio interface: Slot 2 (Radio: Slot 2, port 1)

MRMC script attribute table (Symmetrical ETSI Scripts)

Script ID ▲	Channel Bandwidth	Occupied Bandwidth	Modulation Scheme	Adjacent Channel	Latency Level	Supported QAM	Bit Rate (Mbps)
✓ 4701	62.500	57.500	Adaptive	ACCP	Normal	2 .. 256	42.633 .. 409.183
4702	250.000	230.000	Adaptive	ACCP	Normal	2 .. 256	179.679 .. 1661.123

Note: ✓ Indicates the current configured script

Figure 20: MRMC Symmetrical Scripts Page (NetStream Diplo) (FCC)



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

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

MRMC script attribute table (Symmetrical FCC 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
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
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

Note: ✓ Indicates the current configured script

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

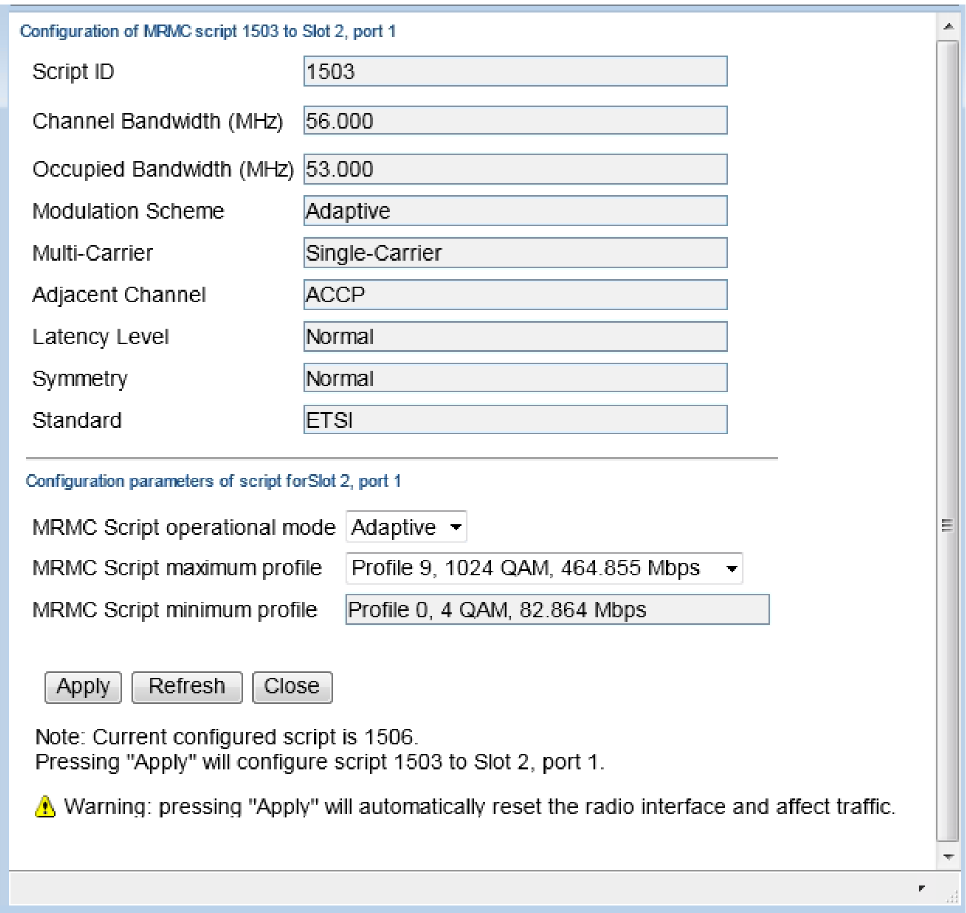
Note

This step is only applicable for NetStream Diplo units.

3 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).

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

2.11.1. Figure 21: MRMC Symmetrical Scripts Page (Configuration)



Configuration of MRMC script 1503 to Slot 2, port 1

Script ID	1503
Channel Bandwidth (MHz)	56.000
Occupied Bandwidth (MHz)	53.000
Modulation Scheme	Adaptive
Multi-Carrier	Single-Carrier
Adjacent Channel	ACCP
Latency Level	Normal
Symmetry	Normal
Standard	ETSI

Configuration parameters of script forSlot 2, port 1

MRMC Script operational mode	Adaptive
MRMC Script maximum profile	Profile 9, 1024 QAM, 464.855 Mbps
MRMC Script minimum profile	Profile 0, 4 QAM, 82.864 Mbps

Note: Current configured script is 1506.
Pressing "Apply" will configure script 1503 to Slot 2, port 1.

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

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.

6. In the **MRMC Script maximum profile** field, enter the maximum profile for the script. Refer to *Radio Profiles* for a list of available radio profiles.
7. Click **Apply**.

Note

Changing the script resets the radio interface and affects traffic.

Table 11 describes the MRMC Symmetrical Scripts page parameters.

Table 11: 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	The ACM mode: **Fixed** or **Adaptive**. ● Fixed ACM mode applies constant TX and RX rates. However, unlike regular scripts, with a Fixed ACM script you can specify a maximum profile to inhibit inefficient transmission levels. ● In Adaptive ACM mode, TX and RX rates are dynamic. An ACM-enabled radio system automatically chooses which profile to use according to the channel fading conditions.
MRMC Script 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	Displays the minimum ACM profile available for the script.

2.11.2. Radio Profiles

Table 12 lists the available radio profiles for NetStream Diplo and NetStream Primo. Table 13 lists the available radio profiles for NS Primo/DiploE.

Table 12: Available Radio Profiles – NetStream Diplo and NetStream Primo

Profile	Modulation
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

Table 13: Available Radio Profiles – NS Primo/DiploE

Profile	Modulation
Profile 0	BPSK
Profile 1	QPSK
Profile 2	8 QAM
Profile 3	16 QAM
Profile 4	32 QAM
Profile 5	64 QAM
Profile 6	128 QAM

2.12. 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 NS Primo/Diplo is capable of adjusting power on the fly, and optimizing the available capacity at every modulation point.

To enable ACM with adaptive transmit power:

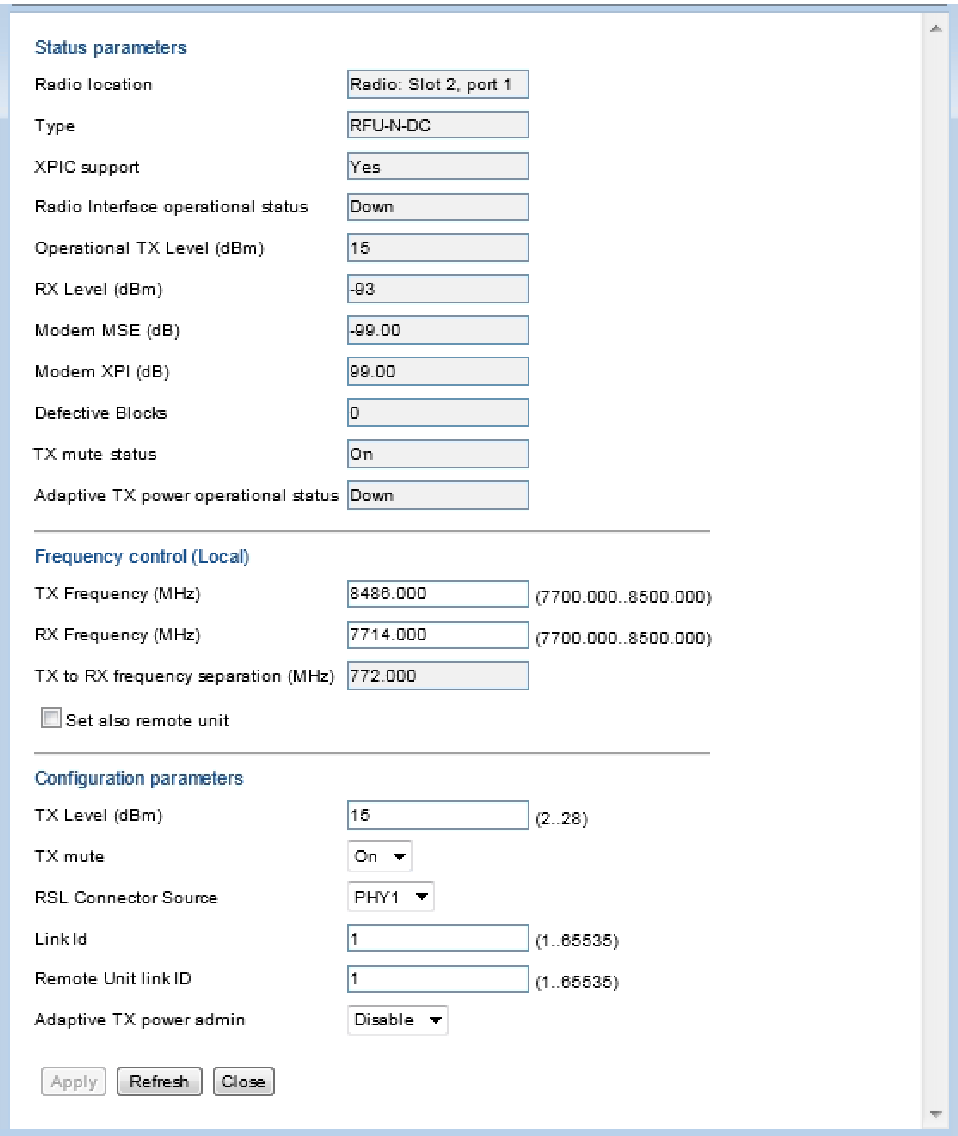
1 Select **Radio > Radio Parameters**. The Radio Parameters page opens.

- For NetStream Diplo units, the Radio Parameters page initially displays a table as shown in *Figure 16*.

- ○ For NetStream Primo units and NS Primo/DiploE units, a page appears, similar to *Figure 17* (which shows an NetStream Diplo page).

2 For NetStream Diplo units, select the carrier in the Radio table (see *Figure 16*) and click **Edit**. A separate Radio Parameters page opens. The page is essentially identical to the NS Primo/DiploE and NetStream Primo page, except for the addition of a **Radio location** parameter.

Figure 22: Radio Parameters Page Per Carrier – NetStream Diplo



Status parameters

Radio location	Radio: Slot 2, port 1
Type	RFU-N-DC
XPIC support	Yes
Radio Interface operational status	Down
Operational TX Level (dBm)	15
RX Level (dBm)	-93
Modem MSE (dB)	-99.00
Modem XPI (dB)	99.00
Defective Blocks	0
TX mute status	On
Adaptive TX power operational status	Down

Frequency control (Local)

TX Frequency (MHz)	8486.000	(7700.000..8500.000)
RX Frequency (MHz)	7714.000	(7700.000..8500.000)
TX to RX frequency separation (MHz)	772.000	

□ Set also remote unit

Configuration parameters

TX Level (dBm)	15	(2..28)
TX mute	On	
RSL Connector Source	PHY1	
Link Id	1	(1..65535)
Remote Unit link ID	1	(1..65535)
Adaptive TX power admin	Disable	

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

2.13. Operating in FIPS Mode

Note

This feature is only relevant for NetStream Diplo and NetStream Primo units.

From NetStream OS version 8.3, NetStream Diplo and NetStream Primo can be configured to be FIPS 140-2-compliant in specific hardware and software configurations, as described in this section.

2.13.1. Requirements for FIPS Compliance

For a full list of FIPS requirements, refer to the *Netronics NS Primo/Diplo FIPS 140-2 Security Policy*, available upon request. It is the responsibility of the customer to ensure that these requirements are met.

For an NetStream Diplo or an NetStream Primo node to be FIPS-compliant, the unit must be FIPS-compliant hardware. A FIPS-compliant NetStream Diplo or NetStream Primo unit has a unique part number ending in the letters AF, in the following format:

- NetStream Diplo-***-AF
- NetStream Primo-***-AF

Note

To display the part numbers of the hardware components of your NS Primo/Diplo unit, see *Displaying Unit Inventory*.

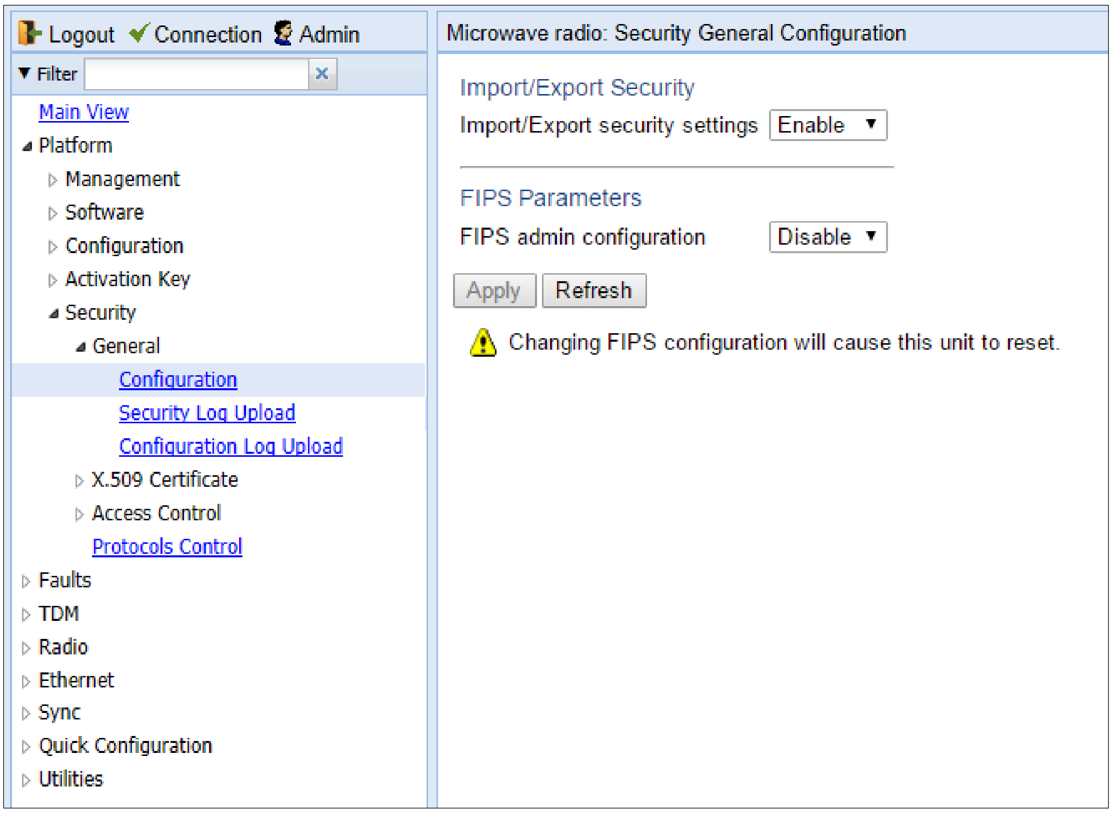
Special labels must be affixed to a FIPS-compliant NetStream Diplo or NetStream Primo unit. These labels are tamper-evident and must be applied in such a way that it is not possible to open or tamper with the unit. Replacement labels can be ordered from Netronics Networks, part number BS-0341-0. Tamper-evident labels should be inspected for integrity at least once every six months. For further details, refer to the *NetStream Diplo Installation Guide* or the *NetStream Primo Installation Guide*.

2.13.2. 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 23: Security General Configuration Page



Microwave radio: Security General Configuration

Import/Export Security

Import/Export security settings: Enable

FIPS Parameters

FIPS admin configuration: Disable

Changing FIPS configuration will cause this unit to reset.

2 In the **FIPS admin configuration** field, select **Enable**.

3 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.

For a full list of FIPS requirements, including software configuration requirements, refer to the *Netronics NS Primo/Diplo FIPS 140-2 Security Policy*, available upon request.

2.14. 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*.

2.15. Creating Service(s) for Traffic

In order to pass traffic through the NS Primo/Diplo, you must configure Ethernet traffic services. For configuration instructions, see *Configuring Ethernet Service(s)*.

3. Configuration Guide

This section includes:

- *System Configurations*
- *Configuring a Link Using the Quick Configuration Wizard*
- *Configuring Multi-Carrier ABC*
- *Configuring Link Aggregation (LAG)*
- *Configuring XPIC*
- *Configuring HSB Radio Protection*
- *Configuring MIMO and Space Diversity*
- *Operating an NetStream Diplo in Single Radio Carrier Mode*

Multi-Carrier ABC, XPIC, MIMO, and Space Diversity are only supported with NetStream Diplo. HSB radio protection is only supported with NetStream Diplo and NetStream Primo.

3.1. System Configurations

This section lists the basic system configurations and the NS Primo/Diplo product types that support them, as well as links to configuration instructions.

Table 14: System Configurations

Configuration	Supported Products	Link to Configuration Instructions
Multi-Carrier ABC (Multi-Radio)	NetStream Diplo	*Configuring Multi-Carrier ABC*
Link Aggregation (LAG)	NetStream Diplo/S/E	*Configuring Link Aggregation (LAG)*
1+1 XPIC	NetStream Diplo	Configuring XPIC
HSB Radio Protection	NetStream Diplo/S	Configuring HSB Radio Protection
MIMO and Space Diversity	NetStream Diplo	Configuring MIMO and Space Diversity
NetStream Diplo in Single Radio Carrier Mode	NetStream Diplo	Operating an NetStream Diplo in Single Radio Carrier Mode

3.2. 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 (or LAG) 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 NetStream Diplo dual-carrier units.

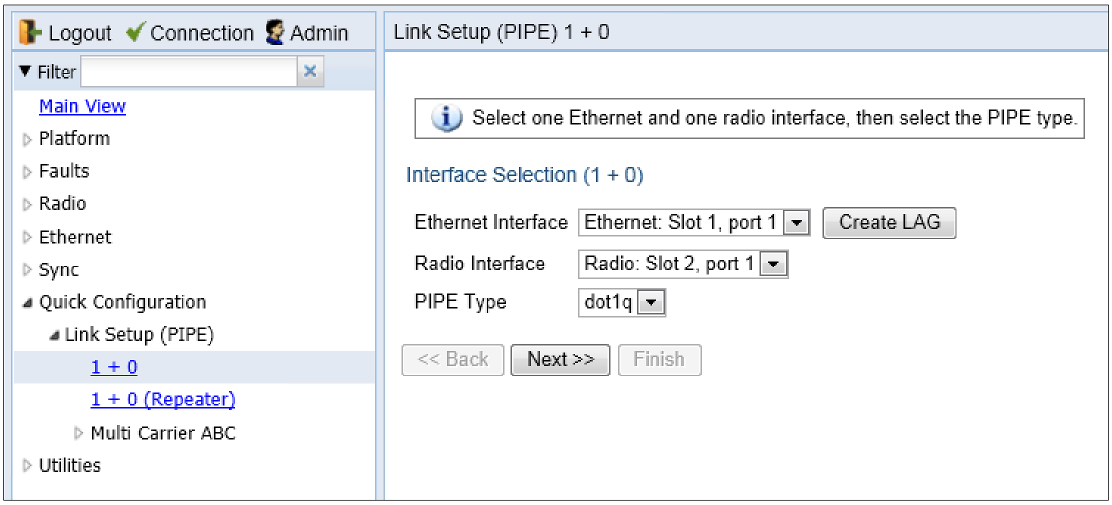
Because the Quick Configuration wizard creates Pipe links, you cannot add an interface to a link using the Quick Configuration wizard if any service points are attached to the interface prior to configuring the link. See *Deleting a Service Point*.

3.2.1. 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 > Link Setup (PIPE) > 1+0**. Page 1 of the 1+0 Quick Configuration wizard opens.

Figure 24: 1+0 Quick Configuration Wizard – Page 1



Link Setup (PIPE) 1 + 0

Select one Ethernet and one radio interface, then select the PIPE type.

Interface Selection (1 + 0)

Ethernet Interface: Ethernet: Slot 1, port 1 | Create LAG

Radio Interface: Radio: Slot 2, port 1

PIPE Type: dot1q

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

Note

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

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:

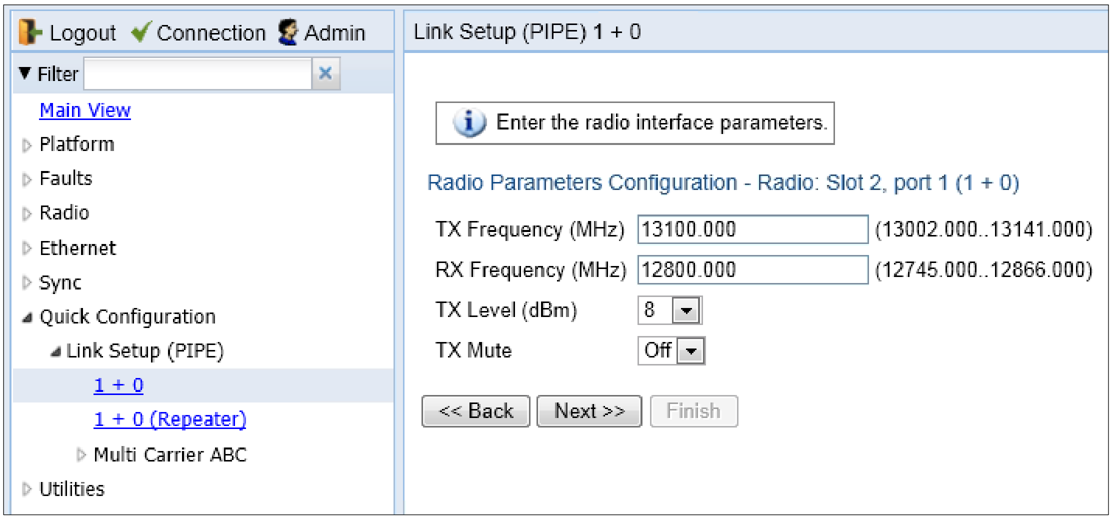
- **s-tag** – A single S-VLAN is classified into the service points.
- **dot1q** - A single C-VLAN is classified into the service points.

Note

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

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

Figure 25: 1+0 Quick Configuration Wizard – Page 2



Link Setup (PIPE) 1 + 0

Enter the radio interface parameters.

Radio Parameters Configuration - Radio: Slot 2, port 1 (1 + 0)

TX Frequency (MHz) 13100.000 (13002.000..13141.000)

RX Frequency (MHz) 12800.000 (12745.000..12866.000)

TX Level (dBm) 8

TX Mute Off

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

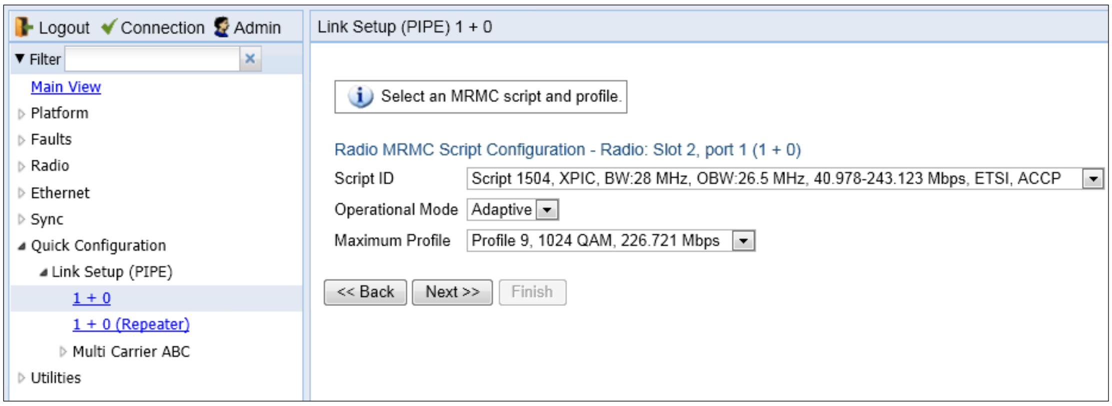
7 In the **RX Frequency (MHz)** field, set the received radio frequency in MHz.

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 26: 1+0 Quick Configuration Wizard – Page 3



Link Setup (PIPE) 1 + 0

Select an MRMC script and profile.

Radio MRMC Script Configuration - Radio: Slot 2, port 1 (1 + 0)

Script ID Script 1504, XPIC, BW:28 MHz, OBW:26.5 MHz, 40.978-243.123 Mbps, ETSI, ACCP

Operational Mode Adaptive

Maximum Profile Profile 9, 1024 QAM, 226.721 Mbps

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**.

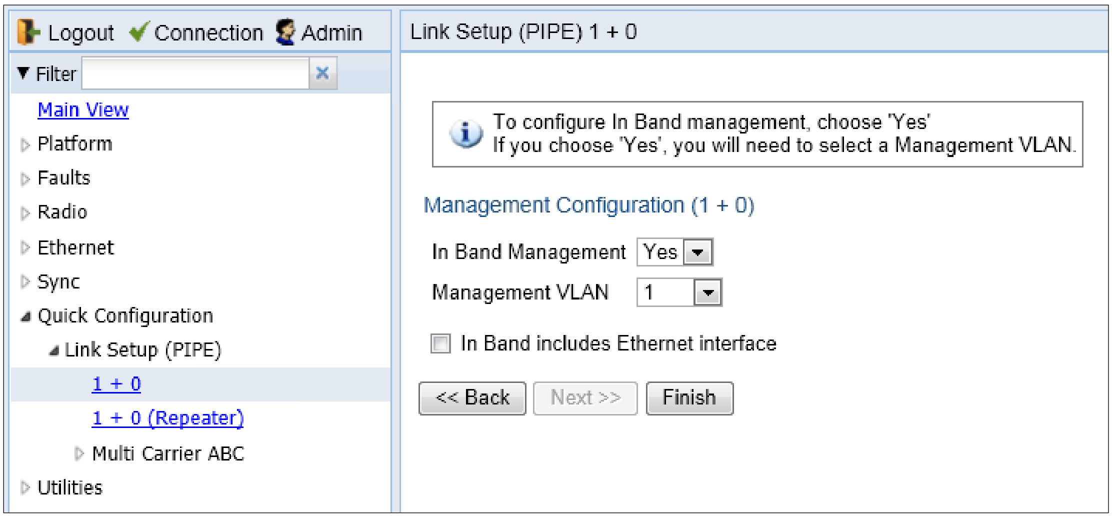
- Fixed ACM mode applies constant TX and RX rates. However, unlike regular scripts, with a Fixed ACM script you can specify a maximum profile to inhibit inefficient transmission levels.
- In Adaptive ACM mode, TX and RX rates are dynamic. An ACM-enabled radio system automatically chooses which profile 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 next field is **Maximum Profile**. Enter the maximum profile for the script in the **Maximum Profile** field. See *Configuring the Radio (MRMC) Script(s)*.

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

Figure 27: 1+0 Quick Configuration Wizard – Page 4



Link Setup (PIPE) 1 + 0

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

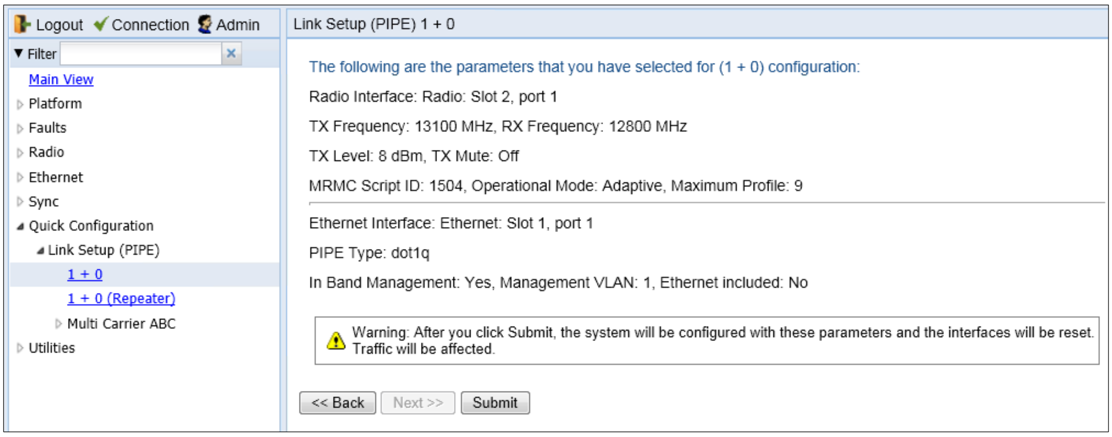
15 In the **In Band Management** field, select **Yes** to configure in-band management, or **No** if you do not need in-band management. If you select **Yes**, the **Management VLAN** field appears.

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

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

18 Click **Finish**. Page 5 of the 1+0 Quick Configuration wizard opens. This page displays the parameters you have selected for the link.

Figure 28: 1+0 Quick Configuration Wizard – Page 5 (Summary Page)



Link Setup (PIPE) 1 + 0

The following are the parameters that you have selected for (1 + 0) configuration:

Radio Interface: Radio: Slot 2, port 1

TX Frequency: 13100 MHz, RX Frequency: 12800 MHz

TX Level: 8 dBm, TX Mute: Off

MRMC Script ID: 1504, Operational Mode: Adaptive, Maximum Profile: 9

Ethernet Interface: Ethernet: Slot 1, port 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.

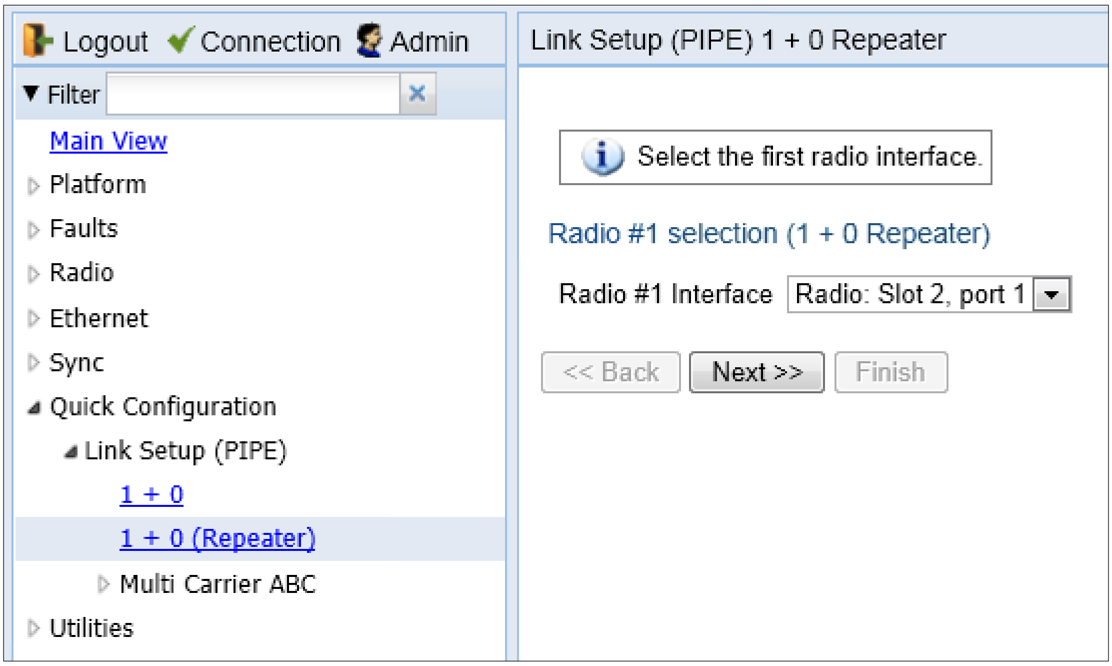
19 To complete configuration of the link, click **Submit**. If you want to go back and change any of the parameters, click **Back**. After you click **Submit**, the unit is reset.

3.2.2. 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 > Link Setup (PIPE) > 1+0 (Repeater)**. Page 1 of the 1+0 Repeater Quick Configuration wizard opens.

Figure 29: 1+0 Repeater Quick Configuration Wizard – Page 1



Link Setup (PIPE) 1 + 0 Repeater

Select the first radio interface.

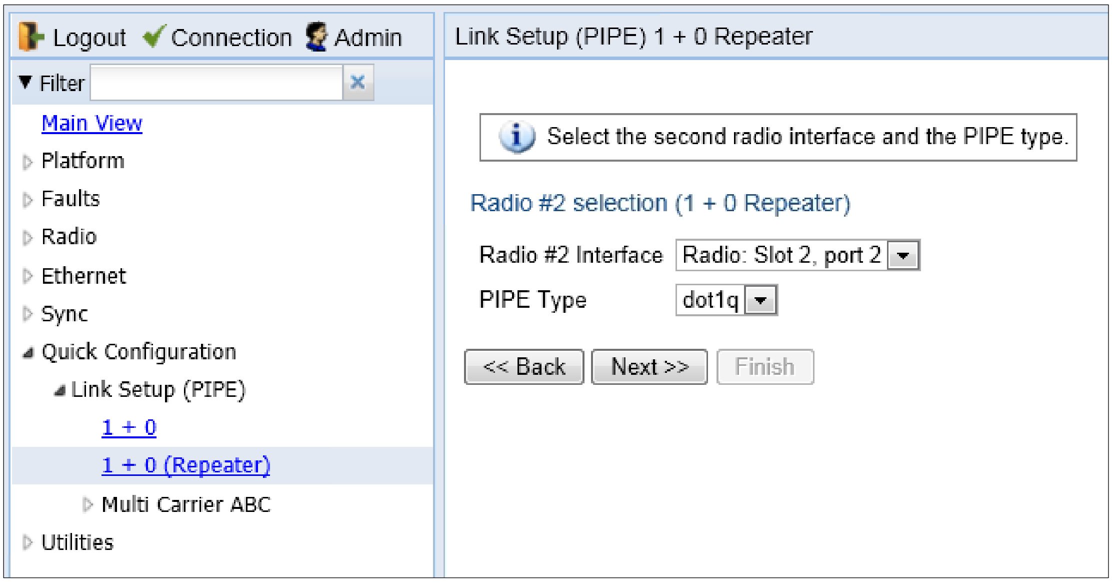
Radio #1 selection (1 + 0 Repeater)

Radio #1 Interface: Radio: Slot 2, port 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 30: 1+0 Repeater Quick Configuration Wizard – Page 2



Link Setup (PIPE) 1 + 0 Repeater

Select the second radio interface and the PIPE type.

Radio #2 selection (1 + 0 Repeater)

Radio #2 Interface: Radio: Slot 2, port 2

PIPE Type: dot1q

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:

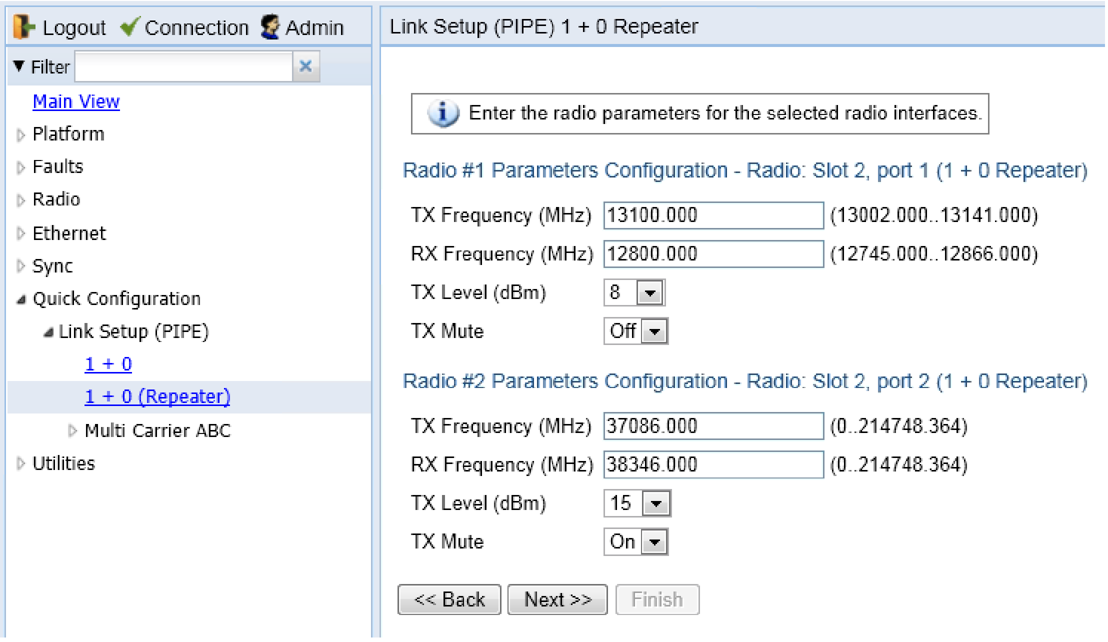
- **s-tag** – A single S-VLAN is classified into the service points.
- **dot1q** - A single C-VLAN is classified into the service points.

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 31: 1+0 Repeater Quick Configuration Wizard – Page 3



Link Setup (PIPE) 1 + 0 Repeater

Enter the radio parameters for the selected radio interfaces.

Radio #1 Parameters Configuration - Radio: Slot 2, port 1 (1 + 0 Repeater)

TX Frequency (MHz) 13100.000 (13002.000..13141.000)
RX Frequency (MHz) 12800.000 (12745.000..12866.000)
TX Level (dBm) 8
TX Mute Off

Radio #2 Parameters Configuration - Radio: Slot 2, port 2 (1 + 0 Repeater)

TX Frequency (MHz) 37086.000 (0..214748.364)
RX Frequency (MHz) 38346.000 (0..214748.364)
TX Level (dBm) 15
TX Mute On

7 For each interface, configure the following radio parameters:

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

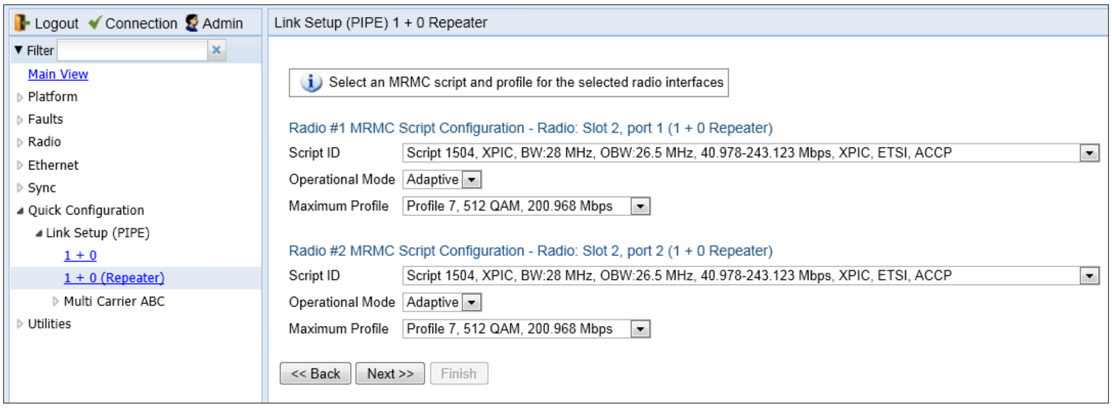
ii In the **RX Frequency (MHz)** field, set the received radio frequency in MHz.

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**.

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

Figure 32: 1+0 Repeater Quick Configuration Wizard – Page 4



Link Setup (PIPE) 1 + 0 Repeater

Select an MRMC script and profile for the selected radio interfaces

Radio #1 MRMC Script Configuration - Radio: Slot 2, port 1 (1 + 0 Repeater)

Script ID Script 1504, XPIC, BW:28 MHz, OBW:26.5 MHz, 40.978-243.123 Mbps, XPIC, ETSI, ACCP
Operational Mode Adaptive
Maximum Profile Profile 7, 512 QAM, 200.968 Mbps

Radio #2 MRMC Script Configuration - Radio: Slot 2, port 2 (1 + 0 Repeater)

Script ID Script 1504, XPIC, BW:28 MHz, OBW:26.5 MHz, 40.978-243.123 Mbps, XPIC, ETSI, ACCP
Operational Mode Adaptive
Maximum Profile Profile 7, 512 QAM, 200.968 Mbps

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

i 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)*.

ii In the **Operational Mode** field, select the ACM mode for the radio: **Fixed** or **Adaptive**.

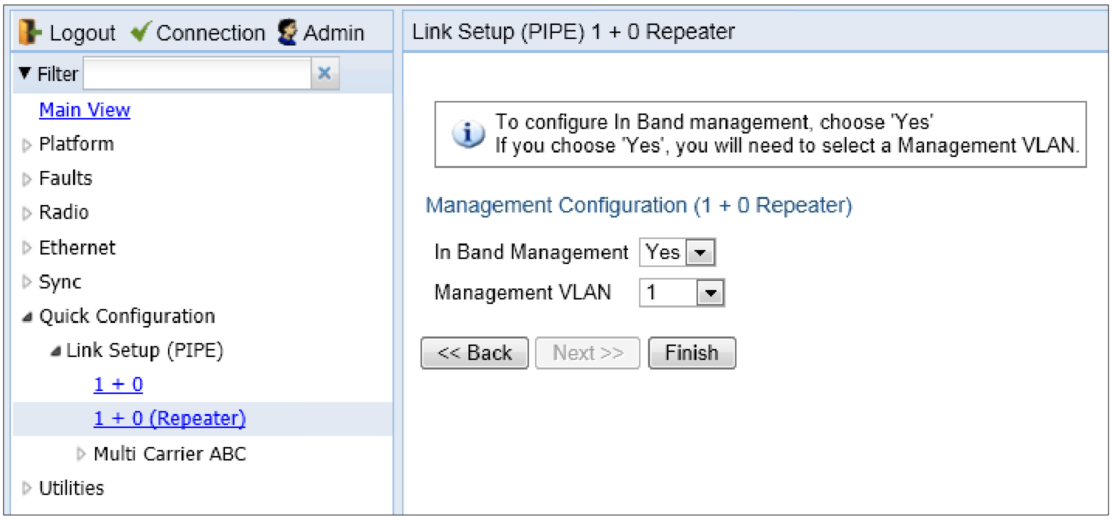
- Fixed ACM mode applies constant TX and RX rates. However, unlike regular scripts, with a Fixed ACM script you can specify a maximum profile to inhibit inefficient transmission levels.
- In Adaptive ACM mode, TX and RX rates are dynamic. An ACM-enabled radio system automatically chooses which profile 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 next field is **Maximum Profile**. Enter the maximum profile for the script in the **Maximum Profile** field. See *Configuring the Radio (MRMC) Script(s)*.

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

Figure 33: 1+0 Repeater Quick Configuration Wizard – Page 5



Link Setup (PIPE) 1 + 0 Repeater

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

Management Configuration (1 + 0 Repeater)

In Band Management: Yes

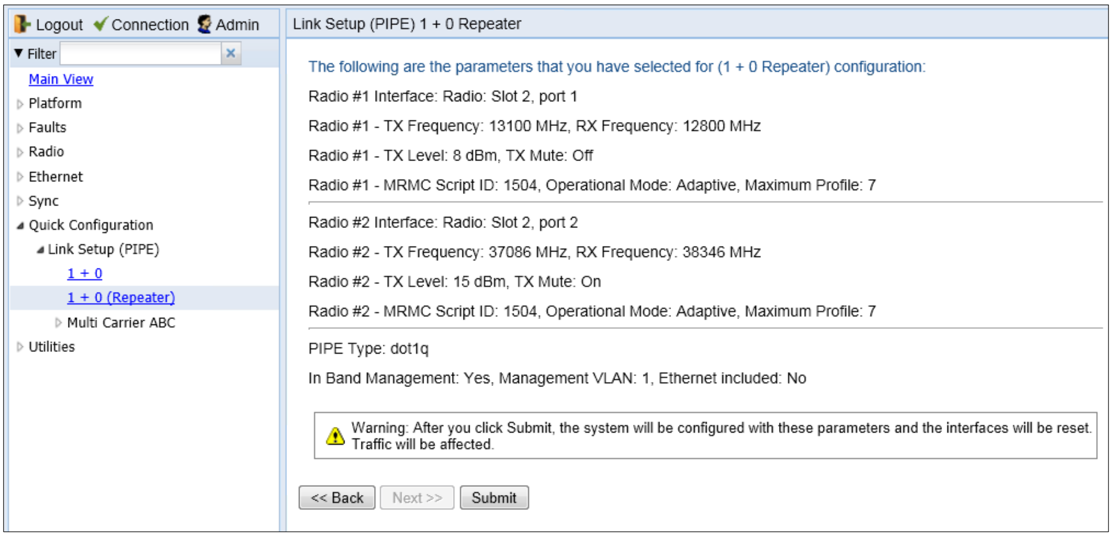
Management VLAN: 1

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 34: 1+0 Repeater Quick Configuration Wizard – Page 6 (Summary Page)



Link Setup (PIPE) 1 + 0 Repeater

The following are the parameters that you have selected for (1 + 0 Repeater) configuration:

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

Radio #1 - TX Frequency: 13100 MHz, RX Frequency: 12800 MHz

Radio #1 - TX Level: 8 dBm, TX Mute: Off

Radio #1 - MRMC Script ID: 1504, Operational Mode: Adaptive, Maximum Profile: 7

Radio #2 Interface: Radio: Slot 2, port 2

Radio #2 - TX Frequency: 37086 MHz, RX Frequency: 38346 MHz

Radio #2 - TX Level: 15 dBm, TX Mute: On

Radio #2 - MRMC Script ID: 1504, Operational Mode: Adaptive, Maximum Profile: 7

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.

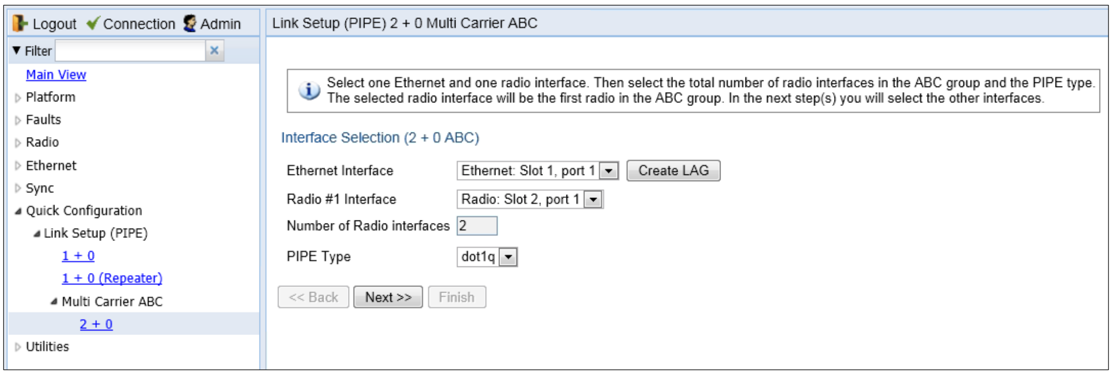
14 To complete configuration of the link, click **Submit**. If you want to go back and change any of the parameters, click **Back**. After you click **Submit**, the unit is reset.

3.2.3. 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 35: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Page 1



Link Setup (PIPE) 2 + 0 Multi Carrier ABC

Select one Ethernet and one radio interface. Then select the total number of radio interfaces in the ABC group and the PIPE type. The selected radio interface will be the first radio in the ABC group. In the next step(s) you will select the other interfaces.

Interface Selection (2 + 0 ABC)

Ethernet Interface: Ethernet: Slot 1, port 1
Radio #1 Interface: Radio: Slot 2, port 1
Number of Radio interfaces: 2
PIPE Type: dot1q

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)*.

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:

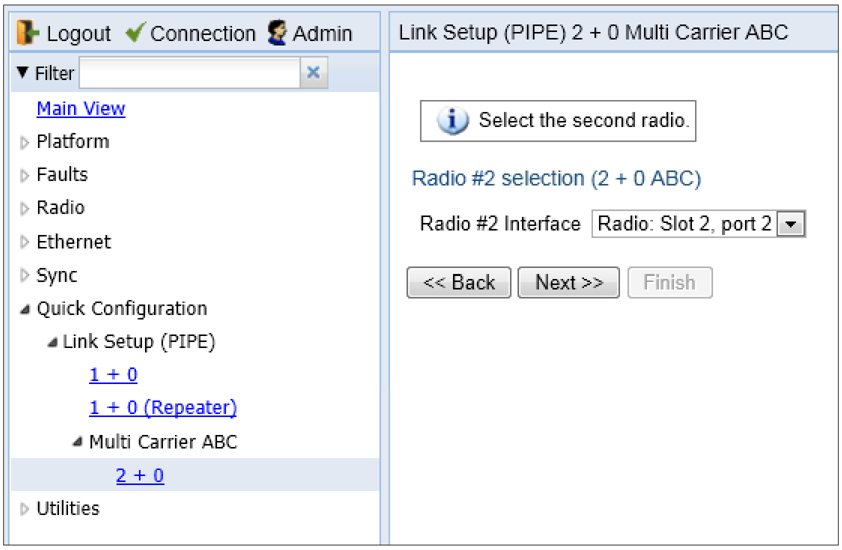
- **s-tag** – A single S-VLAN is classified into the service points.
- **dot1q** - A single C-VLAN is classified into the service points.

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 36: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio #2 Selection Page



Link Setup (PIPE) 2 + 0 Multi Carrier ABC

Select the second radio.

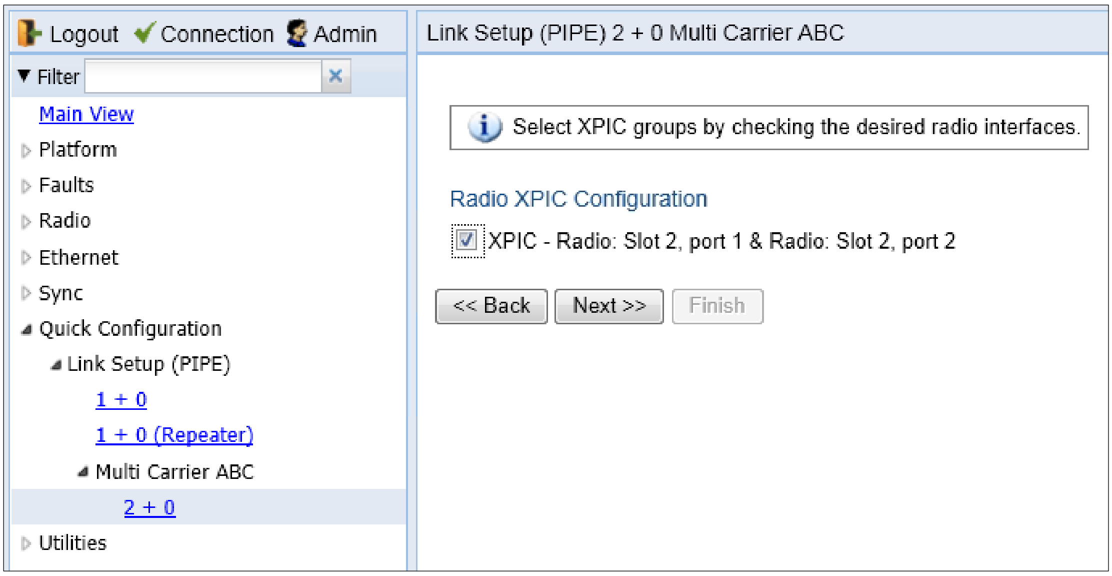
Radio #2 selection (2 + 0 ABC)

Radio #2 Interface: Radio: Slot 2, port 2

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 37: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio XPIC Configuration Page



Link Setup (PIPE) 2 + 0 Multi Carrier ABC

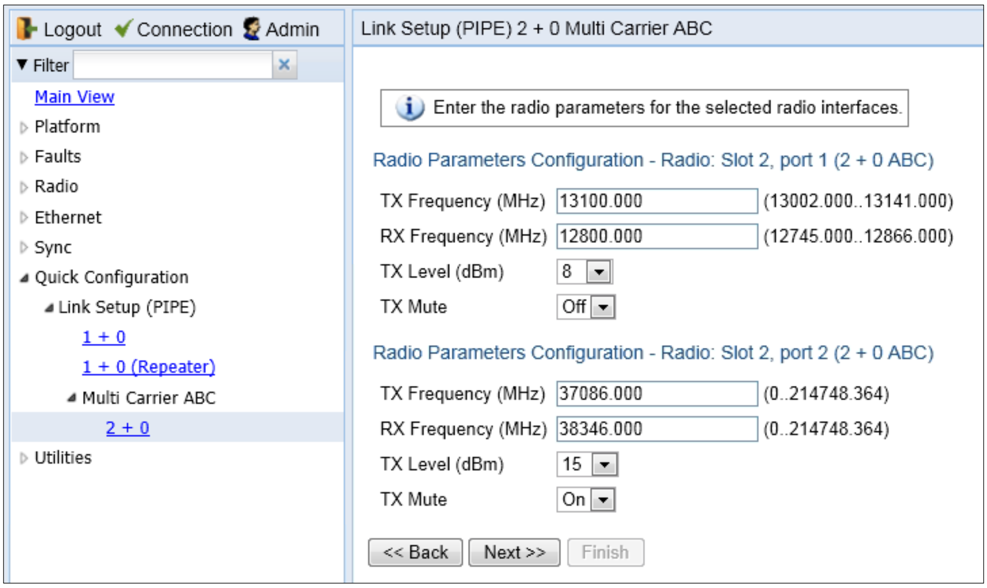
Select XPIC groups by checking the desired radio interfaces.

Radio XPIC Configuration

☑ XPIC - Radio: Slot 2, port 1 & Radio: Slot 2, port 2

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 38: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio Parameters Configuration Page



Link Setup (PIPE) 2 + 0 Multi Carrier ABC

Enter the radio parameters for the selected radio interfaces.

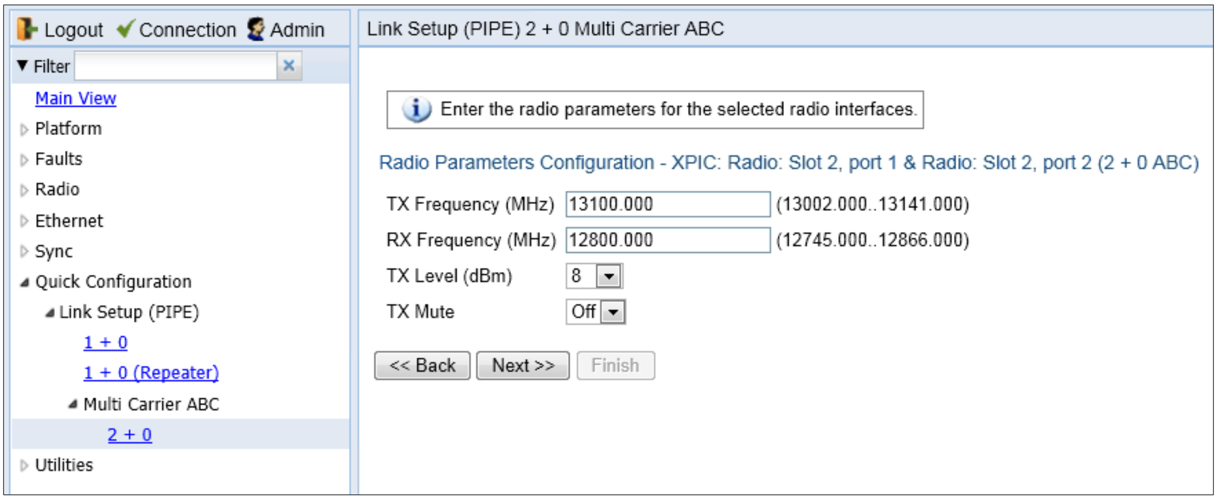
Radio Parameters Configuration - Radio: Slot 2, port 1 (2 + 0 ABC)

TX Frequency (MHz) 13100.000 (13002.000..13141.000)
RX Frequency (MHz) 12800.000 (12745.000..12866.000)
TX Level (dBm) 8
TX Mute Off

Radio Parameters Configuration - Radio: Slot 2, port 2 (2 + 0 ABC)

TX Frequency (MHz) 37086.000 (0..214748.364)
RX Frequency (MHz) 38346.000 (0..214748.364)
TX Level (dBm) 15
TX Mute On

Figure 39: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio Parameters Configuration Page (XPIC)



Link Setup (PIPE) 2 + 0 Multi Carrier ABC

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) 13100.000 (13002.000..13141.000)
RX Frequency (MHz) 12800.000 (12745.000..12866.000)
TX Level (dBm) 8
TX Mute Off

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.

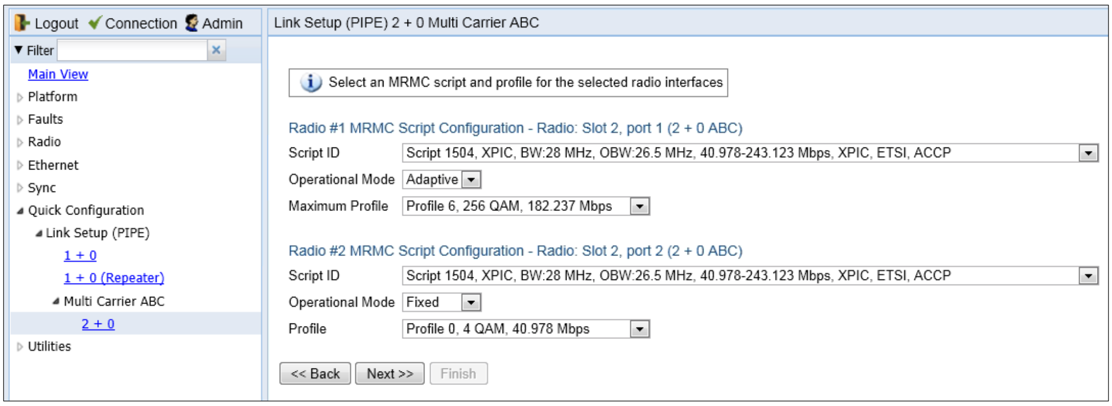
ii In the **RX Frequency (MHz)** field, set the received radio frequency in MHz.

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 MRMC Script Configuration page opens. You can configure the MRMC script parameters for each interface. For an XPIC group, you configure the parameters for the group rather than the individual interfaces.

Figure 40: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio MRMC Script Configuration Page



Link Setup (PIPE) 2 + 0 Multi Carrier ABC

Select an MRMC script and profile for the selected radio interfaces

Radio #1 MRMC Script Configuration - Radio: Slot 2, port 1 (2 + 0 ABC)

Script ID: Script 1504, XPIC, BW:28 MHz, OBW:26.5 MHz, 40.978-243.123 Mbps, XPIC, ETSI, ACCP

Operational Mode: Adaptive

Maximum Profile: Profile 6, 256 QAM, 182.237 Mbps

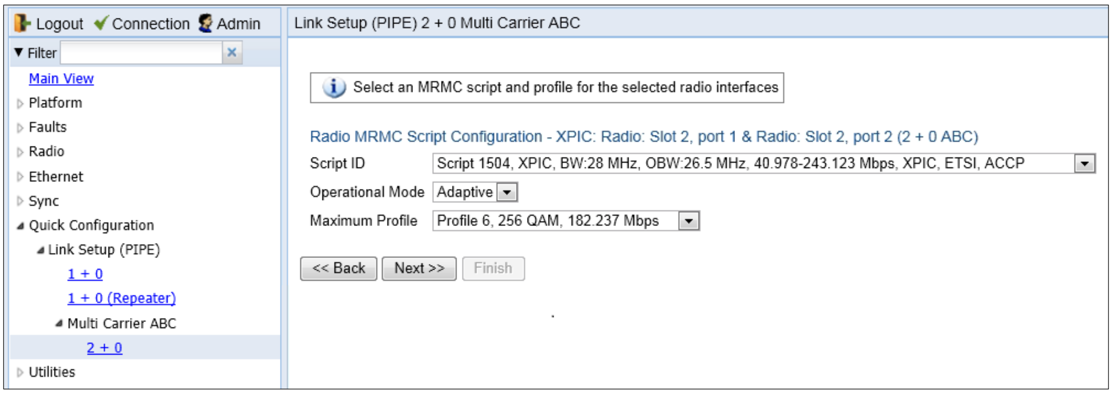
Radio #2 MRMC Script Configuration - Radio: Slot 2, port 2 (2 + 0 ABC)

Script ID: Script 1504, XPIC, BW:28 MHz, OBW:26.5 MHz, 40.978-243.123 Mbps, XPIC, ETSI, ACCP

Operational Mode: Fixed

Profile: Profile 0, 4 QAM, 40.978 Mbps

Figure 41: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Radio MRMC Script Configuration Page - XPIC



Link Setup (PIPE) 2 + 0 Multi Carrier ABC

Select an MRMC script and profile for the selected radio interfaces

Radio MRMC Script Configuration - XPIC: Radio: Slot 2, port 1 & Radio: Slot 2, port 2 (2 + 0 ABC)

Script ID: Script 1504, XPIC, BW:28 MHz, OBW:26.5 MHz, 40.978-243.123 Mbps, XPIC, ETSI, ACCP

Operational Mode: Adaptive

Maximum Profile: Profile 6, 256 QAM, 182.237 Mbps

11 For each interface or XPIC group, configure the following MRMC script parameters:

i In the **Script ID** field, select the MRMC script you want to assign to the radio or XPIC group. For a full explanation of choosing an MRMC script, see *Configuring the Radio (MRMC) Script(s)*.

ii 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.

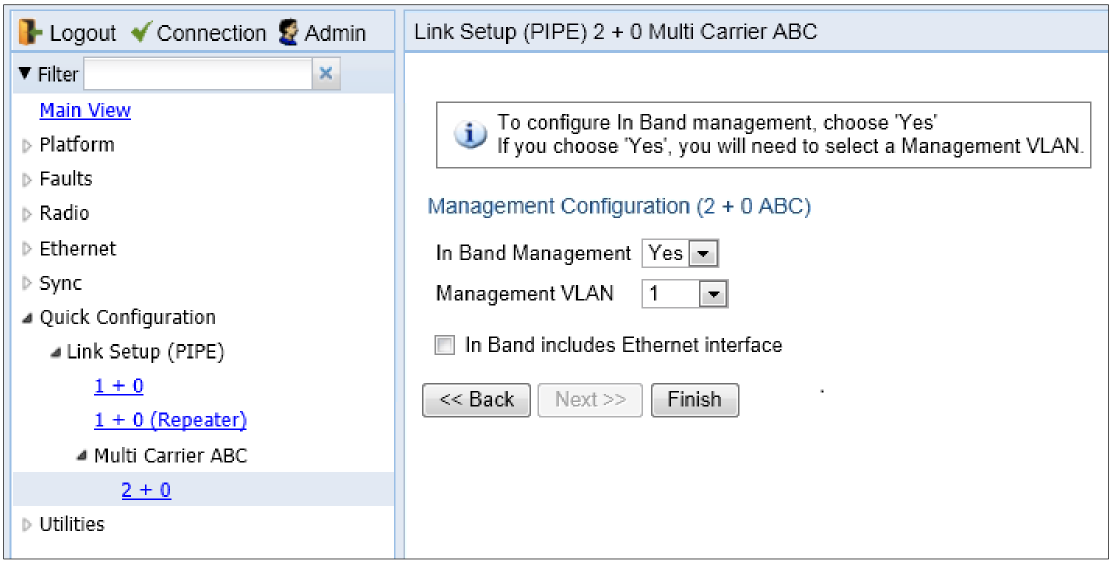
iii Do one of the following:

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

- If you selected **Adaptive** in the **Operational Mode** field, the next field is **Maximum Profile**. Enter the maximum profile for the script in the **Maximum Profile** field. See *Configuring the Radio (MRMC) Script(s)*.

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

Figure 42: 2 + 0 Multi Carrier ABC Quick Configuration Wizard – Management Configuration Page



Link Setup (PIPE) 2 + 0 Multi Carrier ABC

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

Management Configuration (2 + 0 ABC)

In Band Management: Yes

Management VLAN: 1

□ In Band includes Ethernet interface

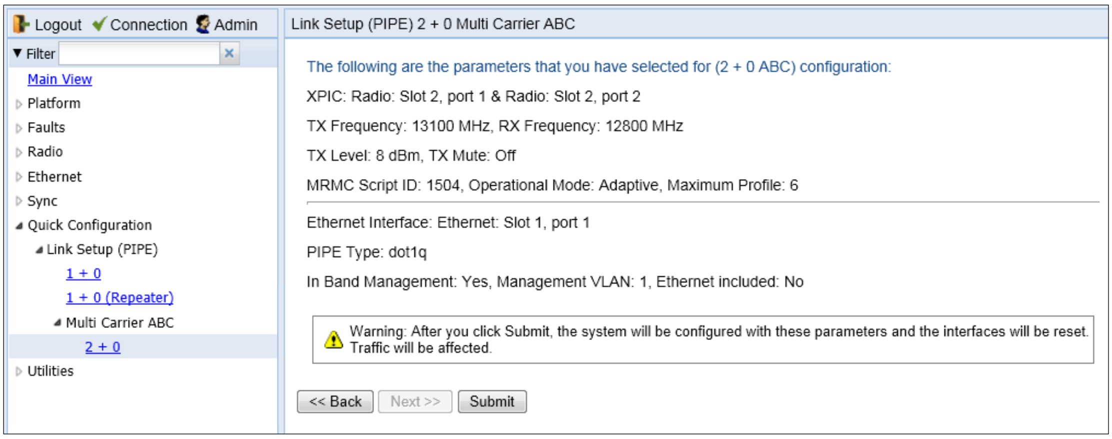
13 In the **In Band Management** field, select **Yes** to configure in-band management, or **No** if you do not need in-band management. If you select **Yes**, the **Management VLAN** field appears.

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 43: 2 + 0 Multi Carrier ABC Quick Configuration Wizard –Summary Page



Link Setup (PIPE) 2 + 0 Multi Carrier ABC

The following are the parameters that you have selected for (2 + 0 ABC) configuration:

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

TX Frequency: 13100 MHz, RX Frequency: 12800 MHz

TX Level: 8 dBm, TX Mute: Off

MRMC Script ID: 1504, Operational Mode: Adaptive, Maximum Profile: 6

Ethernet Interface: Ethernet: Slot 1, port 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.

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.

3.3. Configuring Multi-Carrier ABC

Note

This option is only relevant for NetStream Diplo units.

This section includes:

- *Multi-Carrier ABC Overview*
- *Configuring a Multi-Carrier ABC Group*
- *Deleting a Multi-Carrier ABC Group*

3.3.1. Multi-Carrier ABC Overview

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

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

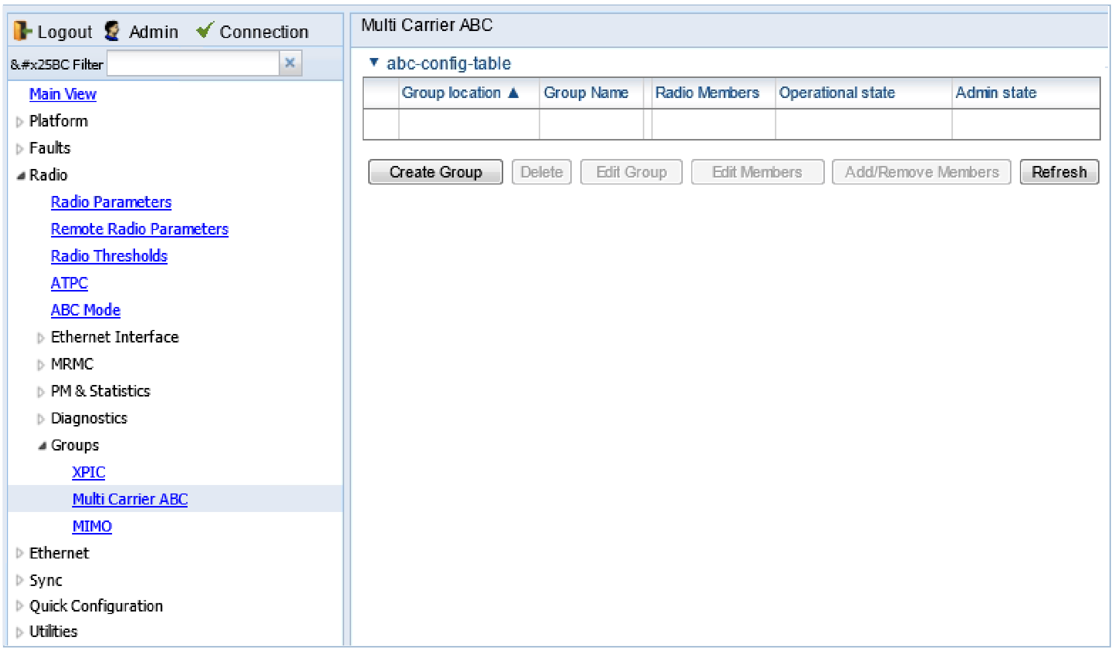
One Multi-Carrier ABC group that includes both radio interfaces can be configured per unit.

3.3.2. 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.

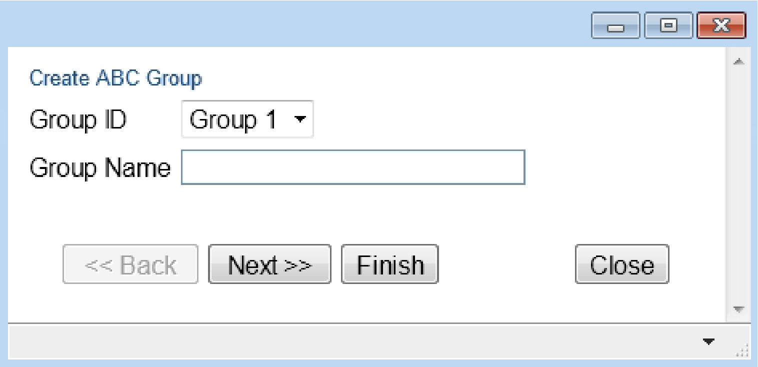
Figure 44: Multi-Carrier ABC Group Page (Empty)



	Group location ▲	Group Name	Radio Members	Operational state	Admin state

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

Figure 45: Create ABC Group Wizard – First Page



Create ABC Group

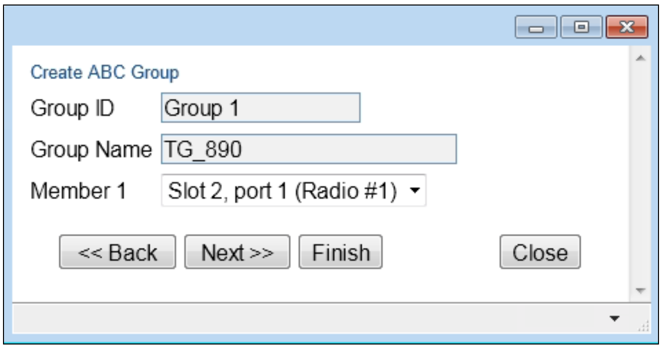
Group ID: Group 1

Group Name:

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

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

Figure 46: Create ABC Group Wizard – Second Page



Create ABC Group

Group ID: Group 1

Group Name: TG_890

Member 1: Slot 2, port 1 (Radio #1)

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

Note

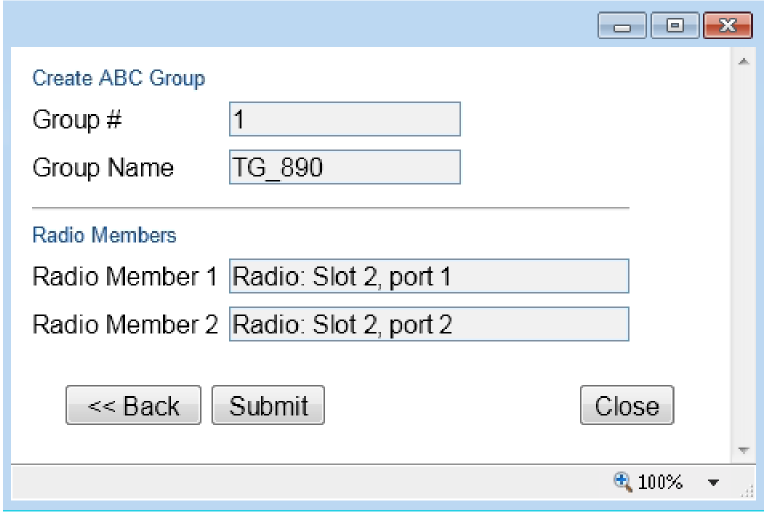
Although you may select the Radio members in any order you wish, ABC configuration will not succeed unless Radio slot 2 port 1 is selected first and Radio slot 2 port 2 is selected second.

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

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

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

Figure 47: Create ABC Group Wizard – Finish Page



Create ABC Group

Group # 1

Group Name TG_890

Radio Members

Radio Member 1 Radio: Slot 2, port 1

Radio Member 2 Radio: Slot 2, port 2

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

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

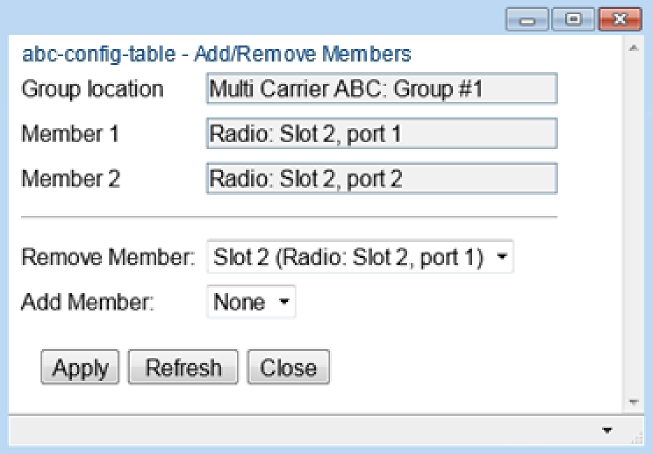
3.3.2.1. Adding and Removing Group Members

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 abc-config-table - Add/Remove Members page opens.

Figure 48: Multi Carrier ABC Group - Add/Remove Members Page



abc-config-table - Add/Remove Members

Group location Multi Carrier ABC: Group #1

Member 1 Radio: Slot 2, port 1

Member 2 Radio: Slot 2, port 2

Remove Member: Slot 2 (Radio: Slot 2, port 1)

Add Member: None

2 Select a member in the **Remove Member** field.

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.

3.3.3. 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 44*).
2 Select the group in the Multi-Carrier ABC table and click **Add/Remove Members**. The abc-config-table – Add/Remove Members page opens (*Figure 48*).
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**.

3.4. Configuring Link Aggregation (LAG)

Link aggregation (LAG) enables you to group several physical Ethernet or radio interfaces into a single logical interface bound to a single MAC address. This logical interface is known as a LAG group. Traffic sent to the interfaces in a LAG group is distributed by means of a load balancing mechanism. NS Primo/Diplo uses a distribution function of up to Layer 4 in order to generate the most efficient distribution among the LAG physical ports.

This section explains how to configure LAG and includes the following topics:

- *LAG Overview*
- *Configuring a LAG Group*
- *Deleting a LAG Group*

3.4.1. LAG Overview

LAG can be used to provide redundancy for Ethernet interfaces, both on the same NS Primo/Diplo 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)*.

3.4.2. Configuring a LAG Group

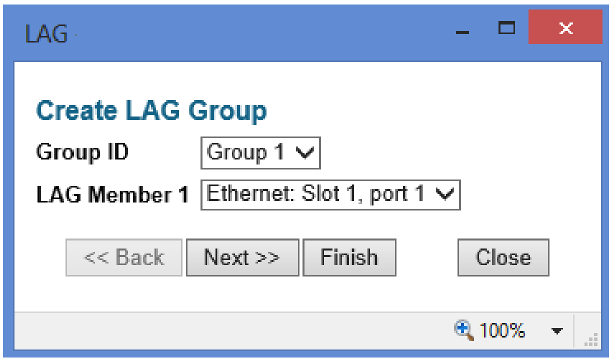
3.4.2.1. Creating a LAG Group

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 49: Create LAG Group – Page 1



Create LAG Group

Group ID: Group 1

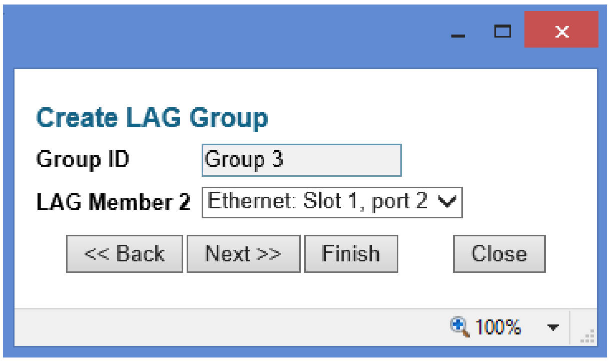
LAG Member 1: Ethernet: Slot 1, port 1

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 **LAG 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.

5 Click **Next**. A new Create LAG Group page opens.

Figure 50: Create LAG Group – Page 2



Create LAG Group

Group ID: Group 3

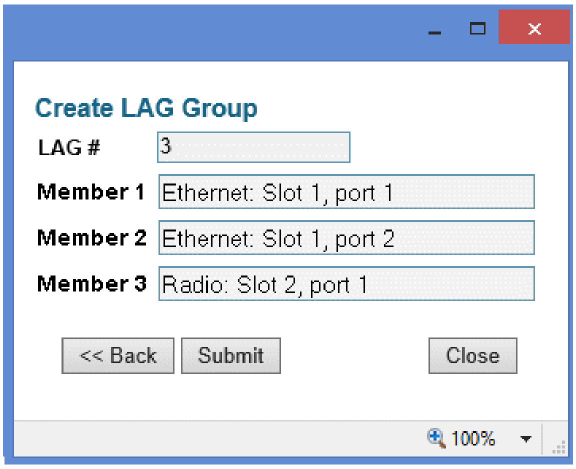
LAG Member 2: Ethernet: Slot 1, port 2

6 In the **LAG Member 2** field, select an additional interface to assign to the LAG Group.

7 To add additional interfaces to the LAG group, repeat steps 5 and 6.

8 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 51: Create LAG Group – Final Page



Create LAG Group

LAG #: 3

Member 1: Ethernet: Slot 1, port 1

Member 2: Ethernet: Slot 1, port 2

Member 3: Radio: Slot 2, port 1

9 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.

3.4.2.2. Editing a LAG Group

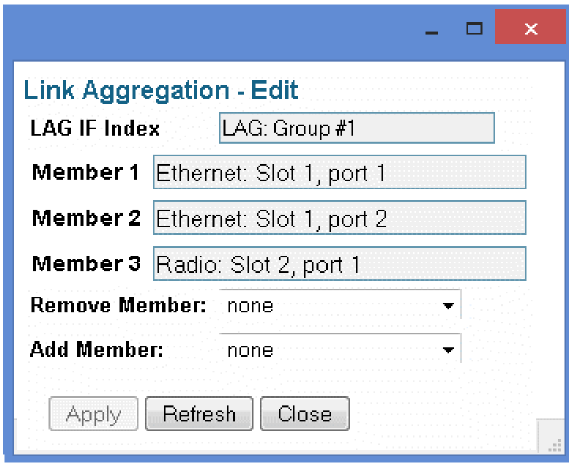
To edit an existing LAG group:

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 52: Link Aggregation - Edit Page



Link Aggregation - Edit

LAG IF Index: LAG: Group #1

Member 1: Ethernet: Slot 1, port 1

Member 2: Ethernet: Slot 1, port 2

Member 3: Radio: Slot 2, port 1

Remove Member: none

Add Member: none

4 Do one or both of the following:

- To remove an interface from the LAG Group, select the interface in the **Remove Member** field.
- To add an interface to the LAG Group, select the interface in the **Add Member** field.

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.

3.4.3. 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.

3.5. Configuring XPIC

Note

This option is only relevant for NetStream Diplo units.

This section includes:

- *XPIC Overview*
- *Configuring the Antennas*
- *Configuring the Radio Carriers*
- *Creating an XPIC Group*

3.5.1. XPIC Overview

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

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 antennas and then configure the carriers, as described below.

3.5.2. Configuring the Antennas

1 Align the antennas for one carrier. While you are aligning these antennas, mute the second carrier. See *Configuring the Radio Parameters*.

2 Adjust the antenna alignment until you achieve the maximum RSL for the first-carrier link (the "RSL$_{wanted}$"). This RSL should be no more than +/-2 dB from the expected level.

3 Record the RSL$_{wanted}$ and mute the first radio carrier at each end of the link.

4 Unmute the second (orthogonal) radio carrier which was muted during the antenna alignment process.

5 Determine the XPI, by either of the following two methods:

   ○ Measure the RSL of the second carrier (the "RSL$_{unwanted}$"). To calculate the XPI, subtract RSL$_{unwanted}$ from the RSL$_{wanted}$.

Note

To measure the second carrier, leave the Voltmeter connected to the BNC connector. In the Radio Parameters page of the Web EMS (*Figure 17*), change the **RSL Connector Source** field from **PHYS1** to **PHYS2** (or vice versa). The BNC connector will now measure RSL from the other carrier.

   ○ Read the XPI from the **Modem XPI** field of the Radio Parameters page in the Web EMS. See *Viewing the Radio Status and Settings*.

6 The XPI should be at least 25dB. If it is not, you should adjust the OMT assembly on the back of the antenna at one side of the link until you achieve the highest 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. It is recommended to achieve XPI levels between 25dB and 30dB.

7 Enable all four radio carriers and check the XPI levels of both carriers at both sides of the link by checking the **Modem XPI** field of the Radio Parameters page in the Web EMS. See *Viewing the Radio Status and Settings*. 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.

3.5.3. 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 NetStream Diplo Release Notes.

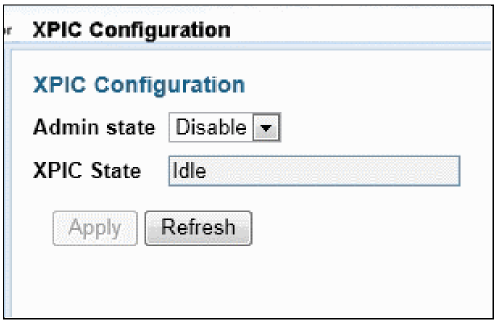
3 In the XPIC page, create an XPIC group that consists of the two RMCs that will be in the XPIC group. See *Creating an XPIC Group*.

3.5.4. Creating an XPIC Group

To create an XPIC group:

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

Figure 53: XPIC Configuration Page



XPIC Configuration

XPIC Configuration

Admin state: Disable

XPIC State: Idle

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**.

3.6. Configuring HSB Radio Protection

This section explains how to configure HSB radio protection and includes the following topics:

- *HSB Radio Protection Overview*
- *Configuring HSB Radio Protection*
- *Configuring 2+2 HSB Protection on an NetStream Diplo 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*

3.6.1. HSB Radio Protection Overview

NetStream Diplo and NetStream Primo support 1+1 HSB radio protection. NetStream Diplo also supports 2+2 HSB radio protection. In HSB radio protection, one NS Primo/Diplo 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 NetStream Diplo, refer to the NetStream Diplo Technical Description.
- For a full explanation of 1+1 HSB radio protection support in NetStream Primo, refer to the NetStream Primo Technical Description.

3.6.2. 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 NetStream Diplo or NetStream Primo.

Ethernet traffic must be routed to each unit via an optical splitter cable.

To configure HSB radio protection:

1 Before enabling protection, you must:

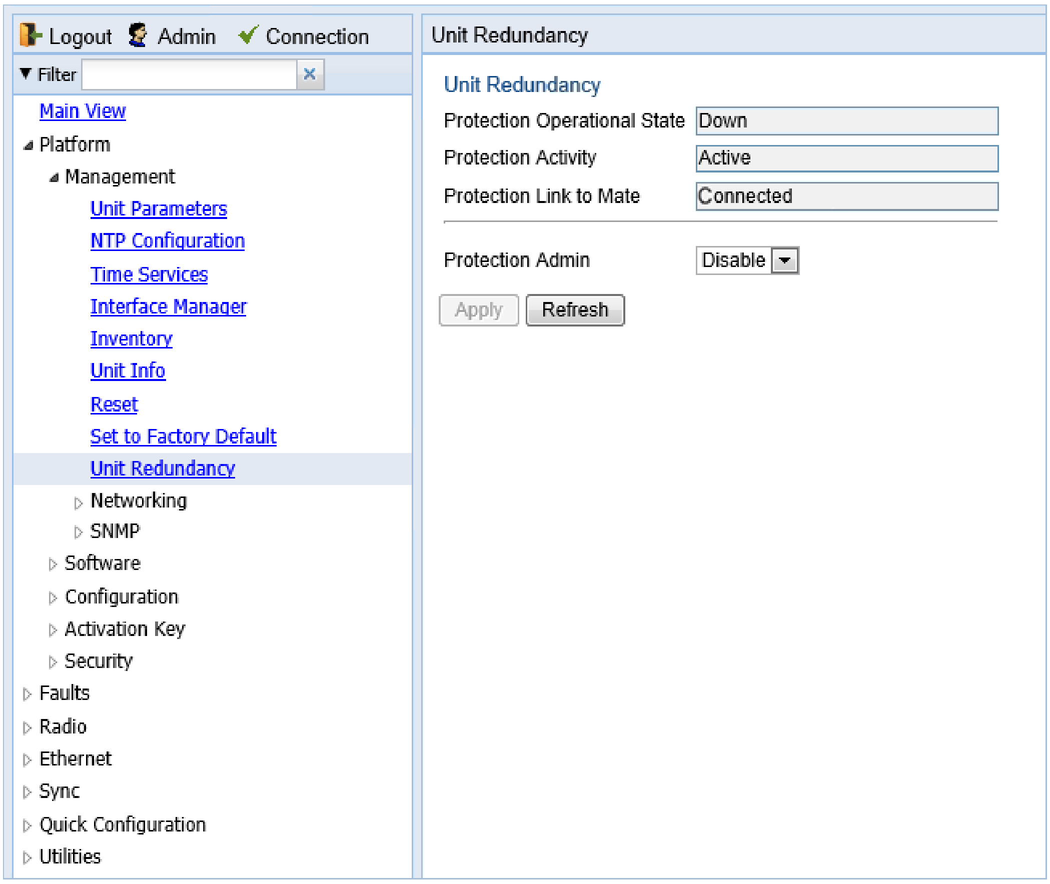
i Verify that both units have the same hardware part number (see *Displaying Unit Inventory*) and the same software version (see *Viewing Current Software Versions*). If the units do not have the same software version, upgrade each unit to the most recent software release (see *Upgrading the Software*).

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 54: Unit Redundancy Page



Unit Redundancy

Protection Operational State: Down

Protection Activity: Active

Protection Link to Mate: Connected

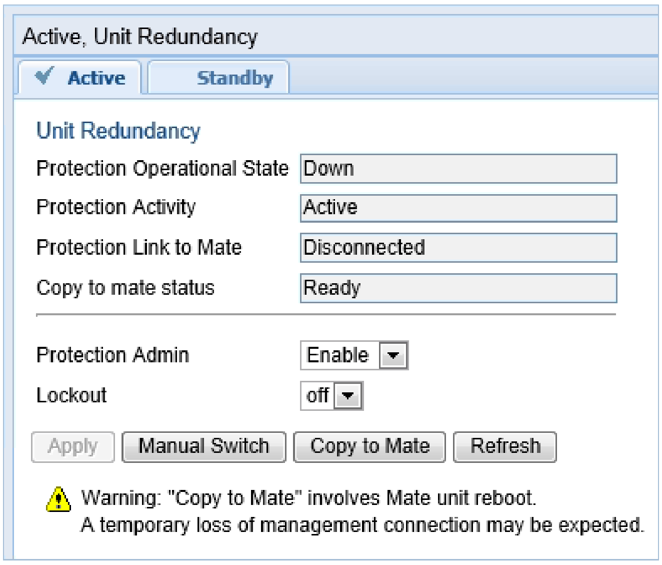
Protection Admin: Disable

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.
- The Unit Redundancy page refreshes to include additional radio protection fields.

Figure 55: Unit Redundancy Page when Redundancy Enabled



Active, Unit Redundancy

Unit Redundancy

Protection Operational State: Down
Protection Activity: Active
Protection Link to Mate: Disconnected
Copy to mate status: Ready

Protection Admin: Enable
Lockout: off

⚠ Warning: "Copy to Mate" involves Mate unit reboot.
A temporary loss of management connection may be expected.

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

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

Note

The parameters that are editable on the **Standby** tab are described in *Editing Standby Unit Settings*.

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:

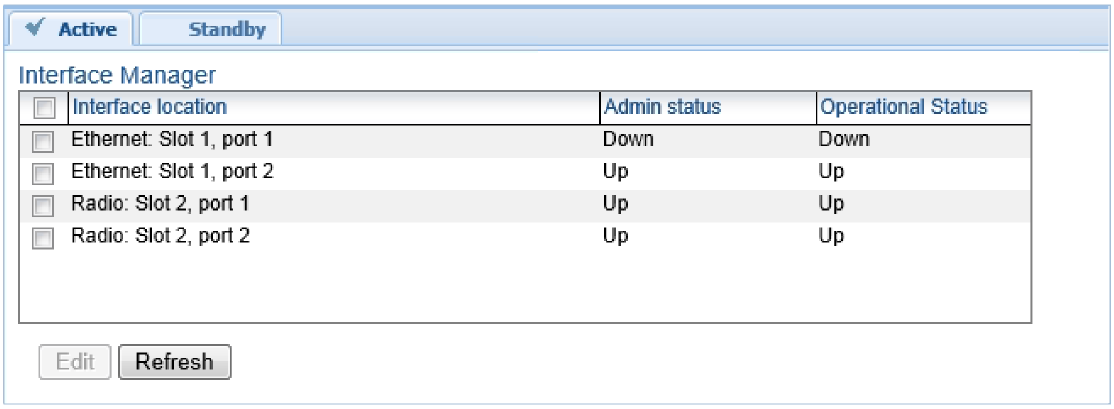
```
root> platform management protection show mismatch details
```

3.6.3. Configuring 2+2 HSB Protection on an NetStream Diplo Unit

In order to configure 2+2 HSB unit protection on an NetStream Diplo 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 13*). The following figure shows the Interface Manager page with both radio carriers enabled.

Figure 56: Interface Manager Page – Both Radio Carriers Enabled



Interface Manager

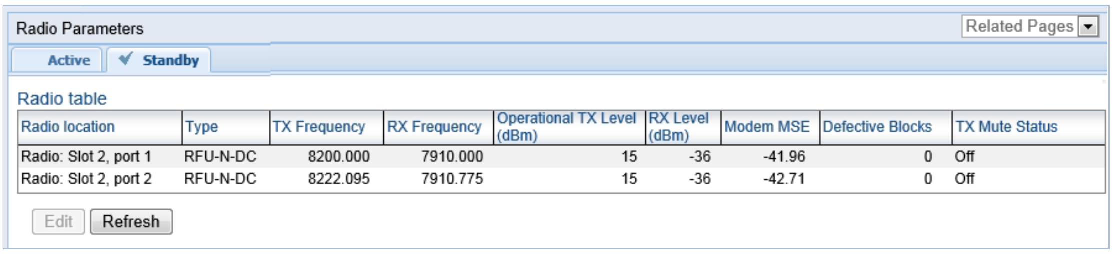
□	Interface location	Admin status	Operational Status
□	Ethernet: Slot 1, port 1	Down	Down
□	Ethernet: Slot 1, port 2	Up	Up
□	Radio: Slot 2, port 1	Up	Up
□	Radio: Slot 2, port 2	Up	Up

3.6.4. 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 57: Standby Tab of Radio Parameters Page



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

3.6.5. 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 *Activation Key Configuration Page* (see *Configuring the Activation Key*).
- Defining user accounts – Refer to the *Access Control User Accounts Page* (see *Configuring Users*).
- Setting synchronization settings – Refer to the *SyncE Regenerator* page (see *Configuring SyncE Regenerator*).

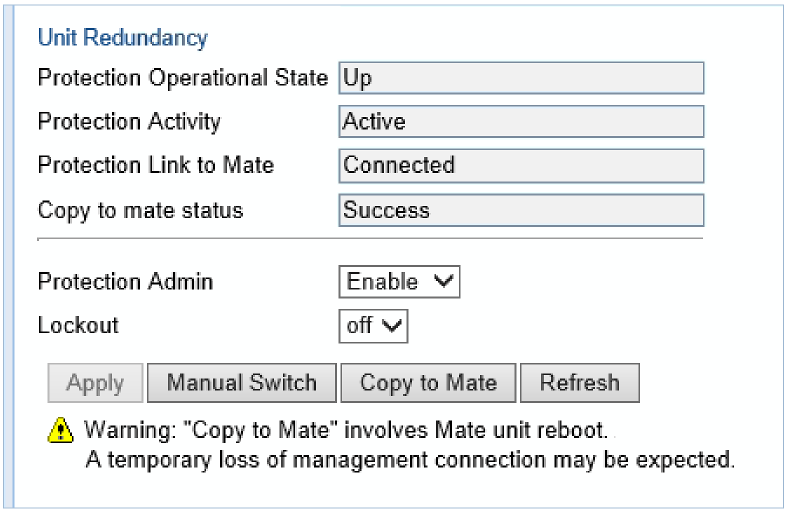
3.6.6. Viewing Link and Protection Status and Activity

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.

Unit Redundancy Page



Unit Redundancy

Protection Operational State	Up
Protection Activity	Active
Protection Link to Mate	Connected
Copy to mate status	Success
Protection Admin	Enable
Lockout	off

⚠ Warning: "Copy to Mate" involves Mate unit reboot.
A temporary loss of management connection may be expected.

The following information is displayed:

- **Protection Operational State** – Indicates whether HSB protection is functional (available in practice). 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.

3.6.7. 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.

3.6.8. 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**.

3.6.9. 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**.

3.7. Configuring MIMO and Space Diversity

Note

This feature is only relevant for NetStream Diplo units.

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

- *MIMO and Space Diversity Overview*
- *MIMO Mate Management Access*
- *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*

3.7.1. 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 an 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.

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

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

Note

Only one MIMO or Space Diversity group can be created per NetStream Diplo unit. All MRMC scripts that support MIMO also support Space Diversity.

3.7.1.1. 2+2 Space Diversity

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 NetStream Diplo units operating in dual core mode. In each NetStream Diplo unit, both radio carriers are connected to a single antenna. One optical GbE port on each NetStream Diplo is connected to an optical splitter. Traffic must be routed to an optical GbE port on each NetStream Diplo unit.

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

3.7.2. MIMO Mate Management Access

For MIMO configurations using in-band management and an external switch operating in LAG mode, you must enable MIMO Mate Management Access in order to manage both units via in-band management. When MIMO Mate Management Access is enabled, the two units exchange incoming management packets, ensuring that all management data is received by both units.

Note that MIMO Mate Management Access should only be enabled if both of the following conditions exist:

- In-band management
- External switch using LAG

If either of these conditions is not present, MIMO Mate Management Access should be disabled. By default, the feature is disabled.

To enable MIMO Mate Management Access, enter the following command:

```
root> radio mimo mate mng access set admin enable
```

To disable MIMO Mate Management Access, enter the following command:

```
root> radio mimo mate mng access set admin disable
```

To display whether MIMO Mate Management Access is enabled, enter the following command:

```
root> radio mimo mate mng access show
```

Note

MIMO Mate Management Access can only be configured via CLI.

3.7.3. Creating a MIMO or Space Diversity Group

Note

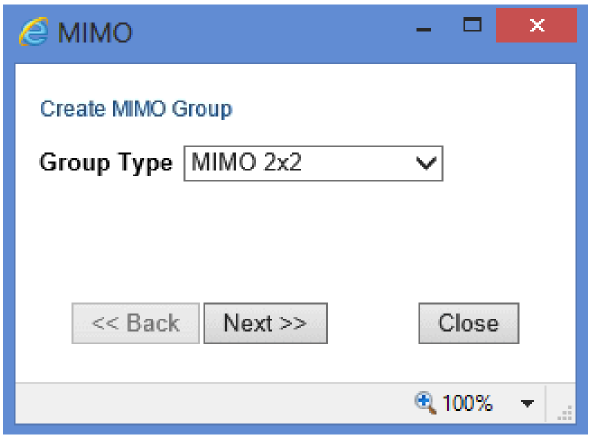
Only one MIMO or Space Diversity group can be created per NetStream Diplo unit.

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 58: Create MIMO Group – Page 1



Create MIMO Group

Group Type: MIMO 2x2

3 In the **Group Type** field, select one of the following according to your desired system configuration:

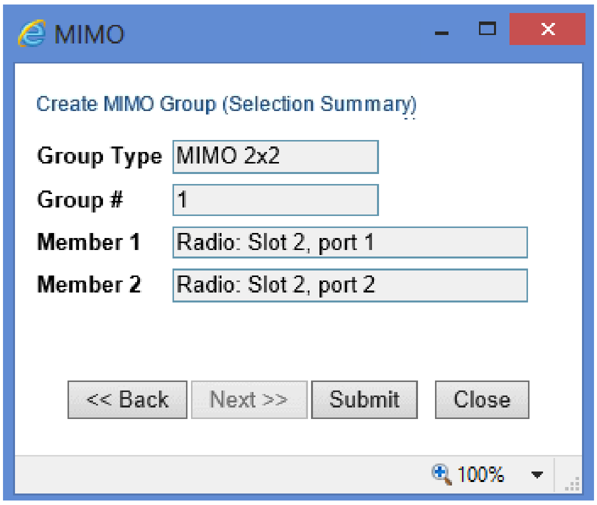
- ○ MIMO 2x2
- ○ MIMO 4x4
- ○ 1+0 Space Diversity
- ○ 2+0 Space Diversity

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 59: Create MIMO Group – Page 2



Create MIMO Group (Selection Summary)

Group Type: MIMO 2x2

Group #: 1

Member 1: Radio: Slot 2, port 1

Member 2: Radio: Slot 2, port 2

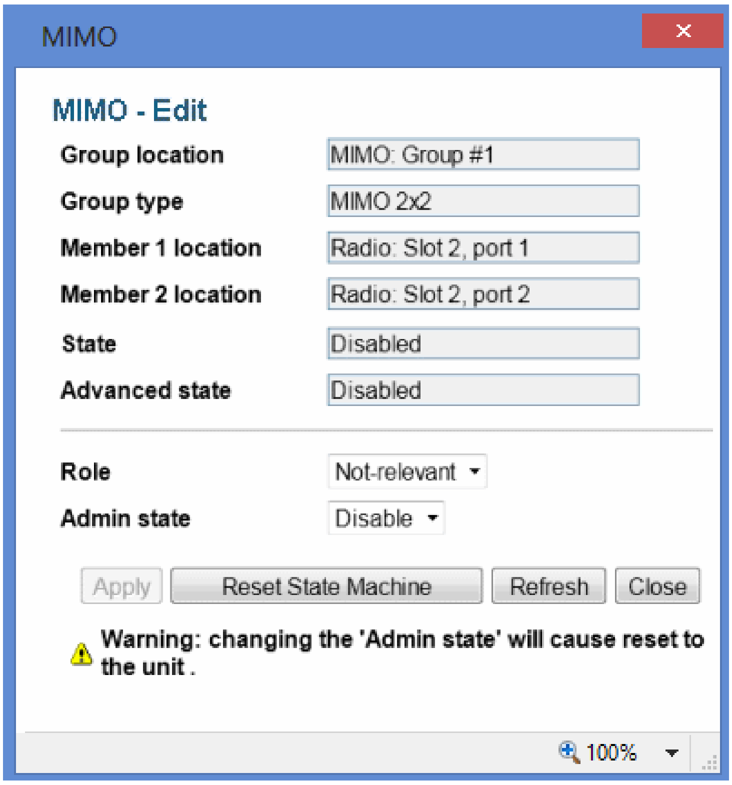
5. Click **Submit**, to create the MIMO or Space Diversity group.
   Click **Close** to cancel and close the window.
6. After creating the group, you must enable the group in the MIMO - Edit page. See *Enabling/Disabling a MIMO or Space Diversity Group*.
7. For 4x4 MIMO configurations and 2+2 Space Diversity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

3.7.4. 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 60: MIMO - Edit Page



MIMO - Edit

Group location	MIMO: Group #1
Group type	MIMO 2x2
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	Disable

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

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**.

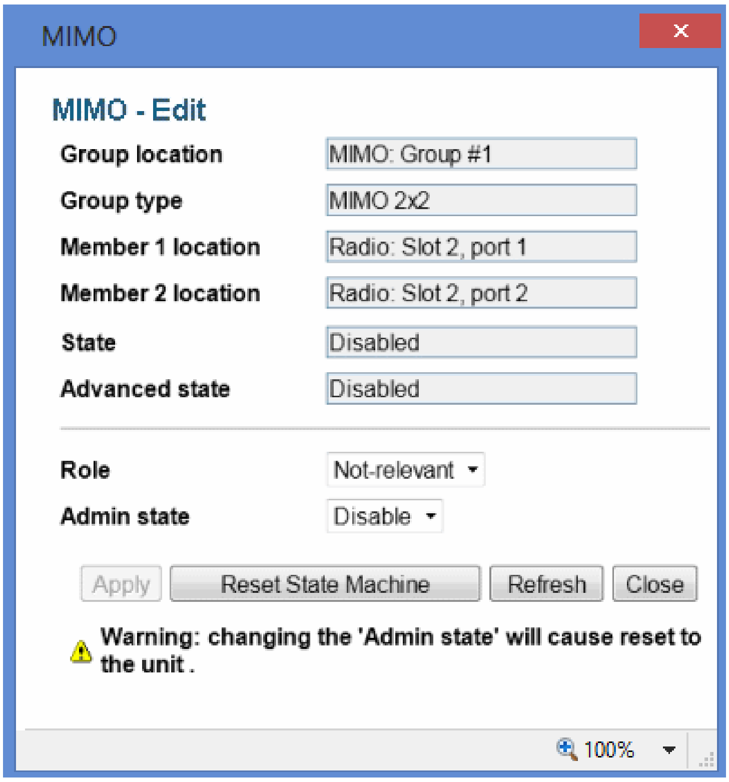
3.7.5. Setting the Role of a MIMO or Space Diversity Group

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 NetStream Diplo 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 61: MIMO - Edit Page



MIMO - Edit

Group location: MIMO: Group #1

Group type: MIMO 2x2

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: Disable

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

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 NetStream Diplo 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**.

3.7.6. 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

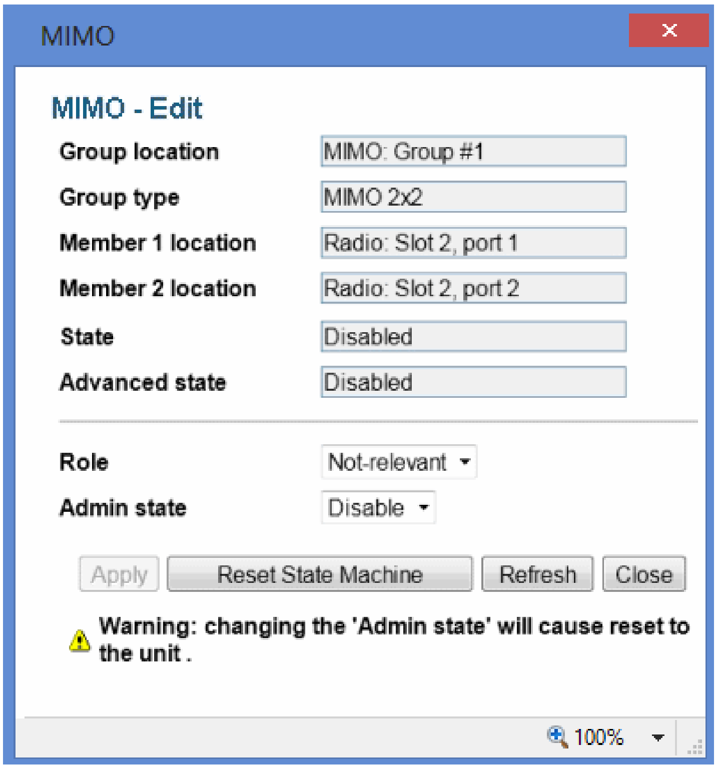
MIMO reset causes a traffic interruption.

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 62: MIMO - Edit Page



MIMO - Edit

Group location: MIMO: Group #1
Group type: MIMO 2x2
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: Disable

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

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

3.7.7. Viewing MMI and XPI Levels

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

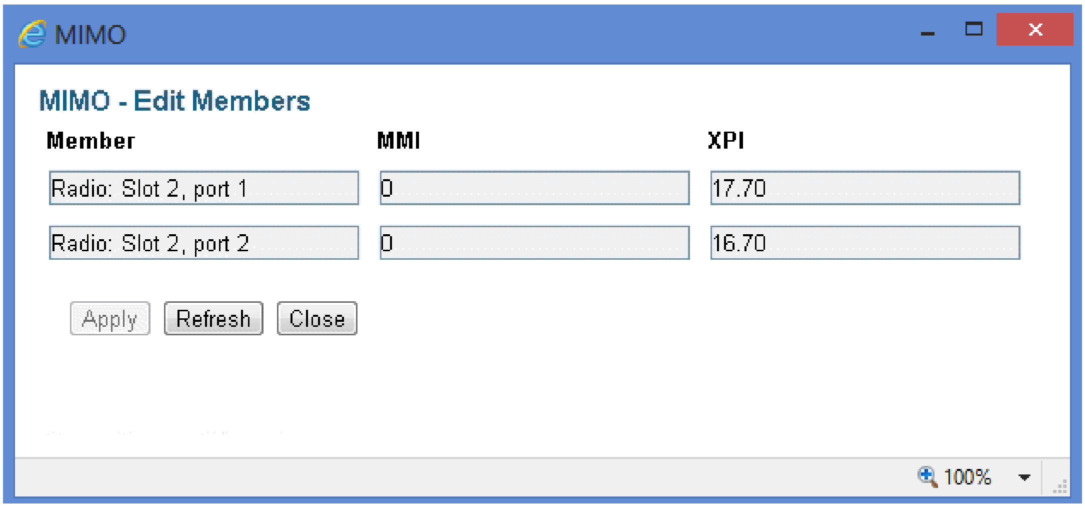
Note that the MMI value can also be calculated manually. To calculate it manually, you must measure the following RSL levels per receiver:

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 63: MIMO - Edit Members Page



MIMO - Edit Members

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

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*.

3.7.8. 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.

3.8. Operating an NetStream Diplo in Single Radio Carrier Mode

If you wish to operate an NetStream Diplo 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 *Deleting a Multi-Carrier ABC Group*.
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*.

4. Unit Management

This section includes:

- *Defining the IP Protocol Version for Initiating Communications*
- *Configuring the Remote Unit's IP Address*
- *Configuring SNMP*
- *Configuring Trap Managers*
- *Installing and Configuring an FTP or SFTP Server*
- *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*

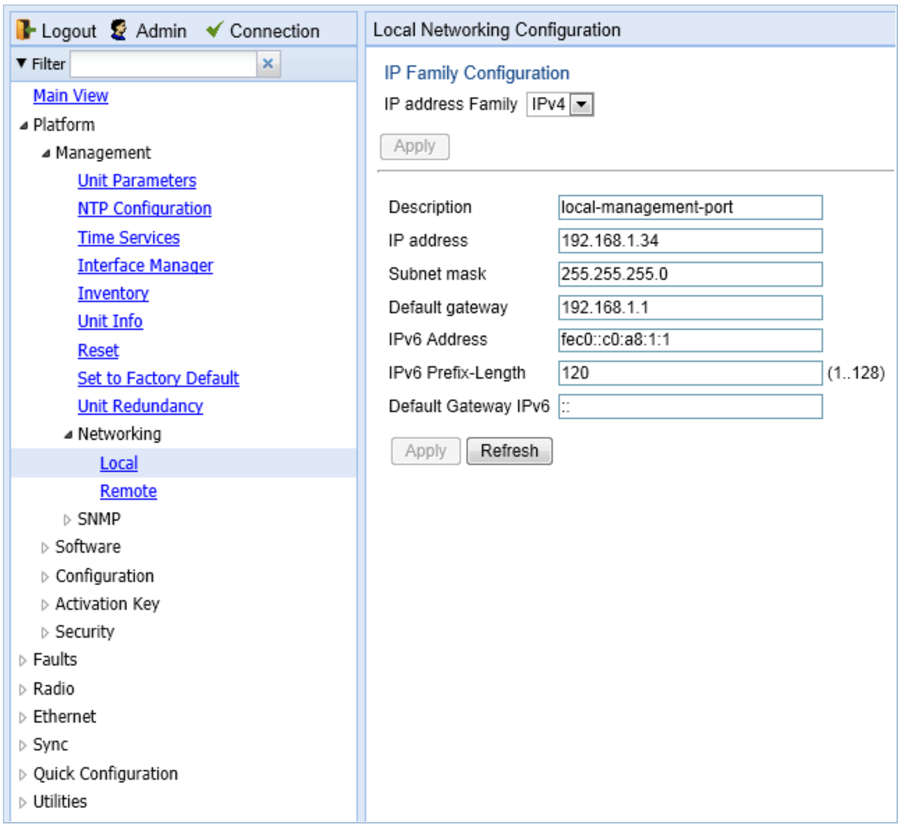
4.1. Defining the IP Protocol Version for Initiating Communications

You can specify which IP protocol the unit will use when initiating communications, such as downloading software, sending traps, pinging, or exporting configurations. The options are IPv4 or IPv6.

To set the IP protocol version of the local unit:

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

Figure 64: Local Networking Configuration Page



Local Networking Configuration

IP Family Configuration

IP address Family: IPv4

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	::

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

4.2. Configuring the Remote Unit's IP Address

You can configure the IP address of a remote unit.

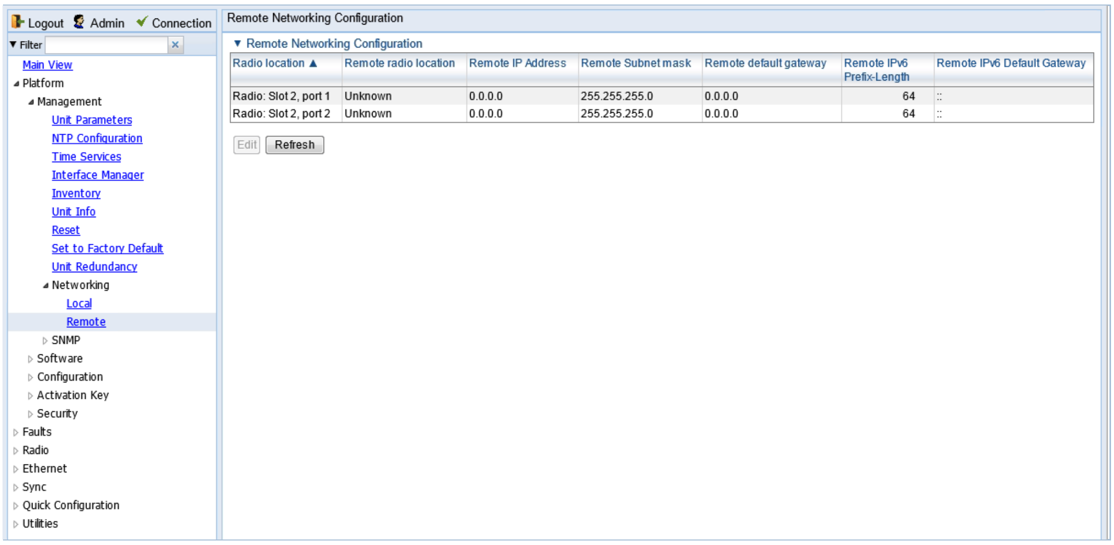
To configure the IP address of a remote unit:

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

- For NetStream Diplo units, the Radio Parameters page initially displays a table as shown in *Figure 65*.

- ○ For NetStream Primo units and NS Primo/DiploE units, the page appears as shown in *Figure 66*.

Figure 65: Remote Networking Configuration Page – NetStream Diplo

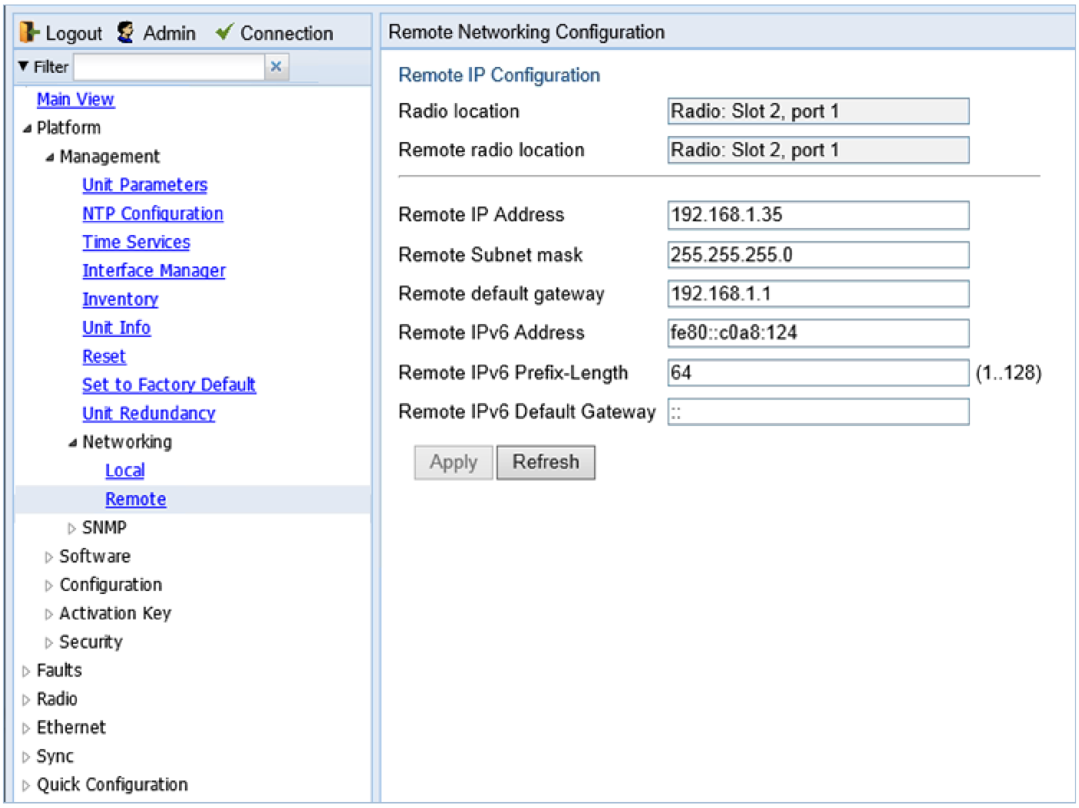


Remote Networking Configuration

▼ Remote Networking Configuration

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	::

Figure 66: Remote Networking Configuration Page – NetStream Primo and NS Primo/DiploE



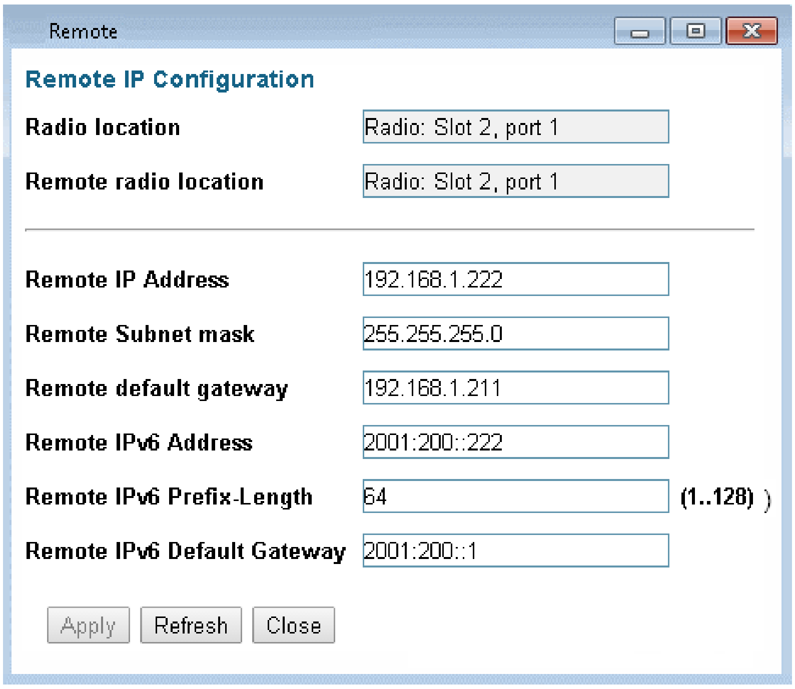
Remote Networking Configuration

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	::

2 For NetStream Diplo units, select the carrier in the Radio table (see *Figure 65*) and click **Edit**. A separate Remote IP Configuration page opens. The page is identical to the NetStream Diplo and NetStream Primo page.

Figure 67: Remote IP Configuration Page Per Carrier – NetStream Diplo



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

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**.

4.2.1. 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.

4.3. Configuring SNMP

NetStream Primo, and NS Primo/Diplo support SNMP v1, V2c, and v3. You can set community strings for access to NS Primo/Diplo units.

NetStream Diplo, NetStream Primo, and NS Primo/DiploE support the following MIBs:

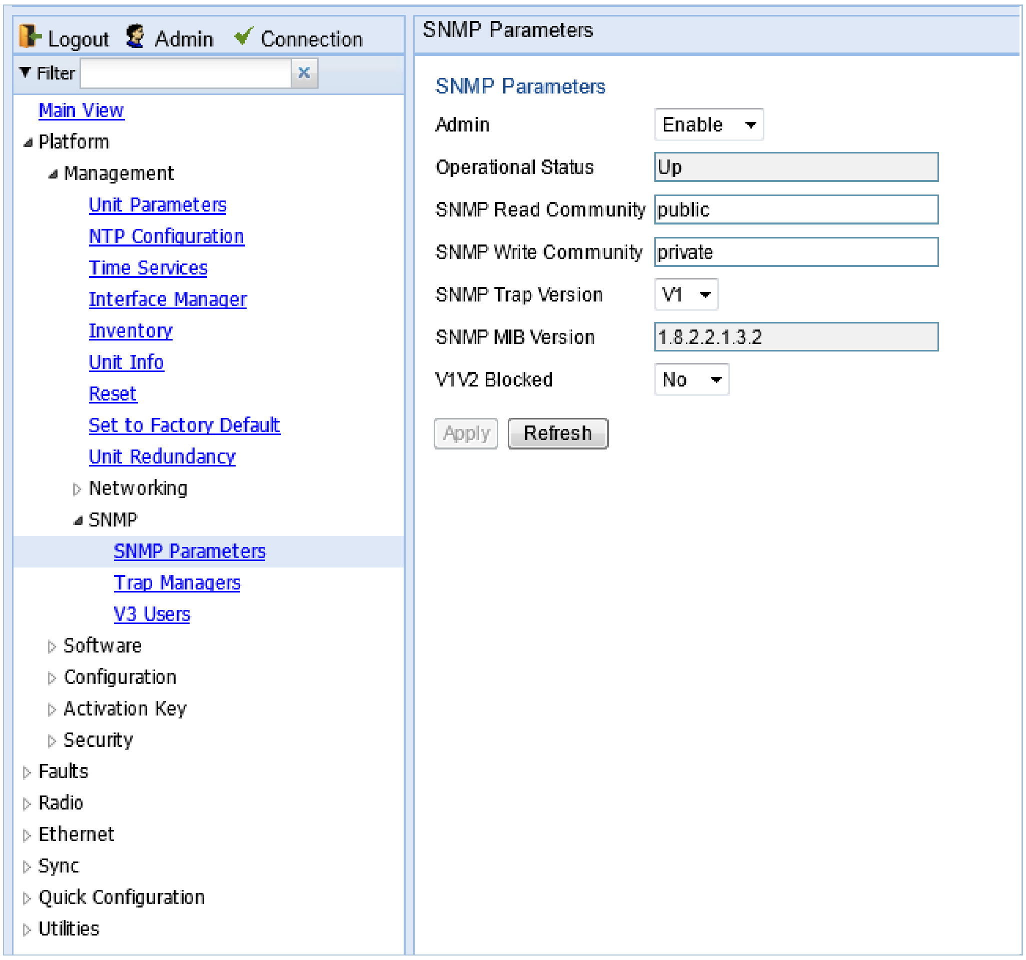
- RFC-1213 (MIB II).
- RMON MIB.
- Proprietary MIB.

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 68: SNMP Parameters Page



SNMP Parameters

Admin	Enable
Operational Status	Up
SNMP Read Community	public
SNMP Write Community	private
SNMP Trap Version	V1
SNMP MIB Version	1.8.2.2.1.3.2
V1V2 Blocked	No

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

Note

The **Operational Status** field indicates whether SNMP monitoring is currently active (**Up**) or inactive (**Down**).

3 In the **SNMP Read Community** field, enter the community string for the SNMP read community.

4 In the **SNMP Write Community** field, enter the community string for the SNMP write community

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

Note

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

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

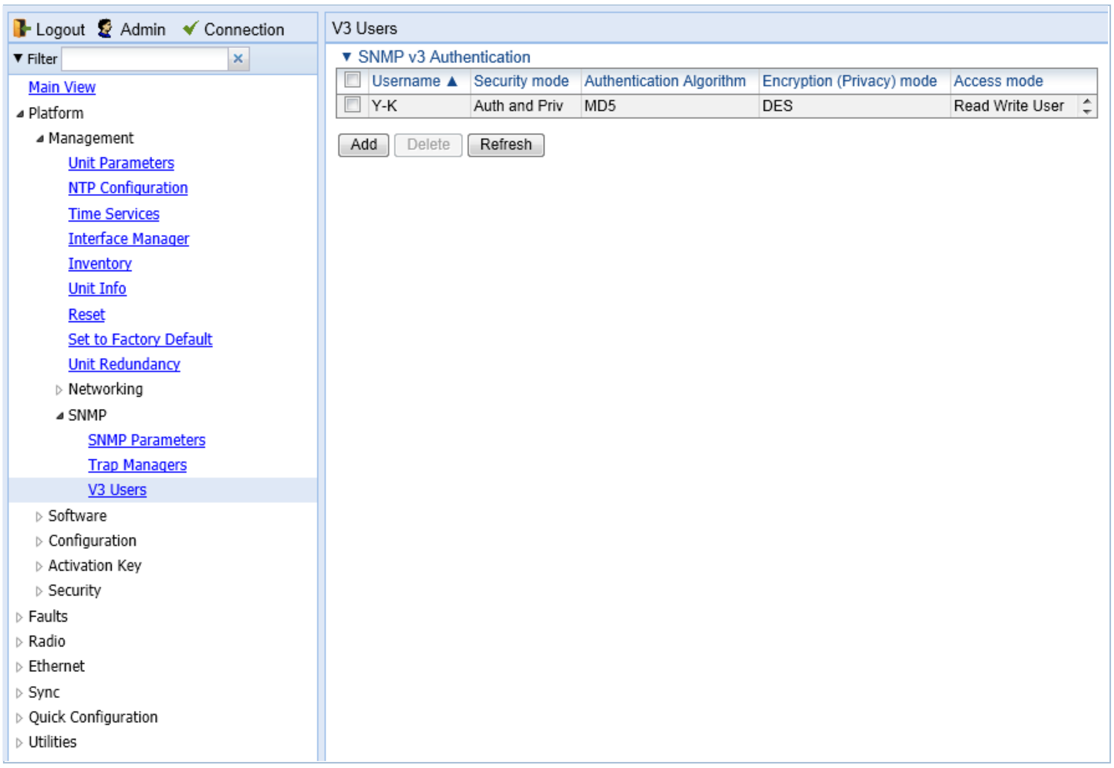
7 Click **Apply**.

If you are using SNMPv3, you must also configure SNMPv3 users. SNMPv3 security parameters are configured per SNMPv3 user.

To add an SNMP user:

1 Select **Platform > Management SNMP > V3 Users**. The V3 Users page opens.

Figure 69: V3 Users Page



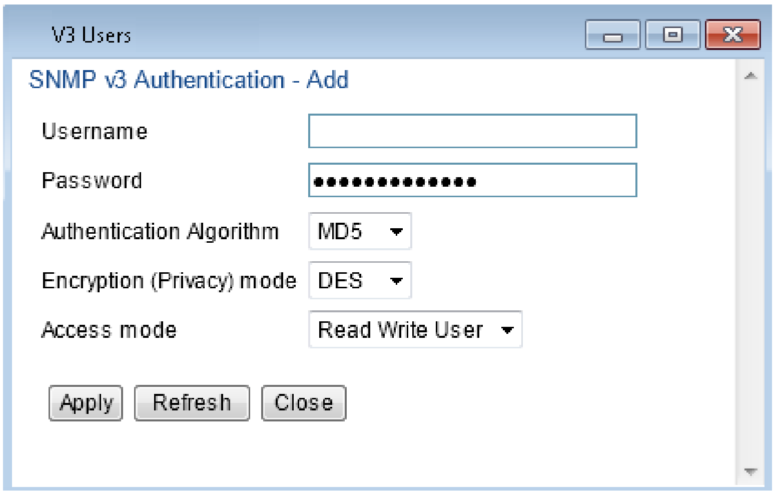
V3 Users

▼ SNMP v3 Authentication

☐	Username ▲	Security mode	Authentication Algorithm	Encryption (Privacy) mode	Access mode
☐	Y-K	Auth and Priv	MD5	DES	Read Write User

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

Figure 70: V3 Users - Add Page



SNMP v3 Authentication - Add

Username

Password ●●●●●●●●●●●●●

Authentication Algorithm MD5

Encryption (Privacy) mode DES

Access mode Read Write User

3 Configure the SNMP V3 Authentication parameters, as described below.

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

Table 15: SNMP V3 Authentication Parameters

Parameter	Definition
User Name	Enter the SNMPv3 user name.
Password	Enter a password for SNMPv3 authentication. The password must be at least eight characters.
Authentication Algorithm	Select an authentication algorithm for the user. Options are: ● **None** ● **SHA** ● **MD5**
Encryption (Privacy) Mode	Select an encryption (privacy) protocol for the user. Options are: ● **None** ● **DES** ● **AES**
Access Mode	Select an access permission level for the user. Options are: ● **Read Write User** ● **Read Only User**

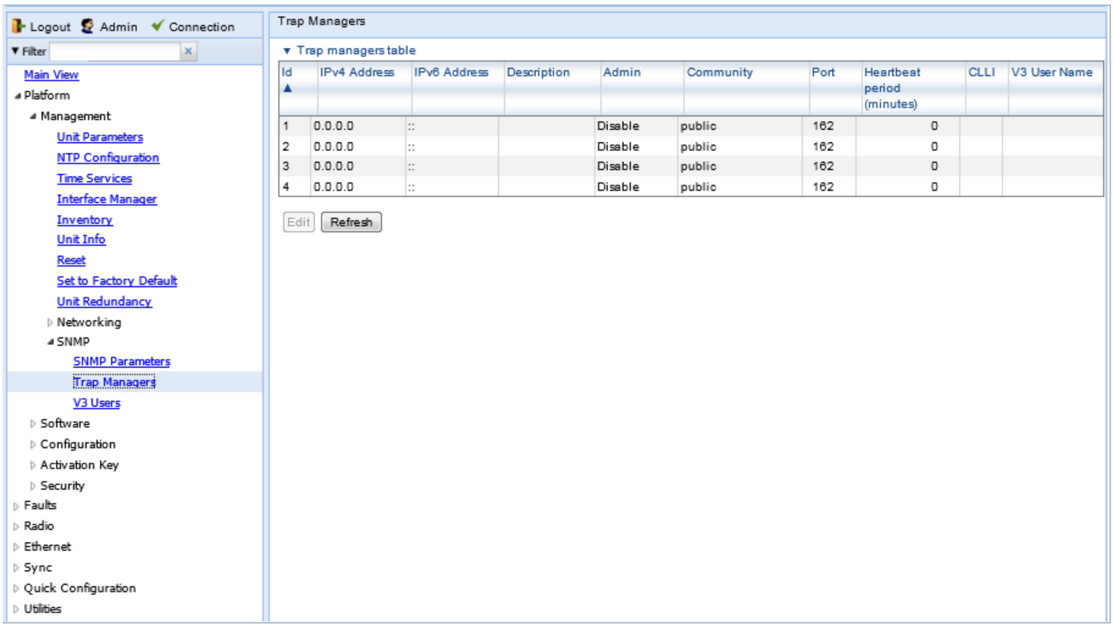
4.4. Configuring Trap Managers

You can configure trap forwarding parameters by editing the Trap Managers table. Each line in the Trap Managers table displays the setup for a manager defined in the system.

To configure trap managers:

1 Select **Platform > Management > SNMP > Trap Managers**. The Trap Managers page opens.

Figure 71: Trap Managers Page



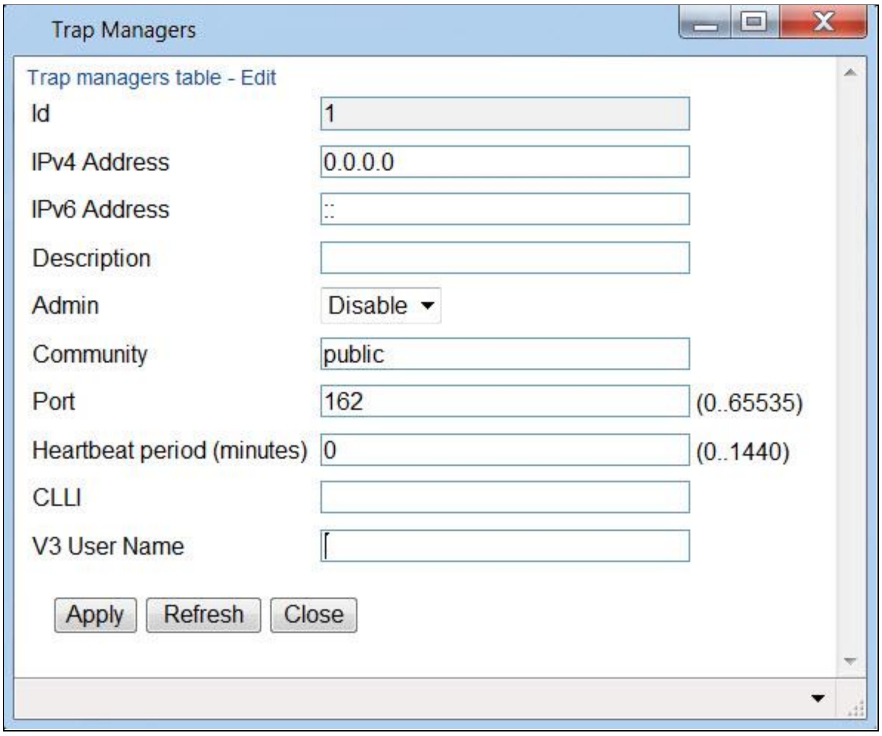
Trap Managers

Trap managers table

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

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

Figure 72: Trap Managers - Edit Page



Trap Managers

Trap managers table - Edit

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

3 Configure the trap manager parameters, as described in *Table 16*.

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

Table 16: Trap Manager Parameters

Parameter	Definition
IPv4 Address	If the IP address family is configured to be IPv4, enter the destination IPv4 address. Traps will be sent to this IP address. See *Defining the IP Protocol Version for Initiating Communications*.
IPv6 Address	If the IP address family is configured to be IPv6, enter the destination IPv6 address. Traps will be sent to this IP address. See *Defining the IP Protocol Version for Initiating Communications*.
Description	Enter a description of the trap manager (optional).
Admin	Select **Enable** or **Disable** to enable or disable the selected trap manager.
Community	Enter the community string for the SNMP read community.
Port	Enter the number of the port through which traps will be sent.
Heartbeat Period	Enter the interval, in minutes, between each heartbeat trap.
CLLI	Enter a Common Language Location Identifier (CLLI). The CLLI is free text that will be sent with the trap. You can enter up to 100 characters.
V3 User Name	If the SNMP Trap version selected in *SNMP Parameters* page is **V3**, enter the name of a V3 user defined in the system. To view or define a V3 user, use the *V3 Users* page. Note Make sure that an identical V3 user is also defined on the manager's side.

4.5. Installing and Configuring an FTP or SFTP Server

Several tasks, such as software upgrade and configuration backup, export, and import, require the use of FTP or SFTP. The NS Primo/Diplo 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).

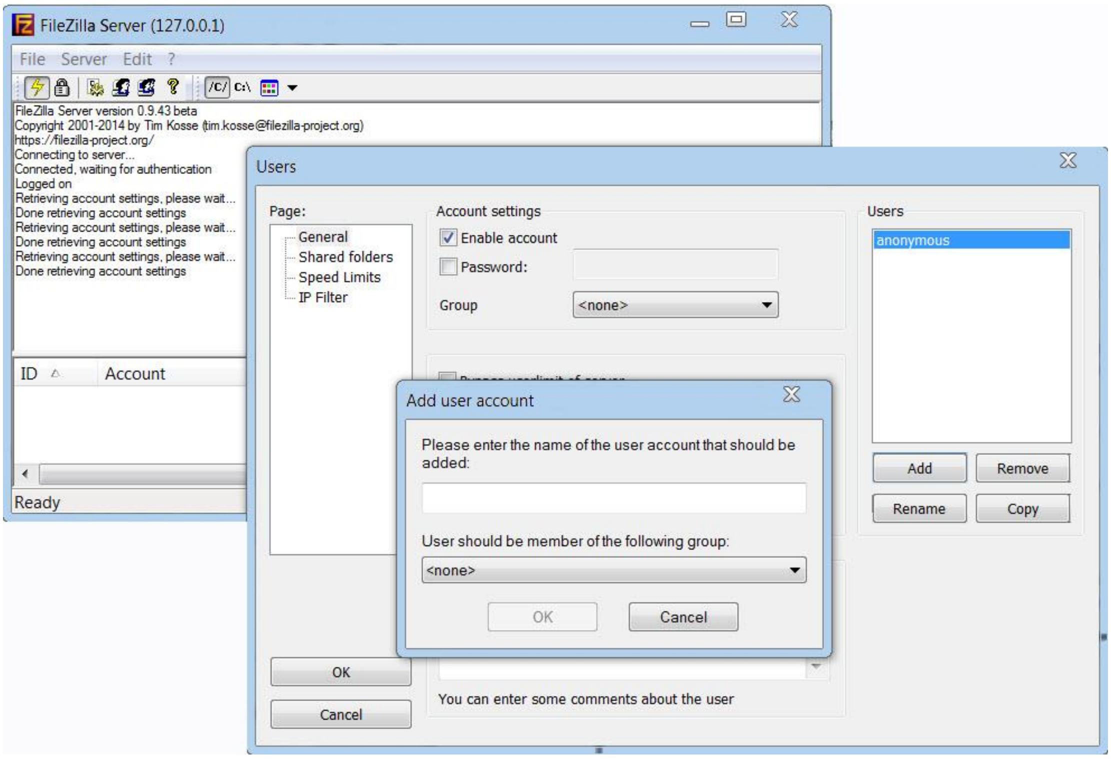
If you are using IPv6 to perform the operation, make sure to use FileZilla version 0.9.38 or higher to ensure IPv6 support. If you are using another type of FTP or SFTP server, make sure the application version supports IPv6.

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:

i From the **Edit** menu, select **Users**.
ii In the Users window, click **Add**.
iii In the Add user account window, enter a user name and click **OK**.
iv In the Users window, select **Enable account** and, optionally, select **Password** and enter a password.
v In the Users window, click **OK**.

Figure 73: FileZilla Server User Configuration



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

☑ Enable account
□ Password:
Group <none>

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

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

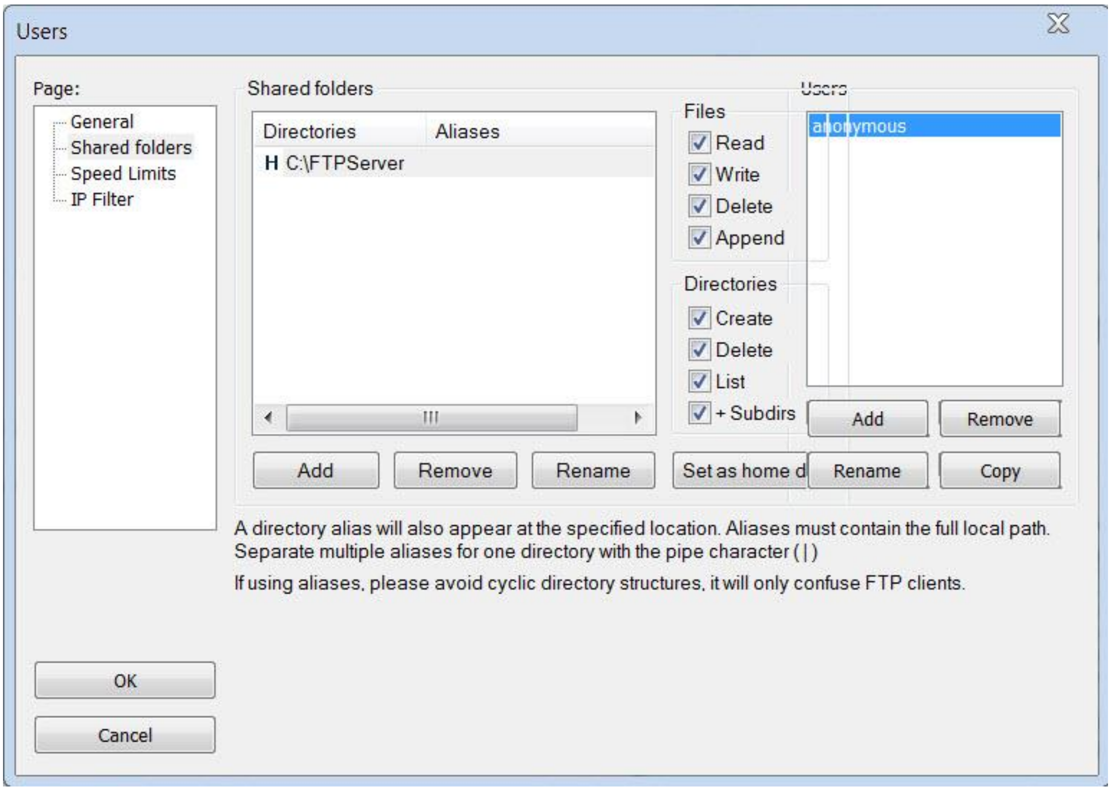
You can enter some comments about the user

2 Create a shared FTP/SFTP folder on the PC or laptop you are using to perform the software upgrade (for example, *C:\FTPServer*).

3 In the FTP/SFTP server, set up the permissions for the shared FTP/SFTP folder. For example, in FileZilla Server:

i From the **Edit** menu, select **Users**.
ii In the Users window, select **Shared folders**.
iii Underneath the Shared folders section, click **Add** and browse for your shared FTP folder.
iv Select the folder and click **OK**.
v In the Shared folders section, select your shared FTP folder.
vi In the Files and Directories sections, select all of the permissions.
vii Click **Set as home directory** to make the Shared folder the root directory for your FTP server.
viii Click **OK** to close the Users window.

Figure 74: FileZilla Server Shared Folder Setup



H C:\FTPServer

Files: ☑ Read ☑ Write ☑ Delete ☑ Append

Directories: ☑ Create ☑ Delete ☑ List ☑ + Subdirs

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

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

4.6. Upgrading the Software

NS Primo/Diplo 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:

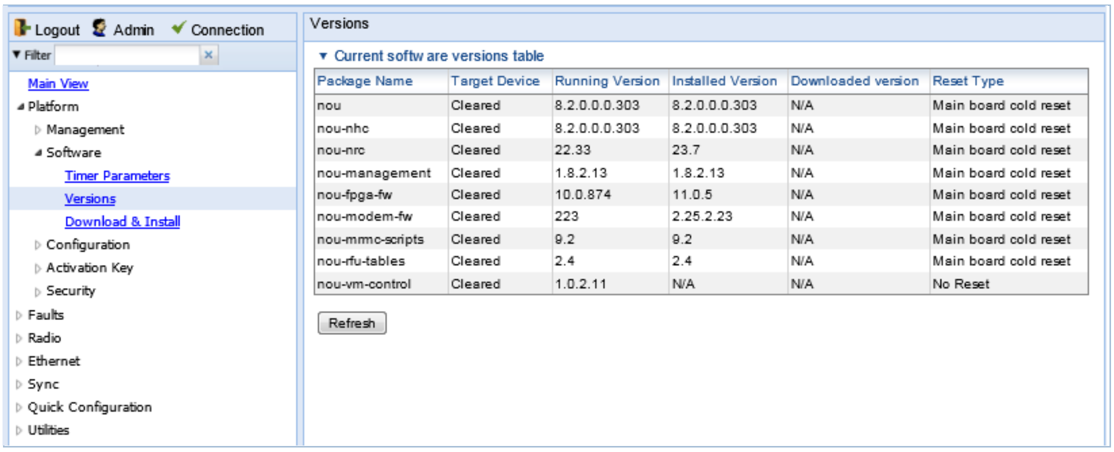
- *Viewing Current Software Versions*
- *Software Upgrade Overview*
- *Downloading and Installing Software*
- *Configuring a Timed Installation*

4.6.1. Viewing Current Software Versions

To display a list of software packages currently installed and running on the system modules:

1 Select **Platform > Software > Versions**. The Versions page opens. For a description of the information provided in the Versions page, see *Table 17: Versions Page Columns*.

Figure 75: Versions Page



Versions

Current softw are versions table

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-mmc-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 17: Versions Page Columns

Parameter	Definition
Package Name	The name of the software package.
Target Device	The specific component on which the software runs.
Running Version	The software version currently running on the component.
Installed Version	The software version currently installed for the component. If the installed version is not already the running version, it will become the running version after the next reset takes place.
Downloaded Version	The version, if any, that has been downloaded from the server but not yet installed. Upon installation, this version will become the Installed Version.
Reset Type	The level of reset required by the component in order for the Installed Version to become the Active Version. A cold (hard) reset powers down and powers back up the component. A warm (soft) reset simply reboots the software or firmware in the component.

4.6.2. Software Upgrade Overview

The NS Primo/Diplo 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 NS Primo/Diplo that are currently running an older version.
3. **Reset** – The NS Primo/Diplo 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 NS Primo/Diplo 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 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)*.

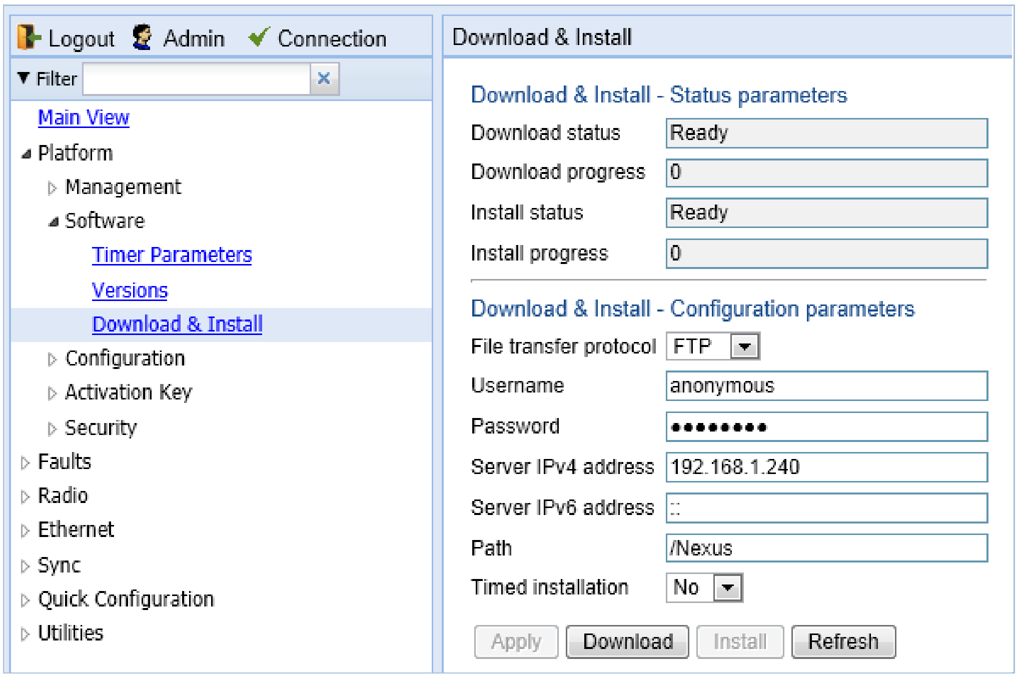
4.6.3. Downloading and Installing Software

When downloading software, the NS Primo/Diplo 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 download and install a new software version:

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 NS Primo/Diplo into your shared FTP or SFTP folder.
4. In the NS Primo/Diplo's Web EMS, select **Platform > Software > Download & Install**. The Download & Install page opens.

Figure 76: Download & Install Page



Download & Install

Download & Install - Status parameters

Download status	Ready
Download progress	0
Install status	Ready
Install progress	0

Download & Install - Configuration parameters

File transfer protocol	FTP
Username	anonymous
Password	••••••••
Server IPv4 address	192.168.1.240
Server IPv6 address	::
Path	/Nexus
Timed installation	No

5 In the **File Transfer Protocol** field, select the file transfer protocol you want to use (**FTP** or **SFTP**).

6 In the **Username** field, enter the user name you configured in the FTP server.

7 In the **Password** field, enter the password you configured in the FTP server. If you did not configure a password for your FTP/SFTP user, simply leave this field blank.

8 If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the FTP/SFTP server in the **Server IPv4 address** field. See *Defining the IP Protocol Version for Initiating Communications*.

9 If the IP address family is configured to be IPv6, enter the IPv6 address of the PC or laptop you are using as the FTP/SFTP server in the **Server IPv6 Address** field. See *Defining the IP Protocol Version for Initiating Communications*.

10 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. To leave the path blank, enter //.

11 To configure a timed installation, in the **Timed installation** field, select **Yes**. Otherwise, select **No**. For more information on timed installations, see *Configuring a Timed Installation*.

12 Click **Apply** to save your settings.

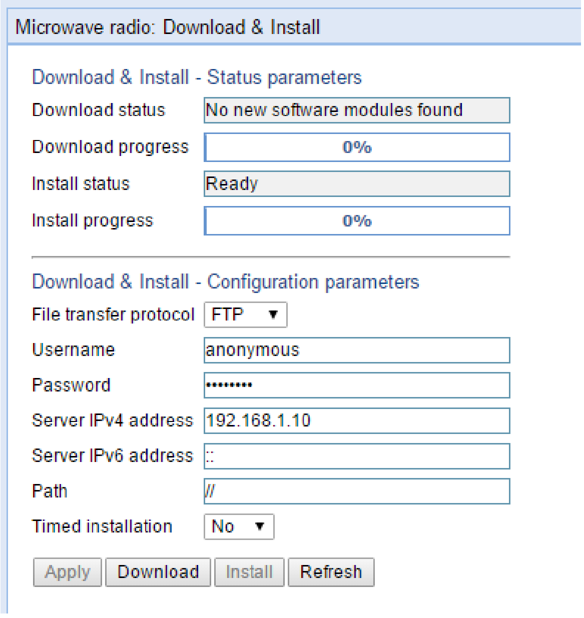
13 Click **Download**. The download begins. You can view the status of the download in the **Download & Install - Status Parameters** section of the Download & Install page. See *Table 18*.

14 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**.



Microwave radio: Download & Install

Download & Install - Status parameters

Download status	No new software modules found
Download progress	0%
Install status	Ready
Install progress	0%

Download & Install - Configuration parameters

File transfer protocol	FTP
Username	anonymous
Password	••••••••
Server IPv4 address	192.168.1.10
Server IPv6 address	::
Path	//
Timed installation	No

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

15 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 18*.

Upon completion of the installation, the system performs an automatic reset.

Note

DO NOT reboot the unit during the software installation process. As soon as the process is successfully completed, the unit will reboot itself.

Sometimes the installation process can take up to 30 minutes.

Only in the event that software installation was not successfully finished and more than 30 minutes have passed can the unit be rebooted.

Table 18: Download & Install Status Parameters

Parameter	Definition
Download status	The status of any pending software download. Possible values are: ● **Ready** – The default value, which appears when no download is in progress. ● **Verifying download files** – The system is verifying the files to be downloaded. ● **Download in progress** – The download files have been verified, and the download is in progress. If an error occurs during the download, an appropriate error message is displayed in this field. When the download is complete, one of the following status indications appears: ● **Download Success** ● **Download Failure** ● **All components already found in the system** When the system is reset, the **Download Status** returns to **Ready**.
Download progress	Displays the progress of the current software download.
Install status	The status of any pending software installation. Possible values are: ● **Ready** – The default value, which appears when no installation is in progress. ● **Verifying installation files** – The system is verifying the files to be installed. ● **Installation in progress** – The installation files have been verified, and the installation is in progress. If an error occurs during the installation, an appropriate error message is displayed in this field. When the installation is complete, one of the following status indications appears: ● **Installation Success** ● **Installation Partial Success** ● **Installation Failure** ● **incomplete-sw-version** When the system is reset, the **Installation Status** returns to **Ready**.
Install progress	Displays the progress of the current software installation.

4.6.4. Configuring a Timed Installation

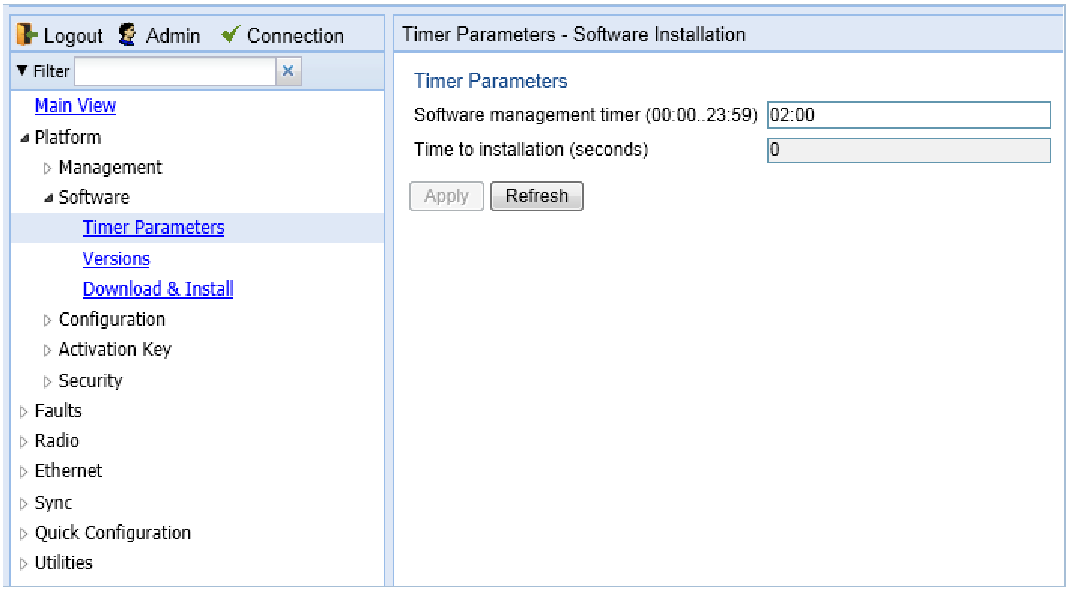
You can schedule a timed (deferred) software installation to take place at any time within 24 hours after you configure the installation.

To schedule a timed software installation:

1 Download the software version you want to install. See *Downloading and Installing Software*.

2 Select **Platform > Software > Timer Parameters**. The Timer Parameters – Software Installation page opens.

Figure 77: Timer Parameters - Software Installation Page



Timer Parameters - Software Installation

Timer Parameters

Software management timer (00:00..23:59): 02:00

Time to installation (seconds): 0

3 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 77*, the timer is set for two hours after the timer was configured (02:00).

4 Click **Apply**.

5 Select **Platform > Software > Download & Install**. The Download & Install page opens (*Figure 76*).

6 In the **Timed Installation** field, select **Yes**.

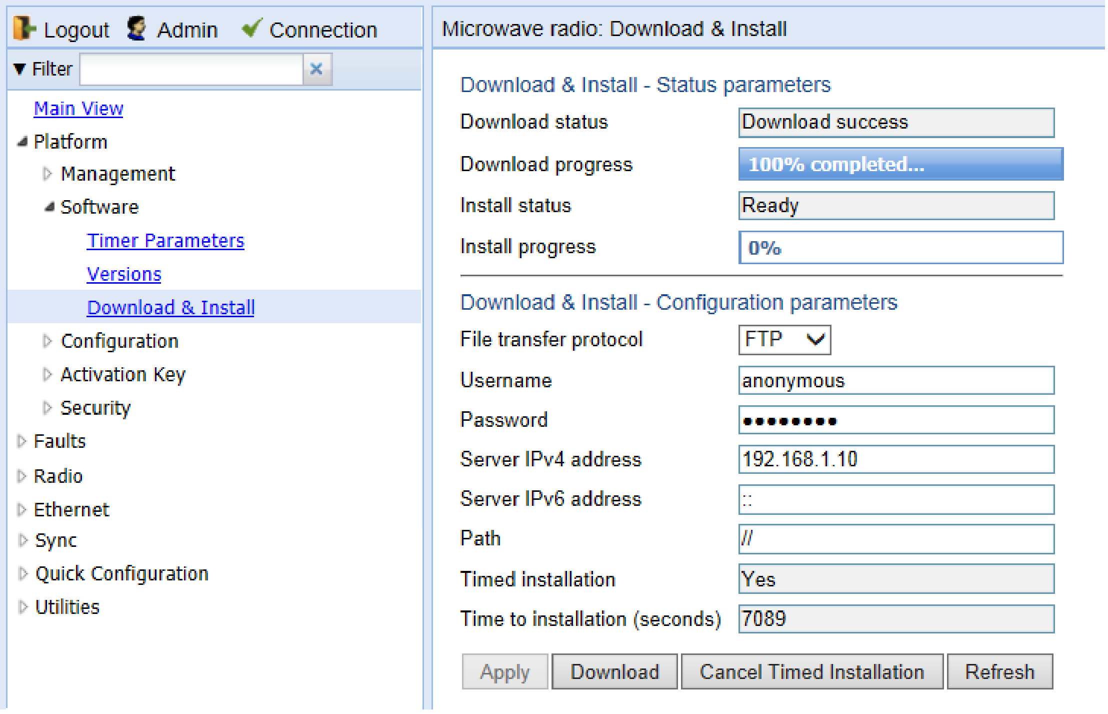
7 Click **Apply**.

8 Click **Install**. A confirmation window opens.

9 Click **OK**. The Download & Installation page is refreshed to include the following fields:

- **Time to installation** – Displays the time remaining, in seconds, until the scheduled installation.
- **Cancel Timed Installation** – Click to cancel the timed installation.

Figure 78: Download & Install Page – Timed Installation



Microwave radio: Download & Install

Download & Install - Status parameters

Download status	Download success
Download progress	100% completed...
Install status	Ready
Install progress	0%

Download & Install - Configuration parameters

File transfer protocol	FTP
Username	anonymous
Password	••••••••
Server IPv4 address	192.168.1.10
Server IPv6 address	::
Path	//
Timed installation	Yes
Time to installation (seconds)	7089

4.7. Backing Up and Restoring Configurations

You can import and export NS Primo/Diplo configuration files. This enables you to copy the system configuration to multiple NS Primo/Diplo units. You can also backup and save configuration files.

Configuration files can only be copied between units of the same type, i.e., NetStream Diplo to NetStream Diplo, NetStream Primo to NetStream Primo, and NS Primo/DiploE to NS Primo/DiploE.

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*

4.7.1. Configuration Management Overview

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

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

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

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

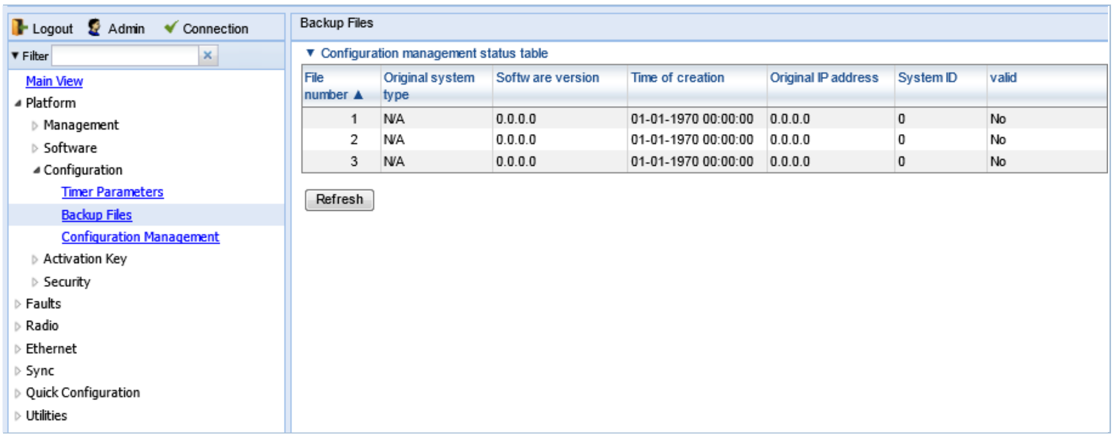
4.7.2. Viewing Current Backup Files

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

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

1 Select **Platform > Configuration > Backup Files**. The Backup Files page opens. For a description of the information provided in the Backup Files page, see *Table 19: Backup Files Page Columns*.

Figure 79: Backup Files Page



Backup Files

▼ Configuration management status table

File number ▲	Original system type	Softw are 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 19: Backup Files Page Columns

Parameter	Definition
File number	A number from 1 to 3 that identifies the restore point.
Original system type	The type of unit from which the backup configuration file was created.
Software version	The software version of the unit from which the backup configuration file was created.
Time of creation	The time and date on which the configuration file was created.
Original IP address	The IP address of the unit from which the configuration file was created.
System ID	The System ID, if any, of the unit from which the configuration file was created. This is taken from the **Name** field in the Unit Parameters page. See *Configuring Unit Parameters*.
Valid	Reserved for future use.

4.7.3. Setting the Configuration Management Parameters

When importing and exporting configuration files, the NS Primo/Diplo 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*.

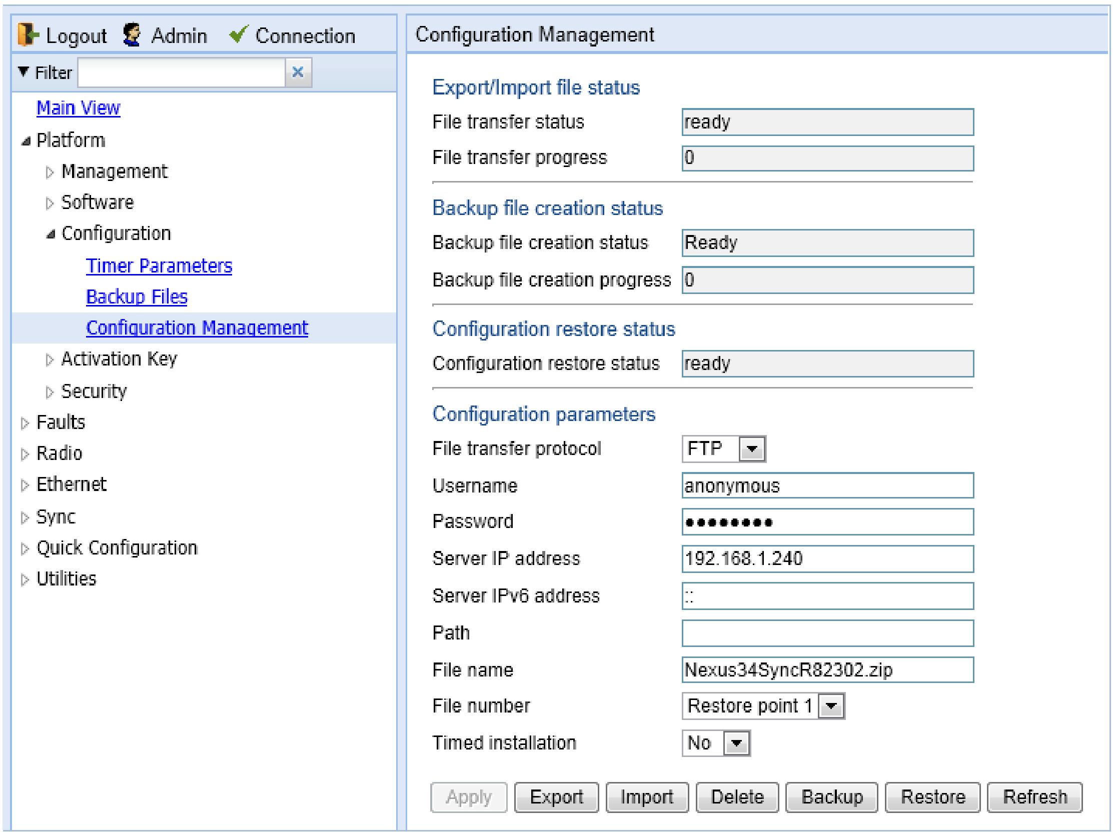
Before importing or exporting a configuration file, you must perform the following steps:

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 NS Primo/Diplo Web EMS, select **Platform > Configuration > Configuration Management**. The Configuration Management page opens.

Figure 80: Configuration Management Page



Configuration Management

Export/Import file status

File transfer status	ready
File transfer progress	0

Backup file creation status

Backup file creation status	Ready
Backup file creation progress	0

Configuration restore status

Configuration restore status	ready

Configuration parameters

File transfer protocol	FTP
Username	anonymous
Password	••••••••
Server IP address	192.168.1.240
Server IPv6 address	::
Path	
File name	Nexus34SyncR82302.zip
File number	Restore point 1
Timed installation	No

4 In the **File transfer protocol** field, select the file transfer protocol you want to use (**FTP** or **SFTP**).

5 In the **Username** field, enter the user name you configured in the FTP server.

6 In the **Password** field, enter the password you configured in the FTP server. If you did not configure a password for your FTP user, simply leave this field blank.

7 If the IP address family is configured to be IPv4, enter the IPv4 address of the PC or laptop you are using as the FTP server in the **Server 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 directory path to or from which you are downloading or uploading the file. Enter the path relative to the FTP user's home directory, not the absolute path. To leave the path blank, enter //.

10 In the **File name** field, enter the name of the file you are importing, or the name you want to give the file you are exporting.

Note

You must add the suffix **.zip** to the file name. Otherwise, the file import may fail. You can export the file using any name, then add the suffix **.zip** manually.

11. 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.

12. Click **Apply** to save your settings.

4.7.4. Exporting a Configuration File

You can export a saved configuration file from one of the system's three restore points to a PC or laptop.

To export a configuration file:

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 80*).
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**.

4.7.5. Importing a Configuration File

You can import a saved configuration file from a PC or laptop to one of the system's three restore points.

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 80*).
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*.

4.7.6. Deleting a Configuration File

You can delete a saved configuration file from any of the system's three restore points:

To delete a configuration file:

1 Select **Platform > Configuration > Configuration Management**. The Configuration Management page opens (*Figure 80*).

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.

4.7.7. Backing Up the Current Configuration

You can back up the current configuration file to one of the system's three restore points.

To back up a configuration file:

1 Select **Platform > Configuration > Configuration Management**. The Configuration Management page opens (*Figure 80*).

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**.

4.7.8. Restoring a Saved Configuration

You can replace the current configuration with any configuration file saved to one of the system's three restore points by restoring the configuration file from the restore point. Restoring a saved configuration does not change the unit's FIPS mode.

To restore a configuration file:

1 Select **Platform > Configuration > Configuration Management**. The Configuration Management page opens (*Figure 80*).
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.

4.7.9. Editing CLI Scripts

The configuration file package includes a text file that enables you to write CLI scripts in a backed-up configuration that are executed after restoring the configuration.

To edit a CLI script:

1 Back up the current configuration to one of the restore points. 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.

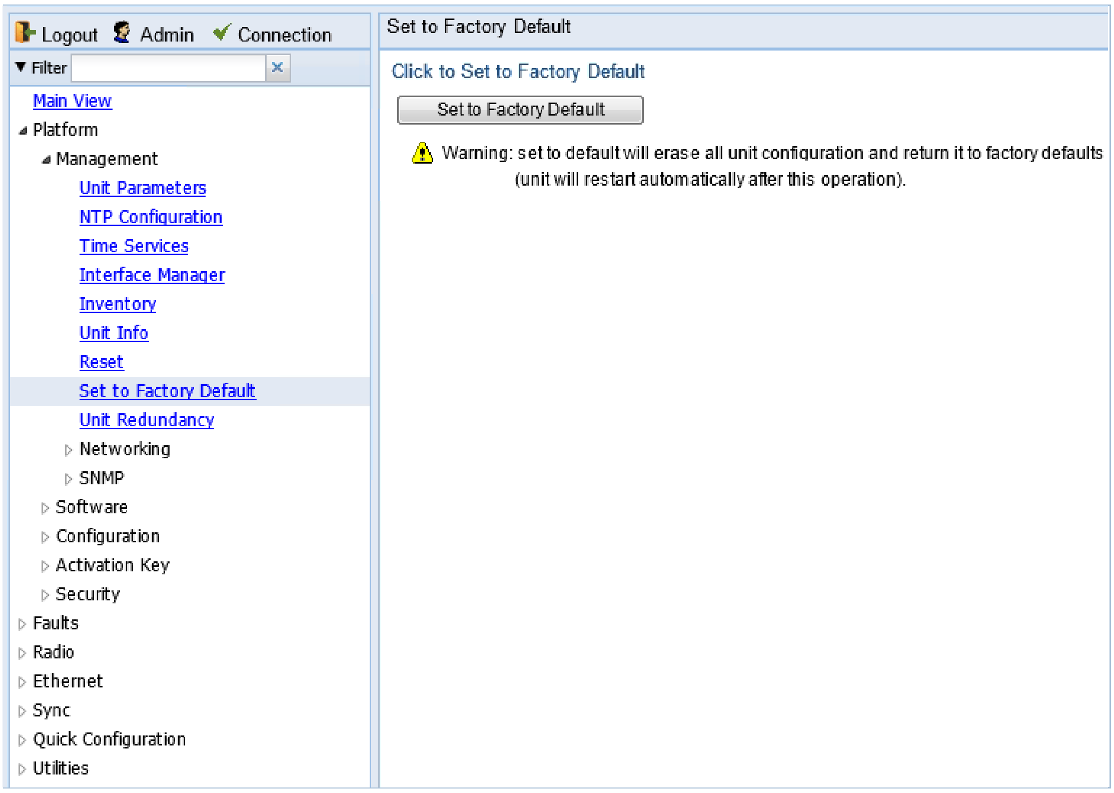
4.8. Setting the Unit to the Factory Default Configuration

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 81: Set to Factory Default Page



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

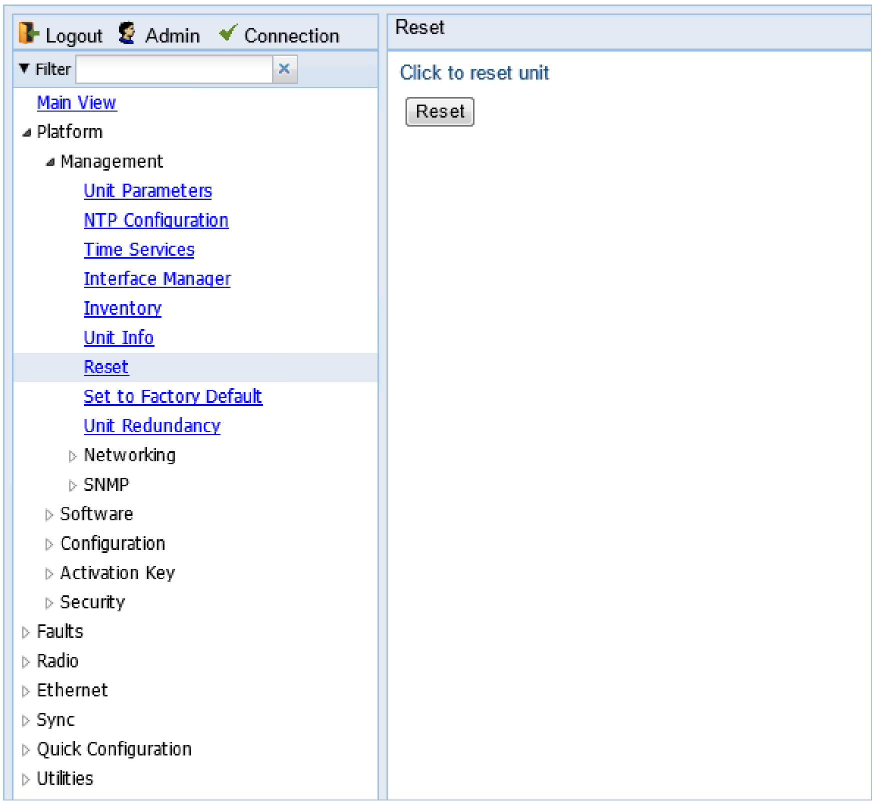
2 Click **Set to Factory Default**. The unit is restored to its factory default settings. This does not change the unit's IP address or FIPS configuration.

4.9. Performing a Hard (Cold) Reset

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

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

Figure 82: Reset Page



2 Click **Reset**.

3 A prompt appears asking if you want to proceed with the reset. Click **Yes** to initiate the reset.

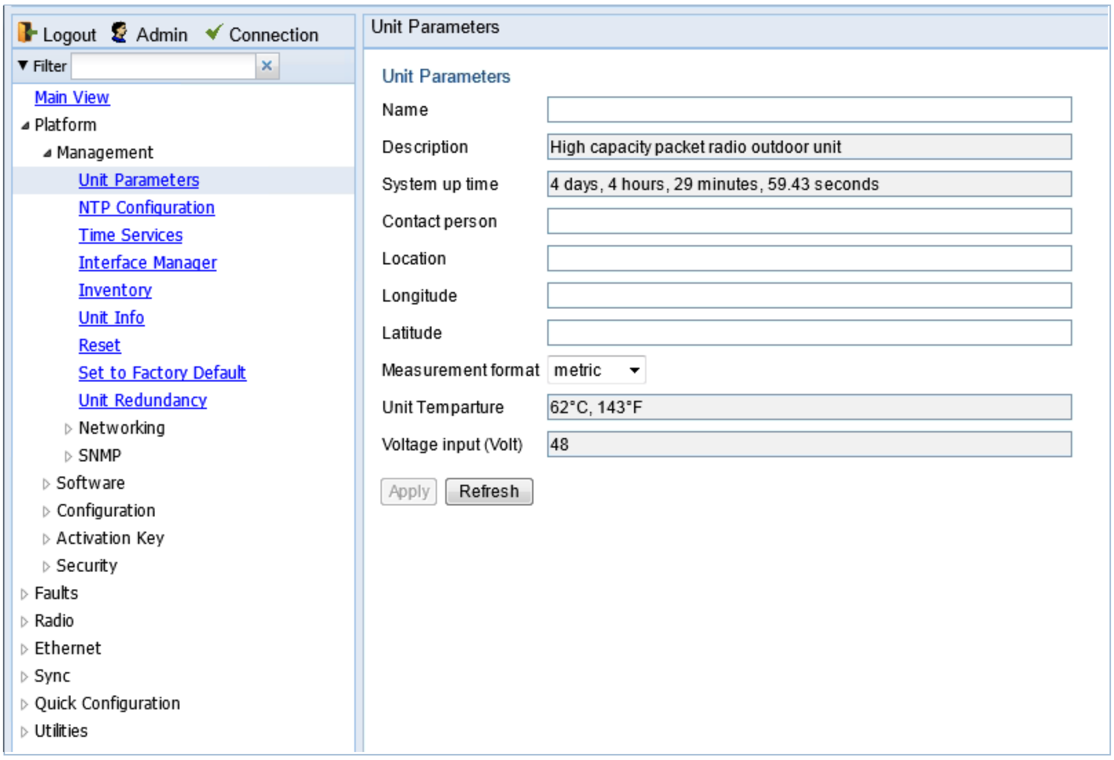
The unit is reset.

4.10. Configuring Unit Parameters

To view and configure system information:

1 Select **Platform > Management > Unit Parameters**. The Unit Parameters page opens. *Table 20* describes the fields in the Unit Parameters page.

Figure 83: Unit Parameters Page



Unit Parameters

Unit Parameters

Name	
Description	High capacity packet radio outdoor unit
System up time	4 days, 4 hours, 29 minutes, 59.43 seconds
Contact person	
Location	
Longitude	
Latitude	
Measurement format	metric
Unit Temparture	62°C, 143°F
Voltage input (Volt)	48

Table 20: 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 unit type.
System up time	The time since the system was last reinitialized.
Contact person	The name of the person to be contacted if and when a problem with the system occurs (optional).
Location	The actual physical location of the node or agent (optional).
Longitude	The unit's longitude coordinates.
Latitude	The unit's latitude coordinates.
Measurement format	The type of measurement you want the system to use: **Metric** or **Imperial**.
Unit Temperature	The current temperature of the unit.
Voltage input (Volt)	The voltage input of the unit.

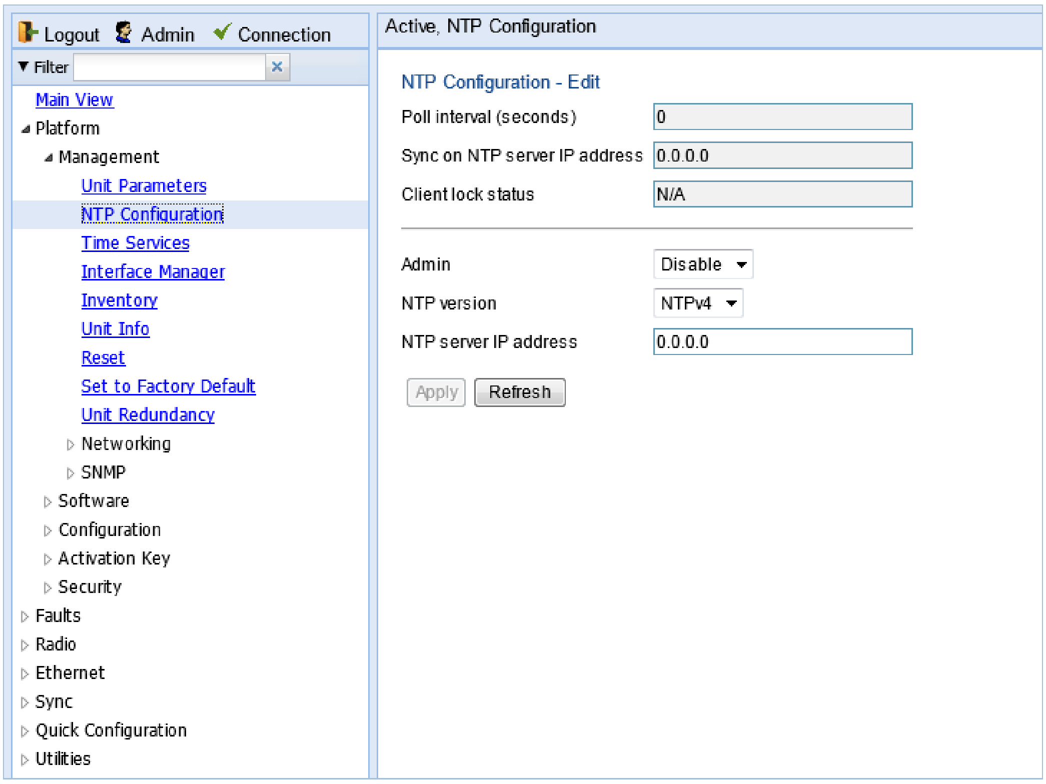
4.11. Configuring NTP

NS Primo/Diplo 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 84: NTP Configuration Page



NTP Configuration - Edit

Poll interval (seconds) 0

Sync on NTP server IP address 0.0.0.0

Client lock status N/A

Admin Disable

NTP version NTPv4

NTP server IP address 0.0.0.0

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 21 describes the status parameters that appear in the NTP Configuration page.

Table 21: NTP Status Parameters

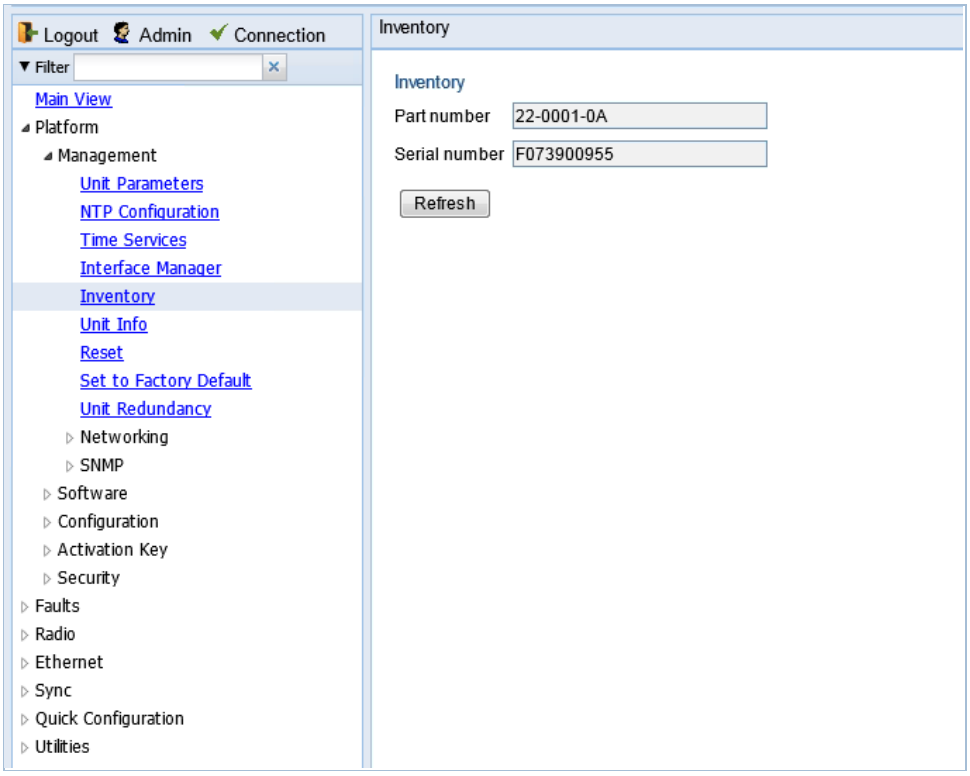
Parameter	Definition
Poll interval	Displays the interval used by the NTP client to maintain synchronization with the current NTP server.
Sync on NTP server IP address	Displays the IP address of the remote NTP server on which the NTP client is currently locked.
Client lock status	Indicates if the NTP client is locked on a remote NTP server. Possible values are: ● **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.

4.12. Displaying Unit Inventory

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

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

Figure 85: Inventory Page



Part number 22-0001-0A

Serial number F073900955

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 HSB Radio Protection*
- *Configuring MIMO and Space Diversity*
- *Operating an NetStream Diplo in Single Radio Carrier Mode*
- *Performing Radio Loopback*

5.1. Viewing the Radio Status and Settings

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

Note

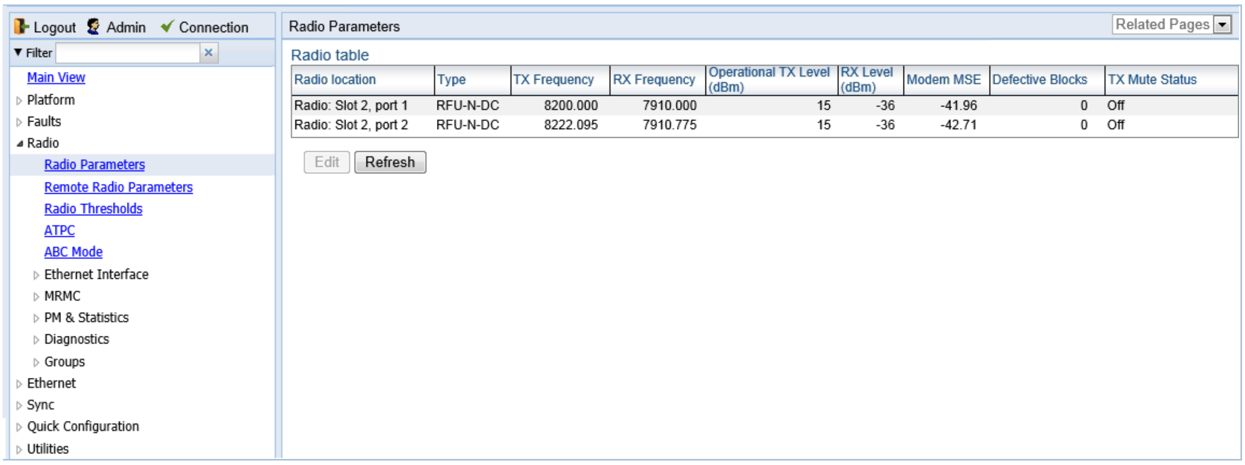
For instructions how to configure the radio parameters, see *Configuring the Radio Parameters*.

To display the radio parameters:

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

- For NetStream Diplo units, the Radio Parameters page initially displays a table as shown in *Figure 86*.
- For NetStream Primo units and NS Primo/DiploE units, a page appears, similar to *Figure 17* (which shows an NetStream Diplo page).

Figure 86: Radio Parameters Page – NetStream Diplo



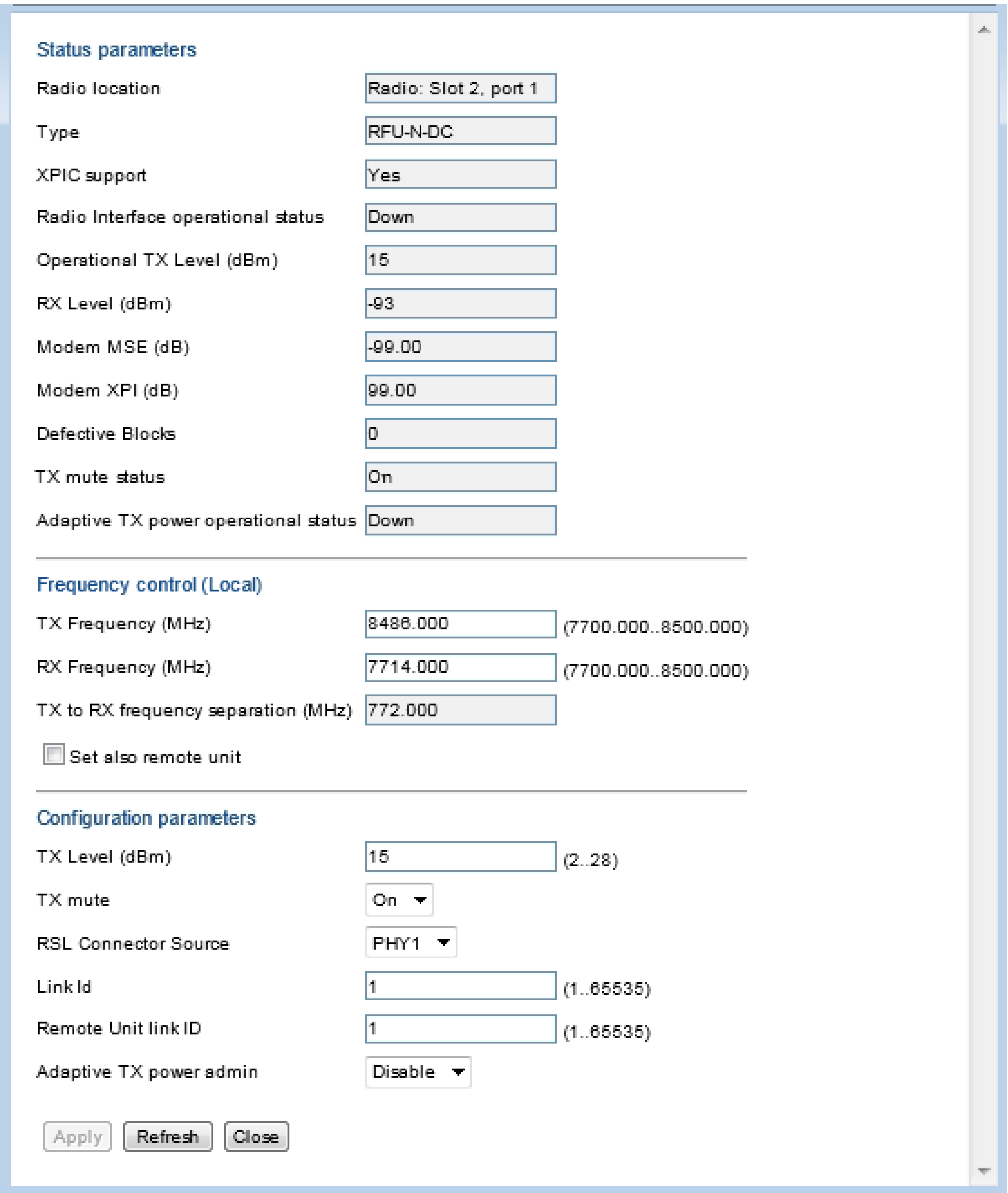
Radio Parameters

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

2 For NetStream Diplo units, select the carrier in the Radio table (see *Figure 86*) and click **Edit**. A separate Radio Parameters page opens. The page is essentially identical to the NS Primo/DiploE and NetStream Primo page, except for the addition of a **Radio location** parameter.

Figure 87: Radio Parameters Page Per Carrier – NetStream Diplo



Status parameters

Radio location	Radio: Slot 2, port 1
Type	RFU-N-DC
XPIC support	Yes
Radio Interface operational status	Down
Operational TX Level (dBm)	15
RX Level (dBm)	-93
Modem MSE (dB)	-99.00
Modem XPI (dB)	99.00
Defective Blocks	0
TX mute status	On
Adaptive TX power operational status	Down

Frequency control (Local)

TX Frequency (MHz)	8486.000	(7700.000..8500.000)
RX Frequency (MHz)	7714.000	(7700.000..8500.000)
TX to RX frequency separation (MHz)	772.000	

☐ Set also remote unit

Configuration parameters

TX Level (dBm)	15	(2..28)
TX mute	On	
RSL Connector Source	PHY1	
Link Id	1	(1..65535)
Remote Unit link ID	1	(1..65535)
Adaptive TX power admin	Disable	

Table 22 lists and describes the parameters in the Radio table of the NetStream Diplo Radio Parameters page and the **Status parameters** section of the Radio Parameters configuration page.

Table 22: Radio Status Parameters

Parameter	Description
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 NetStream Diplo 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 -99.00 dB means that the modem is not locked.
Modem XPI (dB)	The XPI (Cross Polarization Interference) level, measured in dB. Note Only relevant for NetStream Diplo units.
Defective Blocks	The number of defective radio blocks that have been counted.
TX Mute Status	Indicates whether radio transmission is muted.
Adaptive TX power operational status	Indicates whether Adaptive TX power is currently operational.

5.2. Configuring the Remote Radio Parameters

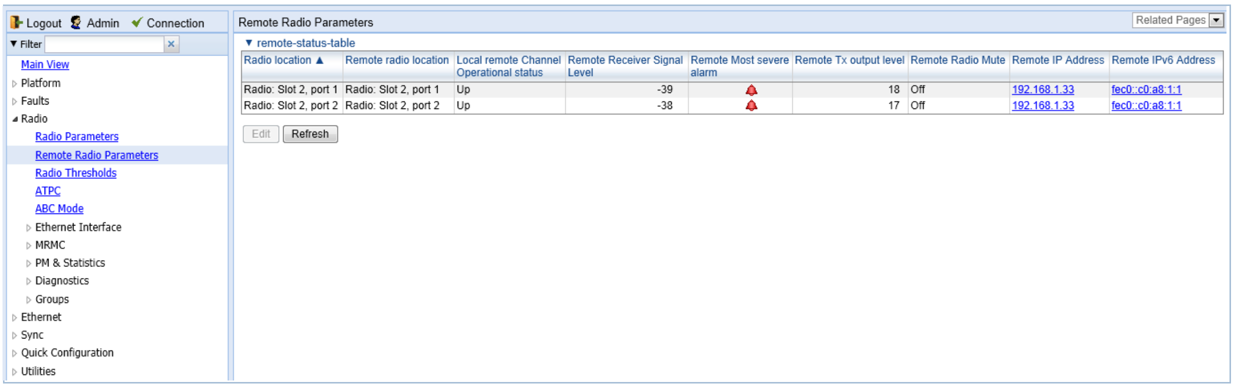
You can view and configure the parameters of the carrier or carriers at the remote side of the link in the Remote Radio Parameters page.

To display the remote radio parameters:

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

  - For NetStream Diplo units, the Radio Parameters page initially displays a table as shown in *Figure 88*.
  - For NetStream Primo units and NS Primo/DiploE units, the page appears as shown in *Figure 89*.

Figure 88: Remote Radio Parameters Page – NetStream Diplo

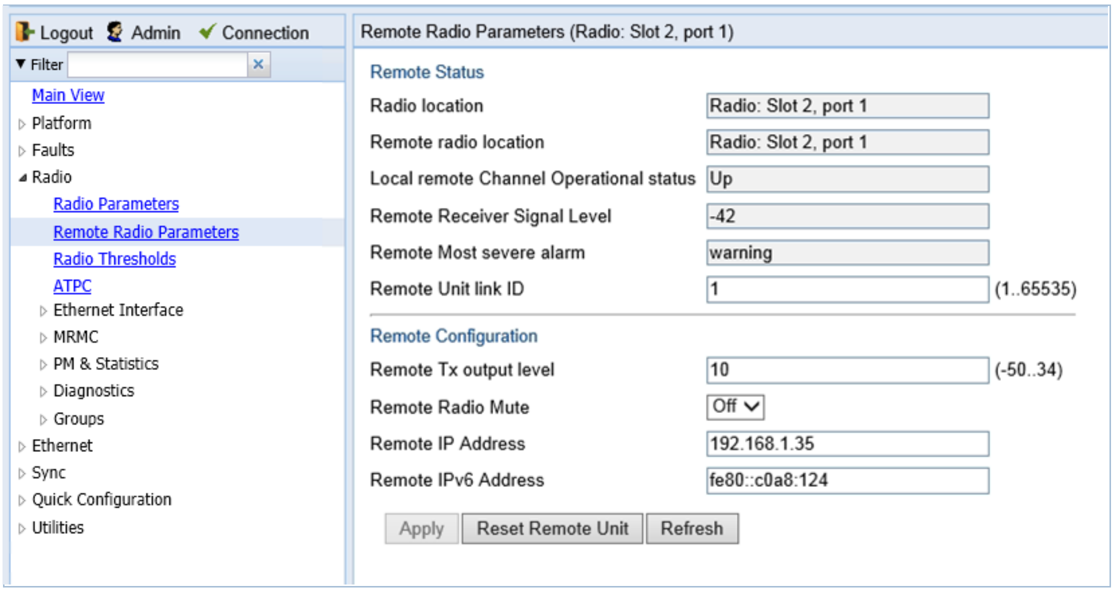


Remote Radio Parameters

▼ remote-status-table

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::c0:a8:1:1
Radio: Slot 2, port 2	Radio: Slot 2, port 2	Up	-38	🔔	17	Off	192.168.1.33	fec0::c0:a8:1:1

Figure 89: Remote Radio Parameters Page – NetStream Primo and NS Primo/DiploE



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

Remote Status

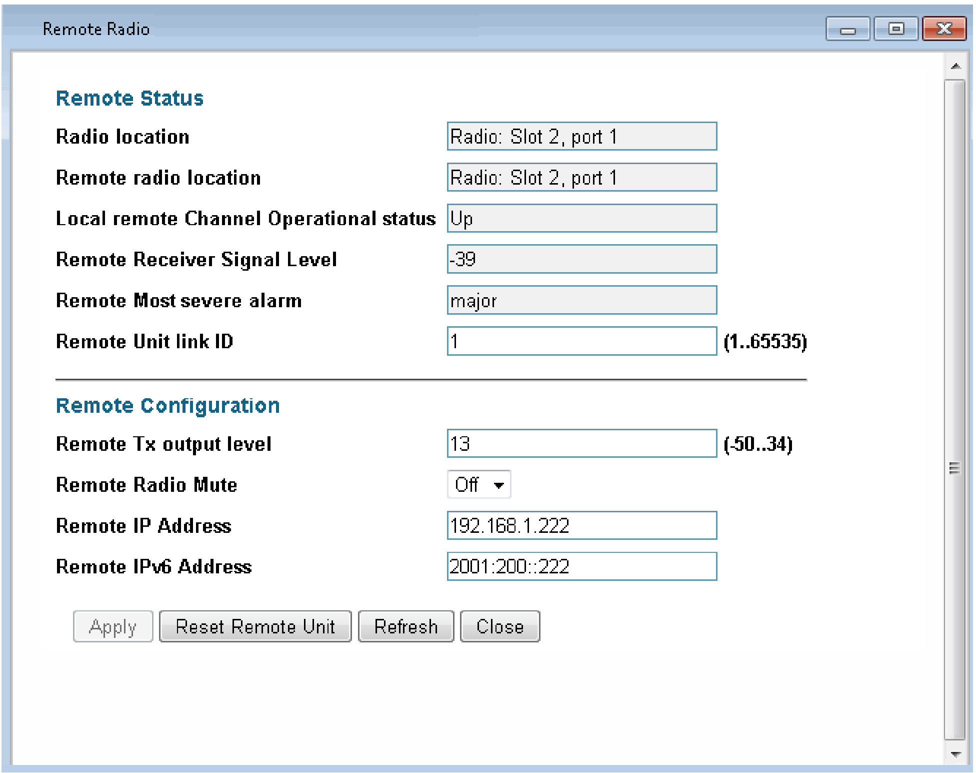
Radio location	Radio: Slot 2, port 1	
Remote radio location	Radio: Slot 2, port 1	
Local remote Channel Operational status	Up	
Remote Receiver Signal Level	-42	
Remote Most severe alarm	warning	
Remote Unit link ID	1	(1..65535)

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	

2 For NetStream Diplo units, select the carrier in the Remote Radio table (see *Figure 88*) and click **Edit**. A separate Remote Radio Parameters page opens. The page is identical to the NS Primo/DiploE and NetStream Primo page.

Figure 90: Remote Radio Parameters Page Per Carrier – NetStream Diplo



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	

3 Configure the remote radio parameters. For a description of these parameters, see *Table 23: Remote Radio Parameters*.

4 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 23: 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.
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.

5.3. Configuring ATPC

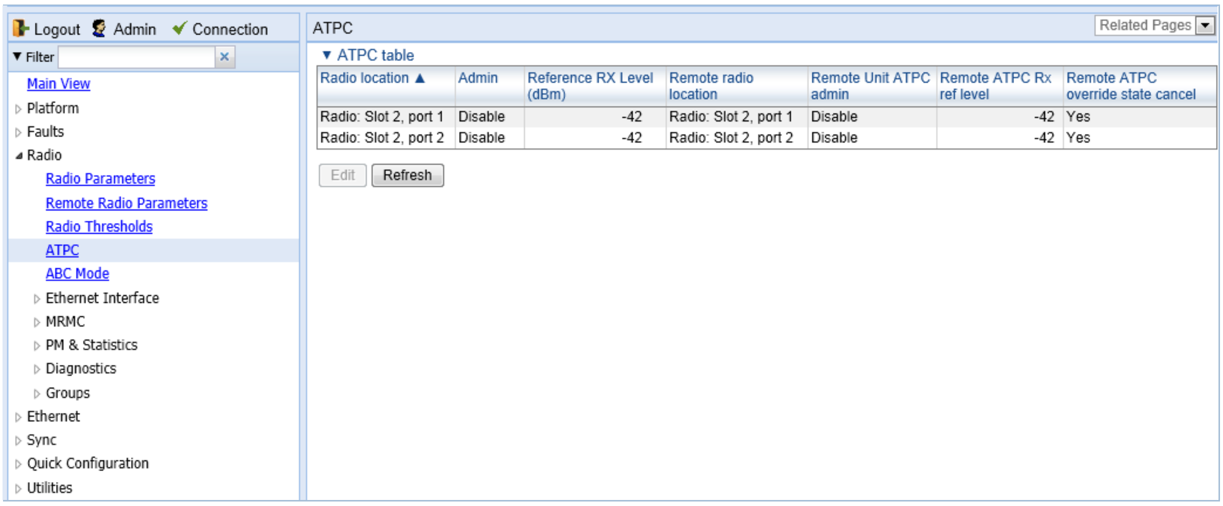
ATPC is a closed-loop mechanism by which each radio adjusts its transmitted signal power according to the indication received across the link, in order to achieve a desired RSL on the other side of the link. Without ATPC, if loss of frame occurs the system automatically increases its transmit power to the configured maximum. This may cause a higher level of interference with other systems until the failure is corrected.

To enable and configure ATPC and display ATPC settings:

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

- ○ For NetStream Diplo units, the Radio Parameters page initially displays a table as shown in *Figure 91*.
- ○ For NetStream Primo units and NS Primo/DiploE units, a page appears, similar to *Figure 92* (which shows an NetStream Diplo page).

Figure 91: ATPC Page – NetStream Diplo

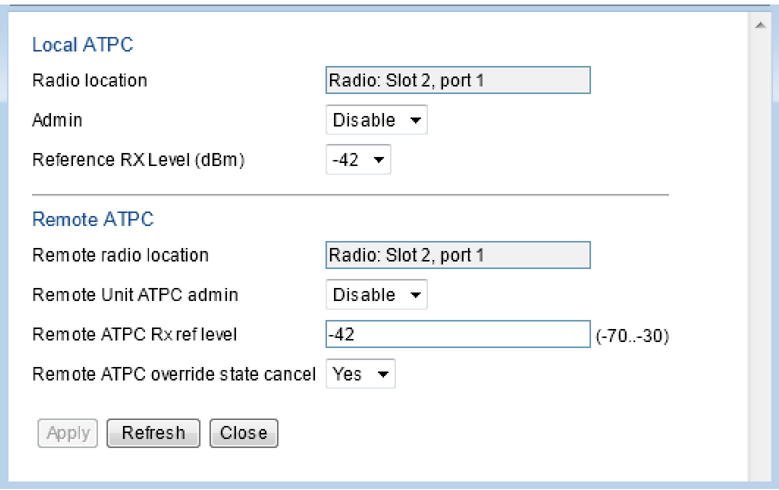


ATPC table

Radio location ▲	Admin	Reference RX Level (dBm)	Remote radio location	Remote Unit ATPC admin	Remote ATPC Rx ref level	Remote ATPC override state cancel
Radio: Slot 2, port 1	Disable	-42	Radio: Slot 2, port 1	Disable	-42	Yes
Radio: Slot 2, port 2	Disable	-42	Radio: Slot 2, port 2	Disable	-42	Yes

2 For NetStream Diplo units, select the carrier you wish to configure in the ATPC table (see *Figure 91*) and click **Edit**. A separate ATPC –Edit page opens. The page is essentially identical to the NS Primo/DiploE and NetStream Primo page.

Figure 92: ATPC – Edit Page Per Carrier – NetStream Diplo



Local ATPC

Radio location	Radio: Slot 2, port 1
Admin	Disable
Reference RX Level (dBm)	-42

Remote ATPC

Remote radio location	Radio: Slot 2, port 1
Remote Unit ATPC admin	Disable
Remote ATPC Rx ref level	-42 (-70..-30)
Remote ATPC override state cancel	Yes

3 In the **Admin** field, select **Enable** to enable ATPC or **Disable** to disable ATPC.

4 In the **Reference RX Level (dBm)** field, enter a number between -70 and -30 as the reference value for the ATPC mechanism.

5 In the **Remote Unit ATPC admin** field, select **Enable** to enable ATPC or **Disable** to disable ATPC on the remote radio carrier.

6 In the **Remote ATPC Rx ref level** field, enter a number between -70 and -30 as the reference value for the ATPC mechanism on the remote radio carrier.

7 In the **Remote ATPC override state cancel** field, select **No** or **Yes** to instruct the system whether to cancel the remote ATPC override state.

5.4. Configuring Header De-Duplication and Frame Cut-Through

Note

Header De-Duplication is supported for NetStream Diplo and NetStream Primo. For NS Primo/DiploE, Header De-Duplication is planned for future release.

Header De-Duplication enables operators to significantly improve Ethernet throughout over the radio link without affecting user traffic. Header De-Duplication can be configured to operate on various layers of the protocol stack, saving bandwidth by reducing unnecessary header overhead. Header De-duplication is also sometimes known as header compression.

Note

The Header De-Duplication 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.

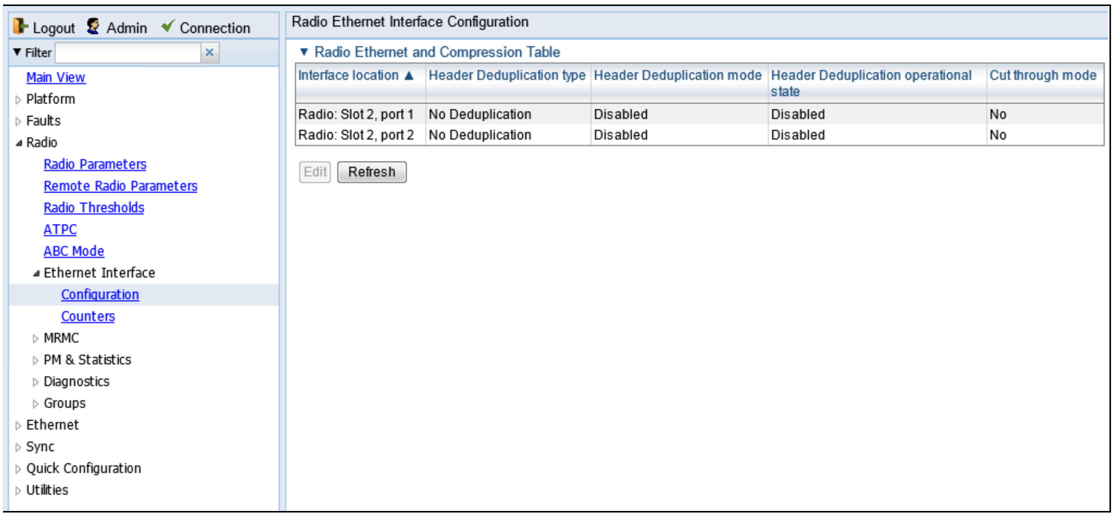
Note

Frame Cut-Through cannot be used together with 1588 Transparent Clock.

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

1 Select **Radio > Ethernet Interface > Configuration**. The Radio Ethernet Interface Configuration page opens.
   - For NetStream Diplo units, the Radio Ethernet Interface Configuration page initially displays a table as shown in *Figure 93*.
   - For NetStream Primo units, a page appears, similar to *Figure 94* (which shows an NetStream Diplo page).

Figure 93: Radio Ethernet Interface Configuration Page – NetStream Diplo



Radio Ethernet Interface Configuration

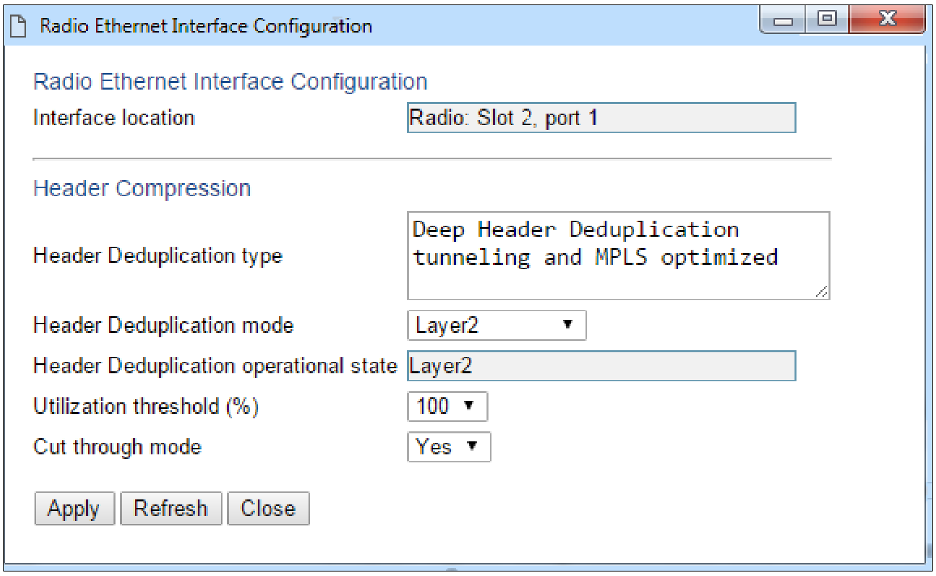
Radio Ethernet and Compression Table

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

2 For NetStream Diplo units, select the carrier in the Radio Ethernet and Compression table (see *Figure 93*) and click **Edit**. A separate Radio Ethernet Interface Configuration page opens. The page is essentially identical to the NS Primo/DiploE and NetStream Primo page.

3 Click **Edit**. The Radio Ethernet Interface Configuration – Edit page opens.

Figure 94: Radio Ethernet Interface Configuration – Edit Page Per Carrier – NetStream Diplo



Radio Ethernet Interface Configuration

Interface location	Radio: Slot 2, port 1

Header Compression

Header Deduplication type	Deep Header Deduplication tunneling and MPLS optimized
Header Deduplication mode	Layer2 ▼
Header Deduplication operational state	Layer2
Utilization threshold (%)	100 ▼
Cut through mode	Yes ▼

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.

5.4.1. Viewing Header De-Duplication and Frame Cut-Through Counters

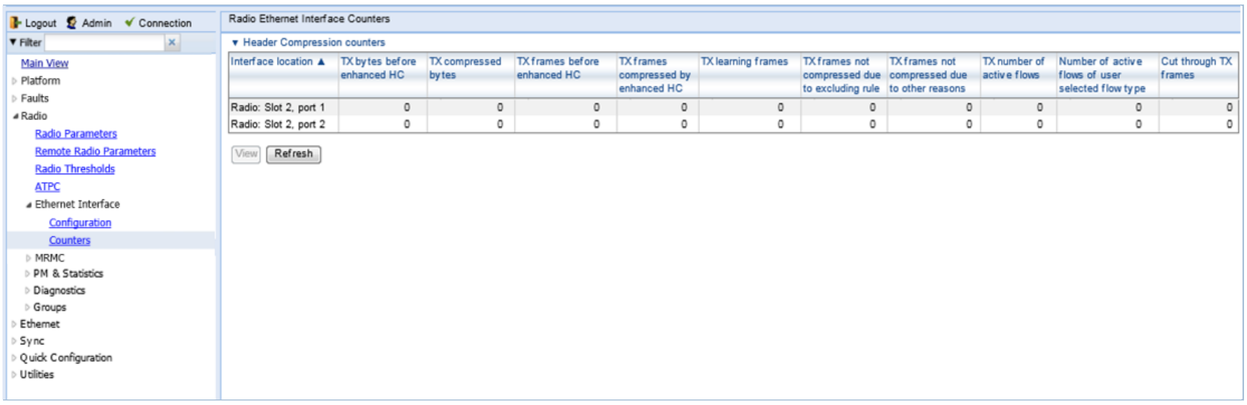
You can view PMs on the usage of Header De-Duplication and Frame Cut-Through.

To view Header De-Duplication and Frame Cut-Through counters:

1 Select **Radio > Ethernet Interface > Counters**. The Radio Ethernet Interface Configuration page opens.

- For NetStream Diplo units, the Radio Ethernet Interface Configuration page initially displays a table as shown in *Figure 95*.
- For NetStream Primo units and NS Primo/DiploE units, the page appears as shown in *Figure 96*.

Figure 95: Radio Ethernet Interface Counters Page – NetStream Diplo

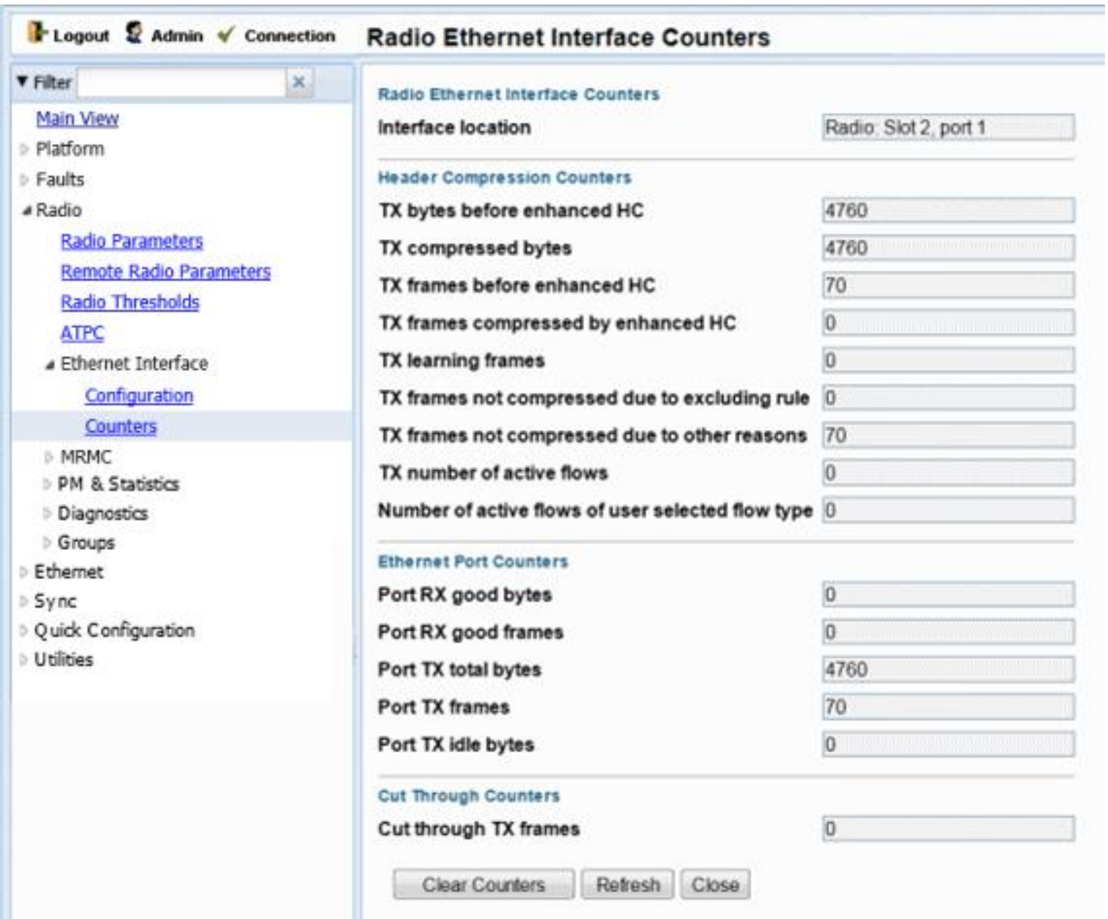


Radio Ethernet Interface Counters

▼ 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 96: Radio Ethernet Interface Counters Page – NetStream Primo and NS Primo/DiploE



Radio Ethernet Interface Counters

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

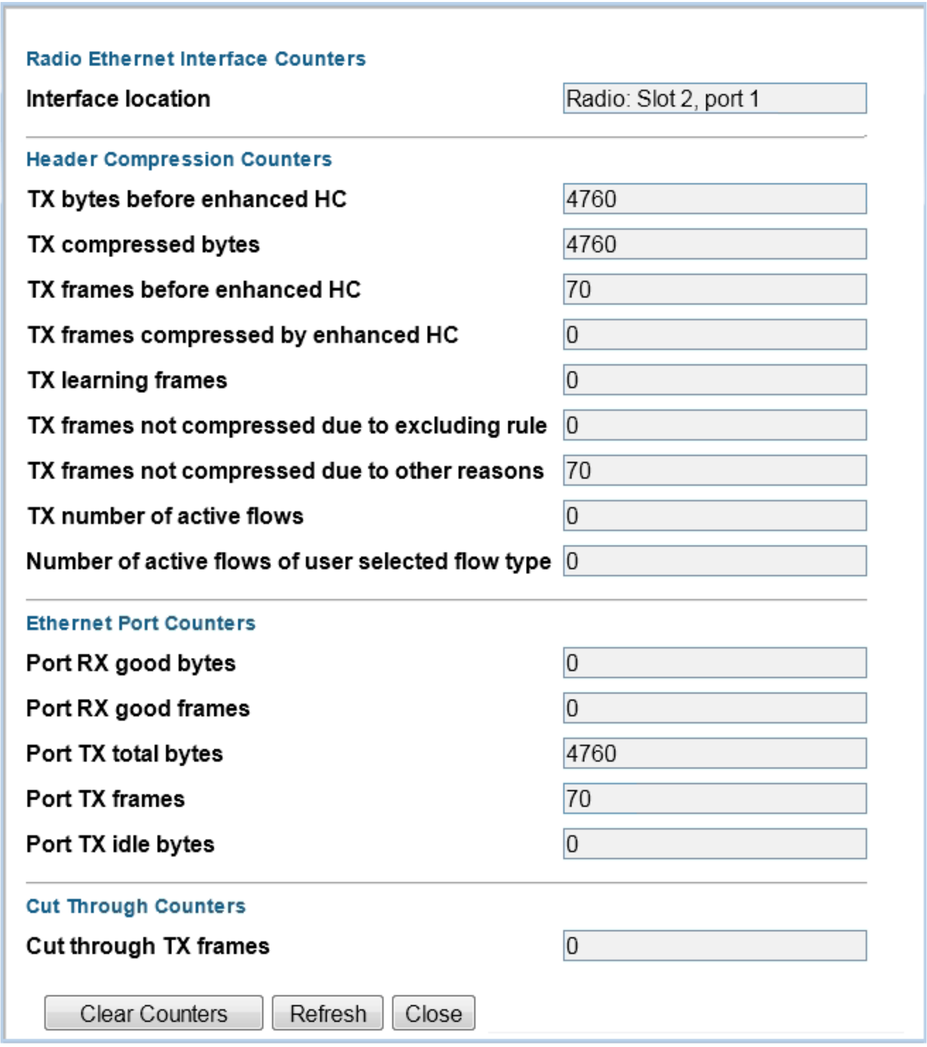
Port RX good bytes	0
Port RX good frames	0
Port TX total bytes	4760
Port TX frames	70
Port TX idle bytes	0

Cut Through Counters

Cut through TX frames	0

2 For NetStream Diplo units, select the carrier in the Header Compression Counters table (*Figure 95*) and click **View**. A separate Radio Ethernet Interface Configuration page opens. The page is essentially identical to the NS Primo/DiploE and NetStream Primo page.

Figure 97: Radio Ethernet Interface Counters Page Per Carrier – NetStream Diplo



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

Table 24 lists and describes the fields in the Radio Ethernet Interface Counters page.

Table 24: Radio Ethernet Interface Counters Fields

Parameter	Description
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.
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.

5.5. Configuring AES-256 Payload Encryption

Note

This feature is only relevant for NetStream Diplo and NetStream Primo units.
This feature is not supported with MIMO links.

This feature requires:

- Requires an activation key. If no valid AES activation key has been applied to the unit, AES will not operate on the unit. See *Configuring the Activation Key*.

Note

In order for the AES activation key to become active, you must reset the unit after configuring a valid AES activation key. Until the unit is reset, an alarm will be present if you enable AES. This is not the case for other activation keys.

NetStream Diplo and NetStream Primo support AES-256 payload encryption. AES is enabled and configured separately for each radio carrier.

NS Primo/Diplo 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.

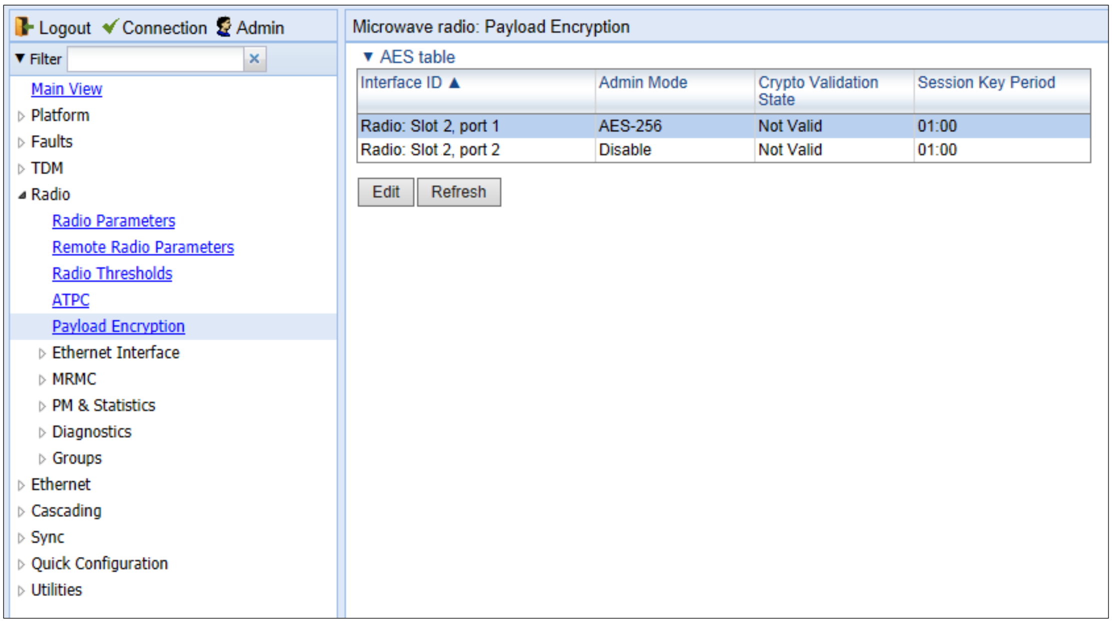
AES key generation is completely hitless, and has no effect on ACM operation.

To configure payload encryption:

1 Select **Radio > Payload Encryption**. The Payload Encryption page opens. Interface Configuration page opens.

- For NetStream Diplo units, the Payload Encryption page initially displays a table as shown in *Figure 98*.
- For NetStream Primo units, a page appears, similar to *Figure 99* (which shows an NetStream Diplo page).

Figure 98: Payload Encryption Page



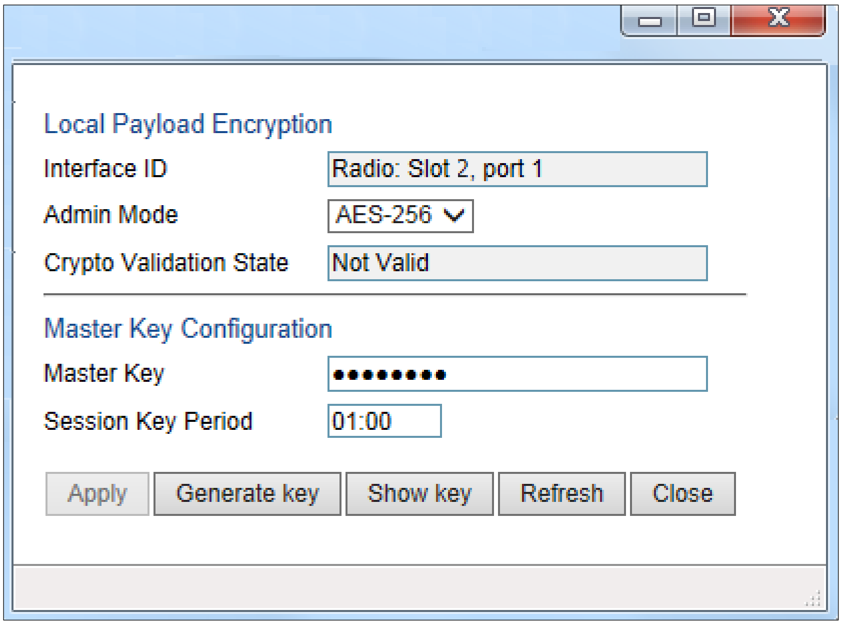
Microwave radio: Payload Encryption

▼ AES table

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

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

Figure 99: Payload Encryption – Edit Page



Local Payload Encryption

Interface ID: Radio: Slot 2, port 1

Admin Mode: AES-256

Crypto Validation State: Not Valid

Master Key Configuration

Master Key: ●●●●●●●●●

Session Key Period: 01:00

3 In the **Admin Mode** field, select **AES-256** to enable payload encryption. To disable payload encryption, select **Disable**.

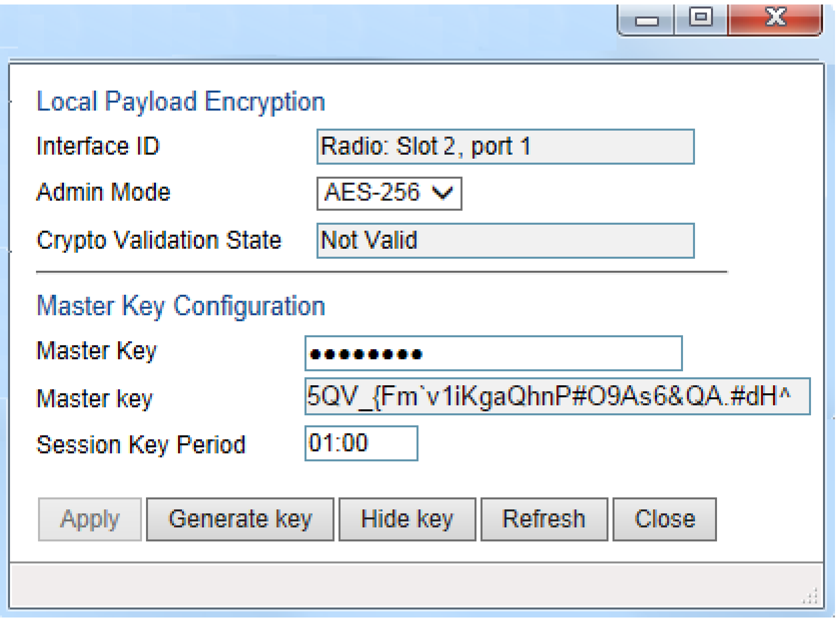
4 Configure the master key by doing one of the following:

- Enter a master key in the **Master Key** field. You must enter between 8 and 32 ASCII characters.
- Click **Generate key** to generate a master key automatically.

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

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

Figure 100: Payload Encryption – Edit Page with Master Key Displayed



Local Payload Encryption

Interface ID: Radio: Slot 2, port 1

Admin Mode: AES-256

Crypto Validation State: Not Valid

Master Key Configuration

Master Key: ●●●●●●●●

Master key: 5QV_{Fm`v1iKgaQhnP#O9As6&QA.#dH^

Session Key Period: 01:00

5 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.

6 When you are finished, click **Apply**.

Note

Any time payload encryption fails, the Operational status of the link is Down until payload encryption is successfully restored.

5.6. Configuring and Viewing Radio PMs and Statistics

This section includes:

- *Configuring Radio Thresholds*
- *Displaying MRMC Status*
- *Displaying MRMC PMs*
- *Displaying and Clearing Defective Block Counters*
- *Displaying Signal Level PMs*
- *Displaying Modem BER (Aggregate) PMs*
- *Displaying Modem MSE PMs*
- *Displaying XPI PMs*
- *Displaying Traffic PMs*

Note

The Radio > PM & Statistics > Diversity and Radio > PM & Statistics > Combined pages are reserved for future use.

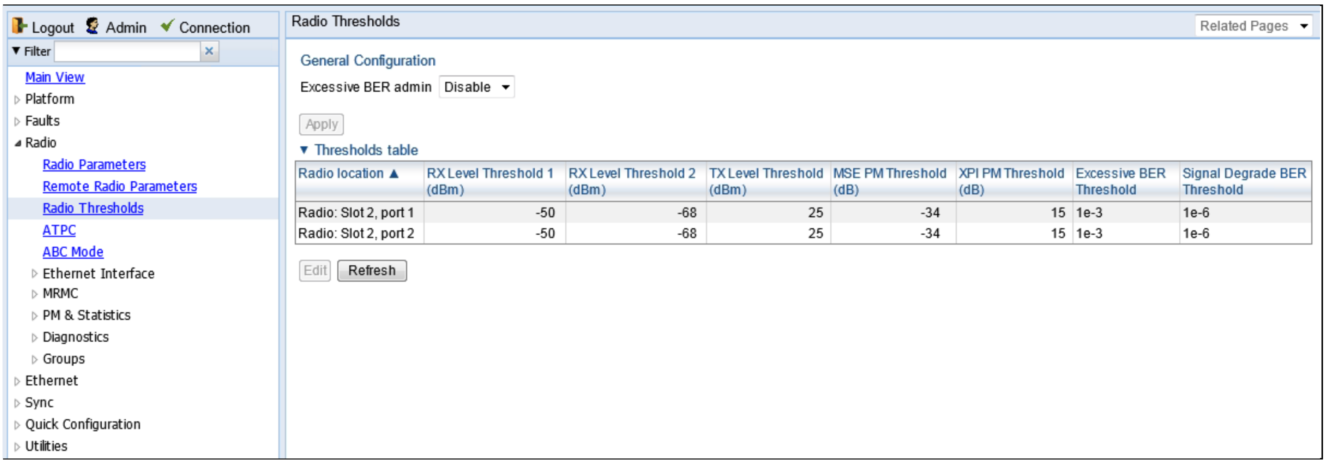
5.6.1. Configuring Radio Thresholds

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.

To configure the radio thresholds:

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

Figure 101: Radio Thresholds Page



Radio Thresholds

General Configuration

Excessive BER admin: Disable

Thresholds table

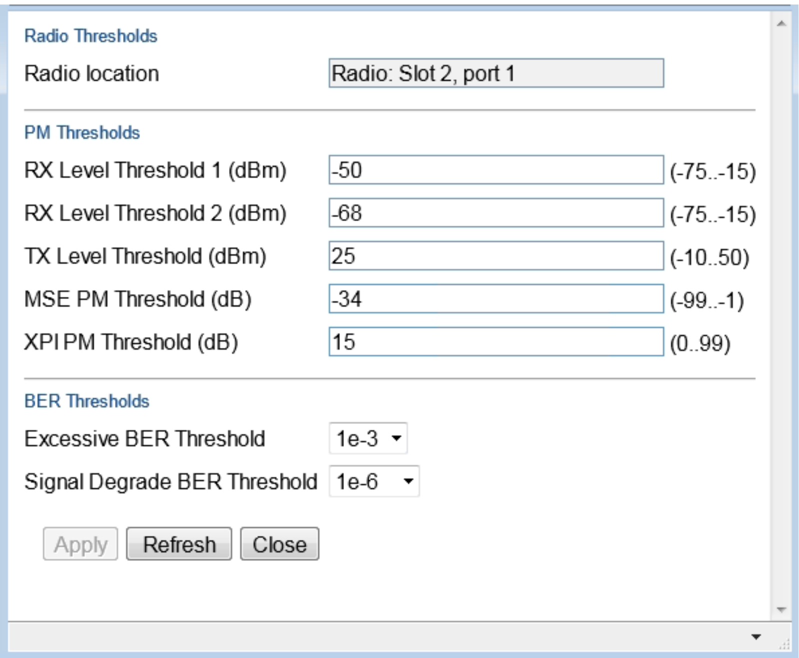
Radio location ▲	RX Level Threshold 1 (dBm)	RX Level Threshold 2 (dBm)	TX Level Threshold (dBm)	MSE PM Threshold (dB)	XPI PM Threshold (dB)	Excessive BER Threshold	Signal Degrade BER Threshold
Radio: Slot 2, port 1	-50	-68	25	-34	15	1e-3	1e-6
Radio: Slot 2, port 2	-50	-68	25	-34	15	1e-3	1e-6

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 Thresholds – Edit page opens.

Figure 102: Radio Thresholds – Edit Page



Radio Thresholds

Radio location: Radio: Slot 2, port 1

PM Thresholds

RX Level Threshold 1 (dBm): -50 (-75..-15)

RX Level Threshold 2 (dBm): -68 (-75..-15)

TX Level Threshold (dBm): 25 (-10..50)

MSE PM Threshold (dB): -34 (-99..-1)

XPI PM Threshold (dB): 15 (0..99)

BER Thresholds

Excessive BER Threshold: 1e-3

Signal Degrade BER Threshold: 1e-6

5 Configure the thresholds, as described in *Table 25*.

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

Table 25: PM and BER Thresholds

Parameter	Definition
Radio Location	Identifies the carrier (Slot 2, port 1 or Slot 2, port 2). Note: Only relevant for NetStream Diplo units.
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.
MSE PM Threshold (dB)	Specify the modem MSE (Mean Square Error) threshold for calculating MSE Exceed Threshold seconds.
XPI PM Threshold (dB)	Specify the modem XPI threshold for calculating XPI Exceed Threshold seconds.
Excessive BER Threshold	Select the level above which an excessive BER alarm is issued for errors detected over the radio link.
Signal Degrade BER Threshold	Select the level above which a Signal Degrade alarm is issued for errors detected over the radio link.

5.6.2. Displaying MRMC Status

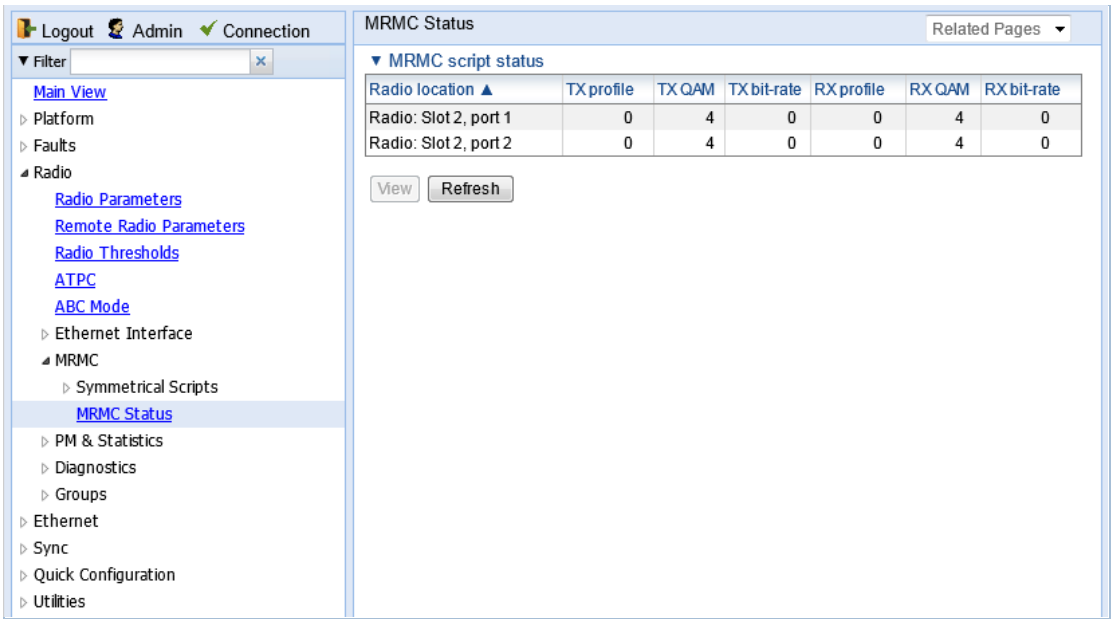
Related Topics:

- *Configuring the Radio (MRMC) Script(s)*

To display the current modulation and bit rate per radio:

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

Figure 103: MRMC Status Page



Radio location ▲	TX profile	TX QAM	TX bit-rate	RX profile	RX QAM	RX bit-rate
Radio: Slot 2, port 1	0	4	0	0	4	0
Radio: Slot 2, port 2	0	4	0	0	4	0

Table 26 describes the MRMC status parameters.

Note

To display the same parameters for an individual radio in a separate page, select the radio in the MRMC script status table and click **View**.

Table 26: MRMC Status Parameters

Parameter	Definition
Radio Location	Identifies the carrier (Slot 2, port 1 or Slot 2, port 2). **Note**: Only relevant for NetStream Diplo units.
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.

5.6.3. Displaying MRMC PMs

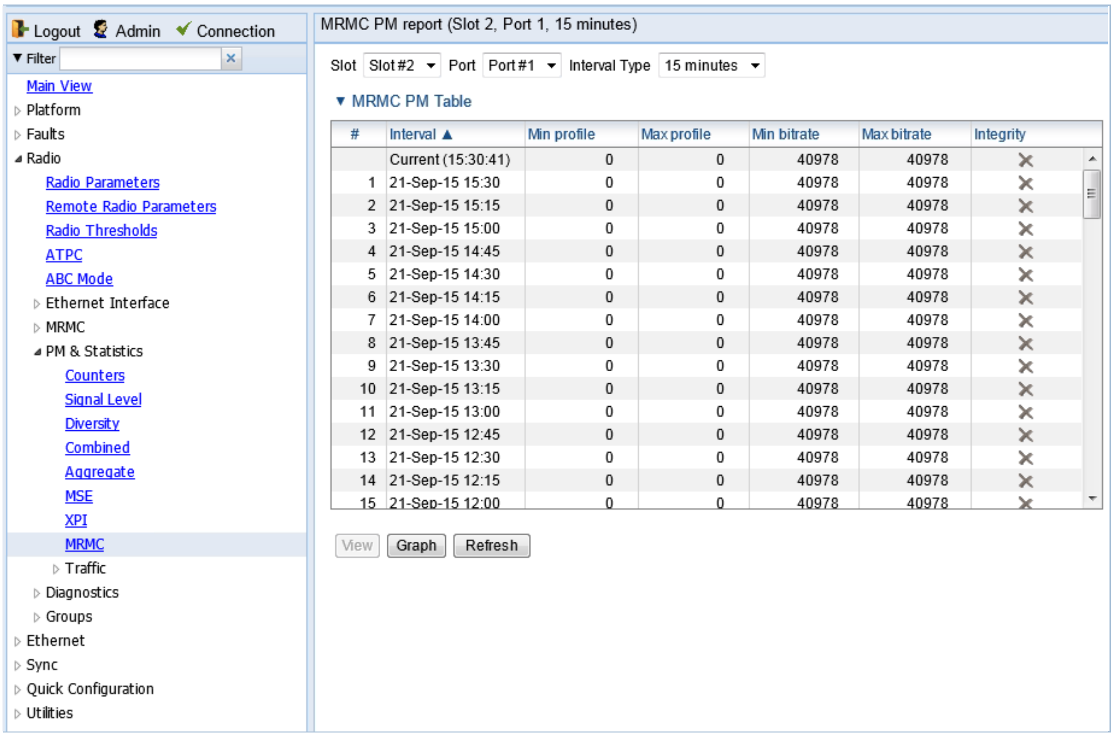
Related Topics:

- *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 104: MRMC PM Report Page



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

Slot: Slot #2 Port: Port #1 Interval Type: 15 minutes

▼ MRMC PM Table

#	Interval ▲	Min profile	Max profile	Min bitrate	Max bitrate	Integrity
	Current (15:30:41)	0	0	40978	40978	✕
1	21-Sep-15 15:30	0	0	40978	40978	✕
2	21-Sep-15 15:15	0	0	40978	40978	✕
3	21-Sep-15 15:00	0	0	40978	40978	✕
4	21-Sep-15 14:45	0	0	40978	40978	✕
5	21-Sep-15 14:30	0	0	40978	40978	✕
6	21-Sep-15 14:15	0	0	40978	40978	✕
7	21-Sep-15 14:00	0	0	40978	40978	✕
8	21-Sep-15 13:45	0	0	40978	40978	✕
9	21-Sep-15 13:30	0	0	40978	40978	✕
10	21-Sep-15 13:15	0	0	40978	40978	✕
11	21-Sep-15 13:00	0	0	40978	40978	✕
12	21-Sep-15 12:45	0	0	40978	40978	✕
13	21-Sep-15 12:30	0	0	40978	40978	✕
14	21-Sep-15 12:15	0	0	40978	40978	✕
15	21-Sep-15 12:00	0	0	40978	40978	✕

2 For the NetStream Diplo, 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 27 describes the MRMC PMs.

Note

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

Table 27: MRMC PMs

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

5.6.4. Displaying and Clearing Defective Block Counters

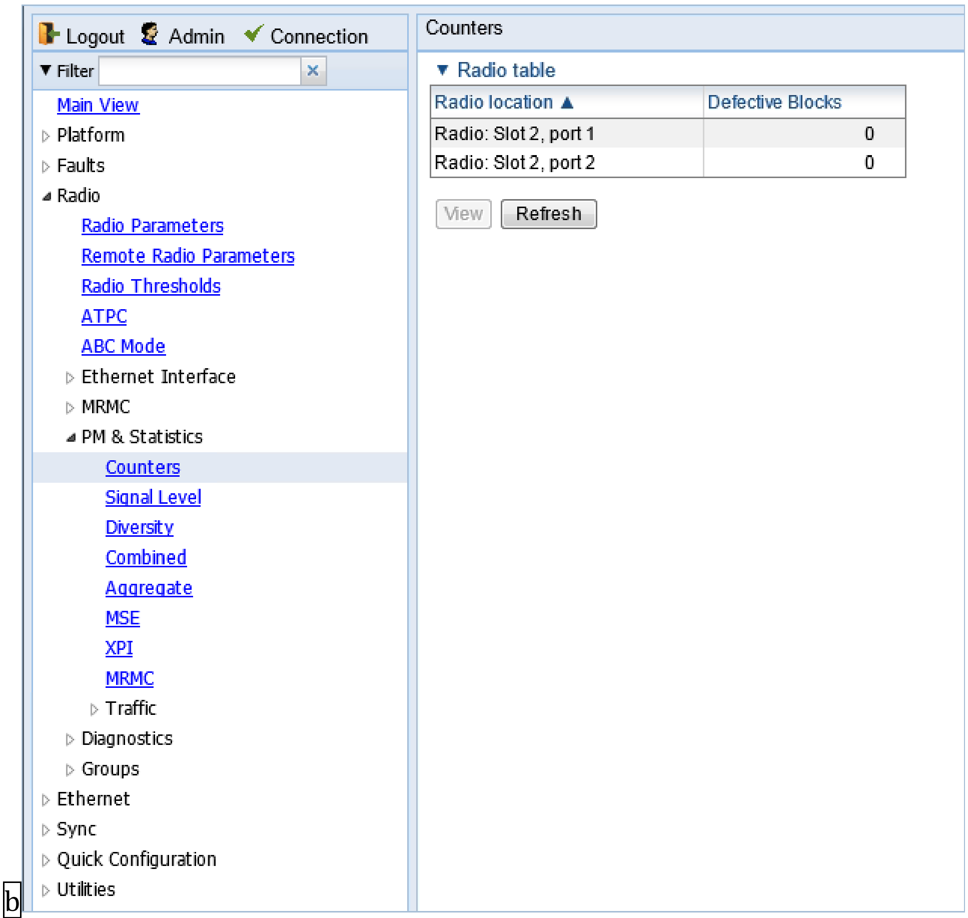
The Counters page displays the number of blocks in which errors were detected. The larger the amount, the poorer the radio link quality.

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

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

- For NetStream Diplo units, the Counters page initially displays a table as shown in Figure 105.
- For NetStream Primo and NS Primo/DiploE units, the Counters page appears as shown in Figure 106.

Figure 105: Counters Page – NetStream Diplo



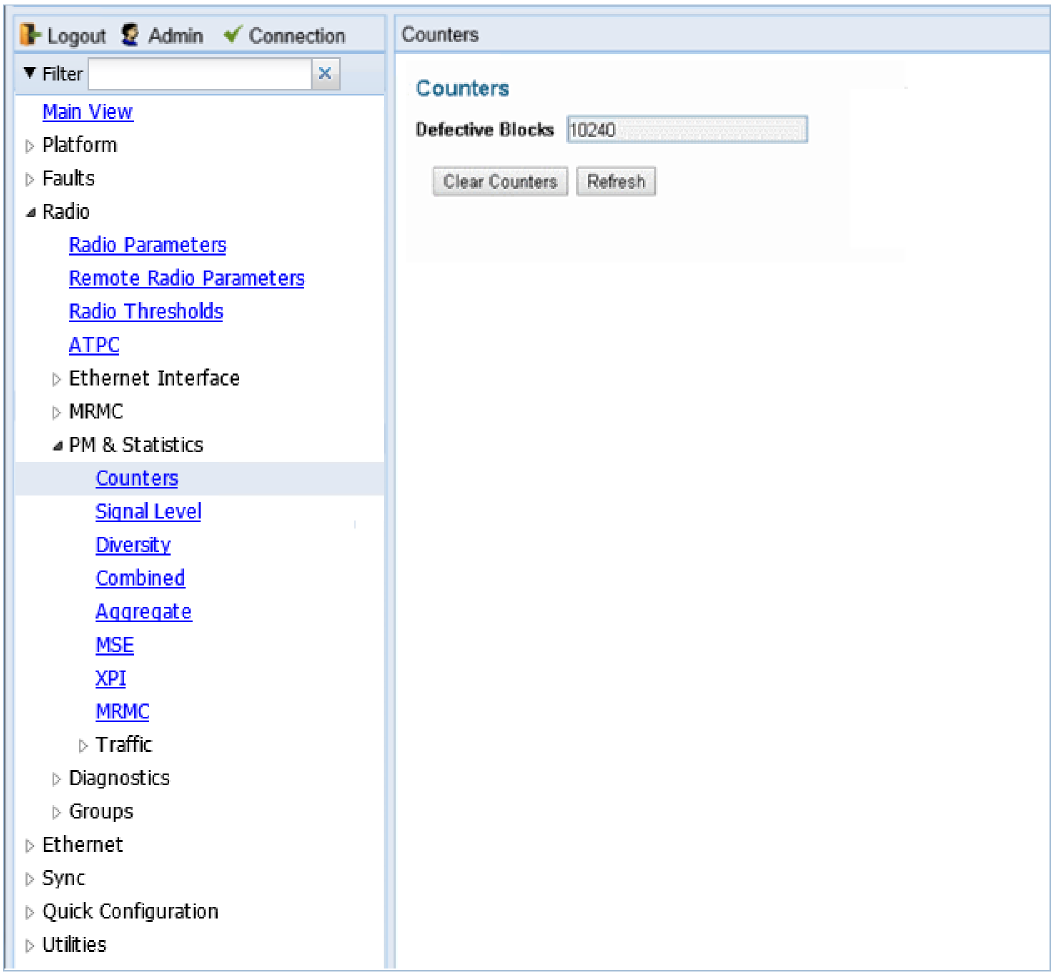
Counters

Radio table

Radio location ▲	Defective Blocks
Radio: Slot 2, port 1	0
Radio: Slot 2, port 2	0

b

Figure 106: Counters Page – NetStream Primo and NS Primo/DiploE

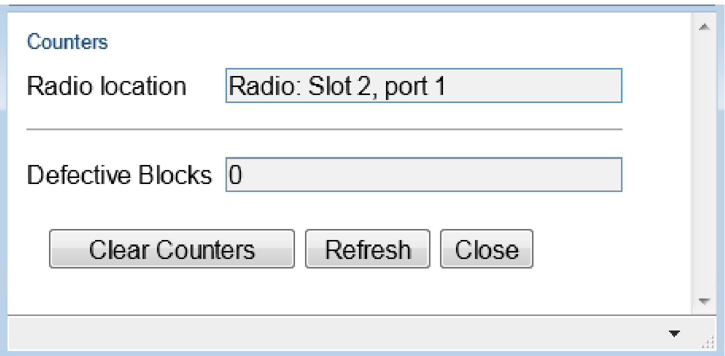


Counters

Defective Blocks 10240

2 For NetStream Diplo units, you can select the carrier in the Radio table (see *Figure 105*) and click **View** to display a page for that carrier. A separate Counters page opens.

Figure 107: Counters Page Per Carrier – NetStream Diplo



Counters

Radio location Radio: Slot 2, port 1

Defective Blocks 0

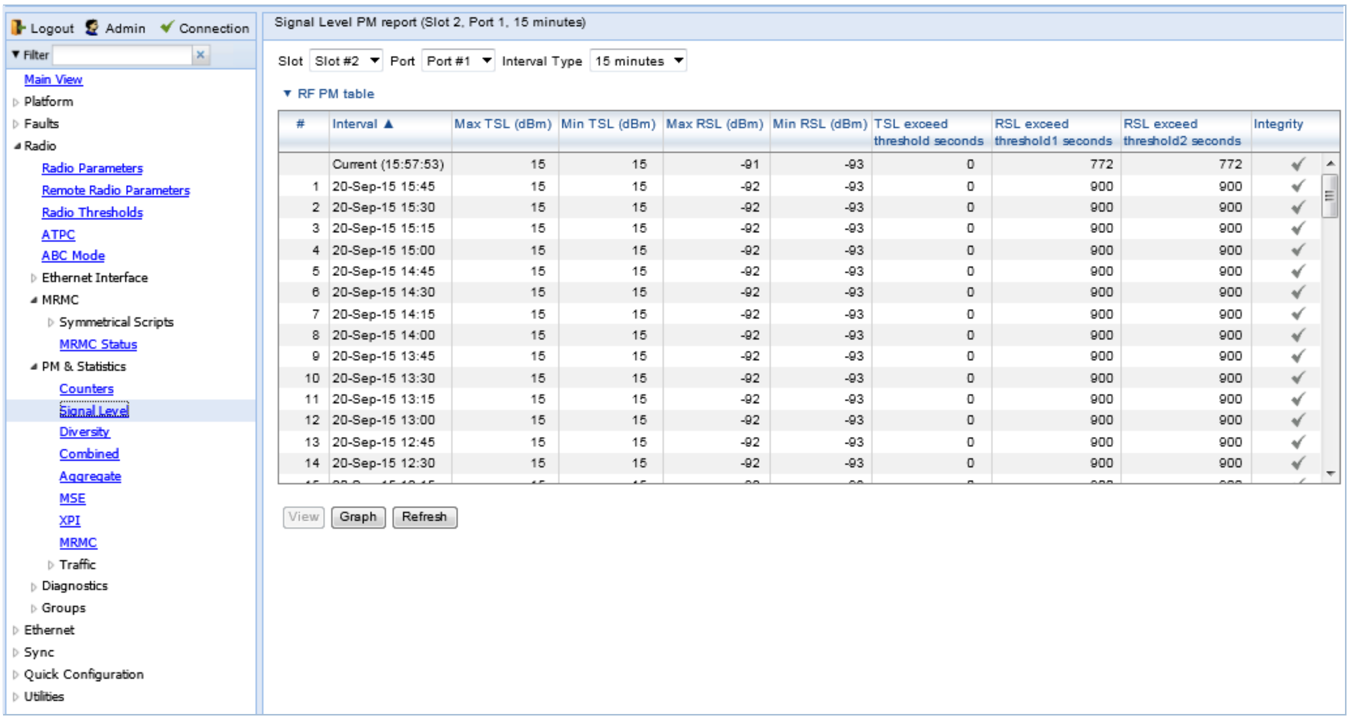
3 To clear the counters, click **Clear Counters**.

5.6.5. Displaying Signal Level PMs

To display signal level PMs per radio:

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

Figure 108: Signal Level PM Report Page



Signal Level PM report (Slot 2, Port 1, 15 minutes)

Slot: Slot #2 Port: Port #1 Interval Type: 15 minutes

RF PM table

#	Interval ▲	Max TSL (dBm)	Min TSL (dBm)	Max RSL (dBm)	Min RSL (dBm)	TSL exceed threshold seconds	RSL exceed threshold1 seconds	RSL exceed threshold2 seconds	Integrity
	Current (15:57:53)	15	15	-91	-93	0	772	772	✓
1	20-Sep-15 15:45	15	15	-92	-93	0	900	900	✓
2	20-Sep-15 15:30	15	15	-92	-93	0	900	900	✓
3	20-Sep-15 15:15	15	15	-92	-93	0	900	900	✓
4	20-Sep-15 15:00	15	15	-92	-93	0	900	900	✓
5	20-Sep-15 14:45	15	15	-92	-93	0	900	900	✓
6	20-Sep-15 14:30	15	15	-92	-93	0	900	900	✓
7	20-Sep-15 14:15	15	15	-92	-93	0	900	900	✓
8	20-Sep-15 14:00	15	15	-92	-93	0	900	900	✓
9	20-Sep-15 13:45	15	15	-92	-93	0	900	900	✓
10	20-Sep-15 13:30	15	15	-92	-93	0	900	900	✓
11	20-Sep-15 13:15	15	15	-92	-93	0	900	900	✓
12	20-Sep-15 13:00	15	15	-92	-93	0	900	900	✓
13	20-Sep-15 12:45	15	15	-92	-93	0	900	900	✓
14	20-Sep-15 12:30	15	15	-92	-93	0	900	900	✓

2 For the NetStream Diplo, 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 28 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 28: Signal Level PMs

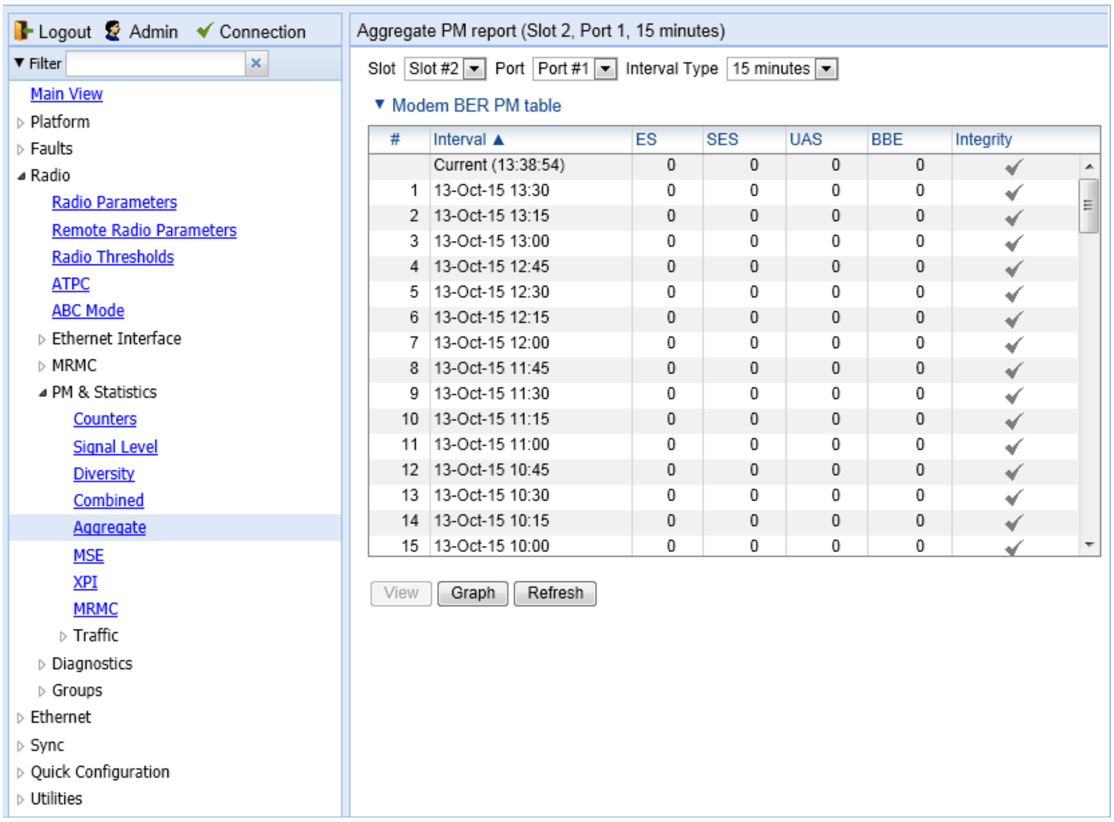
Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Max TSL (dBm)	The maximum TSL (Transmit Signal Level) that was measured during the interval.
Min TSL (dBm)	The minimum TSL (Transmit Signal Level) that was measured during the interval.
Max RSL (dBm)	The maximum RSL (Received Signal Level) that was measured during the interval.
Min RSL (dBm)	The minimum RSL (Received Signal Level) that was measured during the interval.
TSL exceed 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 Radio Thresholds*.
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 Radio Thresholds*.
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 Radio Thresholds*.
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.

5.6.6. Displaying Modem BER (Aggregate) PMs

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

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

Figure 109: Aggregate PM Report Page



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

Slot: Slot #2 Port: Port #1 Interval Type: 15 minutes

Modem BER PM table

#	Interval ▲	ES	SES	UAS	BBE	Integrity
	Current (13:38:54)	0	0	0	0	✓
1	13-Oct-15 13:30	0	0	0	0	✓
2	13-Oct-15 13:15	0	0	0	0	✓
3	13-Oct-15 13:00	0	0	0	0	✓
4	13-Oct-15 12:45	0	0	0	0	✓
5	13-Oct-15 12:30	0	0	0	0	✓
6	13-Oct-15 12:15	0	0	0	0	✓
7	13-Oct-15 12:00	0	0	0	0	✓
8	13-Oct-15 11:45	0	0	0	0	✓
9	13-Oct-15 11:30	0	0	0	0	✓
10	13-Oct-15 11:15	0	0	0	0	✓
11	13-Oct-15 11:00	0	0	0	0	✓
12	13-Oct-15 10:45	0	0	0	0	✓
13	13-Oct-15 10:30	0	0	0	0	✓
14	13-Oct-15 10:15	0	0	0	0	✓
15	13-Oct-15 10:00	0	0	0	0	✓

2 For the NetStream Diplo, 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 29 describes the Modem BER (Aggregate) PMs.

Note

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

Table 29: Modem BER (Aggregate) PMs

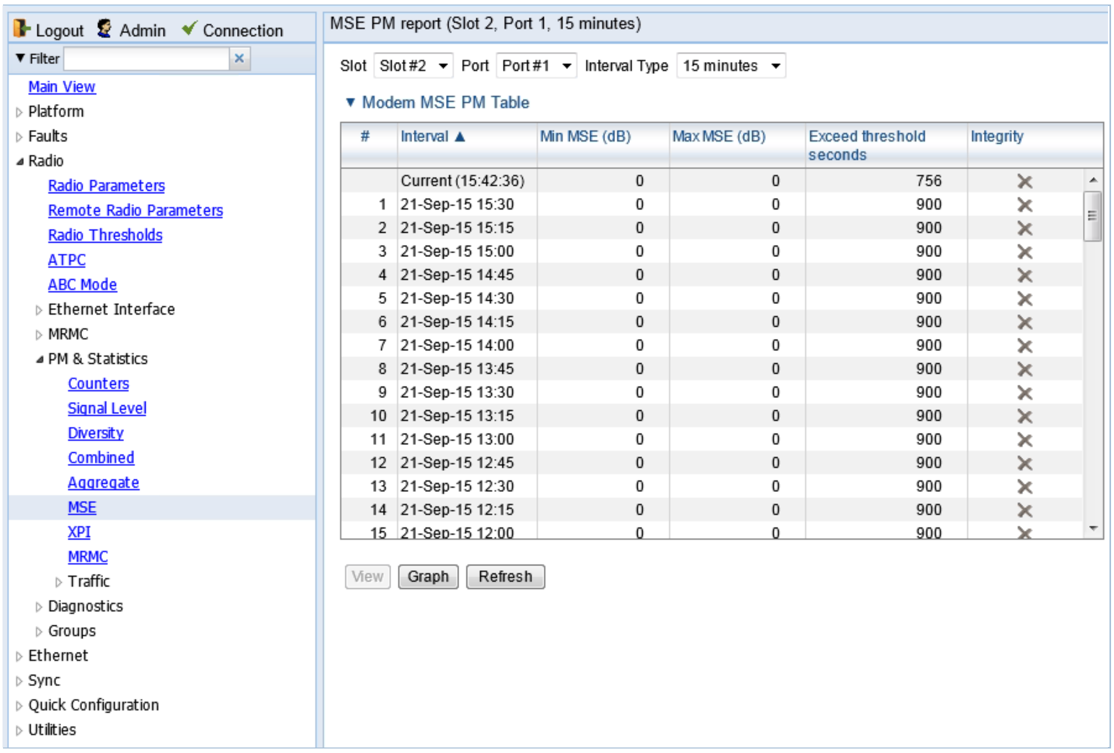
Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
ES	Displays the number of seconds in the measuring interval during which errors occurred.
SES	Displays the number of severe error seconds in the measuring interval.
UAS	Displays the Unavailable Seconds value of the measured interval. The value can be 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.

5.6.7. Displaying Modem MSE PMs

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

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

Figure 110: MSE PM Report Page



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

Slot Slot #2 Port Port #1 Interval Type 15 minutes

▼ Modem MSE PM Table

#	Interval ▲	Min MSE (dB)	Max MSE (dB)	Exceed threshold seconds	Integrity
	Current (15:42:36)	0	0	756	✕
1	21-Sep-15 15:30	0	0	900	✕
2	21-Sep-15 15:15	0	0	900	✕
3	21-Sep-15 15:00	0	0	900	✕
4	21-Sep-15 14:45	0	0	900	✕
5	21-Sep-15 14:30	0	0	900	✕
6	21-Sep-15 14:15	0	0	900	✕
7	21-Sep-15 14:00	0	0	900	✕
8	21-Sep-15 13:45	0	0	900	✕
9	21-Sep-15 13:30	0	0	900	✕
10	21-Sep-15 13:15	0	0	900	✕
11	21-Sep-15 13:00	0	0	900	✕
12	21-Sep-15 12:45	0	0	900	✕
13	21-Sep-15 12:30	0	0	900	✕
14	21-Sep-15 12:15	0	0	900	✕
15	21-Sep-15 12:00	0	0	900	✕

2 For the NetStream Diplo, 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 30 describes the Modem MSE PMs.

Note

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

Table 30: Modem MSE PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Min MSE (dB)	Displays the minimum MSE in dB, measured during the interval.
Max MSE (dB)	Displays the maximum MSE in dB, measured during the interval.
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 Radio Thresholds*.
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.

5.6.8. Displaying XPI PMs

Related topics:

- *Configuring XPIC*

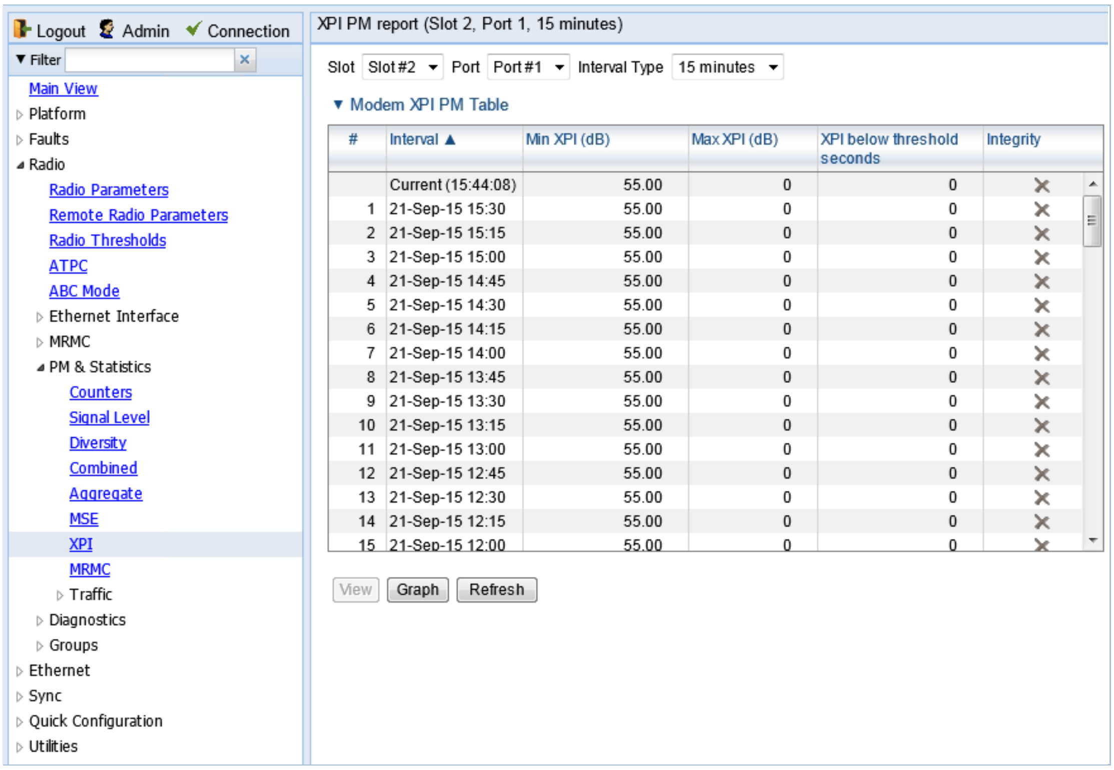
To display XPI (Cross Polarization Interface) PMs per radio:

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

Note

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

Figure 111: XPI PM Report Page



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

Slot: Slot #2 Port: Port #1 Interval Type: 15 minutes

▼ Modem XPI PM Table

#	Interval ▲	Min XPI (dB)	Max XPI (dB)	XPI below threshold seconds	Integrity
	Current (15:44:08)	55.00	0	0	✕
1	21-Sep-15 15:30	55.00	0	0	✕
2	21-Sep-15 15:15	55.00	0	0	✕
3	21-Sep-15 15:00	55.00	0	0	✕
4	21-Sep-15 14:45	55.00	0	0	✕
5	21-Sep-15 14:30	55.00	0	0	✕
6	21-Sep-15 14:15	55.00	0	0	✕
7	21-Sep-15 14:00	55.00	0	0	✕
8	21-Sep-15 13:45	55.00	0	0	✕
9	21-Sep-15 13:30	55.00	0	0	✕
10	21-Sep-15 13:15	55.00	0	0	✕
11	21-Sep-15 13:00	55.00	0	0	✕
12	21-Sep-15 12:45	55.00	0	0	✕
13	21-Sep-15 12:30	55.00	0	0	✕
14	21-Sep-15 12:15	55.00	0	0	✕
15	21-Sep-15 12:00	55.00	0	0	✕

2 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 31 describes the XPI PMs.

Note

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

Table 31: XPI PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Min XPI (dB)	The minimum XPI level that was measured during the interval.
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. XPI thresholds are configured in the Radio Thresholds page. See *Configuring Radio Thresholds*.
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.

5.6.9. Displaying Traffic PMs

This section includes:

- *Displaying Capacity and Throughput PMs*
- *Displaying Utilization PMs*
- *Displaying Frame Error Rate PMs*

5.6.9.1. Displaying Capacity and Throughput PMs

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

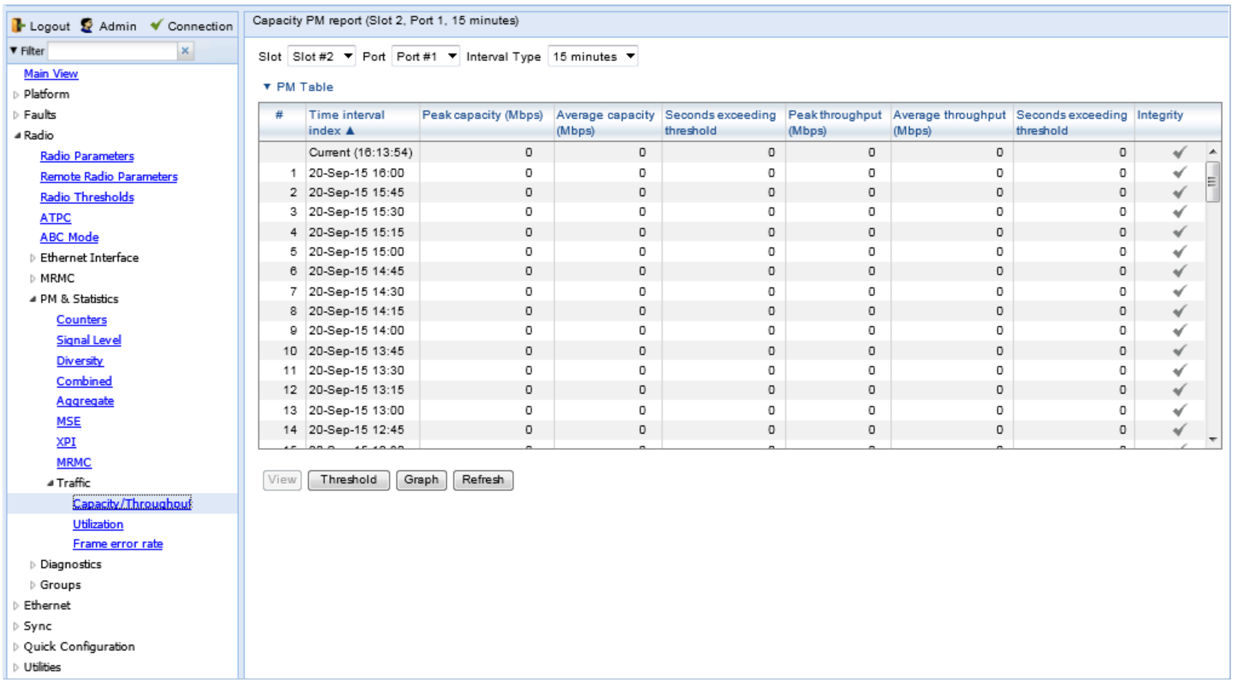
- The total Layer 1 bandwidth (payload plus overheads) sent through the radio (Mbps).
- The total effective Layer 2 traffic sent through the radio.

You can also configure thresholds for capacity and throughput PMs. The number of seconds during which these thresholds are exceeded are among the dispayed PMs.

To display capacity and throughput PMs per radio:

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

Figure 112: 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 (16:13:54)	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	✓

2 For the NetStream Diplo, in the **Port** field, select the port that holds the radio for which you want to display PMs.

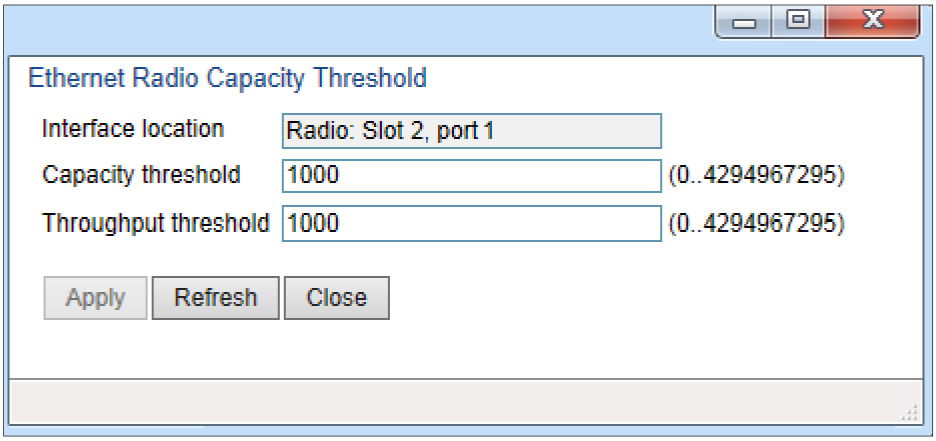
3 In the **Interval Type** field:

- 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 113: Ethernet Radio Capacity and Throughput Threshold Page



Ethernet Radio Capacity Threshold

Interface location: Radio: Slot 2, port 1

Capacity threshold: 1000 (0..4294967295)

Throughput threshold: 1000 (0..4294967295)

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 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: Capacity/Throughput PMs

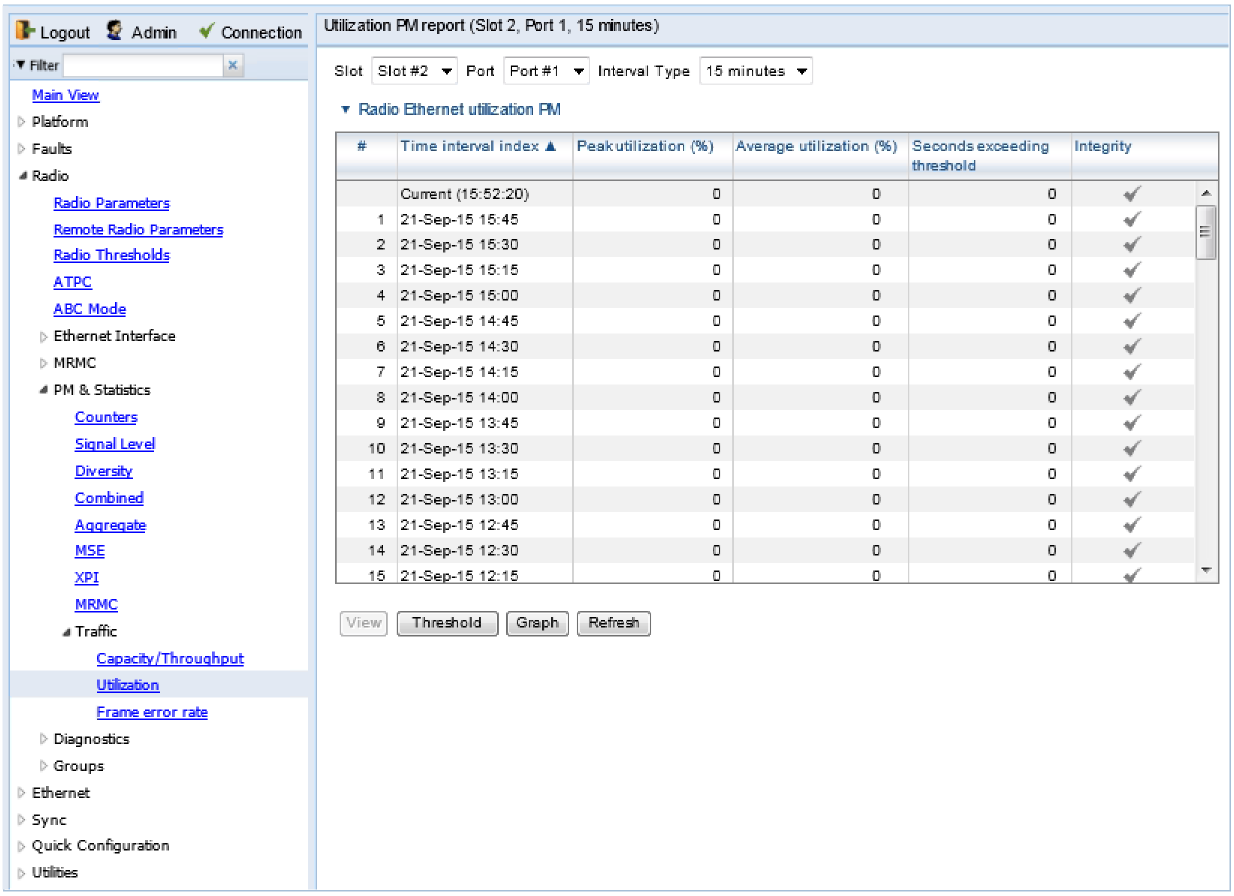
Parameter	Definition
Time interval index	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Peak capacity (Mbps)	Displays the highest L1 bandwidth, in Mbps, sent through the selected radio during the measured time interval.
Average capacity (Mbps)	Displays the average L1 bandwidth, in Mbps, during the measured time interval.
Seconds exceeding Threshold	Displays the number of seconds during the measured time interval during which the L1 bandwidth exceeded the configured capacity threshold.
Peak throughput (Mbps)	Displays the highest throughput, in Mbps, that occurred for the selected radio during the measured time interval.
Average throughput (Mbps)	Displays the average throughput, in Mbps, for the selected radio during the measured time interval.
Seconds exceeding Threshold	Displays the number of seconds during the measured time interval during which the throughput exceeded the configured throughput threshold.
Integrity	Indicates whether the values received at the time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.

5.6.9.2. 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 114: Utilization PM Report Page



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

Slot: Slot #2 Port: Port #1 Interval Type: 15 minutes

Radio Ethernet utilization PM

#	Time interval index ▲	Peak utilization (%)	Average utilization (%)	Seconds exceeding threshold	Integrity
	Current (15:52:20)	0	0	0	✓
1	21-Sep-15 15:45	0	0	0	✓
2	21-Sep-15 15:30	0	0	0	✓
3	21-Sep-15 15:15	0	0	0	✓
4	21-Sep-15 15:00	0	0	0	✓
5	21-Sep-15 14:45	0	0	0	✓
6	21-Sep-15 14:30	0	0	0	✓
7	21-Sep-15 14:15	0	0	0	✓
8	21-Sep-15 14:00	0	0	0	✓
9	21-Sep-15 13:45	0	0	0	✓
10	21-Sep-15 13:30	0	0	0	✓
11	21-Sep-15 13:15	0	0	0	✓
12	21-Sep-15 13:00	0	0	0	✓
13	21-Sep-15 12:45	0	0	0	✓
14	21-Sep-15 12:30	0	0	0	✓
15	21-Sep-15 12:15	0	0	0	✓

2 For the NetStream Diplo, in the **Port** field, select the port that holds the radio for which you want to display PMs.

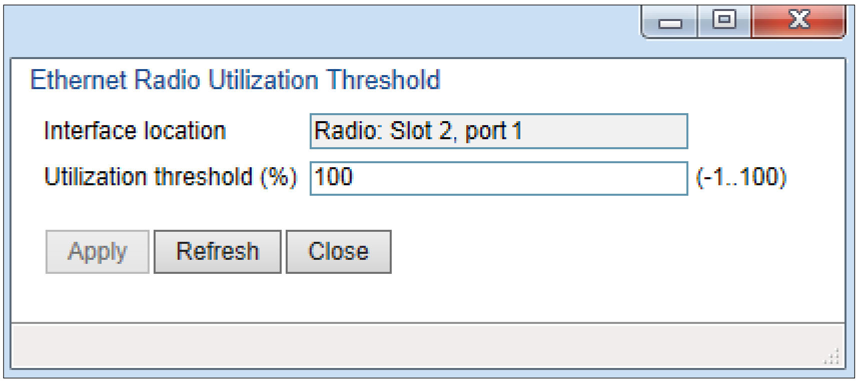
3 In the **Interval Type** field:

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

To set the thresholds for utilization PMs:

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

Figure 115: Ethernet Radio Utilization Threshold Page



Ethernet Radio Utilization Threshold

Interface location: Radio: Slot 2, port 1

Utilization threshold (%): 100 (-1..100)

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

3 Click **Apply**, then **Close**.

Table 33 describes the capacity and throughput PMs.

Note

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

Table 33: Utilization PMs

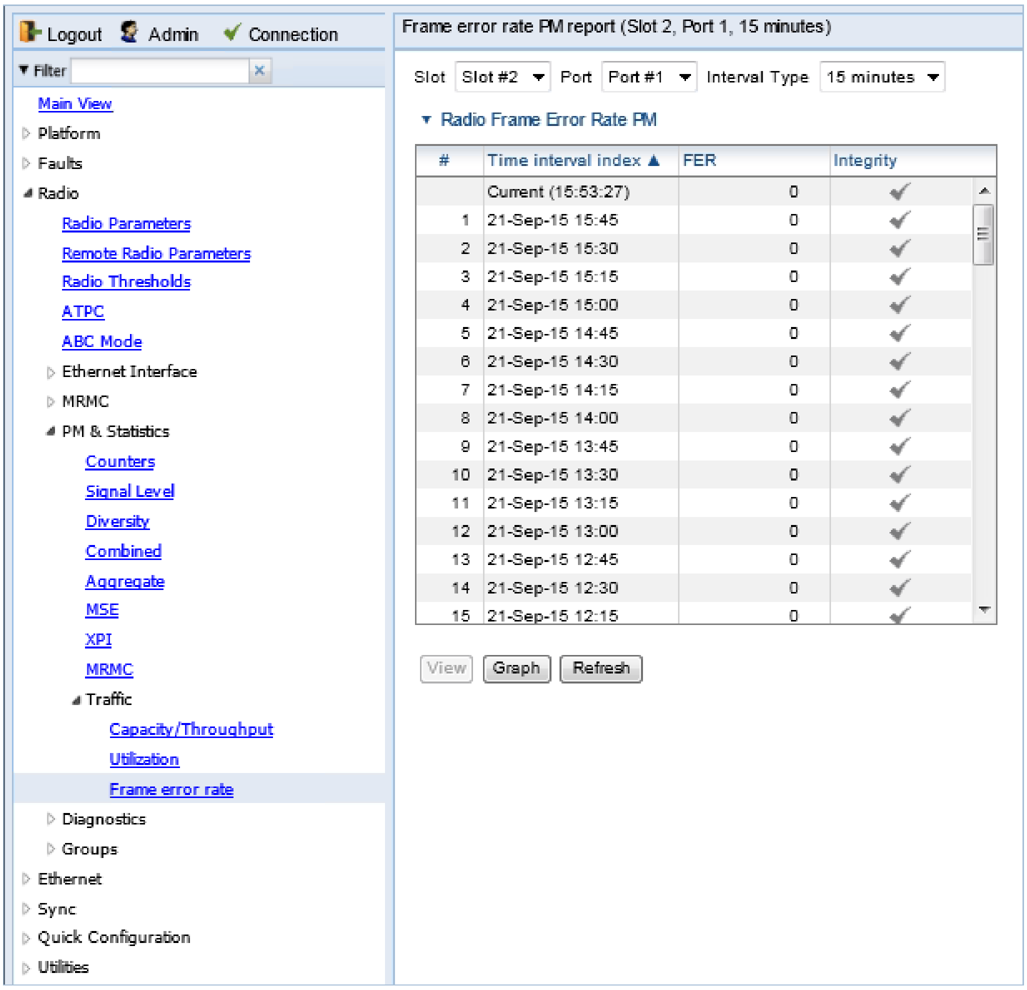
Parameter	Definition
Time interval index	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Peak utilization (%)	Indicates the highest utilization of the radio capacity that occurred for the selected radio or group during the measured time interval.
Average utilization (%)	Indicates the average utilization of the radio capacity for the selected radio or group during the measured time interval.
Seconds exceeding Threshold	Displays the number of seconds during the measured time interval during which the L1 bandwidth exceeded the configured utilization threshold.
Integrity	Indicates whether the values received at time and date of the measured interval are reliable. An x in the column indicates that the values are not reliable due to a possible power surge or power failure that occurred at that time.

5.6.9.3. 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 116: Frame Error PM Report Page



Frame error rate PM report (Slot 2, Port 1, 15 minutes)

Slot: Slot #2 Port: Port #1 Interval Type: 15 minutes

Radio Frame Error Rate PM

#	Time interval index ▲	FER	Integrity
	Current (15:53:27)	0	✓
1	21-Sep-15 15:45	0	✓
2	21-Sep-15 15:30	0	✓
3	21-Sep-15 15:15	0	✓
4	21-Sep-15 15:00	0	✓
5	21-Sep-15 14:45	0	✓
6	21-Sep-15 14:30	0	✓
7	21-Sep-15 14:15	0	✓
8	21-Sep-15 14:00	0	✓
9	21-Sep-15 13:45	0	✓
10	21-Sep-15 13:30	0	✓
11	21-Sep-15 13:15	0	✓
12	21-Sep-15 13:00	0	✓
13	21-Sep-15 12:45	0	✓
14	21-Sep-15 12:30	0	✓
15	21-Sep-15 12:15	0	✓

2 For the NetStream Diplo, 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 34 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 34: 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.

6. Ethernet Services and Interfaces

This section includes:

- *Ethernet Services and Interfaces*
- *Setting the MRU Size and the S-VLAN Ethertype*
- *Configuring Ethernet Interfaces*
- *Configuring Automatic State Propagation*
- *Viewing Ethernet PMs and Statistics*

Related topics:

- *Configuring Link Aggregation (LAG)*
- *Quality of Service (QoS)*
- *Ethernet Protocols*
- *Performing Ethernet Loopback*

6.1. Configuring Ethernet Service(s)

This section includes:

- *Ethernet Services Overview*
- *General Guidelines for Provisioning Ethernet Services*
- *The Ethernet Services Page*
- *Adding an Ethernet Service*
- *Editing a Service*
- *Deleting a Service*
- *Enabling, Disabling, or Deleting Multiple Services*
- *When setting multiple* services to Reserve state**,** make sure to avoid setting the management service to Reserve state**.**
- Viewing Service Details
- *Configuring Service Points*

6.1.1. 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 NS Primo/Diplo network element.

This version of NS Primo/Diplo supports the following service types:

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

In addition to user-defined services, NS Primo/Diplo 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 30 service points.

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

6.1.2. General Guidelines for Provisioning Ethernet Services

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

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

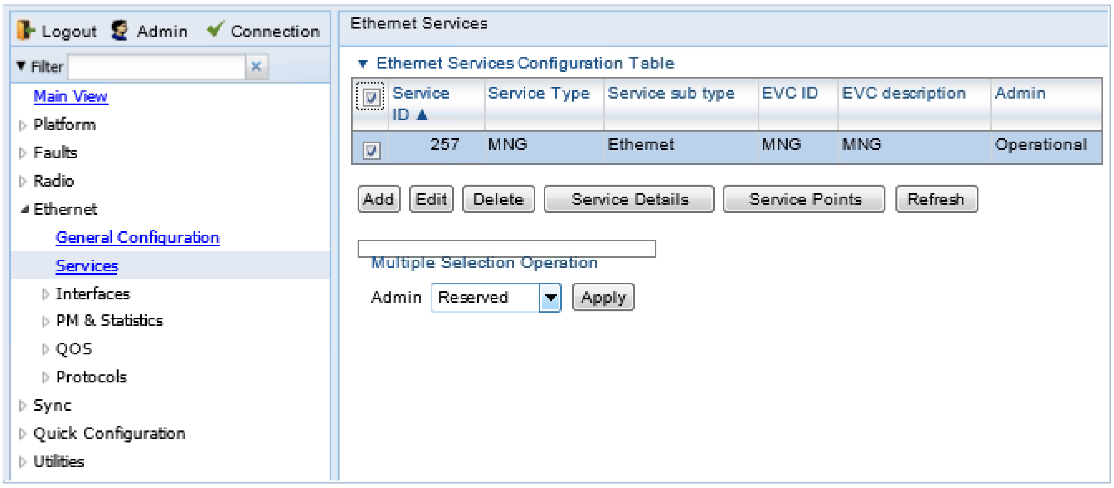
6.1.3. The Ethernet Services Page

The Ethernet Services page is the starting point for defining Ethernet services on the NS Primo/Diplo.

To open the Ethernet Services page:

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

Figure 117: Ethernet Services Page



Ethernet Services

Ethernet Services Configuration Table

☑	Service ID ▲	Service Type	Service sub type	EVC ID	EVC description	Admin
☑	257	MNG	Ethernet	MNG	MNG	Operational

Multiple Selection Operation

Admin: Reserved

Table 35 describes the parameters displayed in the Ethernet Services page.

Table 35: Ethernet Services Page Parameters

Parameter	Definition
Services ID	A unique ID for the service.
Service Type	The service type: ● **MP** – Multipoint ● **P2P** – Point-to-Point ● **MNG** – Management
Service sub type	Indicates the type of service (**Ethernet**).
EVC ID	The Ethernet Virtual Connection (EVC) ID. This parameter does not affect the network element's behavior, but is used by the NMS for topology management.
EVC description	The Ethernet Virtual Connection (EVC) description. This parameter does not affect the network element's behavior, but is used by the NMS for topology management.
Admin	Indicates whether the service is enabled (**Operational**) or disabled (**Reserved**). You can configure services for later use by defining the service as **Reserved**. In Reserved mode, the service occupies system resources but is unable to transmit and receive data.

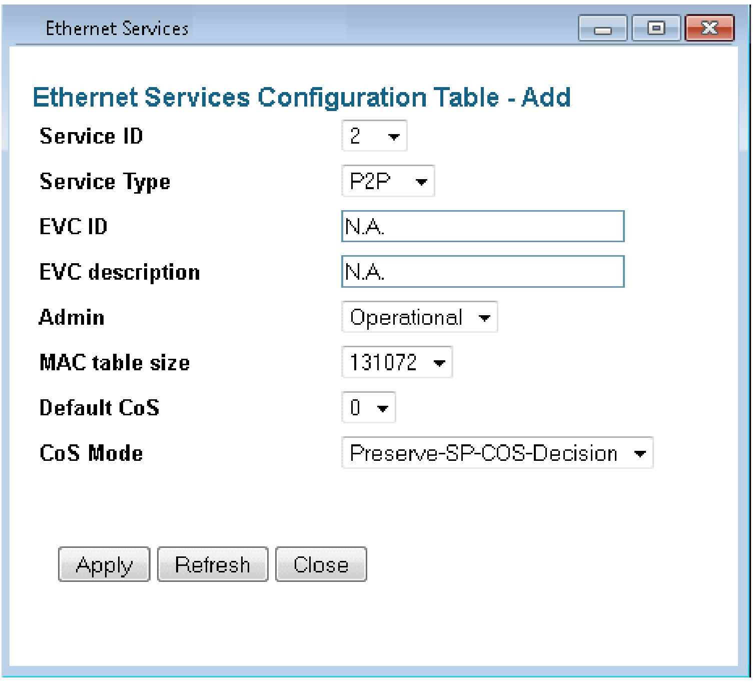
6.1.4. Adding an Ethernet Service

To add an Ethernet service:

1 Select **Ethernet** > **Services**. The Ethernet Services page opens (*Figure 117*).

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

Figure 118: 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

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*.

6.1.5. Editing a Service

To edit a service:

1. Select **Ethernet** > **Services**. The Ethernet Services page opens (*Figure 117*).
2. Select the service in the Service Configuration Table.
3. In the Ethernet Services page, click **Edit**. The Ethernet Services - Edit page opens.

This page is identical to the Ethernet Services - Add page (*Figure 118*). You can edit any parameter that can be configured in the Add page, except the **Service ID**.

6.1.6. Deleting a Service

Before deleting a service, you must first delete any service points attached to the service.

To delete a service:

1. Delete all service points attached to the service you wish to delete, as described in *Deleting a Service Point.*
2. Select **Ethernet** > **Services**. The Ethernet Services page opens (*Figure 117*).
3. Select the service in the Ethernet Service Configuration Table.

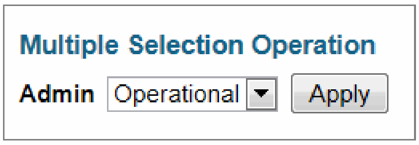
4 Click **Delete.** The service is deleted.

6.1.7. Enabling, Disabling, or Deleting Multiple Services

To enable, disable, or delete multiple services:

1 Select **Ethernet** > **Services**. The Ethernet Services page opens (*Figure 117*).
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 119: Multiple Selection Operation Section (Ethernet Services)



Multiple Selection Operation

Admin: Operational

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

6.1.8. Viewing Service Details

To view the full service parameters:

1 Select **Ethernet > Services**. The Ethernet Services page opens (*Figure 117*).
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 118*). However, in the Service Details page, these fields are read-only.

6.1.9. Configuring Service Points

This section includes:

- *Ethernet Services Points Overview*
- *The Ethernet Service Points Page*
- *Adding a Service Point*

- *Editing a Service Point*
- *Deleting a Service Point*
- *Attaching VLANs*

6.1.9.1. 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.

6.1.9.2. The Ethernet Service Points Page

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

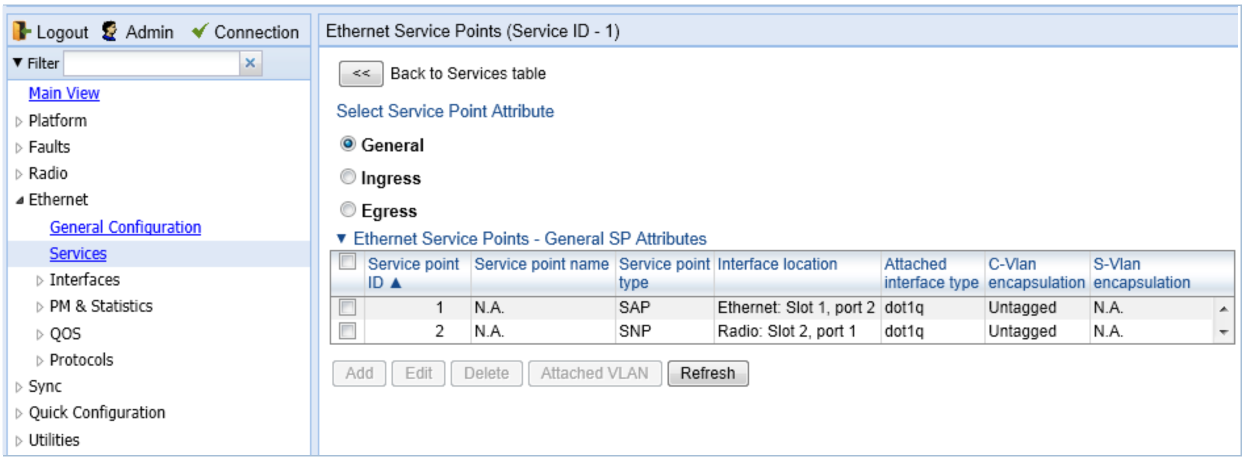
To open the Ethernet Service Points page:

1 Select **Ethernet > Services**. The Ethernet Services page opens (*Figure 117*).

2 Select the relevant service in the Ethernet Services Configuration table.

3 Click **Service Points**. The Ethernet Service Points page opens.

Figure 120: Ethernet Service Points Page



Ethernet Service Points (Service ID - 1)

Select Service Point Attribute

● General
○ Ingress
○ Egress

▼ Ethernet Service Points - General SP Attributes

☐	Service point ID ▲	Service point name	Service point type	Interface location	Attached interface type	C-Vlan encapsulation	S-Vlan encapsulation
☐	1	N.A.	SAP	Ethernet: Slot 1, port 2	dot1q	Untagged	N.A.
☐	2	N.A.	SNP	Radio: Slot 2, port 1	dot1q	Untagged	N.A.

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

- **General** – See *Ethernet Service Points – General SP Attributes Table*
- **Ingress** – See *Ethernet Service Points – Ingress Attributes*
- **Egress** – See *Ethernet Service Points – Egress Attributes*

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

Ethernet Service Points – General SP Attributes Table

The General SP Attributes table is shown in *Figure 120: Ethernet Service Points Page*. *Table 36* describes the parameters displayed in the General SP Attributes table.

Table 36: General Service Point Attributes

Parameter	Definition
Service point ID	This ID is unique within the service. For Point-to-Point and Multipoint services, the range of values is 1-32. For Management services, the range of values is 1-30. When adding a service point, you can select a service point ID from the available options in the **Service point ID** drop-down list in the Ethernet Service Points – Add page. Once you have added the service point, you cannot change the service point ID.
Service point name	A descriptive name for the service point (optional). The Service Point Name can be up to 20 characters.
Service point type	The service point type. Options are: ● **SAP** – Service Access Point. ● **SNP** – Service Network Point. ● **MNG** – Management service point. ● **PIPE** – Pipe service point. The following rules apply to the mixing of different types of service points on a single logical interface: ● You cannot configure both SAPs and SNPs on the same logical interface. ● You can configure both SAPs or SNPs on the same logical interface as a MNG service point. ● If you configure a Pipe service point on an interface, you cannot configure an SAP, SNP, or another Pipe service point on the same interface. You can, however, configure an MNG service point on the same interface. ● You cannot configure more than one MNG service point on a single logical interface. Once you have added the service point, you cannot change this parameter.
Interface location	The physical or logical interface on which the service point is located. Once you have added the service point, you cannot change this parameter.
Attached interface type	The encapsulation type (Ethertype) for frames entering the service point. Once you have added the service point, you cannot change this parameter. The Attached Interface Type determines which frames enter the service via this service point, based on the frame's VLAN tagging. Since more than one service point may be associated with a single interface, frames are assigned to the earliest defined service point in case of conflict. For a list of available Attached Interface Types, the types of frames to which each one applies, and the service point types for which each one is available, see *Table 37*.
C-Vlan encapsulation	The C-VLAN classified into the service point. Options are 1-4094, **Untagged**, or **N.A.** (Not Applicable). Once you have added the service point, you cannot change this parameter. If you selected **Bundle-C** in the **Attached Interface Type** field, select **Untagged** or **N.A**. You can then add multiple C-VLANs via the **Attach VLAN** option. See *Attaching VLANs*.
S-Vlan encapsulation	The S-VLAN classified into the service point. Options are 1-4094, **Untagged**, or **N.A.** (Not Applicable). Once you have added the service point, you cannot change this parameter. If you selected **Bundle-S** in the **Attached Interface Type** field, select the S-VLAN value to classify into the service point (1-4094), or select **Untagged**. You can then add multiple C-VLANs via the **Attach VLAN** option. See *Attaching VLANs*.

Table 37 describes the available Attached Interface Types.

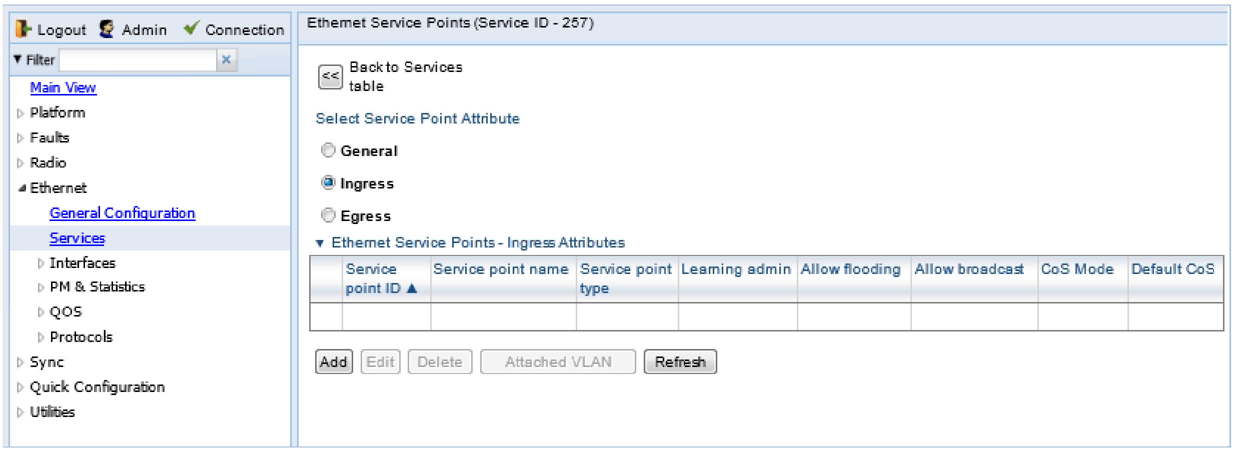
Table 37: Attached Interface Types

Attached Interface Type	Types of Frames	Available for Service Point Types
dot1q	A single C-VLAN is classified into the service point.	All
s-tag	A single S-VLAN is classified into the service point.	SNP, PIPE, and MNG
Bundle-C	A set of C-VLANs is classified into the service point.	SAP
Bundle-S	A single S-VLAN and a set of C-VLANs are classified into the service point.	SAP
All-to-One	All C-VLANs and untagged frames that enter the interface are classified into the service point.	SAP
Q-in-Q	A single S-VLAN and C-VLAN combination is classified into the service point.	SAP and MNG

Ethernet Service Points – Ingress Attributes

Select **Ingress** in the Ethernet Service Points page to display the Ethernet Service Points – Ingress Attributes table. *Table 38* describes the parameters displayed in the Ingress SP Attributes table.

Figure 121: Ethernet Service Points Page – Ingress Attributes



Ethernet Service Points (Service ID - 257)

Select Service Point Attribute

○ General

● Ingress

○ Egress

▾ Ethernet Service Points - Ingress Attributes

Service point ID ▲	Service point name	Service point type	Learning admin	Allow flooding	Allow broadcast	CoS Mode	Default CoS

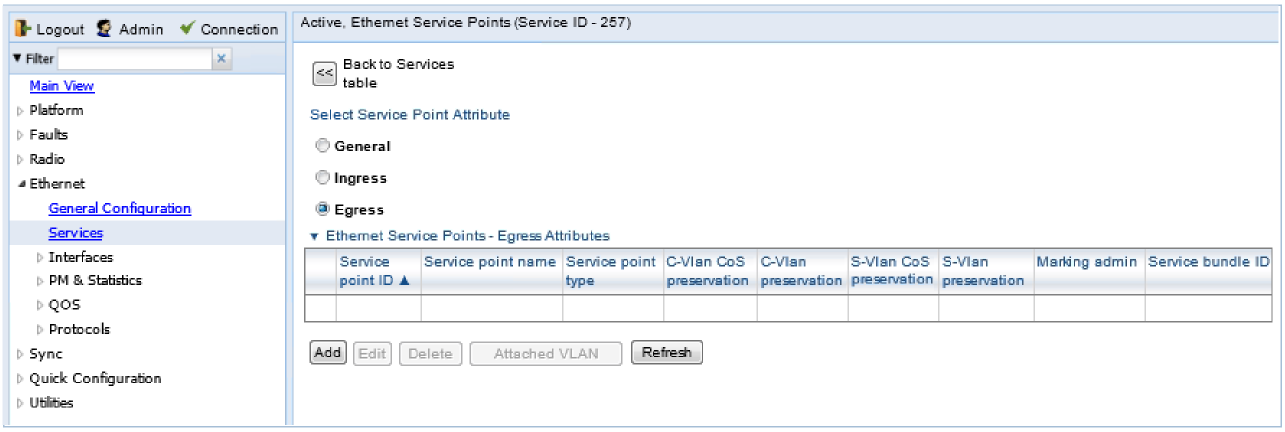
Table 38: Service Point Ingress Attributes

Parameter	Definition
Service point ID	This ID is unique within the service. For Point-to-Point and Multipoint services, the range of values is 1-32. For Management services, the range of values is 1-30.
Service point name	A descriptive name for the service point (optional). The Service Point Name can be up to 20 characters.
Service point type	The service point type. Options are: ● **SAP** – Service Access Point. ● **SNP** – Service Network Point. ● **MNG** – Management service point. ● **PIPE** – Pipe service point.
Learning admin	Determines whether MAC address learning for incoming frames is enabled (**Enable**) or disabled (**Disable**). When enabled, the service point learns the source MAC addresses of incoming frames and adds them to a MAC address forwarding table.
Allow flooding	Determines whether incoming frames with unknown MAC addresses are forwarded to other service points via flooding. Select **Allow** to allow flooding or **Disable** to disable flooding.
Allow broadcast	Indicates whether frames with a broadcast destination MAC address are allowed to ingress the service via this service point. Select **Allow** to allow broadcast or **Disable** to disable broadcast.
CoS Mode	Indicates how the service point handles the CoS of frames that pass through the service point. Options are: ● **sp-def-cos** – The service point re-defines the CoS of frames that pass through the service point, according to the Default CoS (below). This decision can be overwritten on the service level. ● **Interface-Decision** – The service point preserves the CoS decision made at the interface level. The decision can still be overwritten at the service level. ● **PCL** – Reserved for future use. ● **TCAM** – Reserved for future use.
Default CoS	The default CoS. If the **CoS Mode** is **sp-def-cos**, this is the CoS assigned to frames that pass through the service point. This decision can be overwritten at the service level. Possible values are 0 to 7.

Ethernet Service Points – Egress Attributes

Select **Egress** in the Ethernet Service Points page to display the Ethernet Service Points – Egress Attributes table. *Table 39* `describes the parameters displayed in the General SP Attributes table.

Figure 122: Ethernet Service Points Page – Egress Attributes



Active, Ethernet Service Points (Service ID - 257)

Select Service Point Attribute

○ General

○ Ingress

● Egress

▼ Ethernet Service Points - Egress Attributes

	Service point ID ▲	Service point name	Service point type	C-Vlan CoS preservation	C-Vlan preservation	S-Vlan CoS preservation	S-Vlan preservation	Marking admin	Service bundle ID

Table 39: Service Point Egress Attributes

Parameter	Definition
Service point ID	This ID is unique within the service. For Point-to-Point and Multipoint services, the range of values is 1-32. For Management services, the range of values is 1-30.
Service point name	A descriptive name for the service point (optional). The Service Point Name can be up to 20 characters.
Service point type	The service point type. Options are: ● **SAP** – Service Access Point. ● **SNP** – Service Network Point. ● **MNG** – Management service point. ● **PIPE** – Pipe service point.
C-Vlan CoS preservation	Determines whether the original C-VLAN CoS value is preserved or restored for frames egressing from the service point. ● If C-VLAN CoS preservation is enabled, the C-VLAN CoS value of frames egressing the service point is the same as the value when the frame entered the service. ● If C-VLAN CoS preservation is disabled, the C-VLAN CoS value of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking (see **Marking admin**, below).
C-Vlan preservation	Determines whether the original C-VLAN ID is preserved or restored for frames egressing from the service point. ● If C-VLAN preservation is enabled, the C-VLAN ID of frames egressing the service point is the same as the C-VLAN ID when the frame entered the service. ● If C-VLAN preservation is disabled, the C-VLAN ID of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking (see **Marking admin**, below).
S-Vlan CoS preservation	Determines whether the original S-VLAN CoS value is preserved or restored for frames egressing from the service point. ● If S-VLAN CoS preservation is enabled, the S-VLAN CoS value of frames egressing the service point is the same as the value when the frame entered the service. ● If S-VLAN CoS preservation is disabled, the C-VLAN CoS value of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking (see **Marking admin**, below).
S-Vlan preservation	Read-only. Indicates whether the original S-VLAN ID is preserved or restored for frames egressing from the service point. ● If S-VLAN preservation is enabled, the S-VLAN ID of frames egressing the service point is the same as the S-VLAN ID when the frame entered the service. ● If S-VLAN preservation is disabled, the S-VLAN ID of frames egressing the service point is set at whatever value might have been re-assigned by the interface, service point, or service, or whatever value results from marking (see **Marking admin**, below).

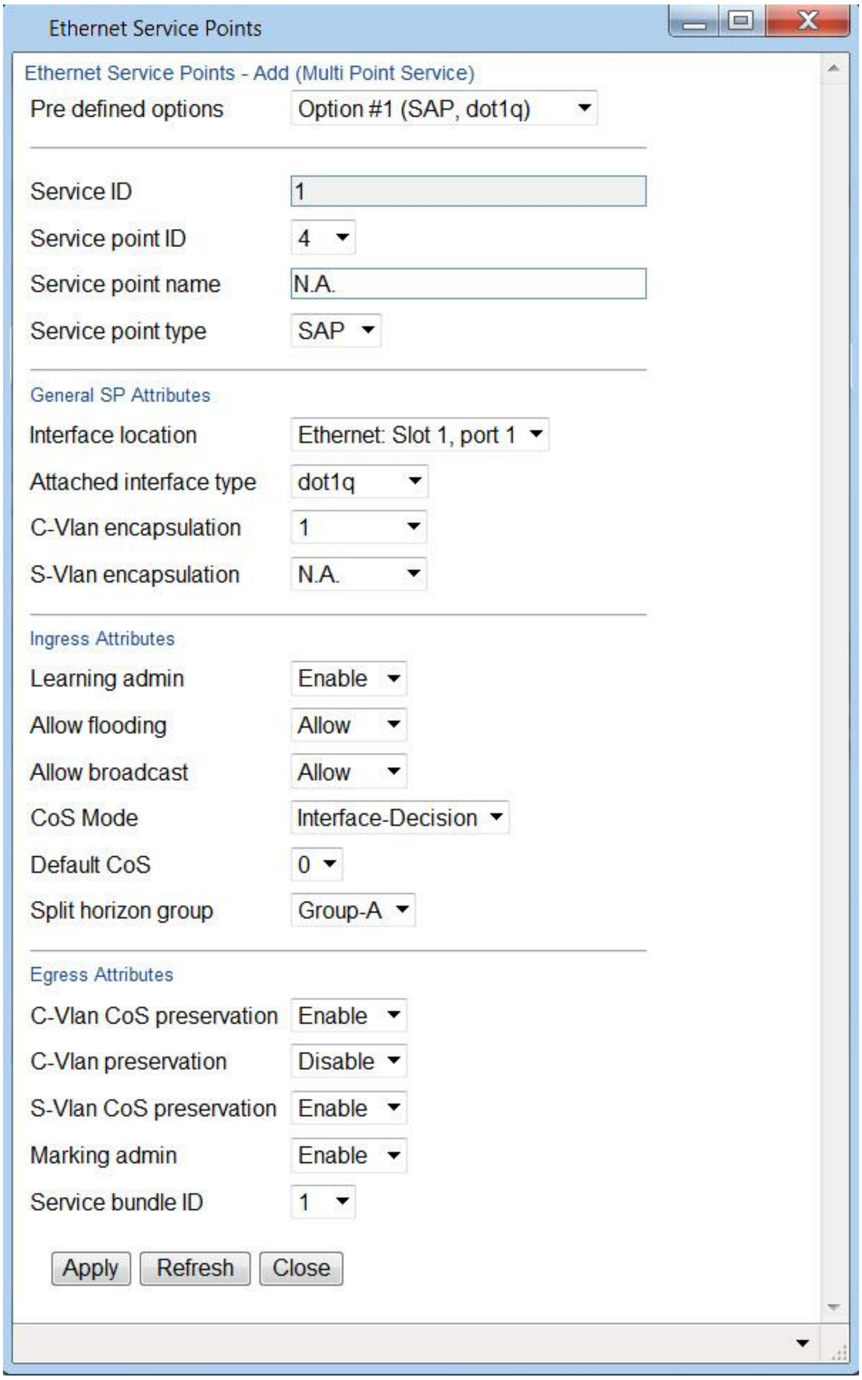
Marking admin	Determines whether re-marking of the outer VLAN (C-VLAN or S-VLAN) of tagged frames that pass through the service point is enabled. ● If **Marking admin** is set to **Enable**, and CoS preservation for the relevant outer VLAN is set to **Disable**, the SAP re-marks the C-VLAN or S-VLAN 802.1p UP bits of egress frames according to the calculated CoS and Color, and the user-configurable 802.1Q and 802.1AD marking tables. You can configure these tables by selecting **Ethernet > QoS > Marking** from the menu on the left side of the Web EMS. ● If **Marking admin** and CoS preservation for the relevant outer VLAN are both set to **Enable**, re-marking is not performed. ● If **Marking admin** and CoS preservation for the relevant outer VLAN are both set to **Disable**, re-marking is applied, but only according to the values defined for Green frames in the 802.1Q and 802.1AD marking tables.
Service Bundle ID	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.

6.1.9.3. Adding a Service Point

To add a service point:

1. Select **Ethernet > Services**. The Ethernet Services page opens (*Figure 117*).
2. Select the relevant service in the Ethernet Services Configuration table.
3. Click **Service Points**. The Ethernet Service Points page opens (*Figure 120*).
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 123: Ethernet Service Points - Add Page



Ethernet Service Points

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

6 Configure the service point attributes, as described in *Table 36*, *Table 38*, and *Table 39*.

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**.

6.1.9.4. Editing a Service Point

To edit a service point:

1 Select **Ethernet > Services**. The Ethernet Services page opens (*Figure 117*).
2 Select the relevant service in the Ethernet Services Configuration table.
3 Click **Service Points**. The Ethernet Service Points page opens (*Figure 120*).
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 123*). 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 36*, *Table 38*, and *Table 39*.
7 Click **Apply**, then **Close**.

6.1.9.5. 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 117*).
2 Select the relevant service in the Ethernet Services Configuration table.
3 Click **Service Points**. The Ethernet Service Points page opens (*Figure 120*).
4 Select the relevant service point in the Ethernet Services Points – General SP Attributes table.
5 Click **Delete**. The service point is deleted.

6.1.9.6. 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.

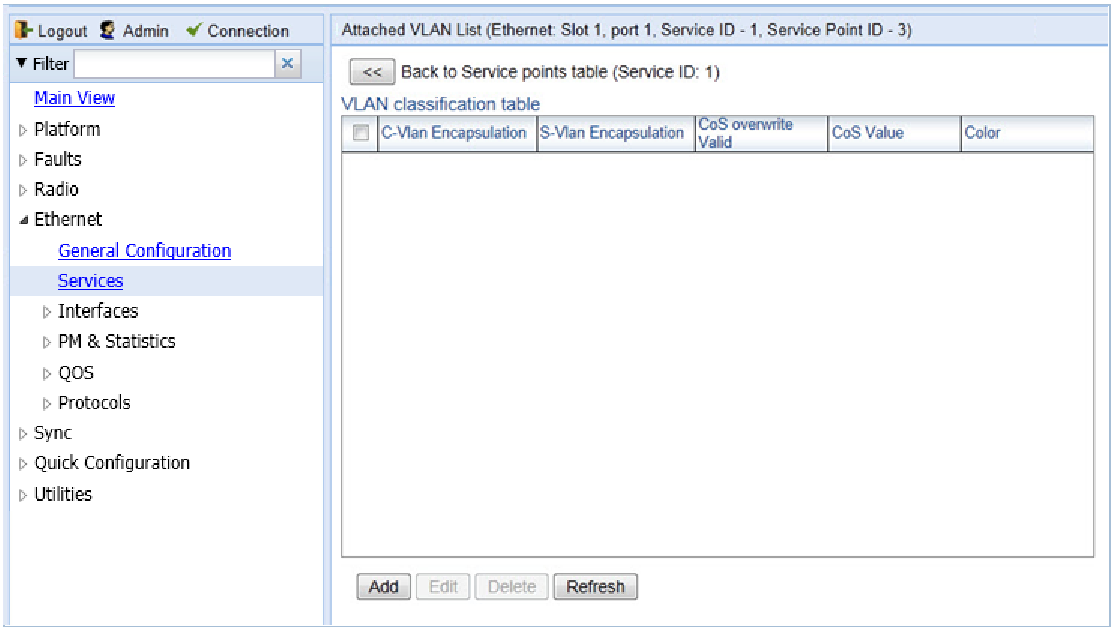
To add multiple C-VLANs:

1 Select **Ethernet > Services**. The Ethernet Services page opens (*Figure 117*).
2 Select the relevant service in the Ethernet Services Configuration table.
3 Click **Service Points**. The Ethernet Service Points page opens (*Figure 120*).

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 124: Attached VLAN List Page



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

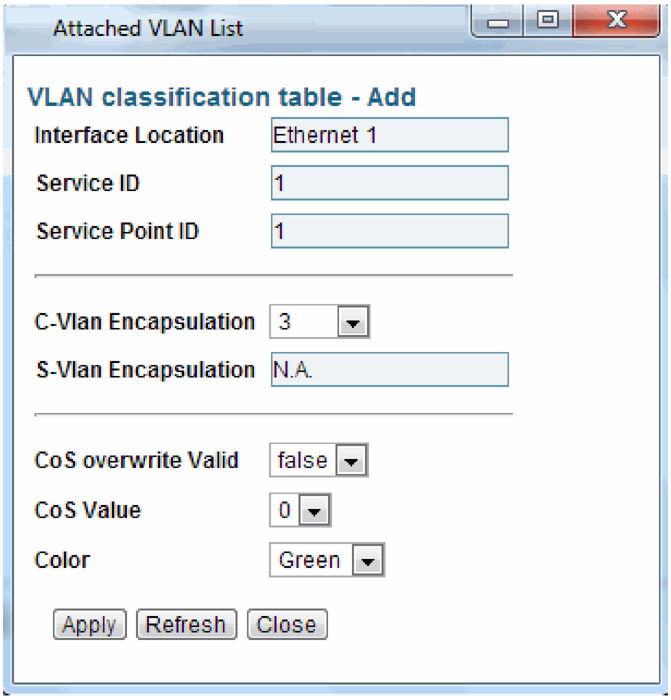
Back to Service points table (Service ID: 1)

VLAN classification table

□	C-Vlan Encapsulation	S-Vlan Encapsulation	CoS overwrite Valid	CoS Value	Color

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

Figure 125: Attached VLAN List - Add Page



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

7 Configure the VLAN Classification parameters, described in *Table 40*.
8 Click **Apply**, then **Close**.

Table 40: VLAN Classification Parameters

Parameter	Definition
Interface Location	Read-only. The physical or logical interface on which the service point is located.
Service ID	Read-only. The ID of the service to which the service point belongs.
Service Point ID	Read-only. The ID of the service point.
C-Vlan Encapsulation	Select the C-VLAN you want to add to the service point.
S-Vlan Encapsulation	Read-only. If the **Attached Interface Type** for the service point is **Bundle-S**, this field displays the S-VLAN encapsulation selected when the service point was created. If the **Attached Interface Type** for the service point is **Bundle-C**, this field is inactive.
CoS Overwrite Valid	If you want to assign a specific CoS and Color to frames with the C-VLAN or S-VLAN defined in the **C-VLAN Encapsulation** field, select **true**. This CoS and Color values defined below override the CoS and Color decisions made at the interface level. However, if the service point or service are configured to apply their own CoS and Color decisions, those decisions override the decision made here.
CoS Value	If **CoS Overwrite Valid** is set to **true**, the CoS value defined in this field is applied to frames with the C-VLAN defined in the **C-VLAN Encapsulation** field. This CoS overrides the CoS decision made at the interface level. However, if the service point or service are configured to apply their own CoS, that decision overrides the decision made here. If CoS Overwrite Valid is set to false, this parameter has no effect.
Color	If **CoS Overwrite Valid** is set to **true**, the Color value defined in this field is applied to frames with the C-VLAN defined in the **C-VLAN Encapsulation** field. This Color overrides the Color decision made at the interface level. However, if the service point or service are configured to apply their own Color, that decision overrides the decision made here. If **CoS Overwrite Valid** is set to **false**, this parameter has no effect.

To edit a VLAN Classification table entry, select the entry in the VLAN Classification table and click **Edit**. You can edit all the fields that can be configured in the Attached VLAN List – Add page, except the **C-VLAN Encapsulation** field.

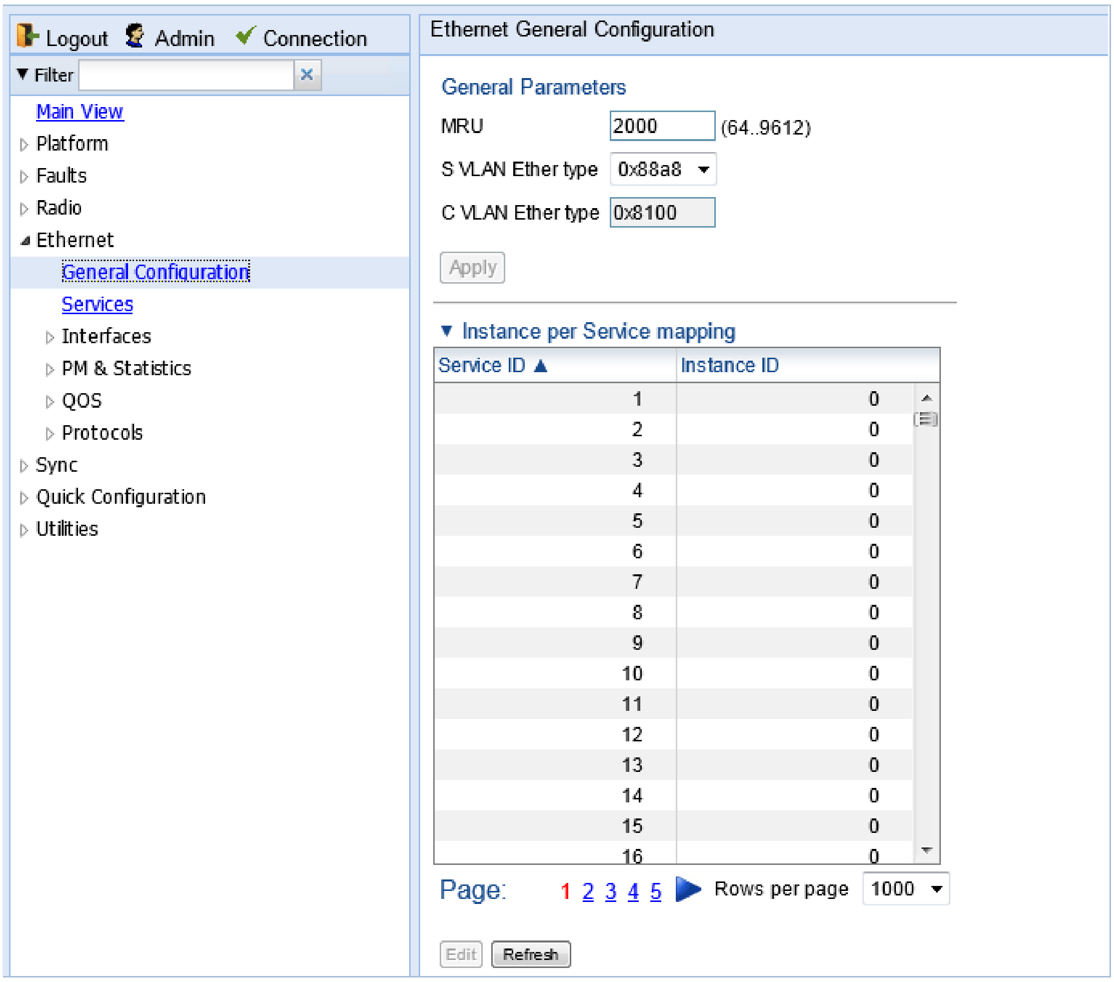
To delete a VLAN Classification table entry, select the entry in the VLAN Classification table and click **Delete**.

6.2. Setting the MRU Size and the S-VLAN Ethertype

To configure the size of the MRU (Maximum Receive Unit) and the S-VLAN Ethertype:

1 Select **Ethernet > General Configuration**. The Ethernet General Configuration page opens.

Figure 126: Ethernet General Configuration Page



Ethernet General Configuration

General Parameters

MRU 2000 (64..9612)

S VLAN Ether type 0x88a8

C VLAN Ether type 0x8100

Apply

Instance per Service mapping

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

Page: 1 2 3 4 5 Rows per page 1000

Edit Refresh

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**.

6.3. Configuring Ethernet Interfaces

Related Topics:

- *Enabling the Interfaces (Interface Manager)*
- *Performing Ethernet Loopback*

- *Configuring Ethernet Service(s)*
- *Quality of Service (QoS)*

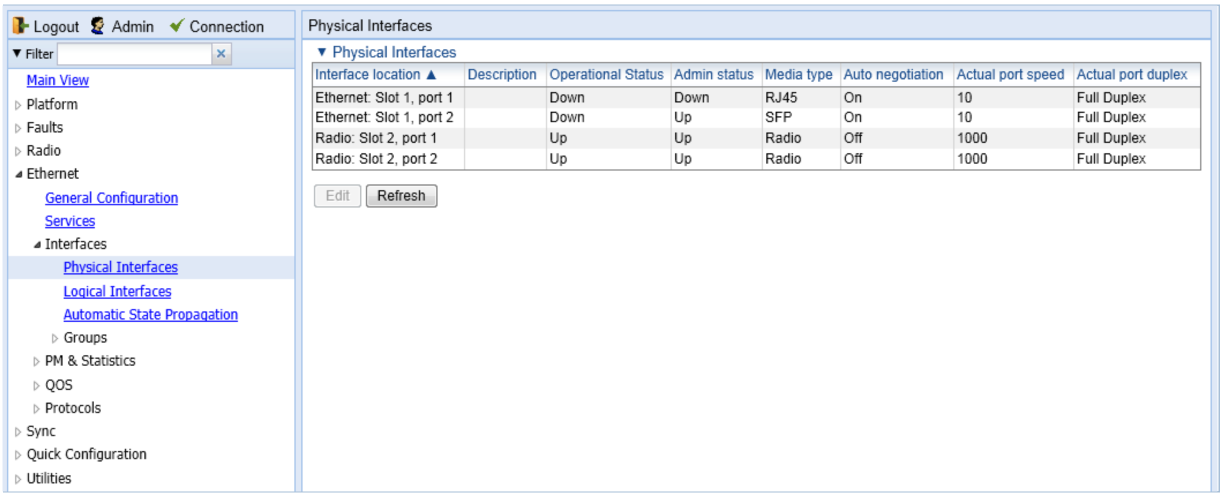
The NS Primo/Diplo's switching fabric distinguishes between physical interfaces and logical interfaces. Physical and logical interfaces serve different purposes in the switching fabric. In some cases, a physical interface corresponds to a logical interface on a one-to-one basis. For some features, such 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.

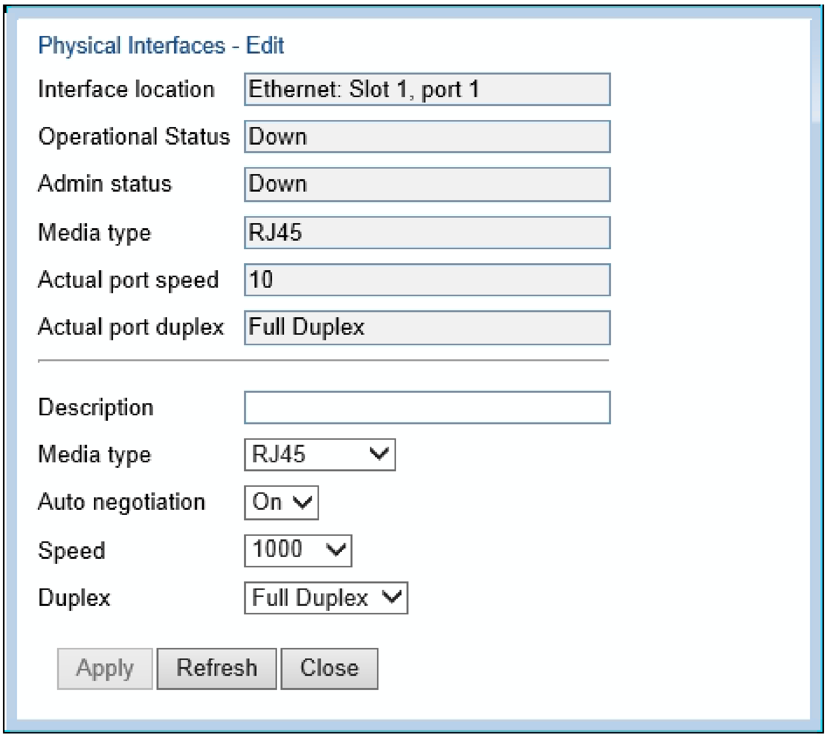
Figure 127: Physical Interfaces Page



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 128: 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

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 – **100Mbps HD**, **100Mbps FD**, and **1000Mpbs FD**.
  - Ethernet SFP interfaces – Only **1000FD** 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 41 describes the status parameters that appear in the Physical Interfaces page.

Table 41: Physical Interface Status Parameters

Parameter	Definition
Interface location	The location of the interface.
Operational Status	Indicates whether the interface is currently operational (**Up**) or non-operational (**Down**).
Admin Status	Indicates whether the interface is currently enabled (**Up**) or disabled (**Down**). You can enable or disable an interface from the Interface Manager page. See *Enabling the Interfaces (Interface Manager)*.
Media Type	The physical interface layer 1 media type.
Actual port speed	Displays the actual speed of the interface for the link as agreed by the two sides of the link after the auto negotiation process.
Actual port 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.

6.4. Configuring Automatic State Propagation

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.

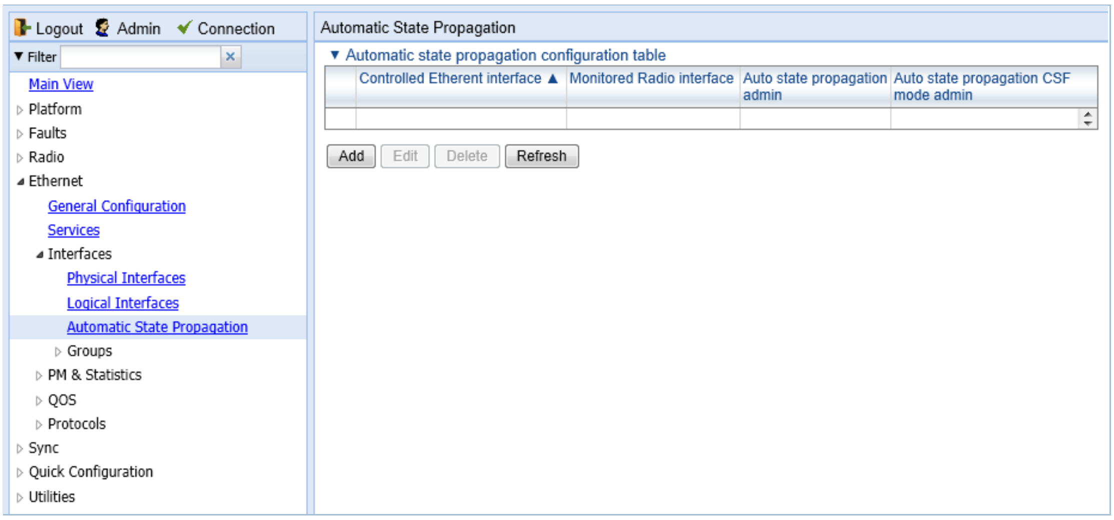
Automatic state propagation is configured as pairs of interfaces. Each interface pair includes a Monitored Interface and a Controlled Interface.

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.

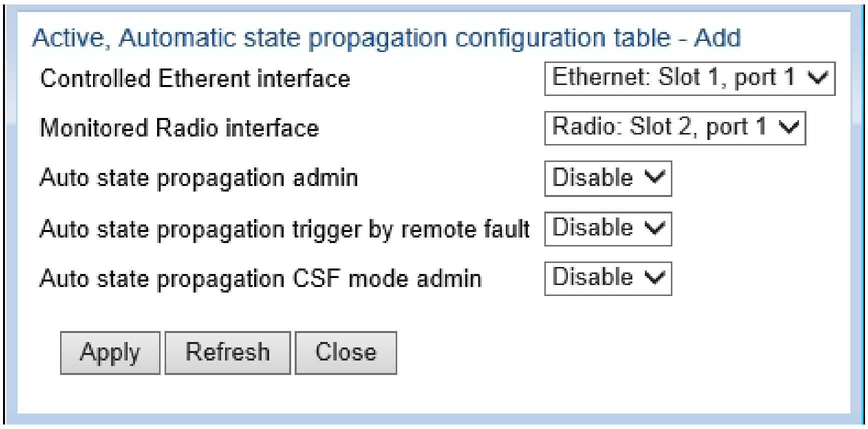
Figure 129: Automatic State Propagation Page



Controlled Ethernet interface ▲	Monitored Radio interface	Auto state propagation admin	Auto state propagation CSF mode admin

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

Figure 130: Automatic State Propagation - Add Page



Active, Automatic state propagation configuration table - Add

Controlled Etherent interface	Ethernet: Slot 1, port 1
Monitored Radio interface	Radio: Slot 2, port 1
Auto state propagation admin	Disable
Auto state propagation trigger by remote fault	Disable
Auto state propagation CSF mode admin	Disable

3 In the **Controlled Ethernet interface** field, select the 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 **Auto state propagation 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 **Auto state propagation 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.

7 Optionally, in the **Auto state propagation 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.

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 130*), 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.

6.5. Viewing Ethernet PMs and Statistics

NS Primo/Diplo 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:

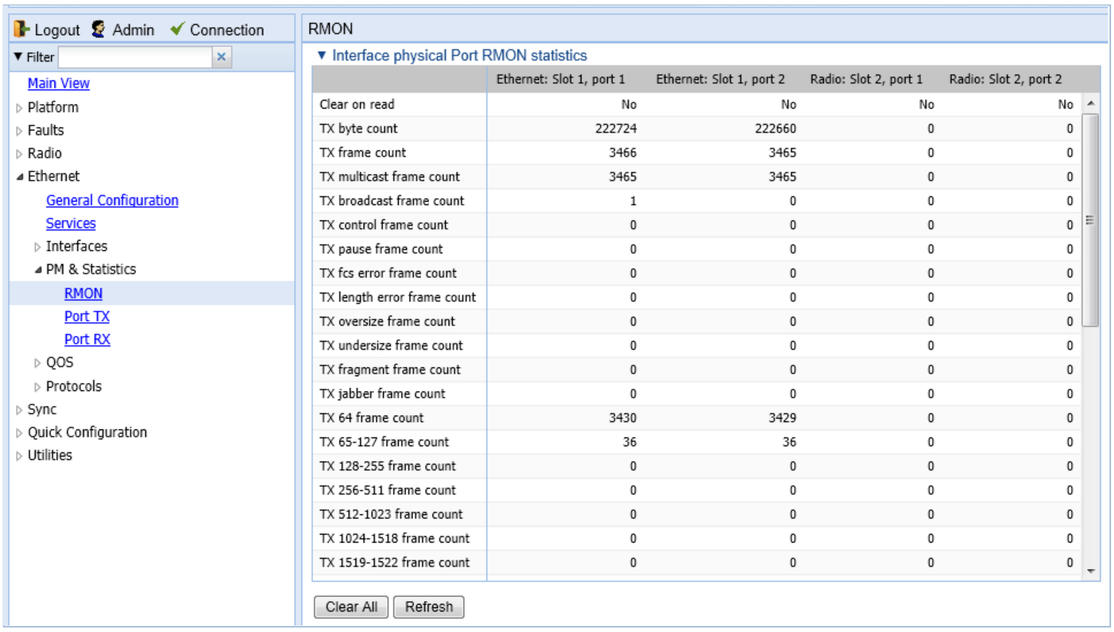
- *RMON Statistics*
- *Port TX Statistics*
- *Port RX Statistics*

6.5.1. RMON Statistics

To view and reset RMON statistics:

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

Figure 131: RMON Page



▼ Interface physical Port RMON statistics

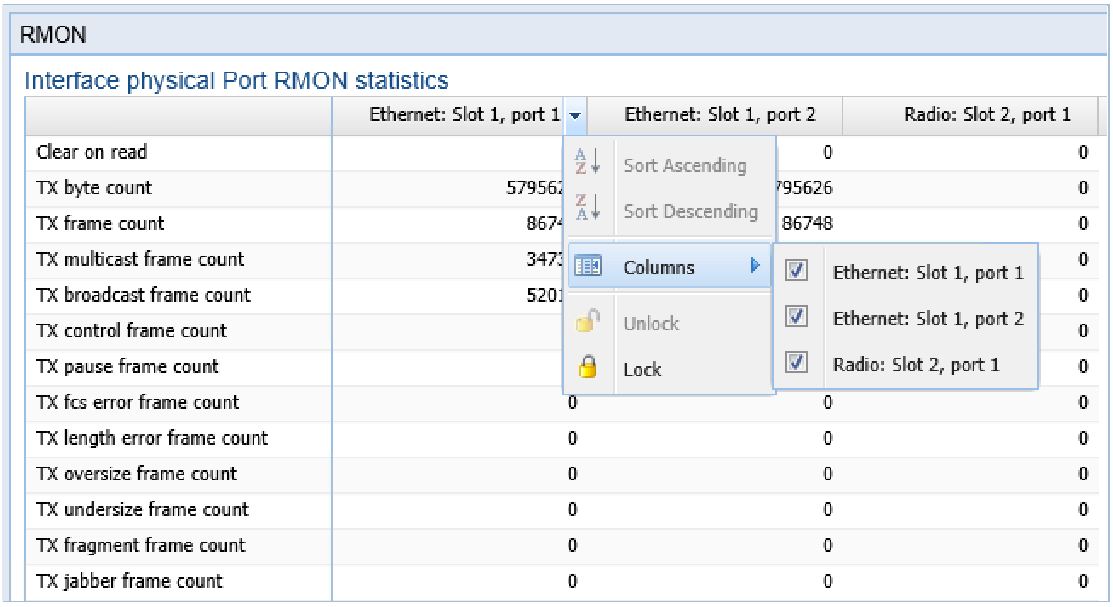
	Ethernet: Slot 1, port 1	Ethernet: Slot 1, port 2	Radio: Slot 2, port 1	Radio: Slot 2, port 2
Clear on read	No	No	No	No
TX byte count	222724	222660	0	0
TX frame count	3466	3465	0	0
TX multicast frame count	3465	3465	0	0
TX broadcast frame count	1	0	0	0
TX control frame count	0	0	0	0
TX pause frame count	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 132: 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

☑ Ethernet: Slot 1, port 1
☑ Ethernet: Slot 1, port 2
☑ Radio: Slot 2, port 1

6.5.2. Port TX Statistics

The Ethernet Port TX PM report page displays PMs that measure various peak transmission rates (in seconds) and average transmission rates (in seconds), 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:

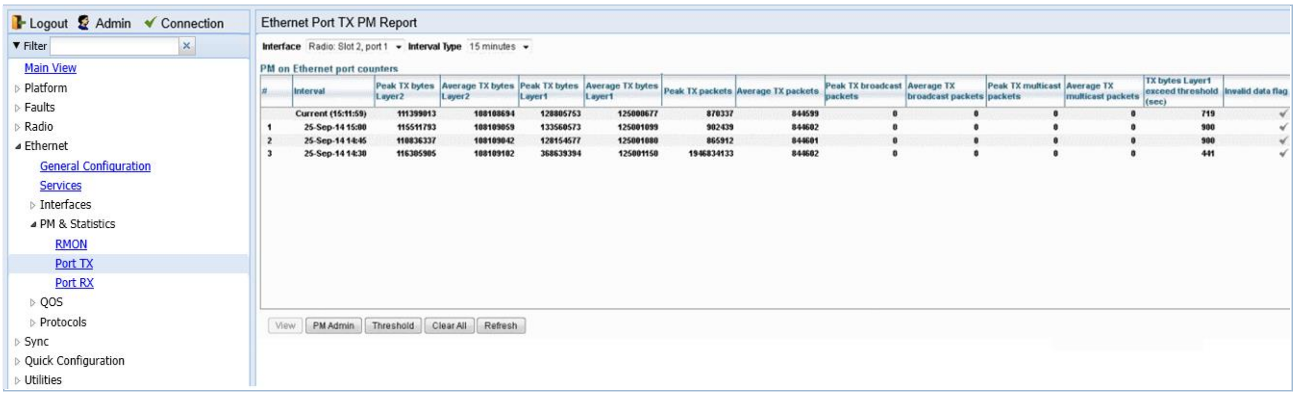
- *Displaying Ethernet Port TX PMs*
- *Enabling or Disabling Gathering of Port TX PM Statistics per Interface*
- *Setting the Ethernet Port TX Threshold*

6.5.2.1. 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 133: Ethernet Port TX PM Report Page



Ethernet Port TX PM Report

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

PM on Ethernet port counters

#	Interval	Peak TX bytes Layer2	Average TX bytes Layer2	Peak TX bytes Layer1	Average TX bytes Layer1	Peak TX packets	Average TX packets	Peak TX broadcast packets	Average TX broadcast packets	Peak TX multicast packets	Average TX multicast packets	TX bytes Layer1 exceed threshold (sec)	Invalid data flag
	Current (15:11:59)	111399013	108108694	128805753	125000677	870337	844599	0	0	0	0	719	✓
1	25-Sep-14 15:00	115511793	108109059	133560573	125001099	902439	844602	0	0	0	0	900	✓
2	25-Sep-14 14:45	110836337	108109042	128154577	125001080	865912	844601	0	0	0	0	900	✓
3	25-Sep-14 14:30	116305905	108109102	368639394	125001150	1946834133	844602	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 42 describes the Ethernet TX port PMs.

Table 42: Ethernet TX Port PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Peak... Average... bytes... Packets...	Various peak transmission rates (in seconds) and average transmission rates (in seconds), 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).

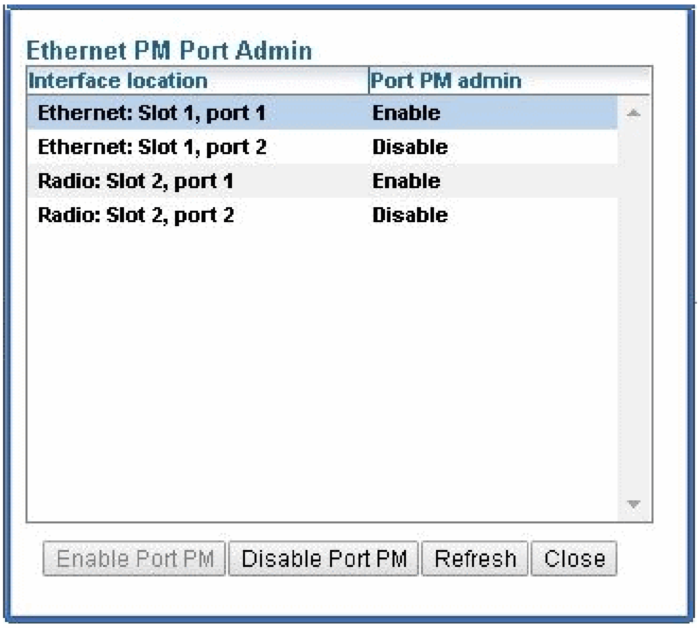
To clear the PMs, click **Clear All**.

6.5.2.2. 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 134: Ethernet PM Port Admin Page



Ethernet PM Port Admin

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

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**.

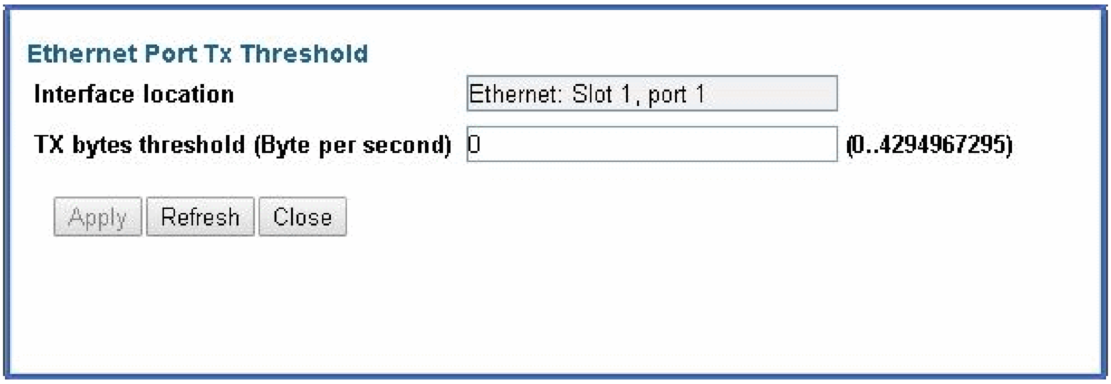
6.5.2.3. Setting the Ethernet Port TX Threshold

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 135: Ethernet Port Tx Threshold Page



Ethernet Port Tx Threshold

Interface location: Ethernet: Slot 1, port 1

TX bytes threshold (Byte per second): 0 (0..4294967295)

2 Enter a threshold, between 0 and 4294967295.

3 Click **Apply**, then **Close**.

6.5.3. Port RX Statistics

The Ethernet Port RX PM report page displays PMs that measure various peak transmission rates (in seconds) and average RX rates (in seconds), 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:

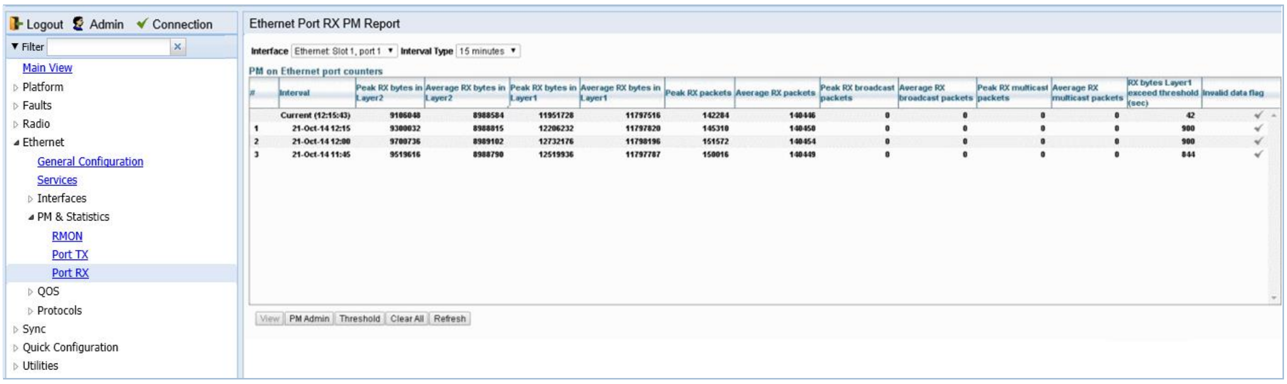
- *Displaying Ethernet Port RX PMs*
- *Enabling or Disabling Gathering of Port RX PM Statistics per Interface*
- *Setting the Ethernet Port RX Threshold*

6.5.3.1. 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 136: Ethernet Port RX PM Report Page



Ethernet Port RX PM Report

Interface Ethernet Slot 1, port 1 **Interval Type** 15 minutes

PM on Ethernet port counters

#	Interval	Peak RX bytes in Layer2	Average RX bytes in Layer2	Peak RX bytes in Layer1	Average RX bytes in Layer1	Peak RX packets	Average RX packets	Peak RX broadcast packets	Average RX broadcast packets	Peak RX multicast packets	Average RX multicast packets	RX bytes Layer1 exceed threshold (sec)	Invalid data flag
	Current (12:15:43)	9106048	8988584	11951728	11797516	142284	140446	0	0	0	0	42	✓
1	21-Oct-14 12:15	9300032	8988815	12206232	11797820	145310	140450	0	0	0	0	900	✓
2	21-Oct-14 12:00	9700736	8989102	12732176	11798196	151572	140454	0	0	0	0	900	✓
3	21-Oct-14 11:45	9519616	8988790	12519936	11797787	150016	140449	0	0	0	0	844	✓

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 43 describes the Ethernet RX port PMs.

Table 43: Ethernet RX Port PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Peak... Average... bytes... Packets...	Various peak transmission rates (in seconds) and average RX rates (in seconds), 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).

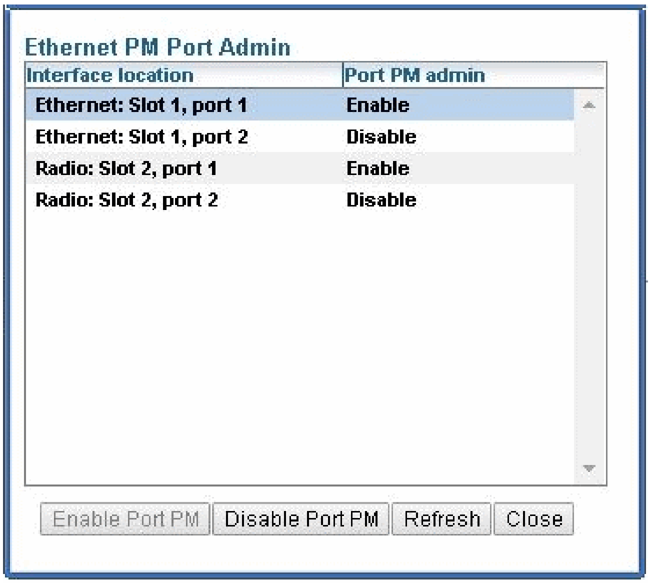
To clear the PMs, click **Clear All**.

6.5.3.2. 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 137: Ethernet PM Port Admin Page



Ethernet PM Port Admin

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

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**.

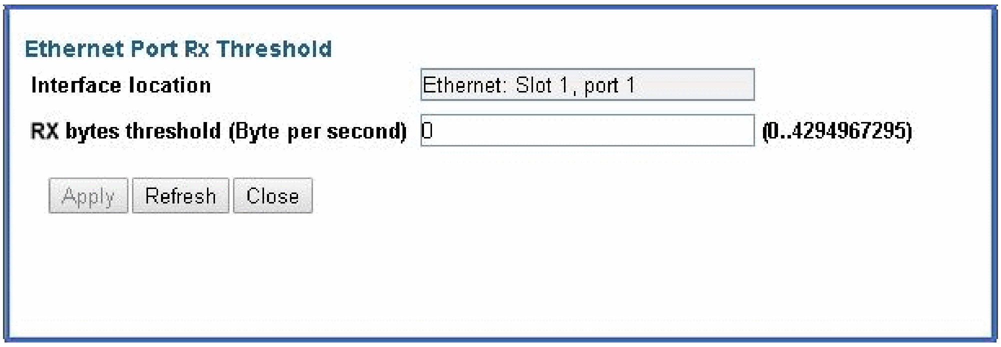
6.5.3.3. Setting the Ethernet Port RX Threshold

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 138: 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)

2 Enter a threshold, between 0 and 4294967295.

3 Click **Apply**, then **Close**.

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)*.

7.1. QoS Overview

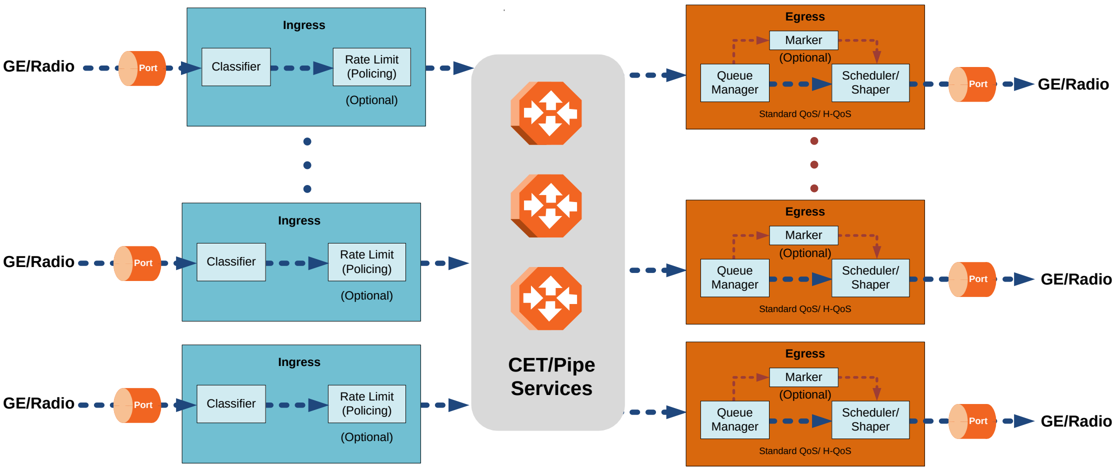
Quality of Service (QoS) deals with the way frames are handled within the switching fabric. QoS is required in order to deal with many different network scenarios, such as traffic congestion, packet availability, and delay restrictions.

NS Primo/Diplo's personalized QoS enables operators to handle a wide and diverse range of scenarios. NS Primo/Diplo'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 139 shows the basic flow of NS Primo/Diplo'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 139: 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 NS Primo/Diplo, refer to the Technical Description for the NS Primo/Diplo product type you are using.

7.2. Configuring Classification

The hierarchical classifier consists of the following levels:

- Logical interface-level classification
- Service point-level classification
- Service level classification

This section explains how to configure classification at the logical interface level.

- For instructions how to configure classification at the service point level, see *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)*.

7.2.1. Classification Overview

NS Primo/Diplo 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

NS Primo/Diplo 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.

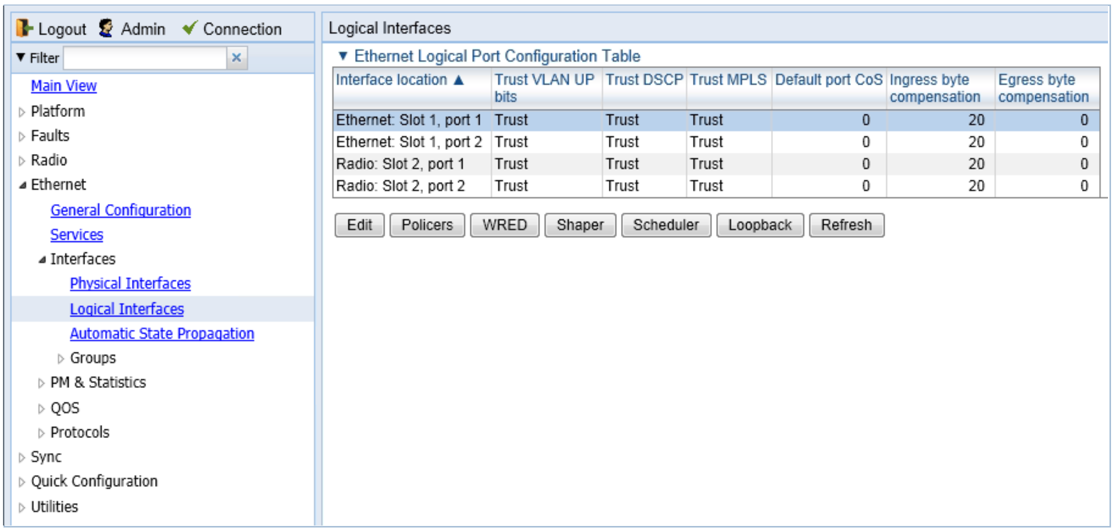
7.2.2. Configuring Ingress Path Classification on a Logical Interface

This section explains how to configure the classification criteria per each logical interface. The following sections explain how to modify the classification tables per bit type.

To configure the classification criteria for a logical interface:

1 Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens.

Figure 140: Logical Interfaces Page

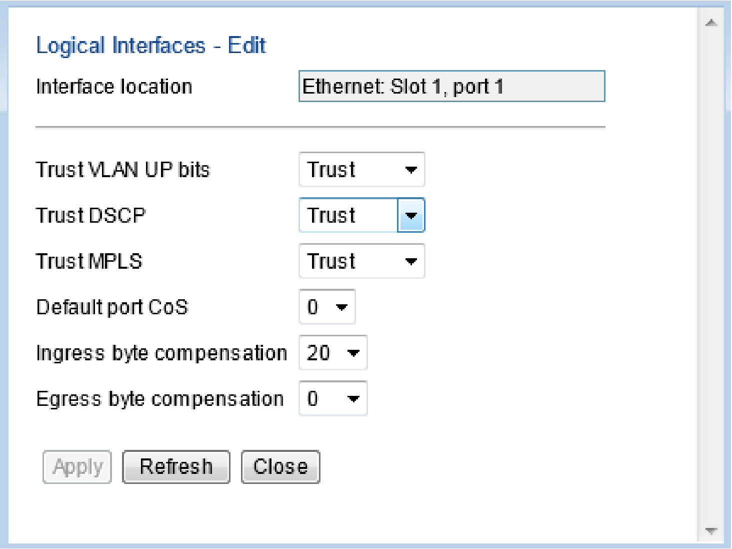


▼ Ethernet Logical Port Configuration Table

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

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

Figure 141: 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

3 Configure the parameters described in *Table 44*.

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

Note

The **Ingress byte compensation** and **Egress byte compensation** fields are described in *Configuring the Ingress and Egress Byte Compensation*.

Table 44: Logical Interface Classification Parameters

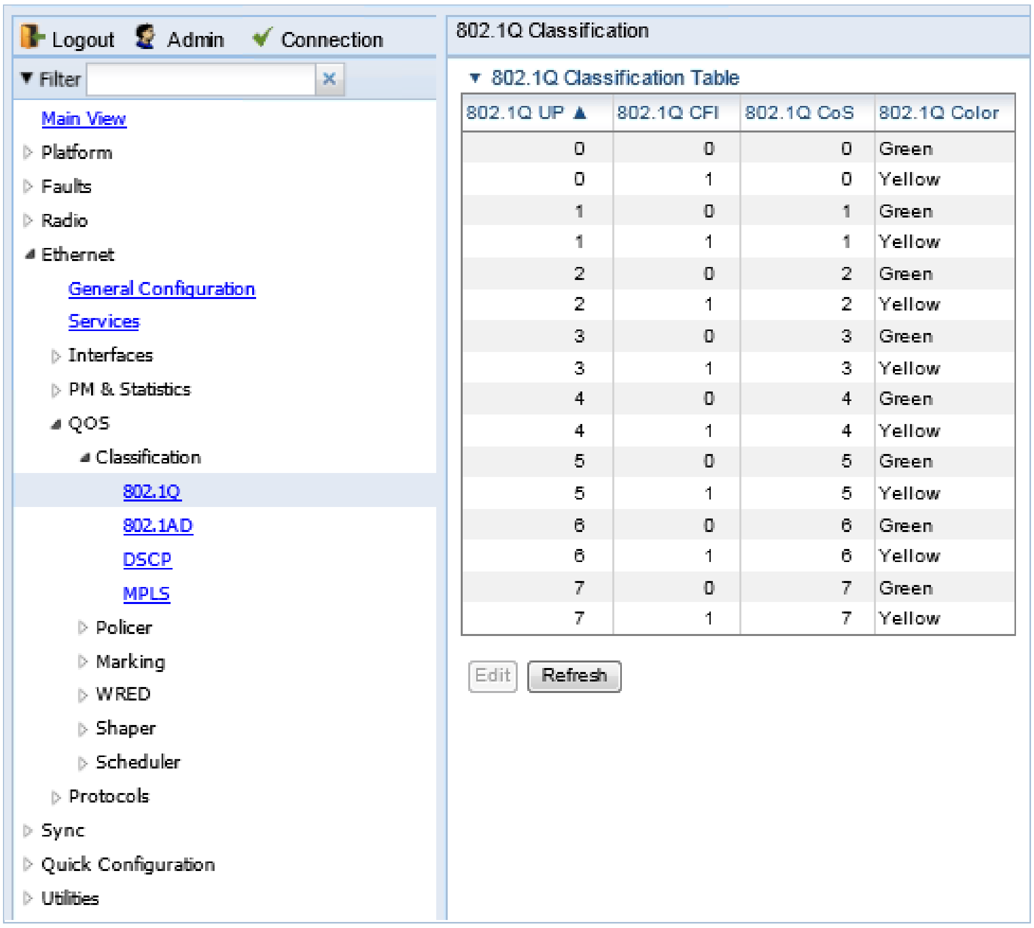
Parameter	Definition
Trust VLAN UP bits	Select the interface's trust mode for user priority (UP) bits: ● **Trust** – The interface performs QoS and color classification according to UP and CFI/DEI bits according to user-configurable tables for 802.1q UP bits (C-VLAN frames) or 802.1AD UP bits (S-VLAN frames). 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. ● **Un-Trust** – The interface does not consider 802.1 UP bits during classification.
Trust DSCP	Select the interface's trust mode for DSCP: ● **Trust** – The interface performs QoS and color classification according to a user-configurable table for DSCP to CoS and color classification. DSCP classification has priority over MPLS classification, so that if a match is found with the DSCP value of the ingressing frame, MPLS bits are not considered. ● **Un-Trust** – The interface does not consider DSCP during classification.
Trust MPLS	Select the interface's trust mode for MPLS bits: ● **Trust** – The interface performs QoS and color classification according to a user-configurable table for MPLS EXP to CoS and color classification. ● **Un-Trust** – The interface does not consider MPLS bits during classification.
Default port CoS	Select the default CoS value for frames passing through the interface (0 to 7). This value can be overwritten on the service point and service level.

7.2.3. Modifying the C-VLAN 802.1Q UP and CFI Bit Classification Table

To modify the classification criteria for 802.1Q User Priority (UP) bits:

1 Select **Ethernet > QoS > Classification > 802.1Q**. The 802.1Q Classification page opens.

Figure 142: 802.1Q Classification Page



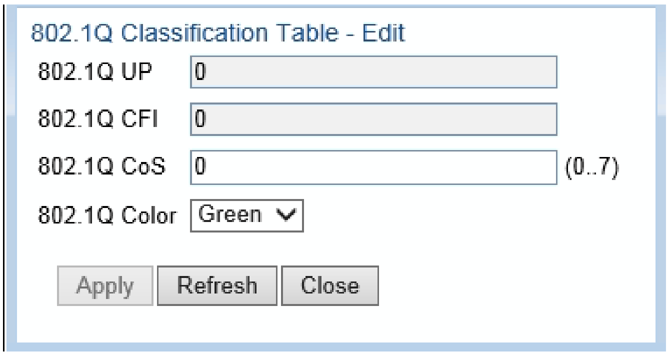
802.1Q Classification

▼ 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

2 Select the row you want to modify and click **Edit**. The 802.1Q Classification – Edit page opens.

Figure 143: 802.1Q Classification - Edit Page



802.1Q Classification Table - Edit

802.1Q UP	0
802.1Q CFI	0
802.1Q CoS	0 (0..7)
802.1Q Color	Green

3 Modify the parameters you want to change:

- ○ **802.1Q UP** – Read-only. The User Priority (UP) bit to be mapped.
- ○ **802.1Q CFI** – Read-only. The CFI bit to be mapped.
- ○ **802.1Q CoS** – The CoS assigned to frames with the designated UP and CFI.

- ○ **802.1Q Color** – The Color assigned to frames with the designated UP and CFI.

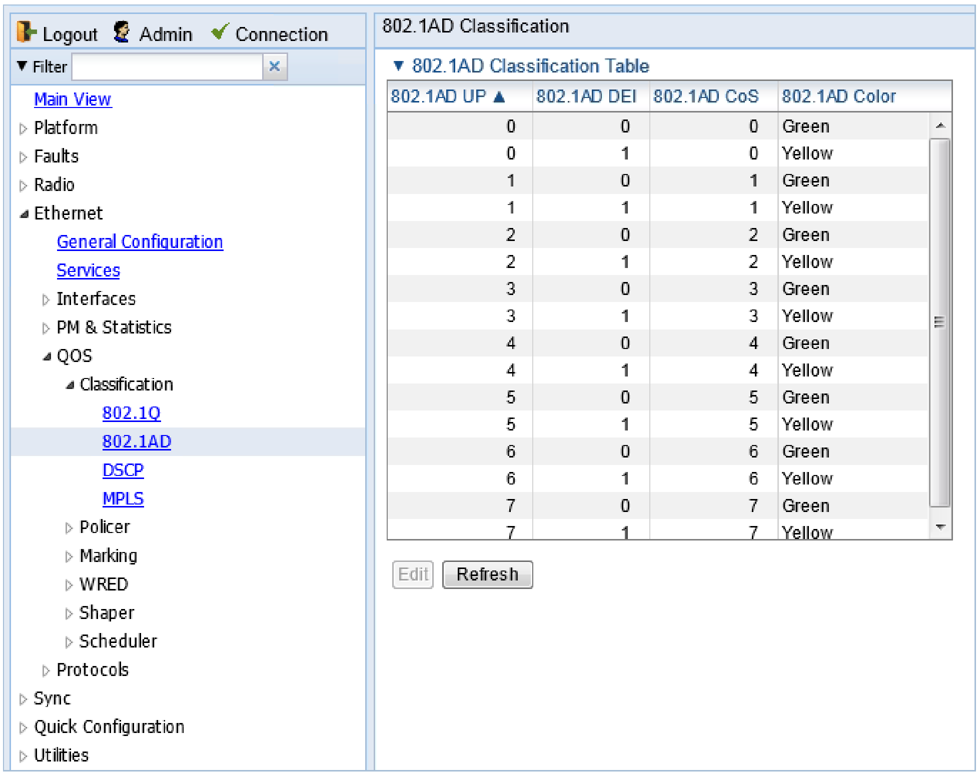
4 Click **Apply**, then **Close**.

7.2.4. Modifying the S-VLAN 802.1 UP and DEI Bit Classification Table

To modify the classification criteria for 802.1AD User Priority (UP) bits:

1 Select **Ethernet > QoS > Classification > 802.1AD**. The 802.1AD Classification page opens.

Figure 144: 802.1AD Classification Page

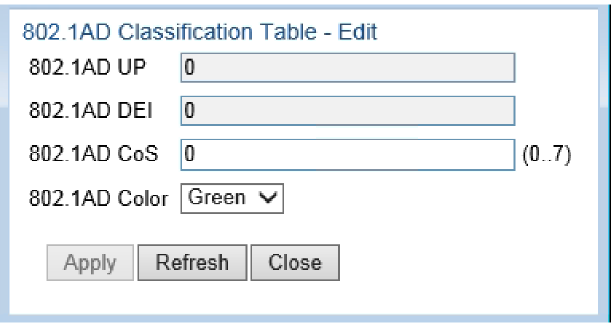


▼ 802.1AD Classification Table

802.1AD UP ▲	802.1AD DEI	802.1AD CoS	802.1AD Color
0	0	0	Green
0	1	0	Yellow
1	0	1	Green
1	1	1	Yellow
2	0	2	Green
2	1	2	Yellow
3	0	3	Green
3	1	3	Yellow
4	0	4	Green
4	1	4	Yellow
5	0	5	Green
5	1	5	Yellow
6	0	6	Green
6	1	6	Yellow
7	0	7	Green
7	1	7	Yellow

2 Select the row you want to modify and click **Edit**. The 802.1AD Classification - Edit page opens.

Figure 145: 802.1Q Classification - Edit Page



802.1AD Classification Table - Edit

802.1AD UP	0	
802.1AD DEI	0	
802.1AD CoS	0	(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**.

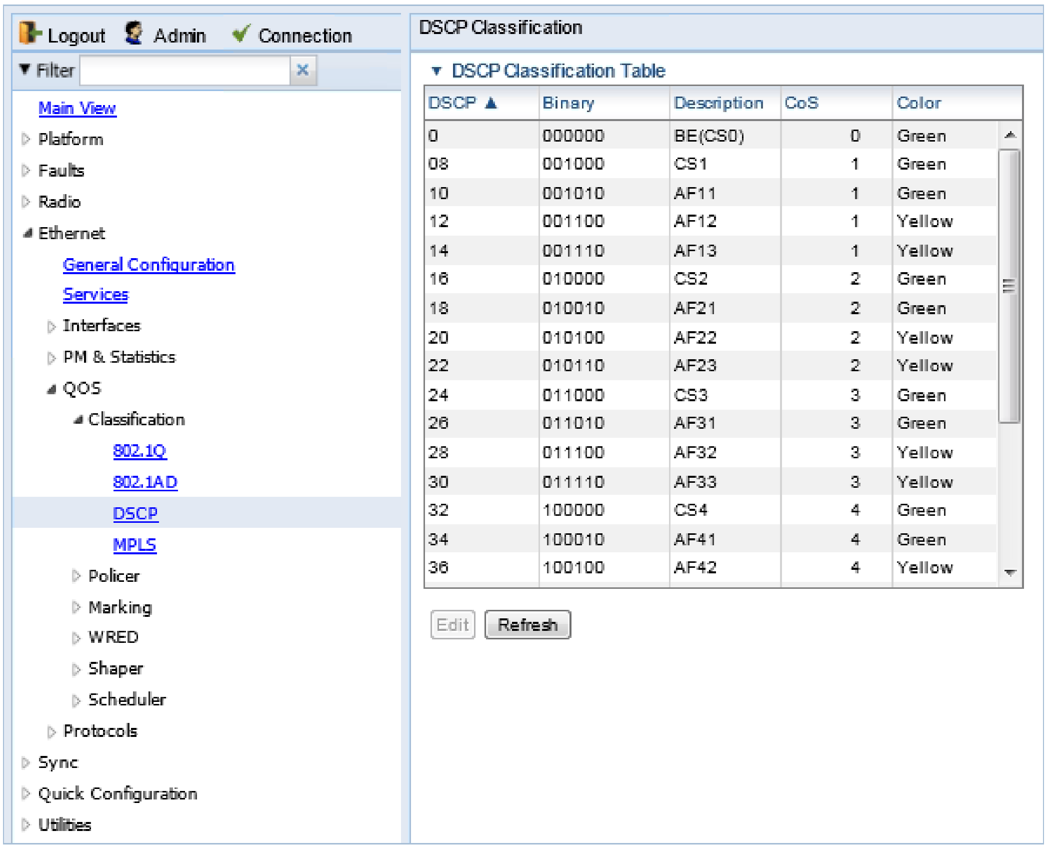
7.2.5. Modifying the DSCP Classification Table

You can configure the classification criteria for Differentiated Service Code Point (DSCP) priority values. The DSCP is a 6-bit length field inside the IP datagram header carrying priority information. Classification by DSCP can be used for untagged frames, as well as 802.1Q tagged or provider VLAN tagged frames.

To modify the classification criteria for DSCPs:

1 Select **Ethernet > QoS > Classification > DSCP**. The DSCP Classification page opens.

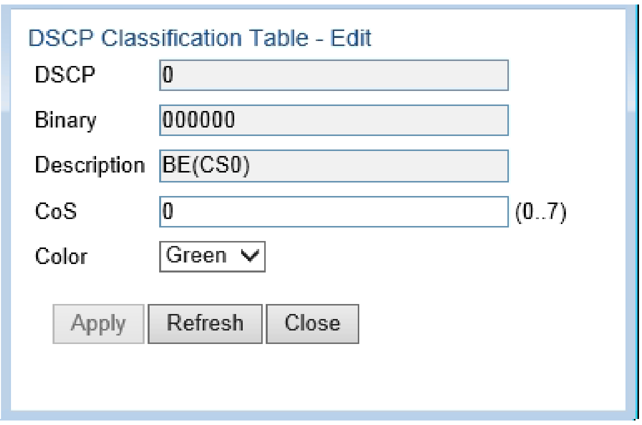
Figure 146: DSCP Classification Page



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

2 Select the row you want to modify and click **Edit**. The DSCP Classification - Edit page opens.

Figure 147: DSCP Classification - Edit Page



DSCP Classification Table - Edit

DSCP	0	
Binary	000000	
Description	BE(CS0)	
CoS	0	(0..7)
Color	Green	

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**.

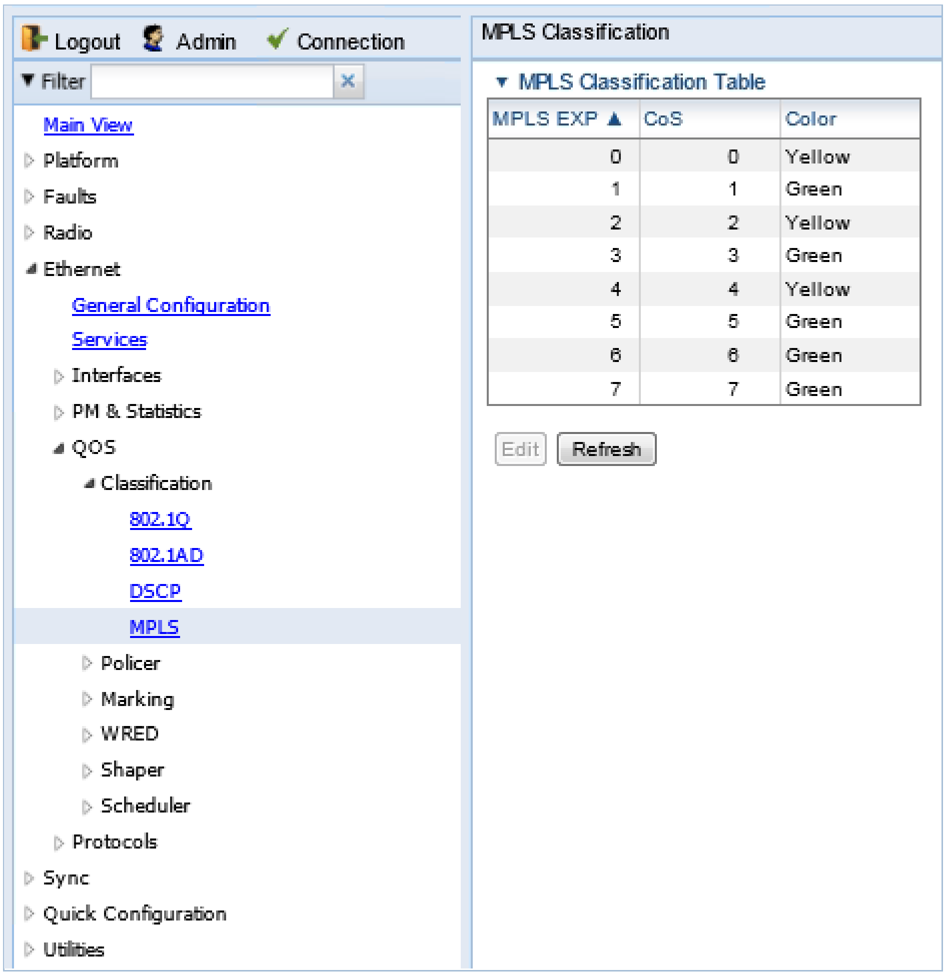
7.2.6. Modifying the MPLS EXP Bit Classification Table

MPLS bits are used to provide QoS capabilities by utilizing the bits set in the MPLS labels. Classification by MPLS bits is supported in both untagged and 802.1Q provider-tagged frames.

To modify the classification criteria for MPLS EXP bits:

1 Select **Ethernet > QoS > Classification > MPLS**. The MPLS Classification page opens.

Figure 148: MPLS Classification Page



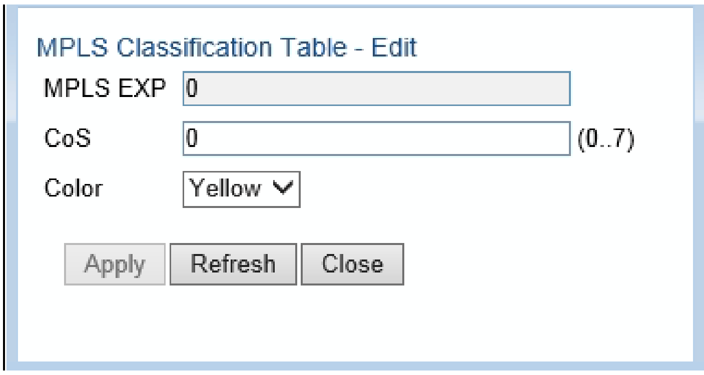
MPLS Classification

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

2 Select the row you want to modify and click **Edit**. The MPLS Classification - Edit page opens.

Figure 149: MPLS Classification - Edit Page


MPLS Classification Table - Edit

MPLS EXP: 0

CoS: 0 (0..7)

Color: Yellow

3 Modify the parameters you want to change:

- **MPLS EXP** – Read-only. The MPLS (experimental) bit to be mapped.
- **CoS** – The CoS assigned to frames with the designated MPLS EXP value.

- **Color** – The Color assigned to frames with the designated MPLS EXP value.

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

7.3. Configuring Policers (Rate Metering)

This section includes:

- *Policer (Rate Metering) Overview*
- *Configuring Policer Profiles*
- *Assigning Policers to Interfaces*
- *Configuring the Ingress and Egress Byte Compensation*

7.3.1. Policer (Rate Metering) Overview

The NS Primo/Diplo 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.

NS Primo/Diplo'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.

7.3.2. Configuring Policer Profiles

This section includes:

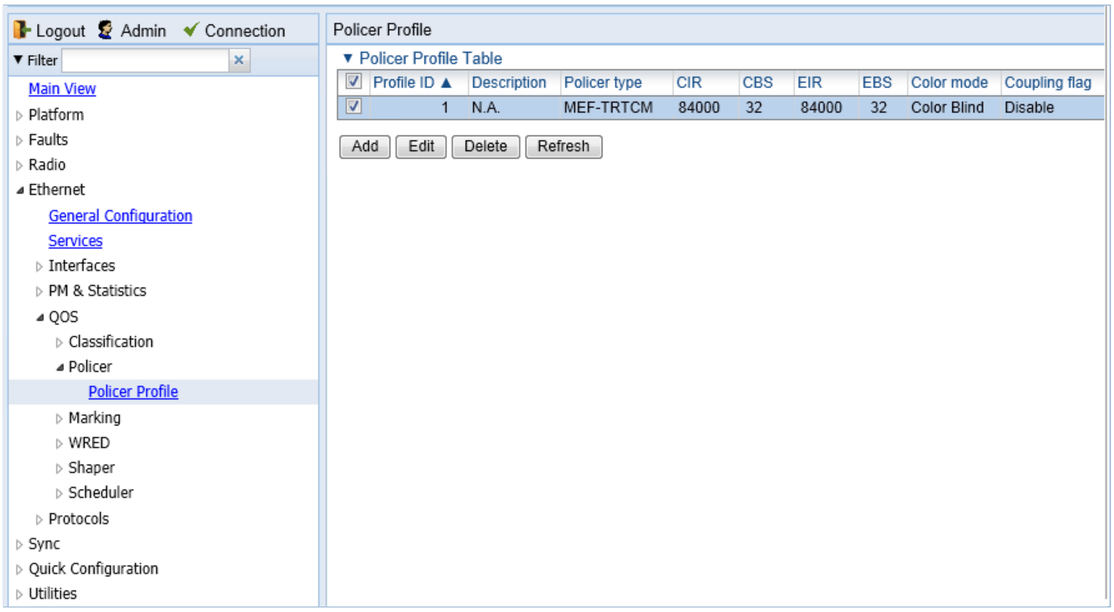
- *Adding a Policer Profile*
- *Editing a Policer Profile*
- *Deleting a Policer Profile*

7.3.2.1. Adding a Policer Profile

To add a policer profile:

1 Select **Ethernet > QoS > Policer > Policer Profile**. The Policer Profile page opens.

Figure 150: Policer Profile Page



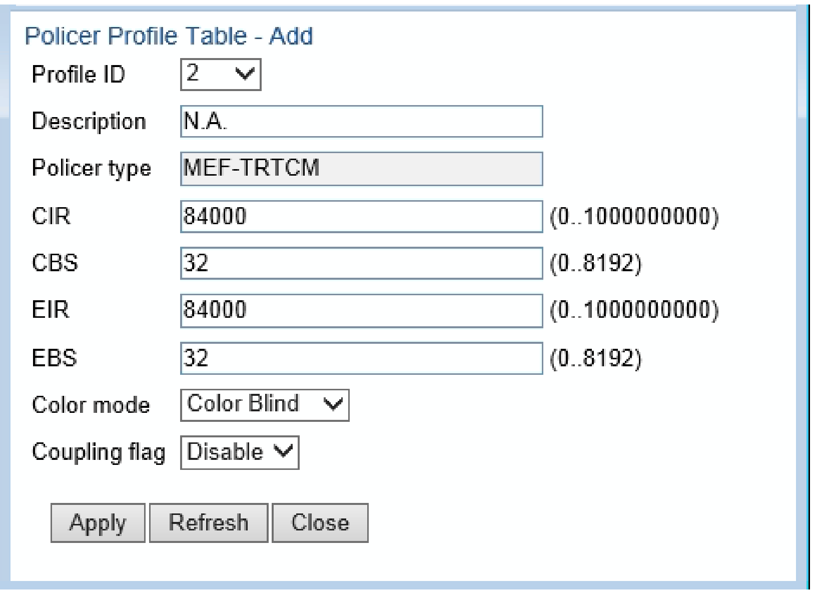
Policer Profile

Policer Profile Table

☑	Profile ID ▲	Description	Policer type	CIR	CBS	EIR	EBS	Color mode	Coupling flag
☑	1	N.A.	MEF-TRTCM	84000	32	84000	32	Color Blind	Disable

2 Click **Add**. The Policer Profile - Add page opens.

Figure 151: Policer Profile - Add Page



Policer Profile Table - Add

Profile ID	2	
Description	N.A.	
Policer type	MEF-TRTCM	
CIR	84000	(0..1000000000)
CBS	32	(0..8192)
EIR	84000	(0..1000000000)
EBS	32	(0..8192)
Color mode	Color Blind	
Coupling flag	Disable	

3 Configure the profile's parameters. See *Table 45* for a description of the policer profile parameters.

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

Table 45: Policer Profile Parameters

Parameter	Definition
Profile ID	A unique ID for the policer profile. You can choose any unused value from 1 to 250. Once you have added the profile, you cannot change the Profile ID.
Description	A description of the policer profile.
Policer type	Read-only. The type of policer. Always set to MEF-TRTCM.
CIR	Enter the Committed Information Rate (CIR) for the policer, in 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.

7.3.2.2. 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 151*). You can edit any parameter that can be configured in the Policer Profile Table Add page, except the **Profile ID**.

7.3.2.3. 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:

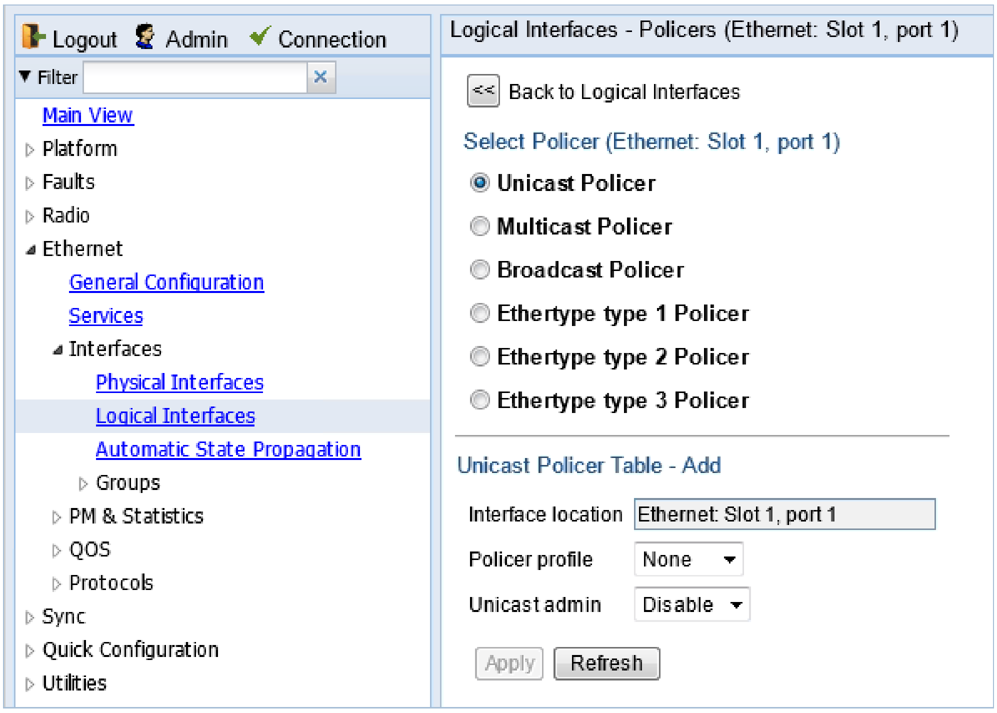
1. Select the profiles in the Policer Profile table or select all the profiles by selecting the check box in the top row.
2. Click **Delete**. The profiles are deleted.

7.3.3. Assigning Policers to Interfaces

To assign policers to a logical interface:

1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (*Figure 140*).
2. Select the interface in the Ethernet Logical Port Configuration table and click **Policers**. The Policers page opens.

Figure 152: Logical Interfaces – Policers Page – Unicast Policer (Default)



Logical Interfaces - Policers (Ethernet: Slot 1, port 1)

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

For a logical interface, you can assign policers to the following traffic flows:

- Unicast Policer
- Multicast Policer
- Broadcast Policer
- Ethertype Policers

7.3.3.1. Assigning Unicast Policers

To assign a policer for unicast traffic to a logical interface:

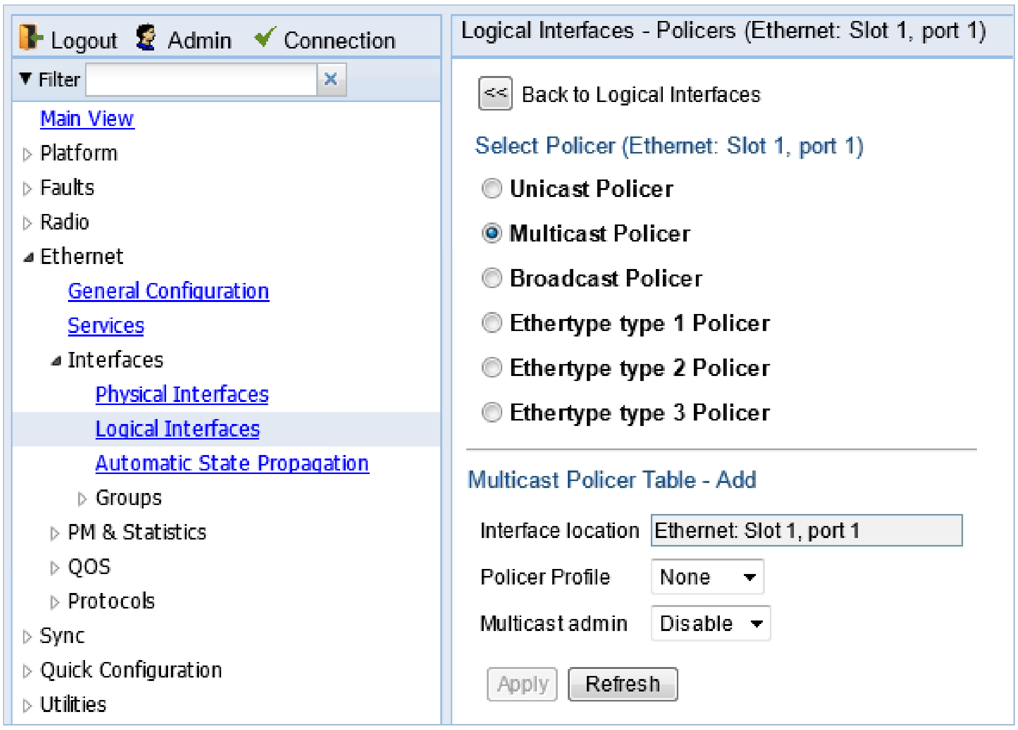
1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (*Figure 140*).
2. Select the interface in the Ethernet Logical Port Configuration Table and click **Policers**. The Policers page opens. By default, the Policers page opens to the Unicast Policer table (*Figure 152*).
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**.

7.3.3.2. 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 140*).
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 152*).
3. Select **Multicast Policer**. The Multicast Policer table appears.

Figure 153: Logical Interfaces – Policers Page – Multicast Policer



Logical Interfaces - Policers (Ethernet: Slot 1, port 1)

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

Multicast Policer Table - Add

Interface location	Ethernet: Slot 1, port 1
Policer Profile	None
Multicast admin	Disable

4 In the **Policer profile** field, select a profile from the policer profiles defined in the system. The **Policer profile** drop-down list includes the ID and description of all defined profiles.

5 In the **Multicast admin** field, select **Enable** to enable policing on multicast traffic flows from the logical interface, or **Disable** to disable policing on multicast traffic flows from the logical interface.

6 Click **Apply**.

7.3.3.3. Assigning Broadcast Policers

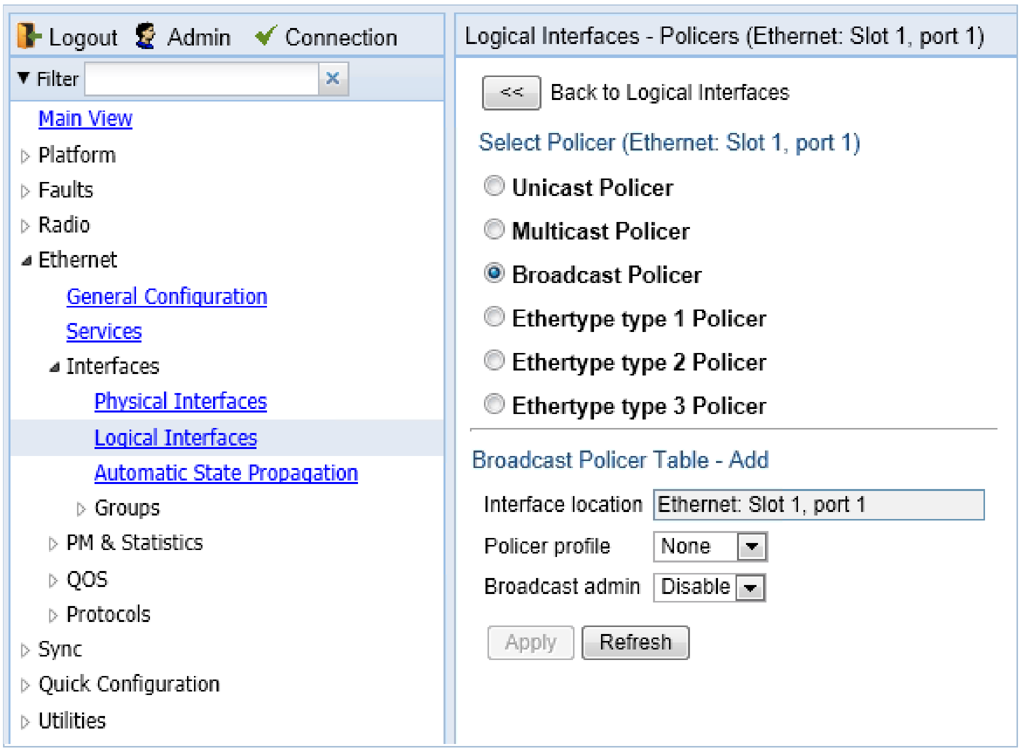
To assign a policer for broadcast traffic to a logical interface:

1 Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (*Figure 140*).

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 152*).

3 Select **Broadcast Policer**. The Broadcast Policer table appears.

Figure 154: Logical Interfaces – Policers Page – Broadcast Policer



Logical Interfaces - Policers (Ethernet: Slot 1, port 1)

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

Broadcast Policer Table - Add

Interface location	Ethernet: Slot 1, port 1
Policer profile	None
Broadcast admin	Disable

4 In the **Policer profile** field, select a profile from the policer profiles defined in the system. The **Policer profile** drop-down list includes the ID and description of all defined profiles.

5 In the **Broadcast admin** field, select **Enable** to enable policing on broadcast traffic flows from the logical interface, or **Disable** to disable policing on broadcast traffic flows from the logical interface.

6 Click **Apply**.

7.3.3.4. Assigning Ethertype Policers

You can define up to three policers per Ethertype value.

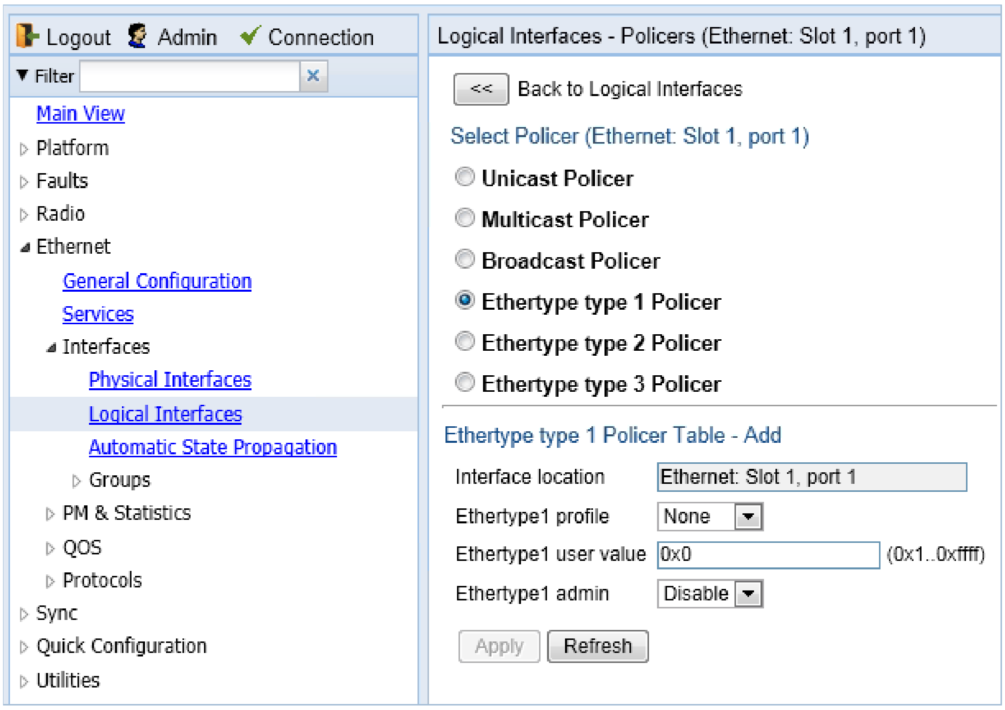
To assign a policer to an Ethertype:

1 Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (*Figure 140*).

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 152*).

3 Select **Ethertype type 1 Policer**. The Ethertype type 1 Policer table appears.

Figure 155: Logical Interfaces – Policers Page – Ethertype Policer



Logical Interfaces - Policers (Ethernet: Slot 1, port 1)

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

4 In the **Ethertype 1 profile** field, select a profile from the policer profiles defined in the system. The **Ethertype 1 profile** drop-down list includes the ID and description of all defined profiles.

5 In the **Ethertype 1 user value** field, enter the Ethertype value to which you want to apply this policer. The field length is 4 nibbles (for example, 0x0806 - ARP).

6 In the **Ethertype 1 admin** field, select **Enable** to enable policing on the logical interface for the specified ethertype, or **Disable** to disable policing on the logical interface for the specified ethertype.

7 Click **Apply**.

8 To assign policers to additional Ethertypes, select **Ethertype type 2 Policer** and **Ethertype type 3 Policer** and repeat the steps above.

7.3.4. Configuring the Ingress and Egress Byte Compensation

You can define the ingress and egress byte compensation value per logical interface. The policer attached to the interface uses these values to compensate for Layer 1 non-effective traffic bytes.

To define the ingress byte compensation value for a logical interface:

1 Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (*Figure 140*).

2 Select the interface you want to configure and click **Edit**. The Logical Interfaces - Edit page opens (*Figure 141*).

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**.

7.4. Configuring Marking

This section includes:

- *Marking Overview*
- *Enabling Marking*
- *Modifying the 802.1Q Marking Table*
- *Modifying the 802.1AD Marking Table*

7.4.1. Marking Overview

When enabled, NS Primo/Diplo'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.

7.4.2. Enabling Marking

Marking is enabled and disabled on the service point level. See *Ethernet Service Points – Egress Attributes*.

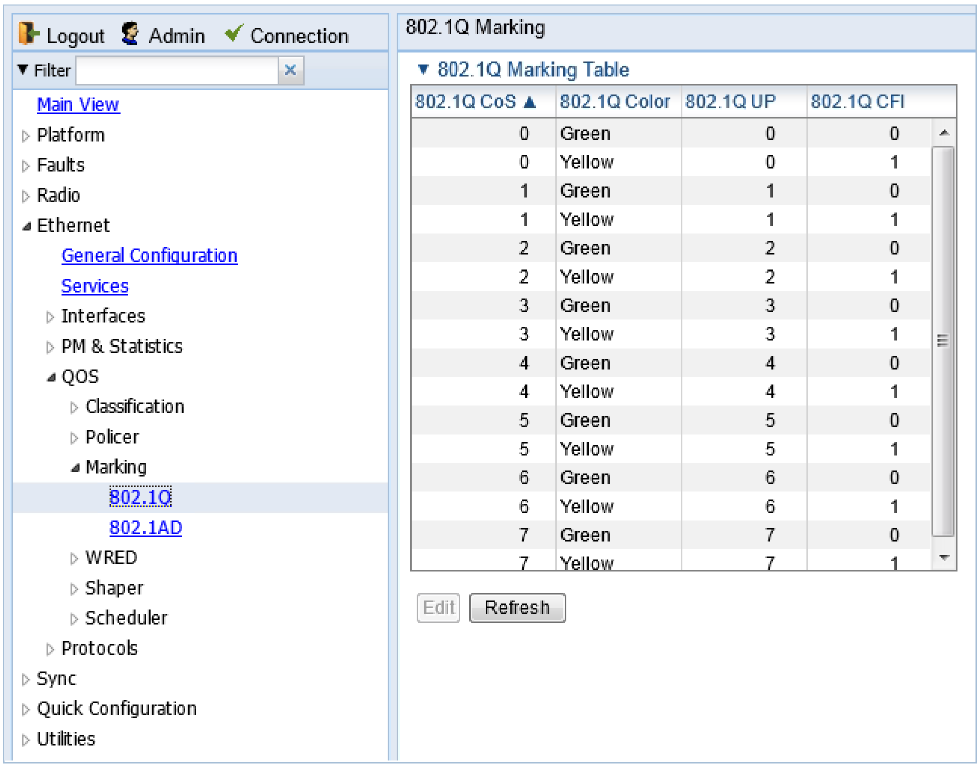
7.4.3. Modifying the 802.1Q Marking Table

The 802.1Q Marking table enables you to modify the CoS to UP and CFI bit mapping that is implemented when marking is enabled.

To modify the 802.1Q Marking table:

1 Select **Ethernet > QoS > Marking > 802.1Q**. The 802.1Q Marking page opens. Each row in the 802.1Q Marking page represents a CoS and color combination.

Figure 156: 802.1Q Marking Page



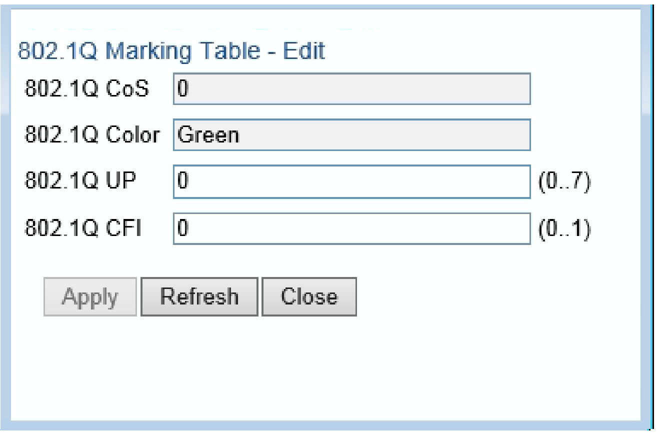
802.1Q Marking

▼ 802.1Q Marking Table

802.1Q CoS ▲	802.1Q Color	802.1Q UP	802.1Q CFI
0	Green	0	0
0	Yellow	0	1
1	Green	1	0
1	Yellow	1	1
2	Green	2	0
2	Yellow	2	1
3	Green	3	0
3	Yellow	3	1
4	Green	4	0
4	Yellow	4	1
5	Green	5	0
5	Yellow	5	1
6	Green	6	0
6	Yellow	6	1
7	Green	7	0
7	Yellow	7	1

2 Select the row you want to modify and click **Edit**. The 802.1Q Marking - Edit page opens.

Figure 157: 802.1Q Marking - Edit Page



802.1Q Marking Table - Edit

802.1Q CoS	0	
802.1Q Color	Green	
802.1Q UP	0	(0..7)
802.1Q CFI	0	(0..1)

3 Enter the new 802.1Q UP and 802.1Q CFI values.

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

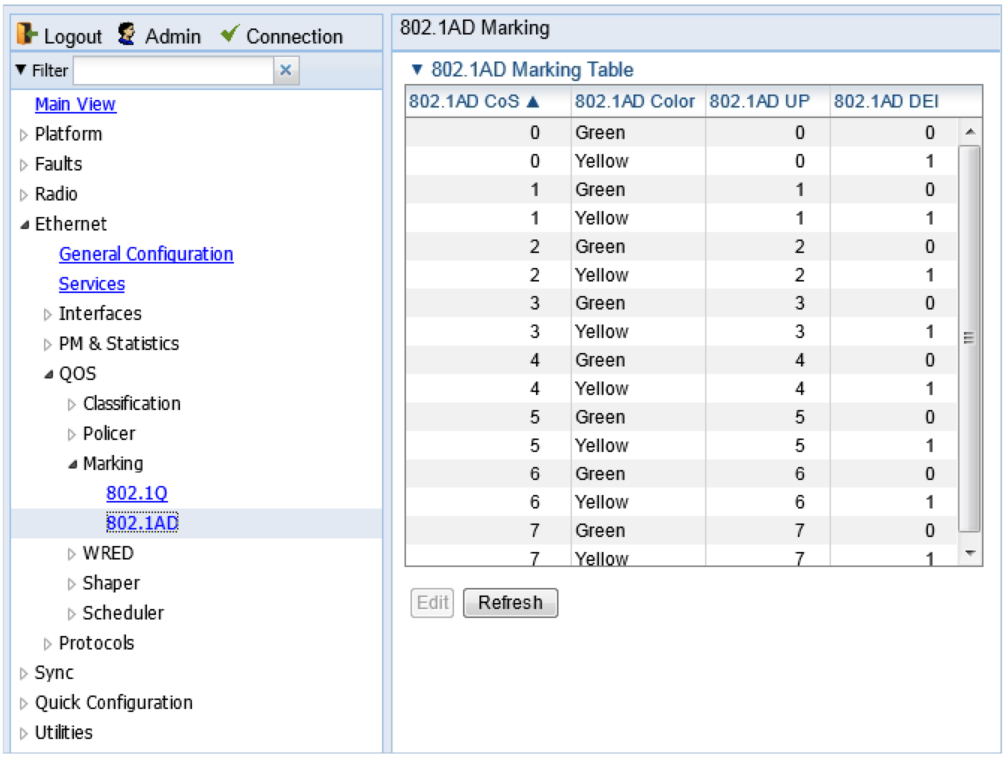
7.4.4. Modifying the 802.1AD Marking Table

The 802.1AD Marking table enables you to modify the CoS to UP and DEI bit mapping that is implemented when marking is enabled.

To modify the 802.1AD Marking table:

1 Select **Ethernet > QoS > Marking > 802.1AD**. The 802.1AD Marking page opens. Each row in the 802.1AD Marking page represents a CoS and color combination.

Figure 158: 802.1AD Marking Page



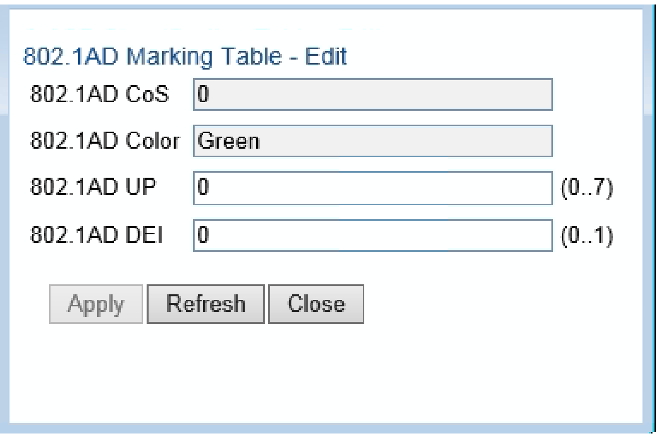
802.1AD Marking

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

2 Select the row you want to modify and click **Edit**. The 802.1AD Marking - Edit page opens.

Figure 159: 802.1AD Marking - Edit Page



802.1AD Marking Table - Edit

802.1AD CoS	0	
802.1AD Color	Green	
802.1AD UP	0	(0..7)
802.1AD DEI	0	(0..1)

3 Enter the new 802.1AD UP and 802.1AD DEI values.

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

7.5. Configuring WRED

This section includes:

- *WRED Overview*
- *Configuring WRED Profiles*

- *Assigning WRED Profiles to Queues*

7.5.1. WRED Overview

Weighted Random Early Detection (WRED) enables differentiation between higher and lower priority traffic based on CoS. You can define up to 30 WRED profiles. Each profile contains a green traffic curve and a yellow traffic curve. This curve describes the probability of randomly dropping frames as a function of queue occupancy.

The system also includes two pre-defined read-only profiles. These profiles are assigned profile IDs 31 and 32.

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.

7.5.2. Configuring WRED Profiles

This section includes:

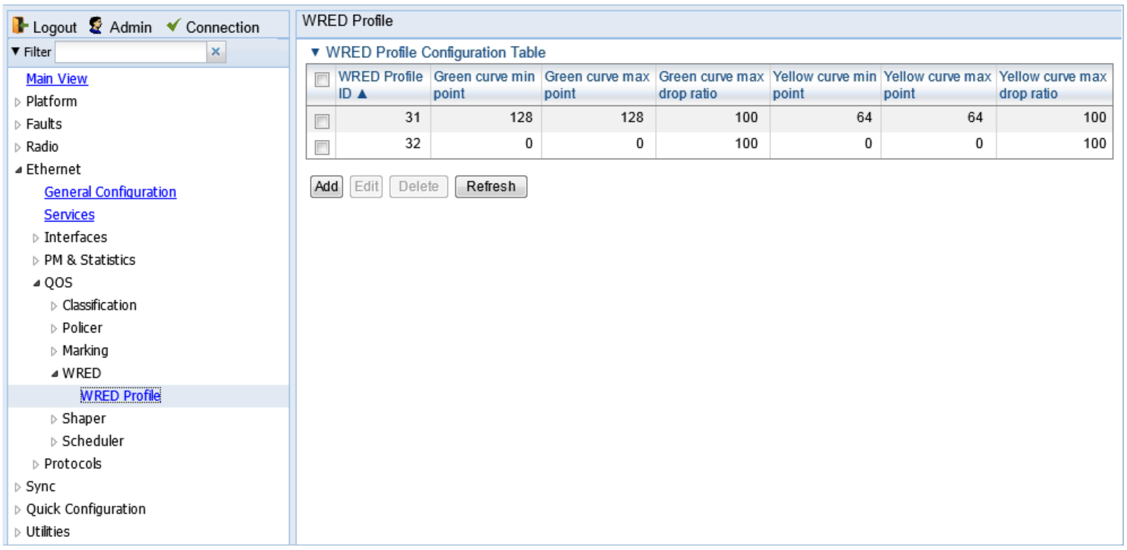
- *Adding a WRED Profile*
- *Editing a WRED Profile*
- *Deleting a WRED Profile*

7.5.2.1. Adding a WRED Profile

To add a WRED profile:

1 Select **Ethernet > QoS > WRED > WRED Profile**. The WRED Profile page opens.

Figure 160: WRED Profile Page



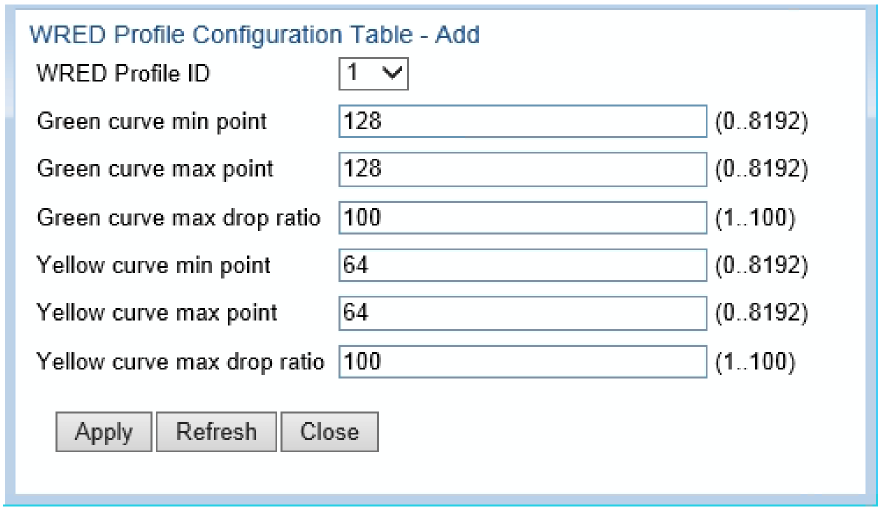
WRED Profile

▼ 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

2 Click **ADD**. The WRED Profile - Add page opens, with default values displayed.

Figure 161: 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)

3 In the **WRED Profile ID** field, select a unique ID to identify the profile. Permitted values are 1-30.

4 In the **Green curve min point** field, enter the minimum throughput of green packets for queues with this profile, in Kbytes (0-8192). When this value is reached, the system begins dropping green packets in the queue.

5 In the **Green curve max point** field, enter the maximum throughput of green packets for queues with this profile, in Kbytes (0-8192). When this value is reached, all green packets in the queue are dropped.
6 In the **Green curve max drop ratio** field, enter the maximum percentage (1-100) of dropped green packets for queues with this profile.
7 In the **Yellow curve min point** field, enter the minimum throughput of yellow packets for queues with this profile, in Kbytes (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**.

7.5.2.2. Editing a WRED Profile

To edit a WRED profile:

1 Select **Ethernet > QoS > WRED > WRED Profile**. The WRED Profile page opens (*Figure 160*).
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 161*). You can edit any parameter except the **WRED Profile ID**.
3 Modify the profile.
4 Click **Apply**, then **Close**.

7.5.2.3. 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 160*) 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.

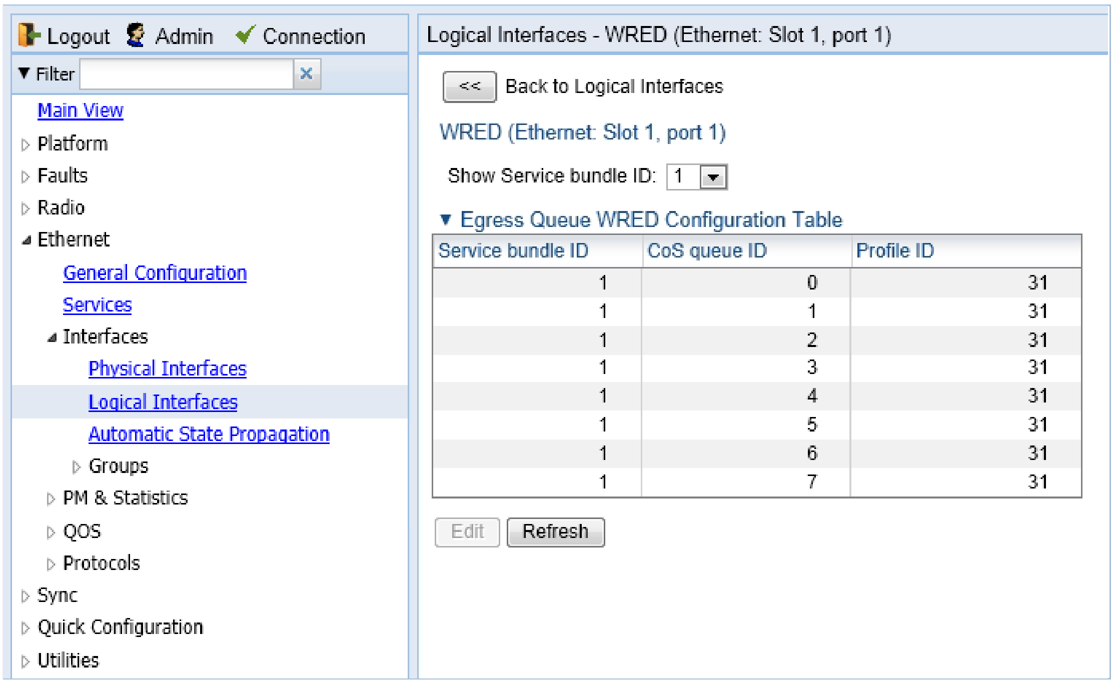
7.5.3. Assigning WRED Profiles to Queues

To assign a WRED profile to a queue:

1 Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (*Figure 140*).

2 Select an interface in the Ethernet Logical Port Configuration table and click **WRED**. The WRED page opens.

Figure 162: Logical Interfaces – WRED Page



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

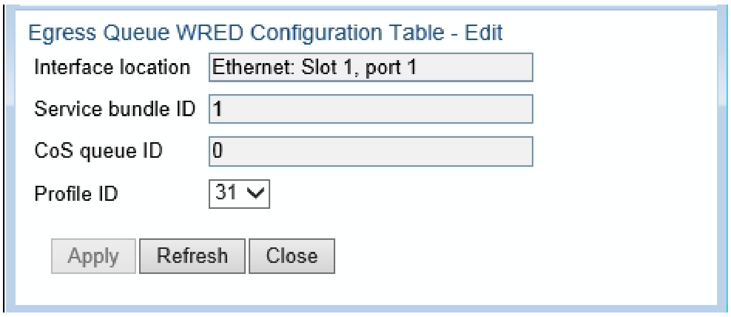
3 In the **Show Service bundle ID** field, select 1.

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 163: 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

5 In the **Profile ID** field, select the WRED profile you want to assign to the selected queue.

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

7.6. Configuring Egress Shaping

This section includes:

- *Egress Shaping Overview*
- *Configuring Queue Shaper Profiles*
- *Configuring Service Bundle Shaper Profiles*
- *Assigning a Queue Shaper Profile to a Queue*
- *Assigning a Service Bundle Shaper Profile to a Service Bundle*

7.6.1. Egress Shaping Overview

Egress shaping determines the traffic profile for each queue. NS Primo/Diplo 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.

7.6.2. Configuring Queue Shaper Profiles

This section includes:

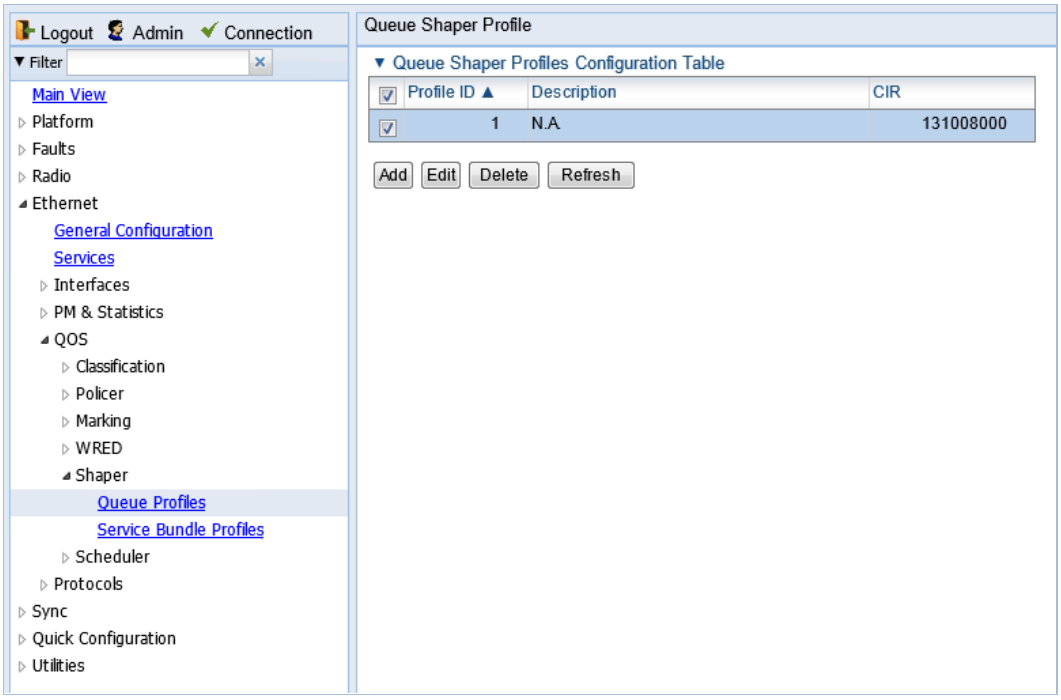
- *Adding a Queue Shaper Profile*
- *Editing a Queue Shaper Profile*
- *Deleting a Queue Shaper Profile*

7.6.2.1. 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 164: Queue Shaper Profile Page



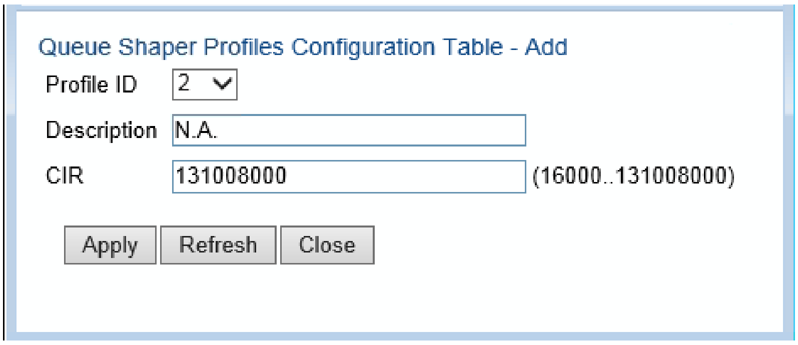
Queue Shaper Profile

Queue Shaper Profiles Configuration Table

☑	Profile ID ▲	Description	CIR
☑	1	N.A	131008000

2 Click **Add**. The Queue Shaper – Add page opens, with default values displayed.

Figure 165: Queue Shaper Profile – Add Page



Queue Shaper Profiles Configuration Table - Add

Profile ID: 2

Description: N.A.

CIR: 131008000 (16000..131008000)

3 In the **Profile ID** field, select a unique ID to identify the profile. Permitted values are 1-31.

4 Optionally, in the **Description** field, enter a description of the profile.

5 In the **CIR** field, enter the Committed Information Rate (CIR) assigned to the profile, in bits per second. Permitted values are:

- 16,000 - 32,000,000 bps, with granularity of 16,000.
- 32,000,000 - 131,008,000 bps, with granularity of 64,000.

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

7.6.2.2. 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 164*).
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 165*). You can edit any parameter except the **Profile ID**.
3 Modify the profile.
4 Click **Apply**, then **Close**.

7.6.2.3. 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 164*) 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.

7.6.3. Configuring Service Bundle Shaper Profiles

This section includes:

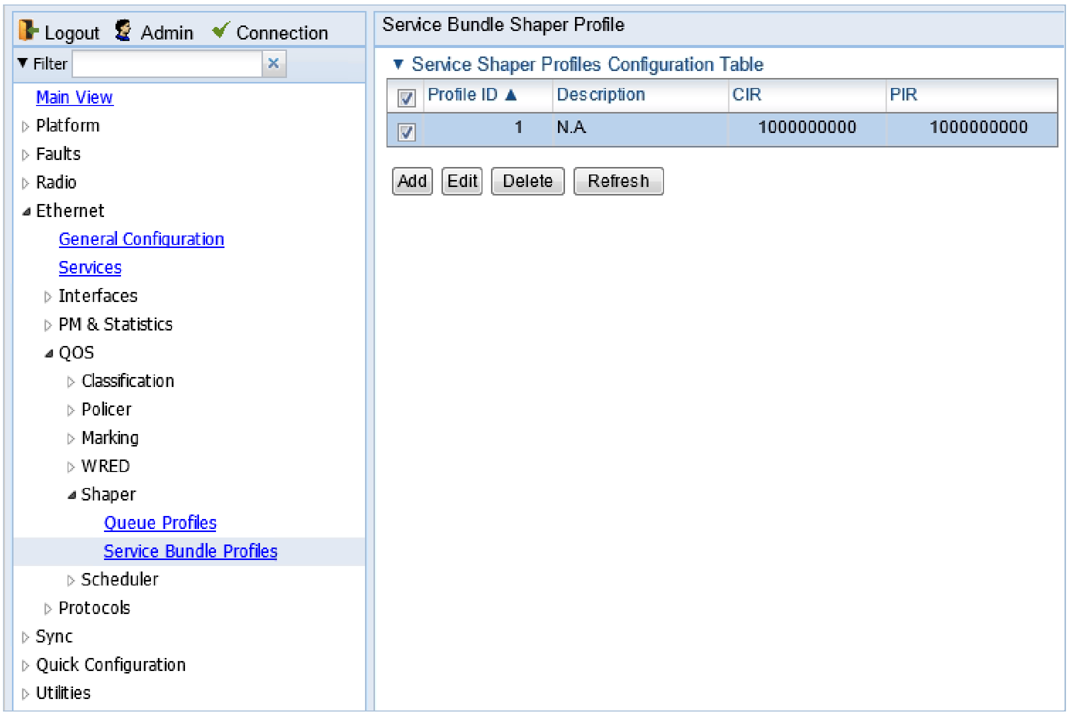
- *Adding a Service Bundle Shaper Profile*
- *Editing a Service Bundle Shaper Profile*
- *Deleting a Service Bundle Shaper Profile*

7.6.3.1. 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 166: Service Bundle Shaper Profile Page



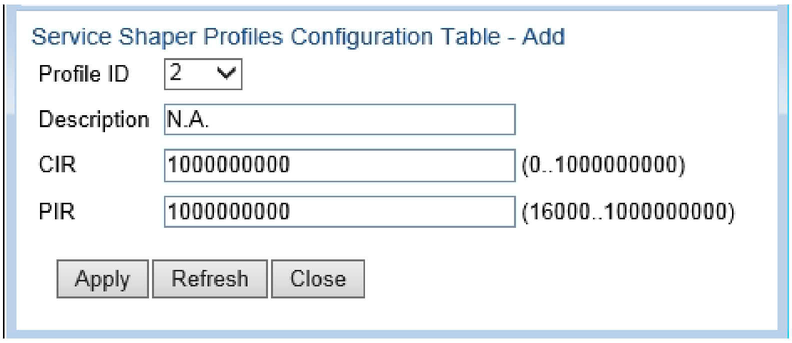
Service Bundle Shaper Profile

▼ Service Shaper Profiles Configuration Table

☑	Profile ID ▲	Description	CIR	PIR
☑	1	N.A	1000000000	1000000000

2 Click **Add**. The Service Bundle Shaper Profile – Add page opens, with default values displayed.

Figure 167: 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)

3 In the **Profile ID** field, select a unique ID to identify the profile. Permitted values are 1-31.

4 Optionally, in the **Description** field, enter a description of the profile.

5 In the **CIR** field, enter the Committed Information Rate (CIR) assigned to the profile, in bits per second. Permitted values are:

- 0 – 32,000,000 bps, with granularity of 16,000.
- 32,000,000 – 1,000,000,000 bps, with granularity of 64,000.

6 In the **PIR** field, enter the Peak Information Rate (PIR) assigned to the profile, in bits per second. Permitted values are:

- 16,000 – 32,000,000 bps, with granularity of 16,000.
- 32,000,000 – 1,000,000,000 bps, with granularity of 64,000.

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

7.6.3.2. 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 166*).
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 167*). You can edit any parameter except the **Profile ID**.
3 Modify the profile.
4 Click **Apply**, then **Close**.

7.6.3.3. 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 166*) and click **Delete**. The profile is deleted.

To delete multiple service bundle shaper profiles:

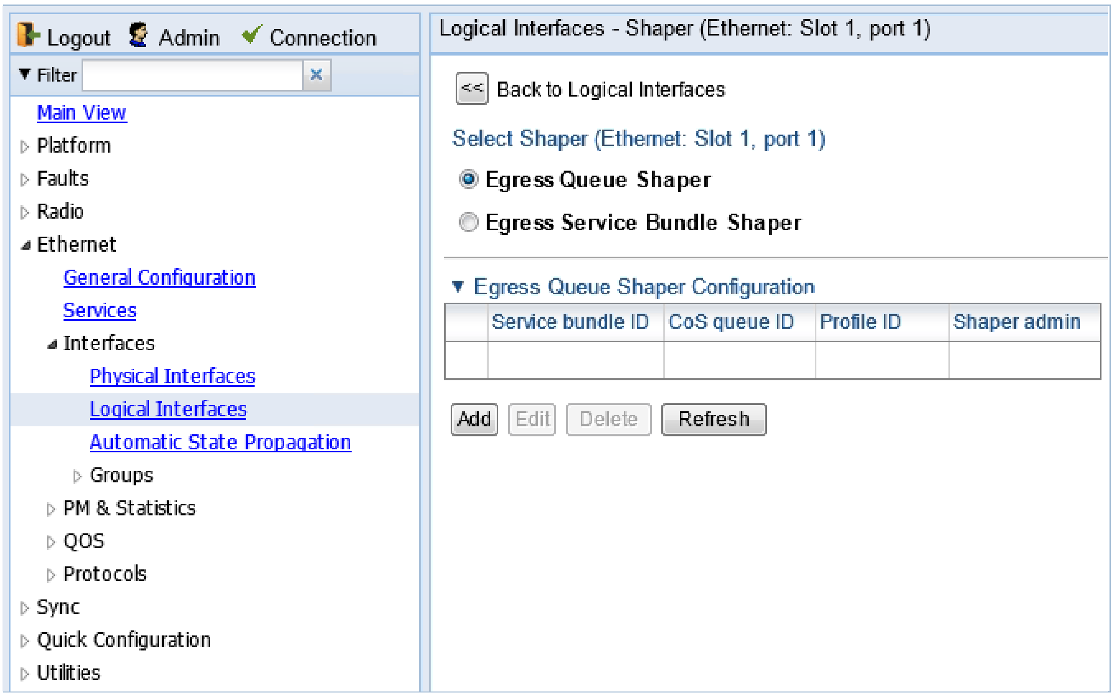
1 Select the profiles in the Service Bundle Shaper Profiles Configuration table or select all the profiles by selecting the check box in the top row.
2 Click **Delete**. The profiles are deleted.

7.6.4. 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 140*).
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 168: Logical Interfaces – Shaper – Egress Queue Shaper



Logical Interfaces - Shaper (Ethernet: Slot 1, port 1)

<< Back to Logical Interfaces

Select Shaper (Ethernet: Slot 1, port 1)

● Egress Queue Shaper

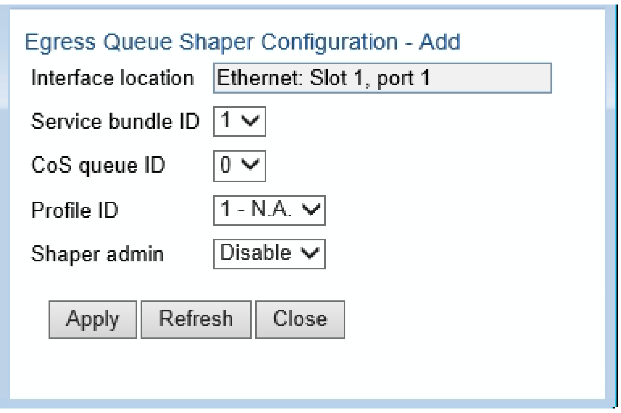
○ Egress Service Bundle Shaper

▼ Egress Queue Shaper Configuration

	Service bundle ID	CoS queue ID	Profile ID	Shaper admin

3 Click **Add**. The Egress Queue Shaper Configuration – Add page opens.

Figure 169: 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

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:

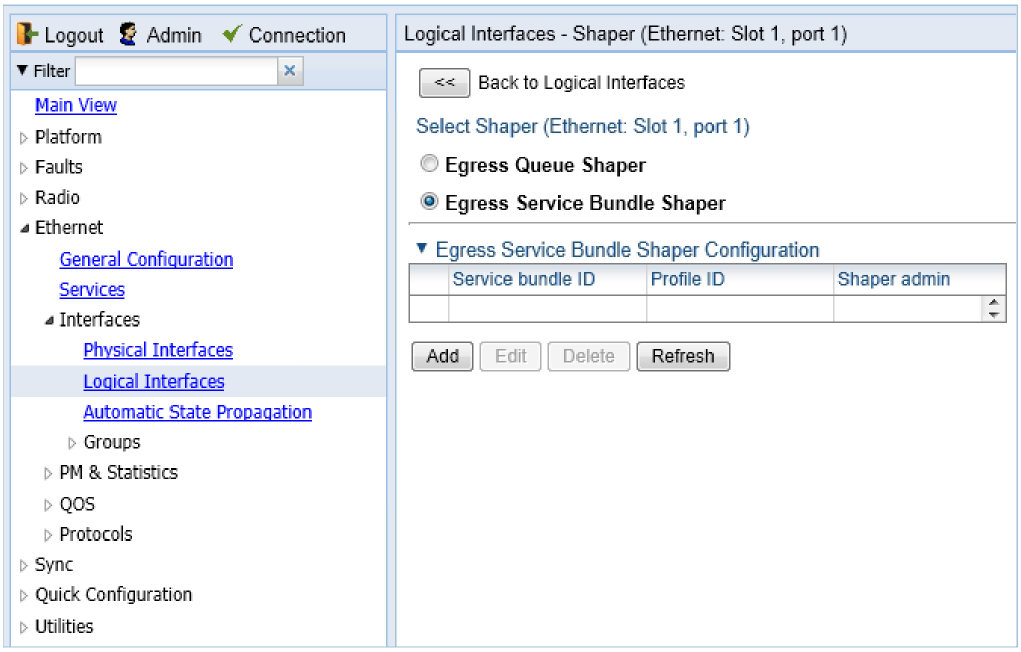
1. Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (*Figure 140*).
2. Select an interface in the Ethernet Logical Port Configuration table and click **Shaper**. The Logical Interfaces – Shaper page opens, with the Egress Queue Shaper Configuration table open by default (*Figure 168*).
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 168*).
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 169*).
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**.

7.6.5. 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 140*).
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 168*).
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 170: Logical Interfaces – Shaper – Egress Service Bundle Shaper



Logical Interfaces - Shaper (Ethernet: Slot 1, port 1)

Select Shaper (Ethernet: Slot 1, port 1)

○ Egress Queue Shaper

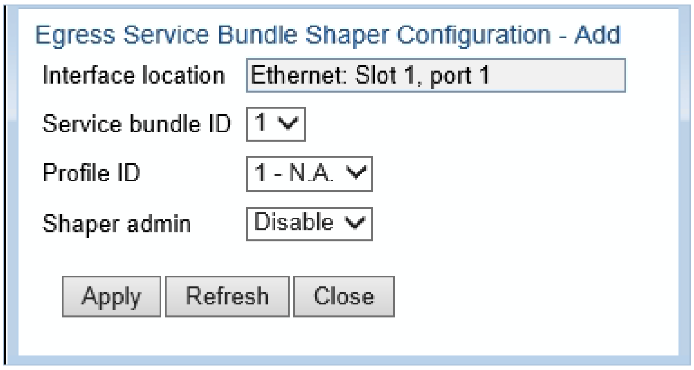
● Egress Service Bundle Shaper

Egress Service Bundle Shaper Configuration

	Service bundle ID	Profile ID	Shaper admin

4 Click **Add**. The Egress Service Bundle Shaper Configuration – Add page opens.

Figure 171: Logical Interfaces – Egress Service Bundle Shaper Configuration – Add Page



Egress Service Bundle Shaper Configuration - Add

Interface location	Ethernet: Slot 1, port 1
Service bundle ID	1
Profile ID	1 - N.A.
Shaper admin	Disable

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 140*).

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 168*).
3 Select **Egress Service Bundle Shaper**. The Egress Service Bundle Shaper Configuration table appears (*Figure 170*). 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 171*).
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**.

7.7. 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*

7.7.1. Scheduling Overview

Scheduling determines the priority among the queues. NS Primo/Diplo 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.

7.7.2. Configuring Priority Profiles

Scheduling priority profiles determine the queue priority. Each profile contains eight CoS-based priorities, corresponding to eight queues in an interface to which the profile is assigned. You can configure up to eight priority profiles. A ninth profile, Profile ID 9, is pre-configured. You can configure Green priorities from 4 (highest) to 1 (lowest). An additional four Yellow priority profiles are defined automatically.

This section includes:

- *Adding a Scheduler Priority Profile*

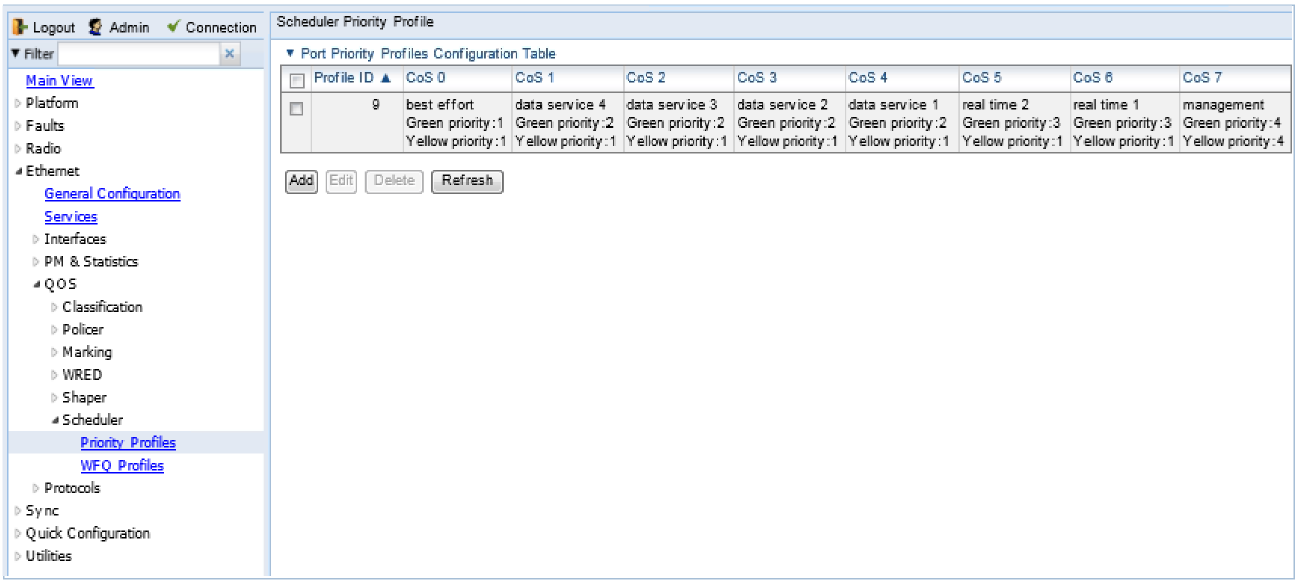
- *Editing a Service Scheduler Priority Profile*
- *Deleting a Scheduler Priority Profile*

7.7.2.1. 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 172: Scheduler Priority Profile Page



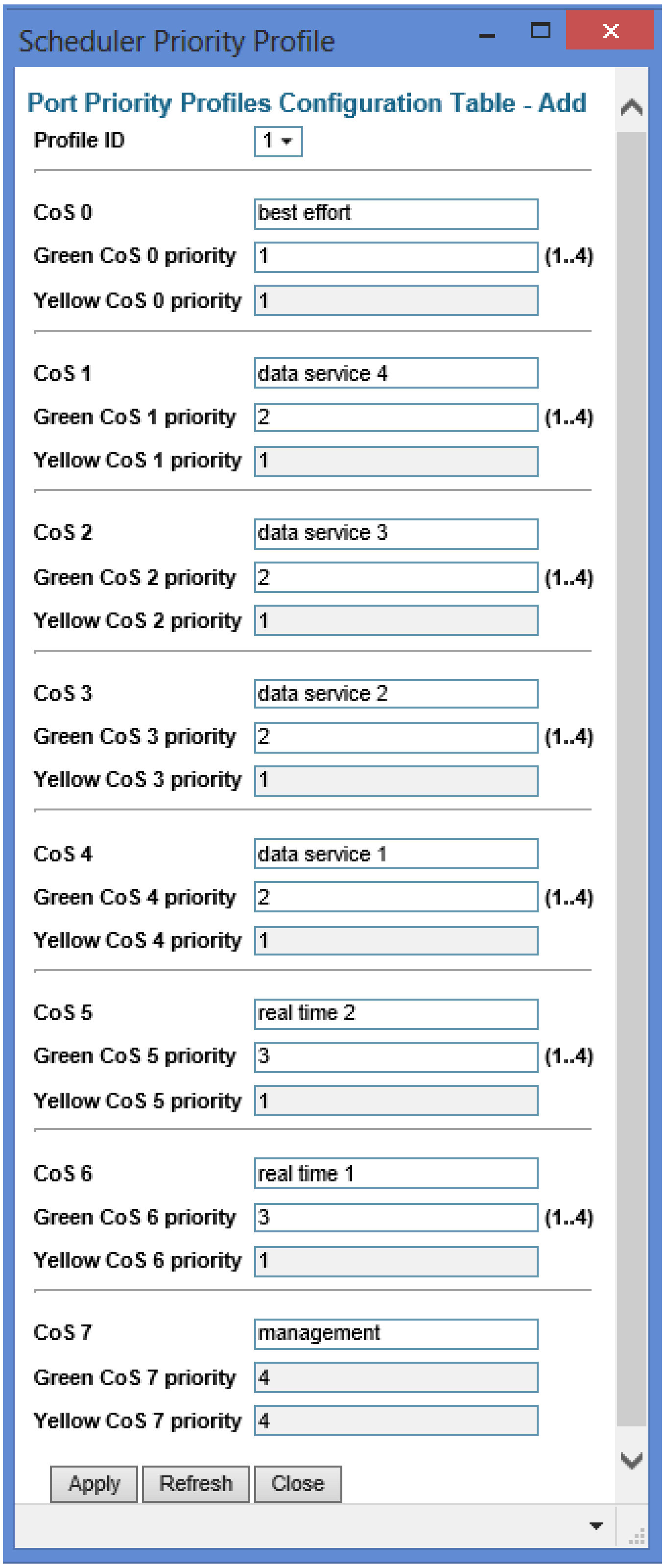
Scheduler Priority Profile

▼ Port Priority Profiles Configuration Table

□	Profile ID ▲	CoS 0	CoS 1	CoS 2	CoS 3	CoS 4	CoS 5	CoS 6	CoS 7
□	9	best effort Green priority:1 Yellow priority:1	data service 4 Green priority:2 Yellow priority:1	data service 3 Green priority:2 Yellow priority:1	data service 2 Green priority:2 Yellow priority:1	data service 1 Green priority:2 Yellow priority:1	real time 2 Green priority:3 Yellow priority:1	real time 1 Green priority:3 Yellow priority:1	management Green priority:4 Yellow priority:4

2 Click **Add**. The Scheduler Priority Profile – Add page opens, with default values displayed.

Figure 173: Scheduler Priority Profile – Add Page



Scheduler Priority Profile

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	

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.

7.7.2.2. 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 172*).
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 173*). You can edit any parameter except the **Profile ID**.
3. Modify the profile.
4. Click **Apply**, then **Close**.

7.7.2.3. Deleting a Scheduler Priority Profile

To delete a scheduler priority profile, select the profile in the Scheduler Priority Profiles page (*Figure 172*) 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.

7.7.3. Configuring WFQ Profiles

WFQ profiles determine the relative weight per queue. Each profile contains eight CoS-based weight values, corresponding to eight queues in an interface to which the profile is assigned. You can configure up to five WFQ profiles. A sixth profile, Profile ID 1, is pre-configured.

This section includes:

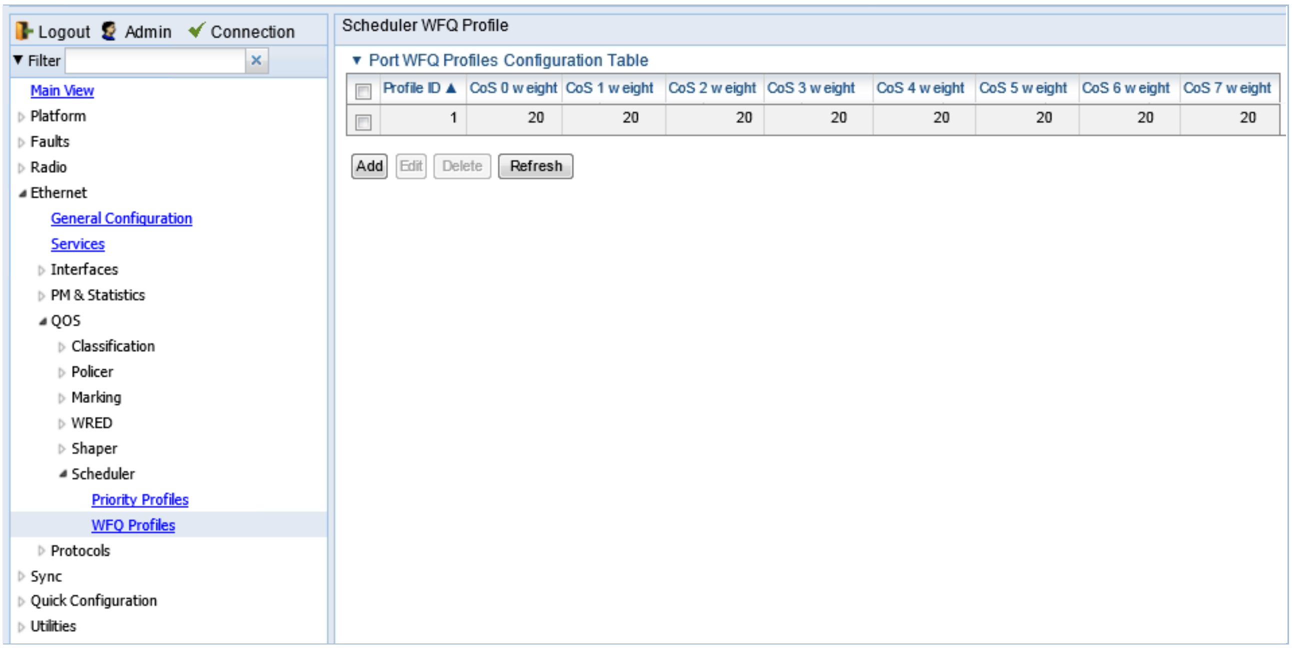
- *Adding a WFQ Profile*
- *Editing a WFQ Priority Profile*
- *Deleting a WFQ Profile*

7.7.3.1. Adding a WFQ Profile

To add a WFQ profile:

1 Select **Ethernet > QoS > Scheduler > WFQ Profiles**. The Scheduler WFQ Profile page opens.

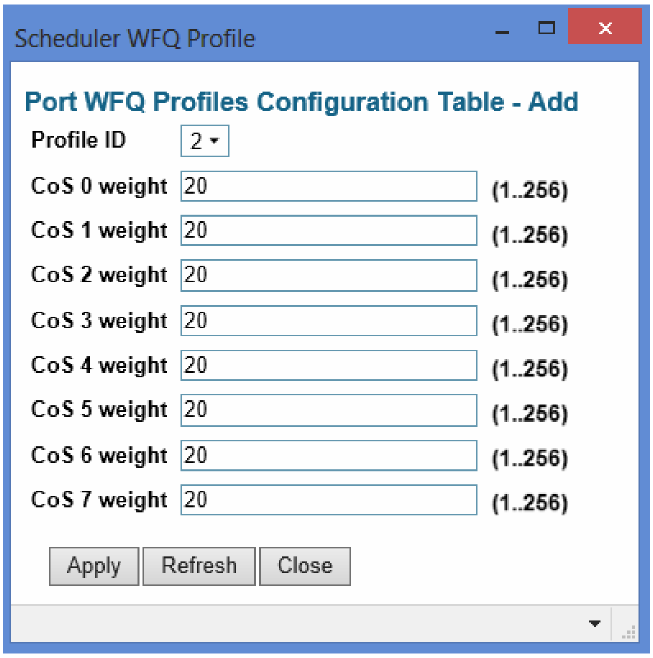
Figure 174: Scheduler WFQ Profile Page



□	Profile ID ▲	CoS 0 w eight	CoS 1 w eight	CoS 2 w eight	CoS 3 w eight	CoS 4 w eight	CoS 5 w eight	CoS 6 w eight	CoS 7 w eight
□	1	20	20	20	20	20	20	20	20

2 Click **Add**. The Scheduler WFQ Profile – Add page opens, with default values displayed.

Figure 175: Scheduler WFQ Profile – Add Page



Scheduler WFQ Profile

Port WFQ Profiles Configuration Table - Add

Profile ID	2	
CoS 0 weight	20	(1..256)
CoS 1 weight	20	(1..256)
CoS 2 weight	20	(1..256)
CoS 3 weight	20	(1..256)
CoS 4 weight	20	(1..256)
CoS 5 weight	20	(1..256)
CoS 6 weight	20	(1..256)
CoS 7 weight	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**.

7.7.3.2. 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 174*).

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 175*). You can edit any parameter except the **Profile ID**.

3 Modify the profile.

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

7.7.3.3. Deleting a WFQ Profile

To delete a scheduler WFQ profile, select the profile in the Scheduler WFQ Profiles page (*Figure 174*) 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.

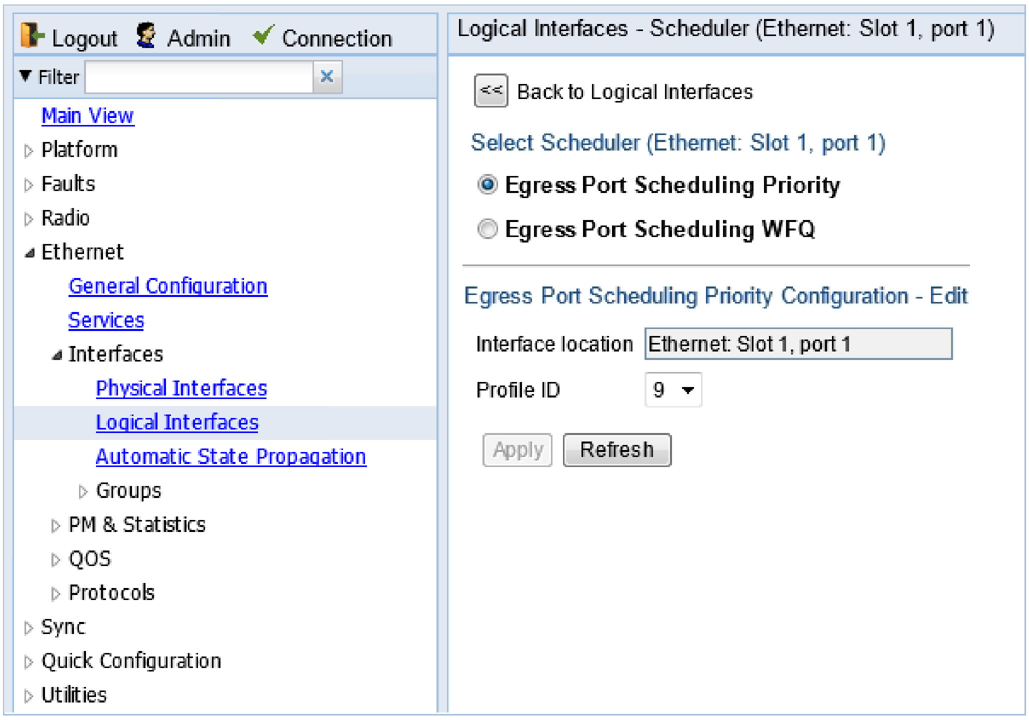
2 Click **Delete**. The profiles are deleted.

7.7.4. 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 140*).
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 176: Logical Interfaces – Scheduler – Egress Port Scheduling Priority



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

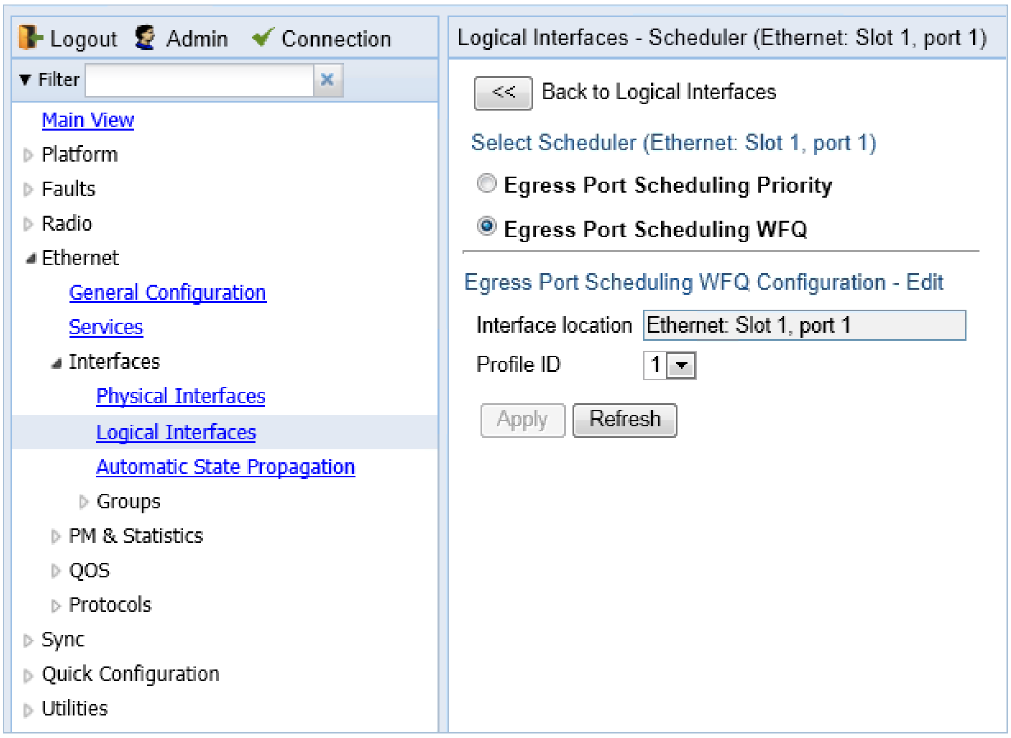
3 In the **Profile ID** field, select from a list of configured scheduling priority profiles. See *Configuring Priority Profiles*.
4 Click **Apply**, then **Close**.

7.7.5. 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 140*).
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 176*).
3 Select **Egress Port Scheduling WFQ**. The Egress Port Scheduling WFQ Configuration – Edit page opens.

Figure 177: Logical Interfaces – Scheduler – Egress Port Scheduling WFQ



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 WFQ Configuration - Edit

Interface location: Ethernet: Slot 1, port 1

Profile ID: 1

4 In the **Profile ID** field, select from a list of configured scheduling priority profiles. See *Configuring WFQ Profiles*.

5 Click **Apply**, then **Close**.

8. Ethernet Protocols

This section includes:

- *Configuring Adaptive Bandwidth Notification (ABN)*
- *Configuring LLDP*

Related Topics:

- *Configuring Service OAM (SOAM) Fault Management (FM)*

8.1. 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*

8.1.1. 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.

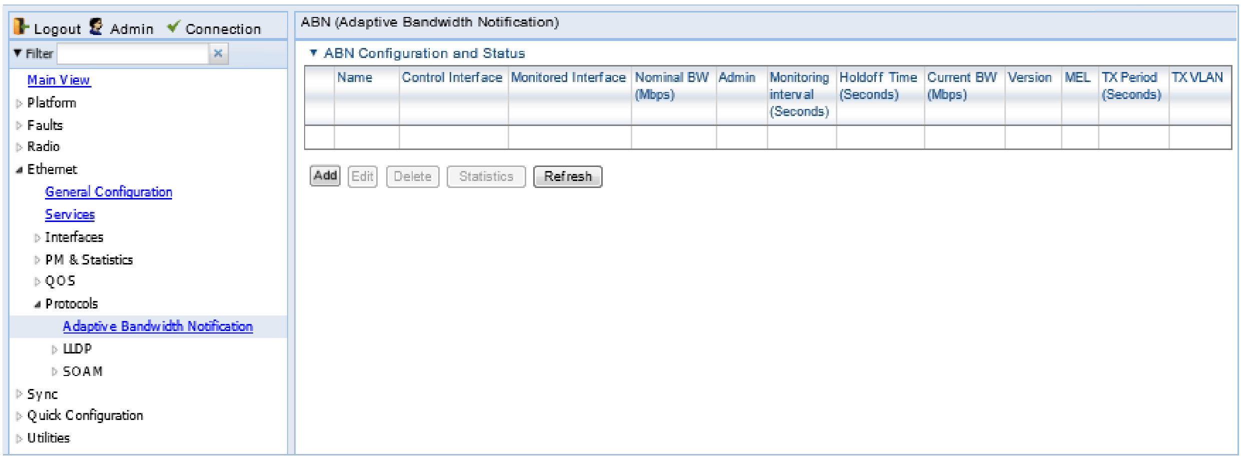
The ABN entity creates a logical relationship between a radio interface or a logical group of radio interfaces, called the Monitored Interface, and an Ethernet interface or a logical group of Ethernet interface, called the Control Interface. When bandwidth degrades from the nominal value in the Monitored 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.

8.1.2. Adding an ABN entity

To add an ABN entity:

1 Select **Ethernet > Protocols > Adaptive Bandwidth Notification**. The ABN (Adaptive Bandwidth Notification) page opens.

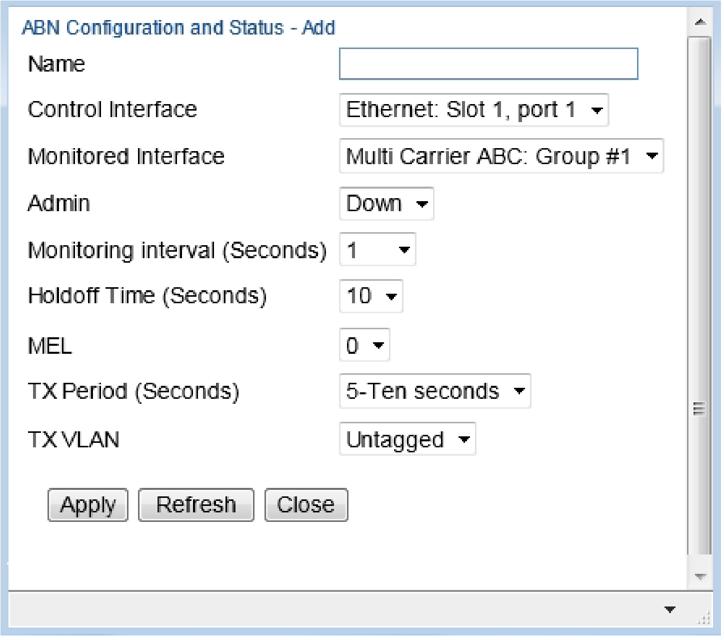
Figure 178: ABN (Adaptive Bandwidth Notification) Page



	Name	Control Interface	Monitored Interface	Nominal BW (Mbps)	Admin	Monitoring interval (Seconds)	Holdoff Time (Seconds)	Current BW (Mbps)	Version	MEL	TX Period (Seconds)	TX VLAN

2 Click **Add** underneath the ABN Configuration and Status table. The ABN Configuration and Status – Add page opens.

Figure 179: ABN Configuration and Status – Add Page



ABN Configuration and Status - Add

Name	
Control Interface	Ethernet: Slot 1, port 1
Monitored Interface	Multi Carrier ABC: Group #1
Admin	Down
Monitoring interval (Seconds)	1
Holdoff Time (Seconds)	10
MEL	0
TX Period (Seconds)	5-Ten seconds
TX VLAN	Untagged

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 46 describes the status (read-only) fields in the ABN Configuration and Status table.

Table 46: 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.

8.1.3. Editing an ABN Entity

To edit an ABN entity:

1 Select **Ethernet > Protocols > Adaptive Bandwidth Notification**. The ABN (Adaptive Bandwidth Notification) page opens (*Figure 178*).
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 179*). 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**.

8.1.4. Deleting an ABN Entity

To delete an ABN entity:

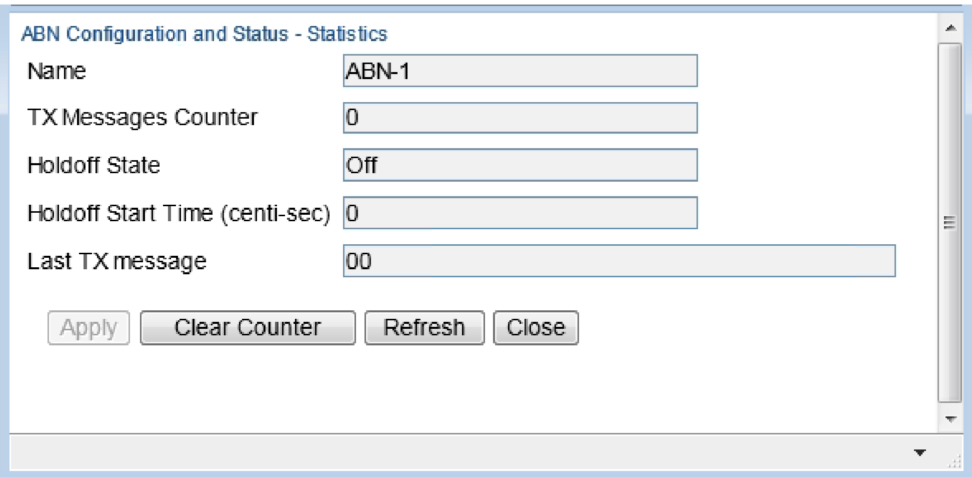
1 Select **Ethernet > Protocols > Adaptive Bandwidth Notification**. The ABN (Adaptive Bandwidth Notification) page opens (*Figure 178*).
2 Select the ABN entity in the ABN Configuration and Status Table.
3 Click **Delete**. The ABN entity is removed from the ABN Configuration and Status Table.

8.1.5. 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 178*).
2 Select the ABN entity in the ABN Configuration and Status Table.
3 Click **Statistics**. The ABN Configuration and Status - Statistics page opens.

Figure 180: 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

Table 47 describes the ABN entity statistics.

Table 47: 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.

8.2. 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*

8.2.1. LLDP Overview

Link Layer Discovery Protocol (LLDP) is a vendor-neutral layer 2 protocol that can be used by a network element attached to a specific LAN segment to advertise its identity and capabilities and to receive identity and capacity information from physically adjacent layer 2 peers. LLDP is a part of the IEEE 802.1AB – 2005 standard that enables automatic network connectivity discovery by means of a port identity information exchange between each port and its peer. Each port periodically sends and also expects to receive frames called Link Layer Discovery Protocol Data Units (LLDPDU). LLDPDUs contain information in TLV format about port identity, such as MAC address and IP address.

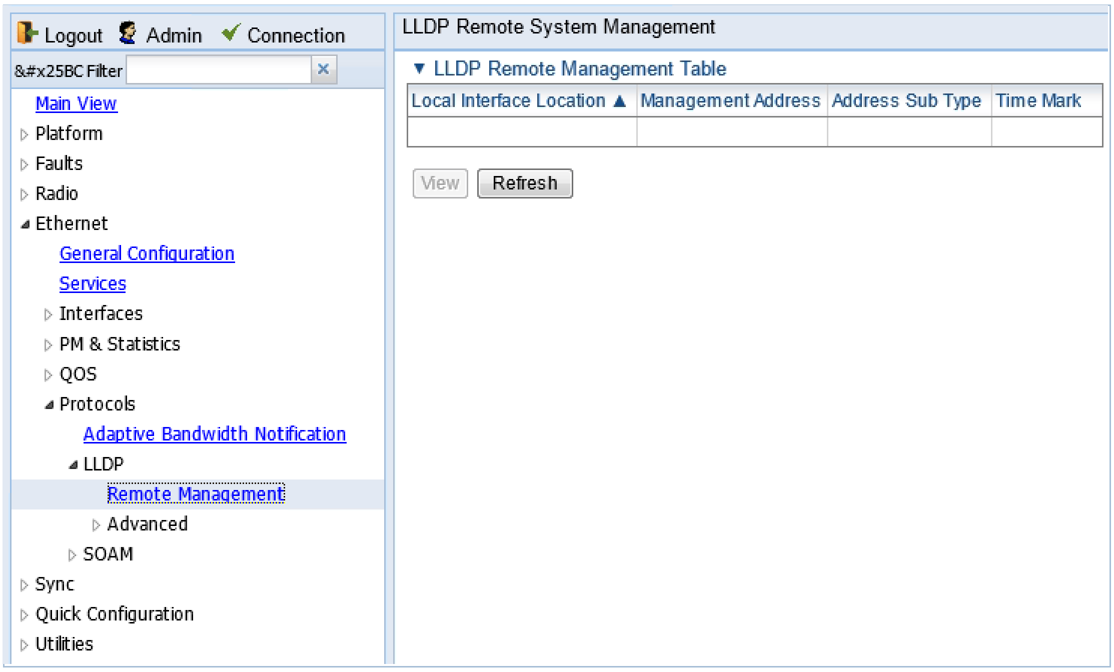
LLDP is used to send notifications to the NMS, based on data of the local unit and data gathered from peer systems. These notifications enable the NMS to build an accurate network topology.

8.2.2. 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 181: LLDP Remote System Management Page



LLDP Remote System Management

▼ LLDP Remote Management Table

Local Interface Location ▲	Management Address	Address Sub Type	Time Mark

Table 48 describes the LLDP remote system management parameters. These parameters are read-only.

Table 48: 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.

8.2.3. 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*.

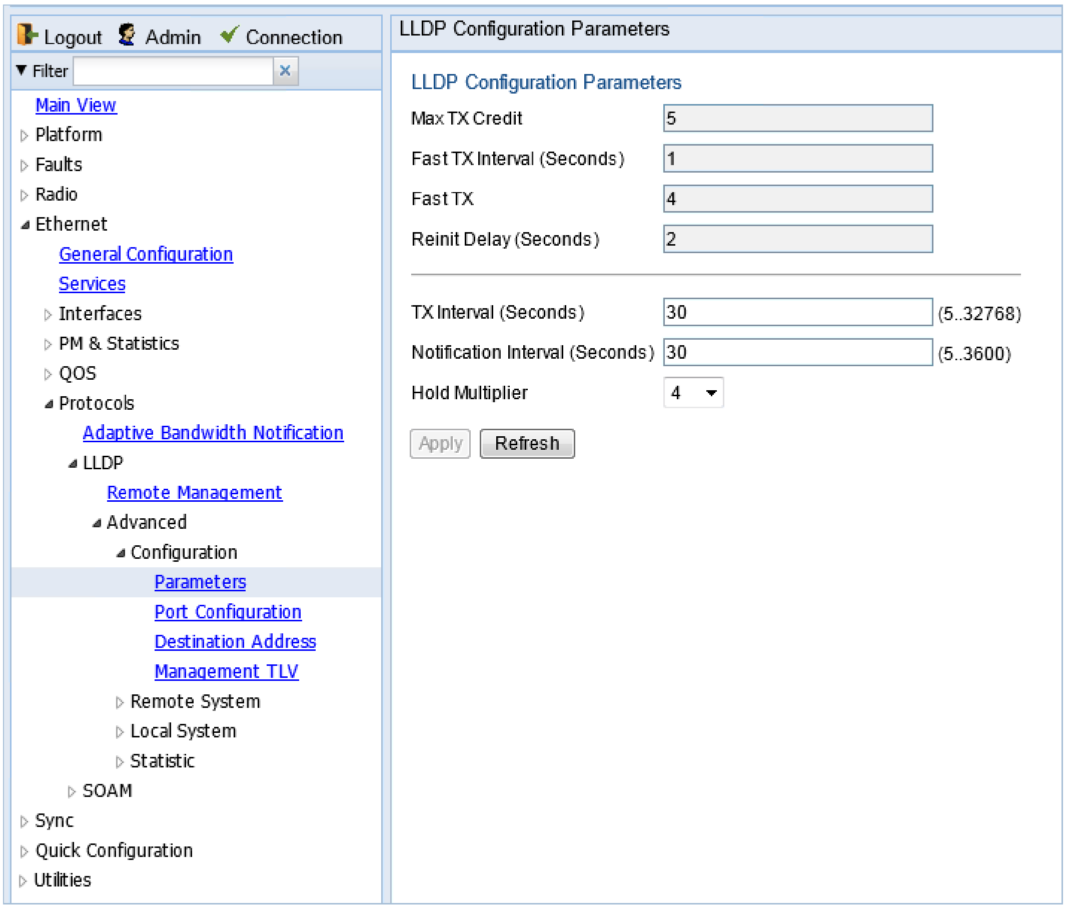
Note

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 182: LLDP Configuration Parameters Page



LLDP Configuration Parameters

LLDP Configuration Parameters

Max TX Credit: 5

Fast TX Interval (Seconds): 1

Fast TX: 4

Reinit Delay (Seconds): 2

TX Interval (Seconds): 30 (5..32768)

Notification Interval (Seconds): 30 (5..3600)

Hold Multiplier: 4

2 Modify the configurable parameters, described in *Table 50*.

3 Click **Apply**.

Table 49 lists and describes the status parameters in the LLDP Configuration Parameters page.

Table 49: 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.
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 50: LLDP Configurable Configuration Parameters

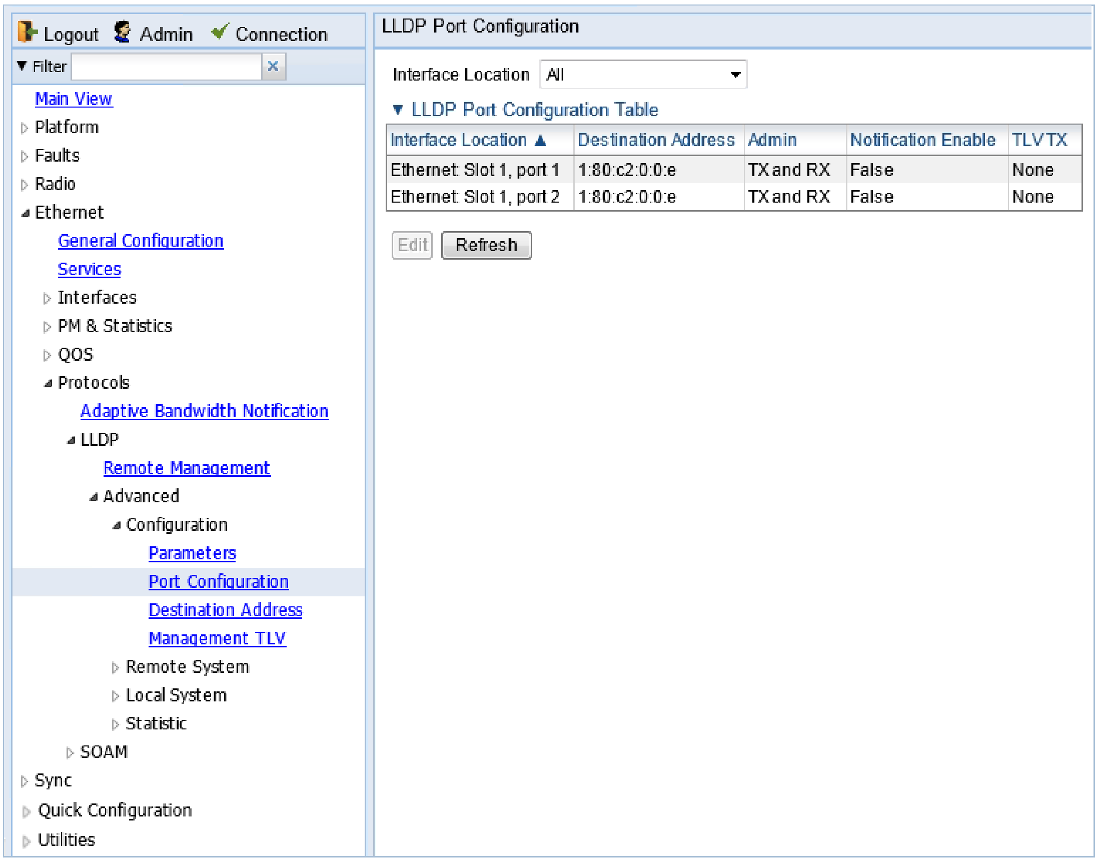
Parameter	Definition
TX Interval (Seconds)	Defines the interval, in seconds, at which LLDP frames are transmitted. You can select a value from 5 to 32768. The default value is 30.
Notification Interval (Seconds)	Defines the interval, in seconds, between transmission of LLDP notifications during normal transmission periods. You can select a value from 5 to 3600. The default value is 10.
Hold Multiplier	Defines the time-to-live (TTL) multiplier. The TTL determines the length of time LLDP frames are retained by the receiving device. The TTL is determined by multiplying the TX Interval by the Hold Multiplier. You can select a value from 2 to 10. The default value is 4.

8.2.4. 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 183: LLDP Port Configuration Page



LLDP Port Configuration

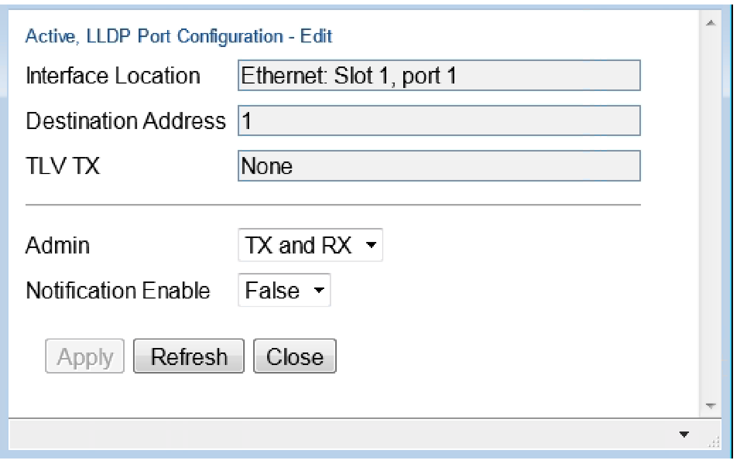
Interface Location: All

▼ 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

2 Select an interface and click **Edit**. The LLDP Port Configuration - Edit page opens.

Figure 184: LLDP Port Configuration - Edit Page



Active, LLDP Port Configuration - Edit

Interface Location: Ethernet: Slot 1, port 1

Destination Address: 1

TLV TX: None

Admin: TX and RX

Notification Enable: False

3 In the **Admin** field, select from the following options to define how the LLDP protocol operates for this port:

- **TX Only** – LLDP agent transmits LLDP frames on this port but does not update information about its peer.
- **RX Only** – LLDP agent receives but does not transmit LLDP frames on this port.
- **TX and RX** – LLDP agent transmits and receives LLDP frames on this port (default value).
- **Disabled** – LLDP agent does not transmit or receive LLDP frames on this port.

4 In the **Notification Enable** field, select from the following options to define, on a per agent basis, whether or not notifications from the agent to the NMS are enabled:

- **True** – The agent sends a Topology Change trap to the NMS whenever the system information received from the peer changes.
- **False** – Notifications to the NMS are disabled (default value).

5 Click **Apply**, then **Close**.

Table 51 lists and describes the status parameters in the LLDP Port Configuration page.

Table 51: LLDP Port Configuration Status Parameters

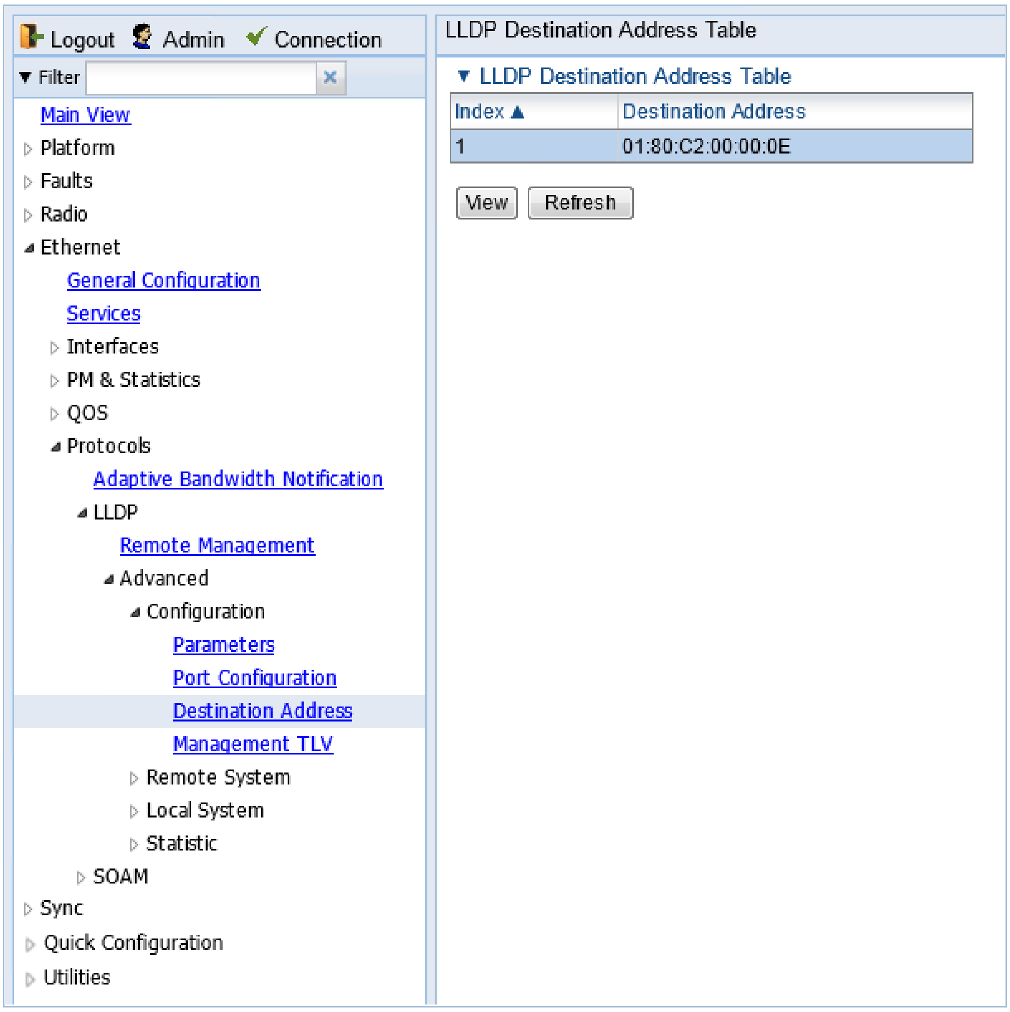
Parameter	Definition
Interface Location	Identifies the port.
Destination Address	The destination address of the LLDP agent associated with this port.
TLV TX	Indicates which of the unit's capabilities is transmitted by the LLDP agent for the port: ● **PortDesc** – The LLDP agent transmits Port Description TLVs. ● **SysName** – The LLDP agent transmits System Name TLVs. ● **SysDesc** – The LLDP agent transmits System Description TLVs. ● **SysCap** – The LLDP agent transmits System Capabilities TLVs.

8.2.5. 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 185: LLDP Destination Address Table Page



LLDP Destination Address Table

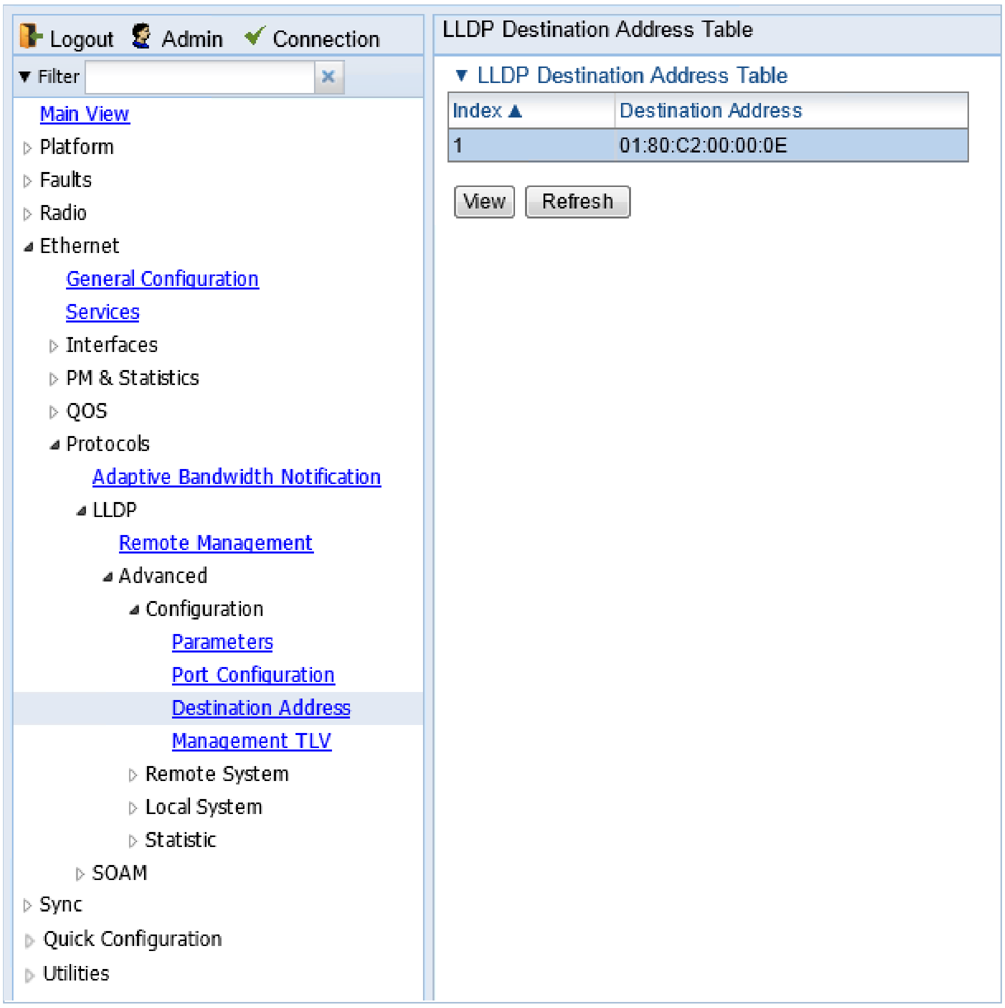
▼ LLDP Destination Address Table

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 186: LLDP Management TLV Configuration Page



LLDP Destination Address Table

▼ LLDP Destination Address Table

Index ▲	Destination Address
1	01:80:C2:00:00:0E

Table 52 lists and describes the status parameters in the LLDP Management TLV Configuration page.

Table 52: LLDP Management TLV Parameters

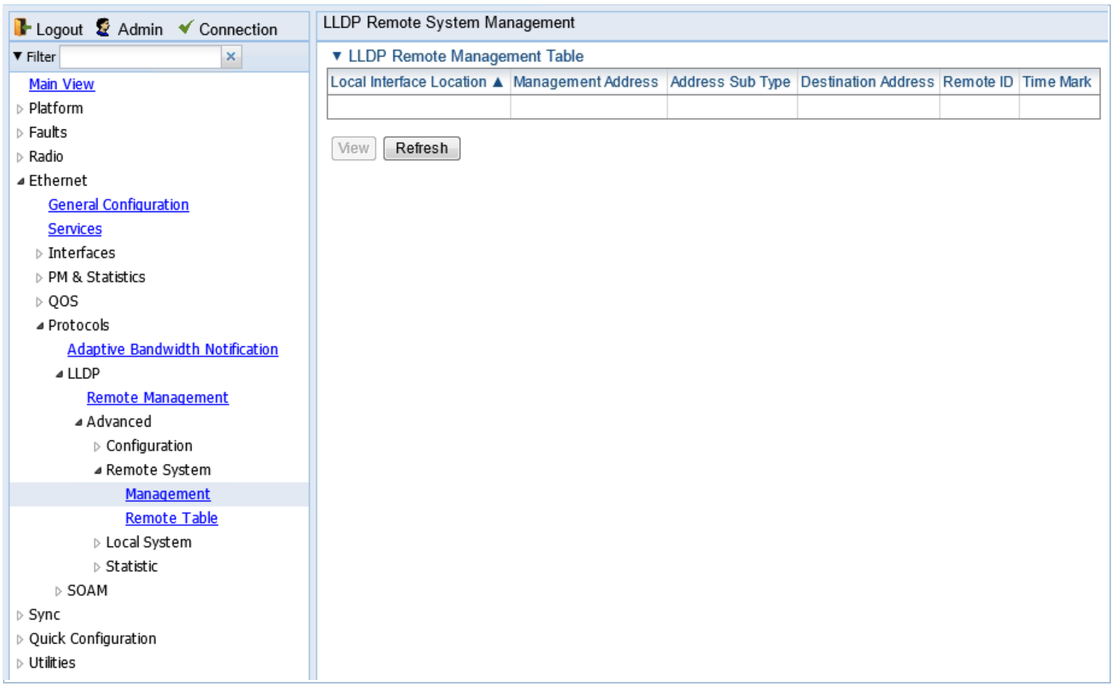
Parameter	Definition
Interface Location	Identifies the port.
Destination Address	Defines the MAC address associated with the port for purposes of LLDP transmissions.
Management Address	The unit's IP address.
Address Subtype	Defines the type of the management address identifier encoding used for the Management Address.
Tx Enable	Indicates whether the unit's Management Address is transmitted with LLDPDUs. In this release, the Management Address is always sent.

8.2.6. 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 187: LLDP Remote System Management Page



LLDP Remote System Management

▼ LLDP Remote Management Table

Local Interface Location ▲	Management Address	Address Sub Type	Destination Address	Remote ID	Time Mark

Table 53 describes the LLDP remote system management parameters. These parameters are read-only.

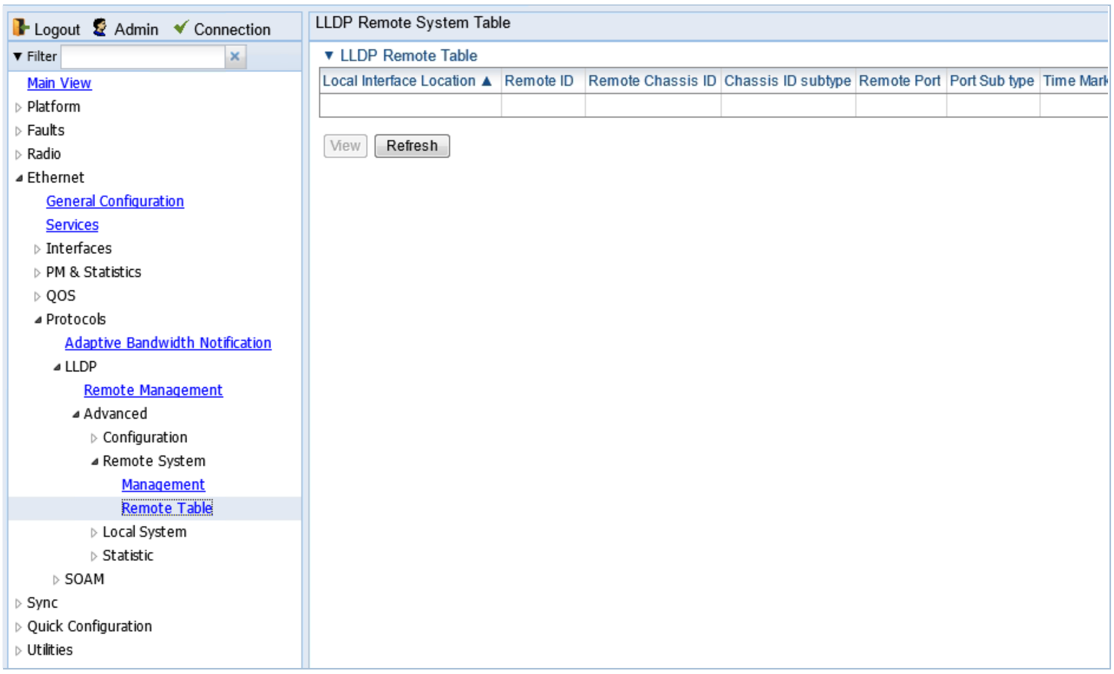
Table 53: LLDP Remote System Management Parameters

Parameter	Definition
Local Interface Location	The location of the local interface.
Management Address	The octet string used to identify the management address component associated with the remote system.
Address Sub Type	The type of management address identifier encoding used in the associated LLDP Agent Remote Management Address.
Destination Address	The peer LLDP agent's destination MAC Address.
Remote ID	An arbitrary local integer value used by this agent to identify a particular connection instance, unique only for the indicated remote system.
Time Mark	The time the entry was created.

To display unit parameter information received via LLDP from the unit's nearest neighbor (peer):

1 Select **Ethernet > Protocols > LLDP > Advanced > Remote System > Remote Table**. The LLDP Remote System Table page opens.

Figure 188: LLDP Remote System Table Page



LLDP Remote System Table

▼ LLDP Remote Table

Local Interface Location ▲	Remote ID	Remote Chassis ID	Chassis ID subtype	Remote Port	Port Sub type	Time Mark

Table 54 describes the parameters in the LLDP Remote System Table page. These parameters are read-only.

Table 54: LLDP Remote System Table Parameters

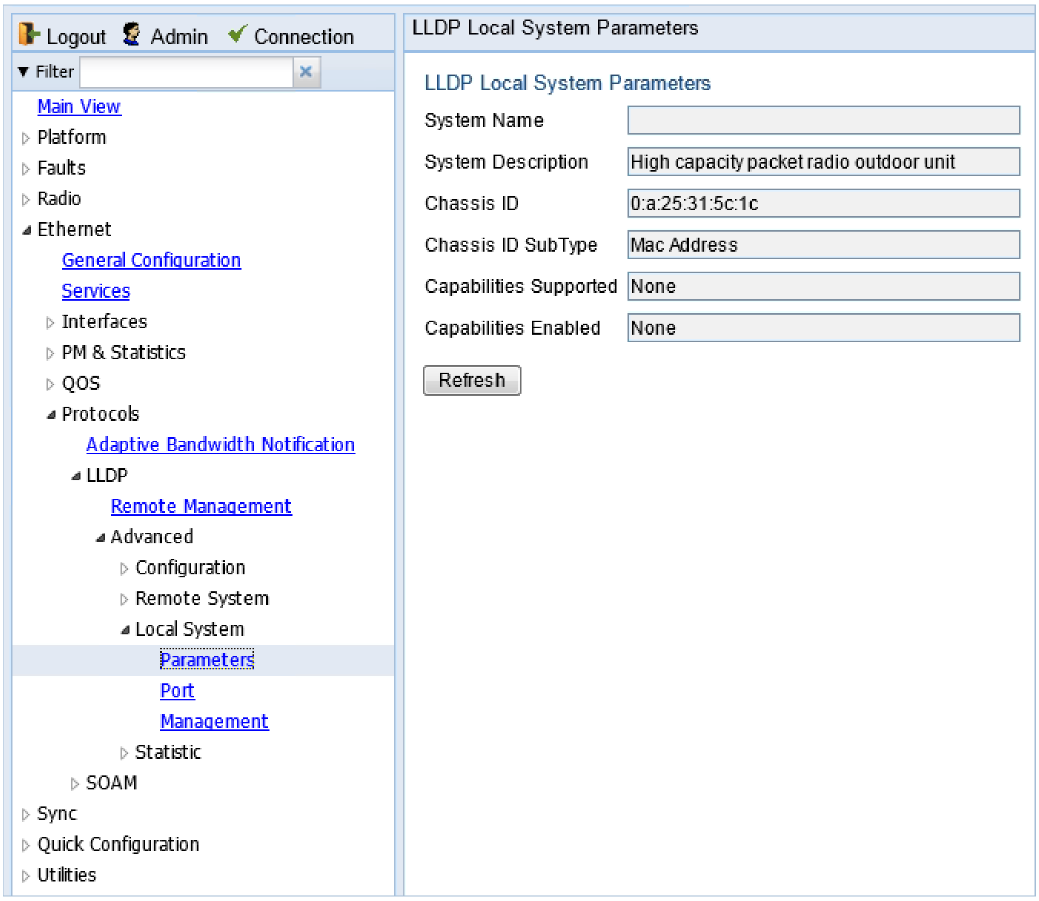
Parameter	Definition
Local Interface Location	The location of the local interface.
Remote ID	An arbitrary local integer value used by this agent to identify a particular connection instance, unique only for the indicated peer.
Remote Chassis ID	An octet string used to identify the peer's hardware unit.
Chassis ID Subtype	The type of encoding used to identify the peer's hardware unit.
Remote Port	An octet string used to identify the port component associated with the remote system.
Port Sub type	The type of port identifier encoding used in the peer's Port ID.
Time Mark	The time the entry was created.

8.2.7. 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 189: LLDP Local System Parameters Page



LLDP Local System Parameters

System Name	
System Description	High capacity packet radio outdoor unit
Chassis ID	0:a:25:31:5c:1c
Chassis ID SubType	Mac Address
Capabilities Supported	None
Capabilities Enabled	None

Table 55 describes the parameters in the LLDP Local System Parameters page. These parameters are read-only.

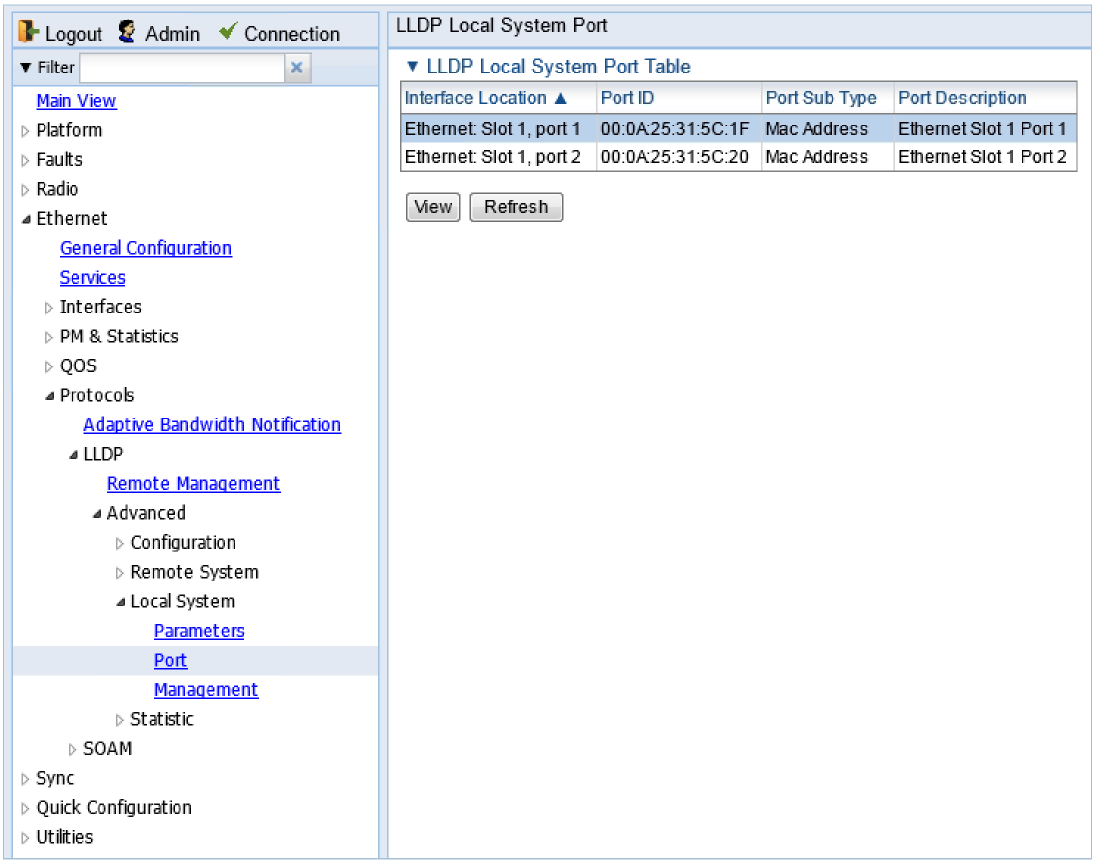
Table 55: LLDP Local System Parameters

Parameter	Definition
System Name	The system name included in TLVs transmitted by the LLDP agent, as defined in the **Name** field of the Unit Parameters page. See *Configuring Unit Parameters*.
System Description	The system description included in TLVs transmitted by the LLDP agent, as defined in the **Description** field of the Unit Parameters page. See *Configuring Unit Parameters*.
Chassis ID	The MAC Address of the local unit.
Chassis ID SubType	The type of encoding used to identify the local unit. In this release, this parameter is always set to MAC Address.
Capabilities Supported	A bitmap value used to identify which system capabilities are supported on the local system, as included in TLVs transmitted by the LLDP agent. The bitmap is defined by the following parameters: 0 – other 1 – repeater 2 – bridge 3 – wlanAccessPoint 4 – router 5 – telephone 6 – docsisCableDevice 7 – stationOnly 8 – cVLANComponent 9 – sVLANComponent 10 – twoPortMACRelay
Capabilities Enabled	A bitmap value used to identify which system capabilities are enabled on the local system, as included in TLVs transmitted by the LLDP agent. The bitmap is defined by the following parameters: 0 – other 1 – repeater 2 – bridge 3 – wlanAccessPoint 4 – router 5 – telephone 6 – docsisCableDevice 7 – stationOnly 8 – cVLANComponent 9 – sVLANComponent 10 – twoPortMACRelay

To display the unit's port parameters, as transmitted by the LLDP agents:

1. Select **Ethernet > Protocols > LLDP > Advanced > Local System > Port**. The LLDP Local System Port page opens.

Figure 190: LLDP Local System Port Page



LLDP Local System Port

LLDP Local System Port Table

Interface Location ▲	Port ID	Port Sub Type	Port Description
Ethernet: Slot 1, port 1	00:0A:25:31:5C:1F	Mac Address	Ethernet Slot 1 Port 1
Ethernet: Slot 1, port 2	00:0A:25:31:5C:20	Mac Address	Ethernet Slot 1 Port 2

Table 56 describes the parameters in the LLDP Local System Port page. These parameters are read-only.

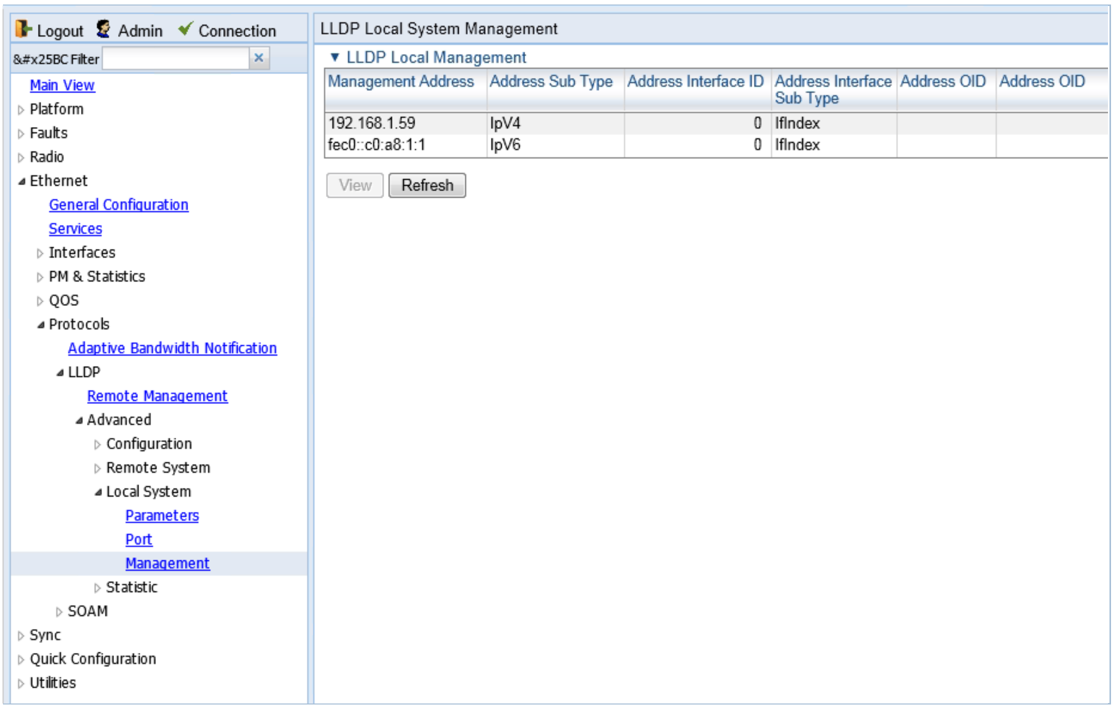
Table 56: LLDP Local System Port Parameters

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 191: LLDP Local System Management Page



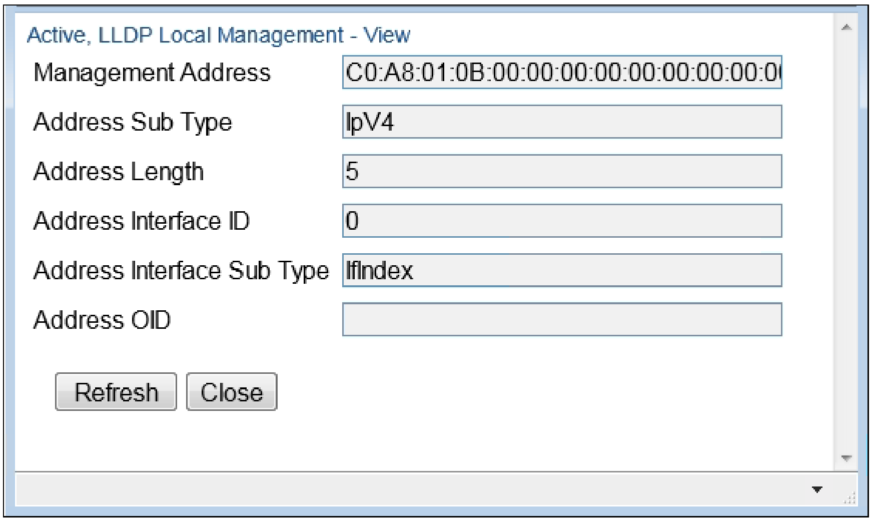
LLDP Local System Management

▼ LLDP Local Management

Management Address	Address Sub Type	Address Interface ID	Address Interface Sub Type	Address OID	Address OID
192.168.1.59	IpV4	0	IfIndex		
fec0::c0:a8:1:1	IpV6	0	IfIndex		

2 To display all the parameters, select a row and click **View**.

Figure 192: LLDP Local System Management – View Page



Active, LLDP Local Management - View

Management Address	C0:A8:01:0B:00:00:00:00:00:00:00:00:0(
Address Sub Type	IpV4
Address Length	5
Address Interface ID	0
Address Interface Sub Type	IfIndex
Address OID	

Table 57 describes the parameters in the LLDP Local System Management page. These parameters are read-only.

Table 57: LLDP Local System Management Parameters

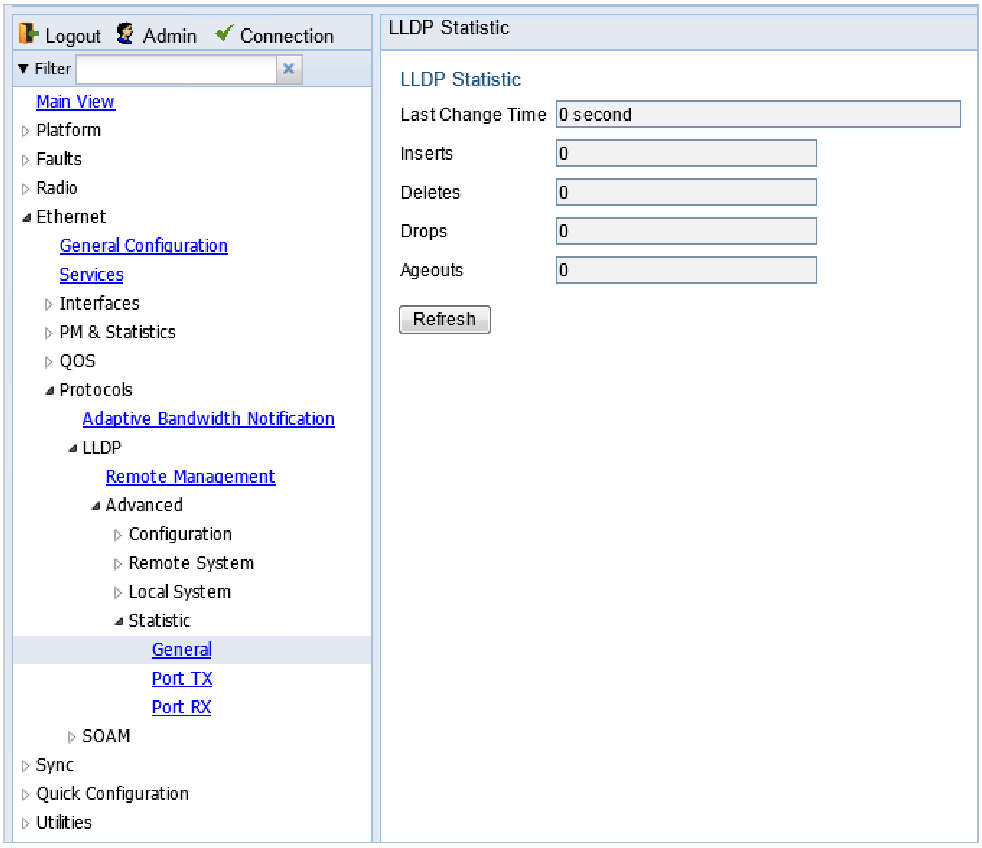
Parameter	Definition
Management Address	The local unit's IP address.
Address Sub Type	The format of the local unit's IP Address.
Address Length	Reserved for future use.
Address Interface ID	Reserved for future use.
Address Interface Sub Type	Reserved for future use.
Address OID	Reserved for future use.

8.2.8. 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 193: LLDP Statistic Page



LLDP Statistic

Last Change Time	0 second
Inserts	0
Deletes	0
Drops	0
Ageouts	0

Table 58 describes the statistics in the LLDP Statistic page.

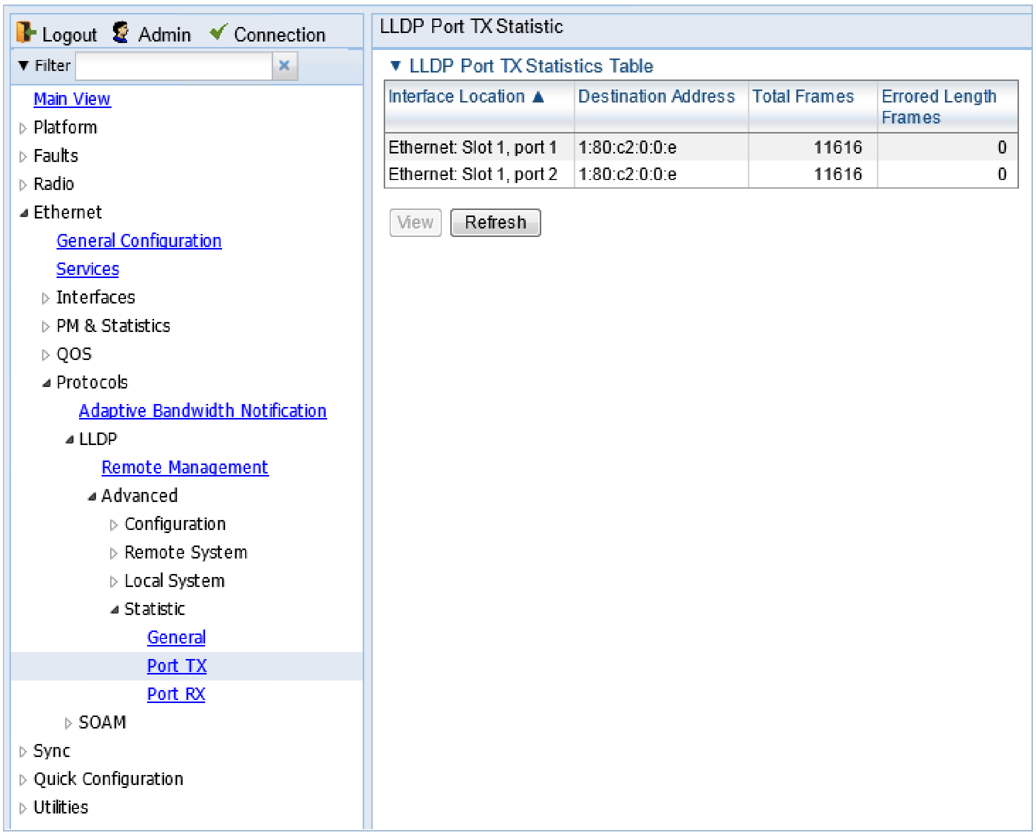
Table 58: LLDP Statistics

Parameter	Definition
Last Change Time	The time of the most recent change in the remote unit, as reported via LLDP.
Inserts	The number of times the information from the remote system has changed.
Deletes	The number of times the information from the remote system has been deleted.
Drops	Reserved for future use.
Ageouts	The number of times the information from the remote system has been deleted from the local unit's database because the information's TTL has expired. The **RX Ageouts** counter in the Port RX page is similar to this counter, but is for specific ports rather than the entire unit.

To display statistics about LLDP transmissions and transmission errors:

1 Select **Ethernet** > **Protocols** > **LLDP** > **Advanced** > **Statistic** > **Port TX**. The LLDP Port TX Statistic page opens.

Figure 194: LLDP Port TX Statistic Page



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 59 describes the statistics in the LLDP Port TX Statistic page.

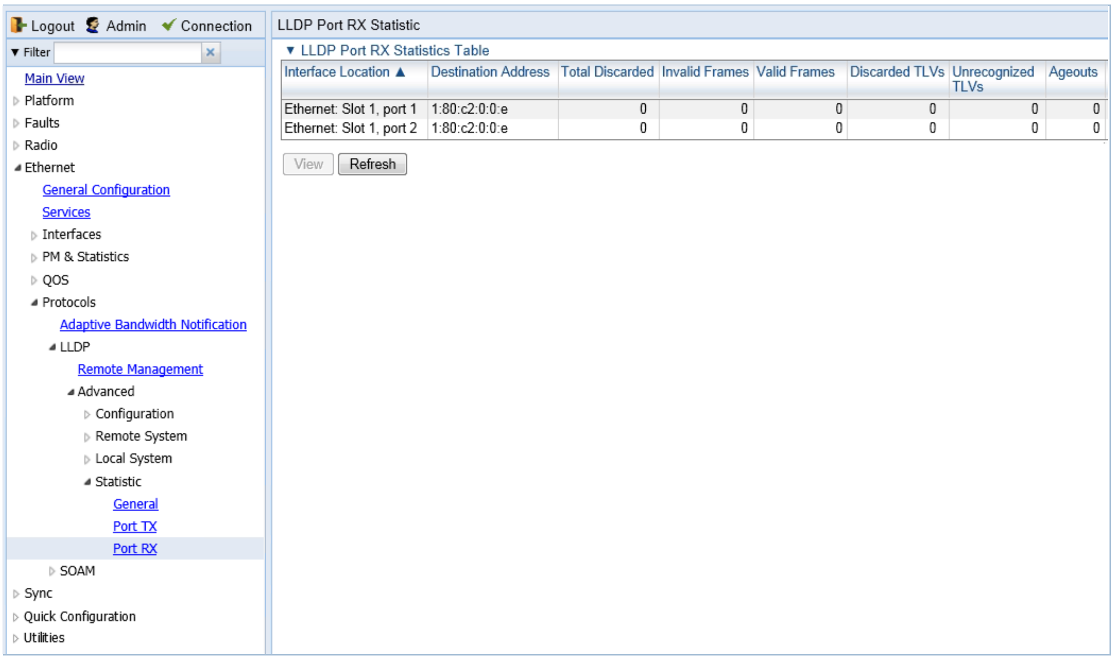
Table 59: LLDP Port TX Statistics

Parameter	Definition
Interface Location	The index value used to identify the port in LLDP transmissions.
Destination Address	The LLDP MAC address associated with this entry.
Total Frames	The number of LLDP frames transmitted by the LLDP agent on this port to the destination MAC address.
Errored Length Frames	The number of LLDPDU Length Errors recorded for this port and destination MAC address. If the set of TLVs that is selected in the LLDP local system MIB by network management would result in an LLDPDU that violates LLDPDU length restrictions, then the No. of Length Error statistic is incremented by 1, and an LLDPDU is sent containing the mandatory TLVs plus as many of the optional TLVs in the set as will fit in the remaining LLDPDU length.

To display statistics about LLDP frames received by the unit:

1 Select **Ethernet > Protocols > LLDP > Advanced > Statistic > Port RX**. The LLDP Port TX Statistic page opens.

Figure 195: LLDP Port RX Statistic Page



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

Table 60 describes the statistics in the LLDP Port TX Statistic page.

Table 60: 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	The number of age-outs that occurred on the port. An age-out is the number of times the complete set of information advertised by the remote system has been deleted from the unit's database because the information timeliness interval has expired. This counter is similar to the **LLDP No. of Ageouts** counter in the LLDP Statistic page, except that it is per port rather than for the entire unit. This counter is set to zero during agent initialization. This counter is incremented only once when the complete set of information is invalidated (aged out) from all related tables on a particular port. Partial ageing is not allowed.

9. Synchronization

This section includes:

- *Configuring SyncE Regenerator*

Note

The Sync Source and Outgoing Clock pages are reserved for future use.

9.1. Configuring SyncE Regenerator

Note

SyncE Regenerator is supported for NetStream Diplo and NetStream Primo. For NS Primo/DiploE, SyncE Regenerator support is planned for future release.

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.

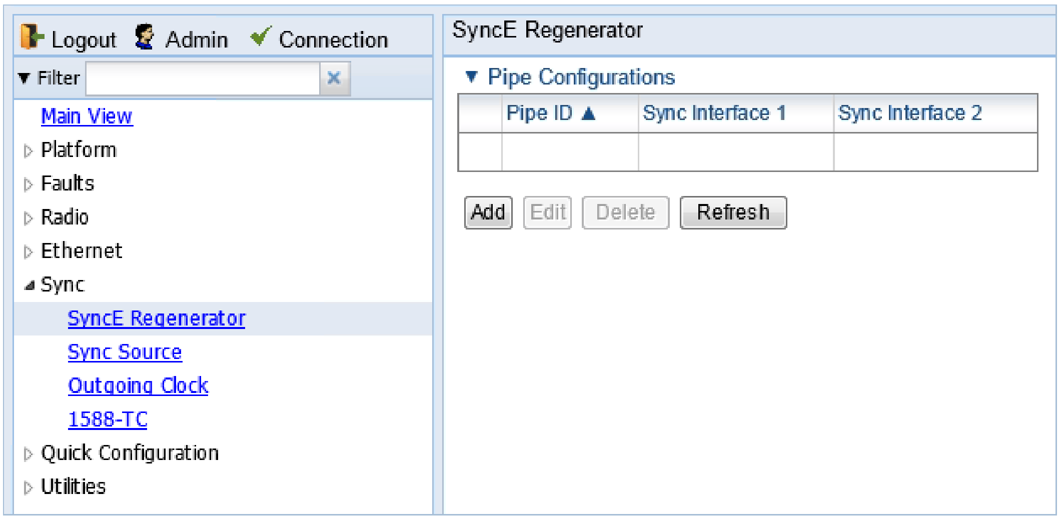
Note

SyncE Regenerator currently supports only a single pipe configuration.
When working with Transparent Clock, Sync Regenerator is only supported with optical interfaces.

To add a pipe configuration:

1 Select **Sync > SyncE Regenerator**. The SyncE Regenerator page opens.

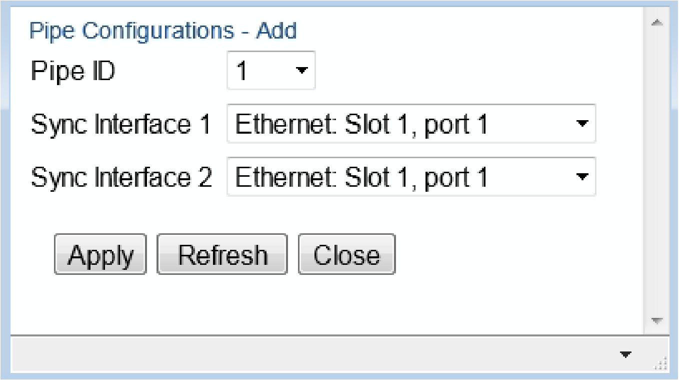
Figure 196: SyncE Regenerator Page



	Pipe ID ▲	Sync Interface 1	Sync Interface 2

2 Click **Add** underneath the Pipe Configurations Table. The Pipe Configuration - Add window opens.

Figure 197: Pipe Configurations - Add Page



Pipe Configurations - Add

Pipe ID: 1

Sync Interface 1: Ethernet: Slot 1, port 1

Sync Interface 2: Ethernet: Slot 1, port 1

3 Select a Pipe ID.
4 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 NetStream Primo and NS Primo/DiploE units.

5 Click **Apply**.

Configuring 1588 Transparent Clock

NetStream Diplo, NetStream Primo, and NS Primo/DiploE use 1588v2-compliant Transparent Clock to counter the effects of delay variation. Transparent Clock measures and adjusts for delay variation, enabling the NetStream Diplo/S/E to guarantee ultra-low PDV.

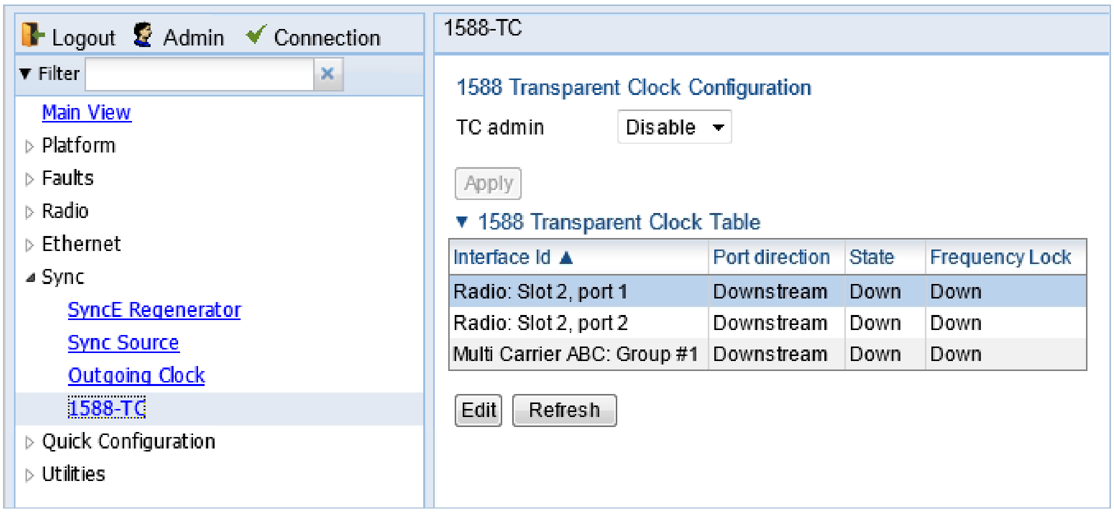
A Transparent Clock node resides between a master and a slave node, and updates the timestamps of PTP packets passing from the master to the slave to compensate for delay, enabling the terminating clock in the slave node to remove the delay accrued in the Transparent Clock node. The Transparent Clock 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 C8.0.7:

To configure Transparent Clock:

1 Make sure that synchronization is properly configured for the radio on which you are configuring Transparent Clock.
2 Configure a service and service points to carry the PTP packets that will be passing between the master and slave nodes. See . It is recommended to:

3 Select . The 1588-TC page opens.



1588-TC

1588 Transparent Clock Configuration

TC admin: Disable

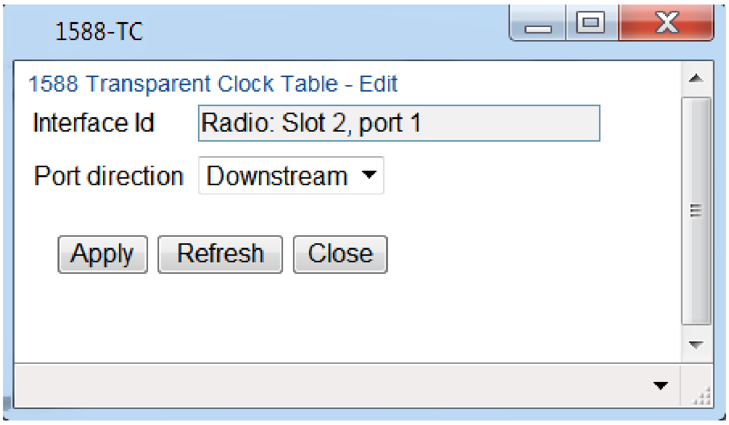
▼ 1588 Transparent Clock Table

Interface Id ▲	Port direction	State	Frequency Lock
Radio: Slot 2, port 1	Downstream	Down	Down
Radio: Slot 2, port 2	Downstream	Down	Down
Multi Carrier ABC: Group #1	Downstream	Down	Down

4 In the **TC admin** field, select **Enable**.

5 Click **Apply**.

6 Select a radio and click **Edit**. The 1588-TC – Edit page opens.



1588 Transparent Clock Table - Edit

Interface Id: Radio: Slot 2, port 1

Port direction: Downstream

7 In the field, select or to determine the direction of the PTP packet flow.

Note

This parameter must be set to on one side of the 1588 link and on the other.

8 Click , then .

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*
- *Blocking Telnet Access*
- *Uploading the Security Log*
- *Uploading the Configuration Log*

Related topics:

- *Changing Your Password*
- *Operating in FIPS Mode*
- *Configuring AES-256 Payload Encryption*

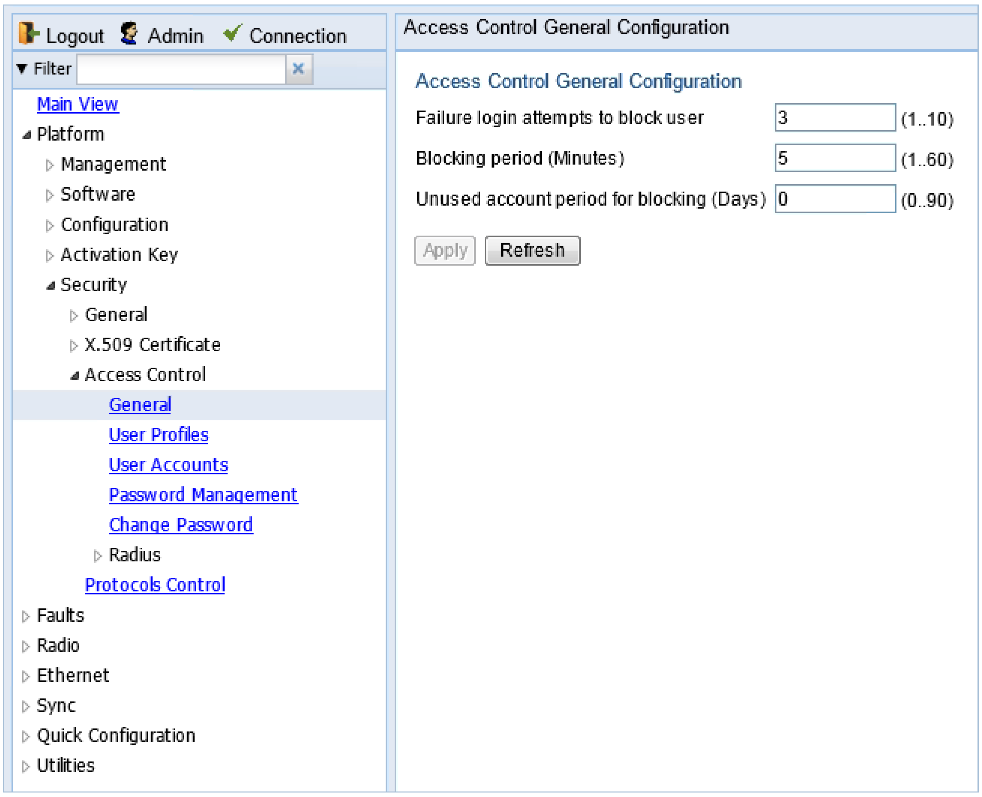
10.1. Configuring the General Access Control Parameters

To avoid unauthorized login to the system, NS Primo/Diplo automatically blocks users upon a configurable number of failed login attempts. You can also configure NS Primo/Diplo 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 200: Access Control General Configuration Page



Access Control General Configuration

Access Control General Configuration

Failure login attempts to block user	3	(1..10)
Blocking period (Minutes)	5	(1..60)
Unused account period for blocking (Days)	0	(0..90)

2 In the **Failure login attempts to block user** field, select the number of failed login attempts that will trigger blocking. If a user attempts to login to the system with incorrect credentials this number of times consecutively, the user will temporarily be prevented from logging into the system for the time period defined in the **Blocking period** field. Valid values are 1-10. The default value is 3.

3 In the **Blocking period (Minutes)** field, enter the length of time, in minutes, that a user is prevented from logging into the system after the defined number of failed login attempts. Valid values are 1-60. The default value is 5.

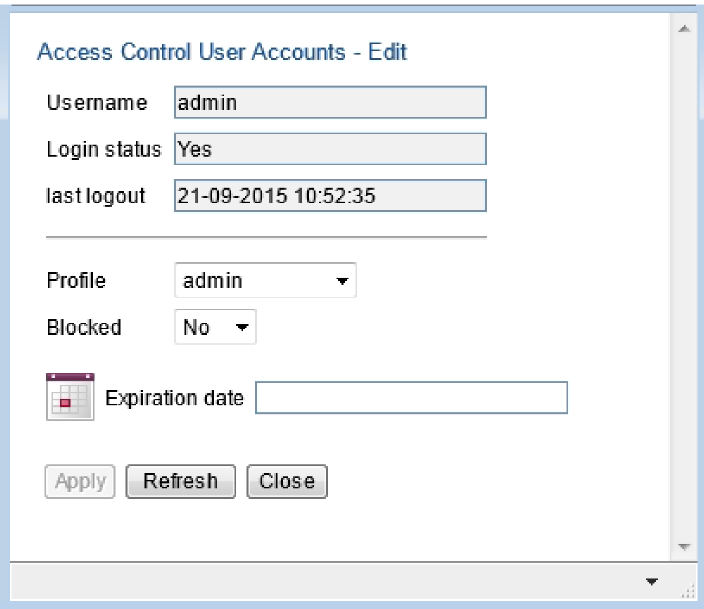
4 In the **Unused account period for blocking (Days)** field, you can configure a number of days after which a user is prevented from logging into the system if the user has not logged in for the configured number of days. Valid values are 0, or 30-90. If you enter 0, this feature is disabled. The default value is 0.

5 Click **Apply**.

Once a user is blocked, you can unblock the user from the User Accounts page. To unblock a user:

1 Select **Platform > Security > Access Control > User Accounts**. The Access Control User Accounts page opens (*Figure 206*).
2 Select the user and click **Edit**. The Access Control User Accounts - Edit page opens.

Figure 201: Access Control User Accounts - Edit Page



Access Control User Accounts - Edit

Username: admin
Login status: Yes
last logout: 21-09-2015 10:52:35

Profile: admin
Blocked: No
Expiration date:

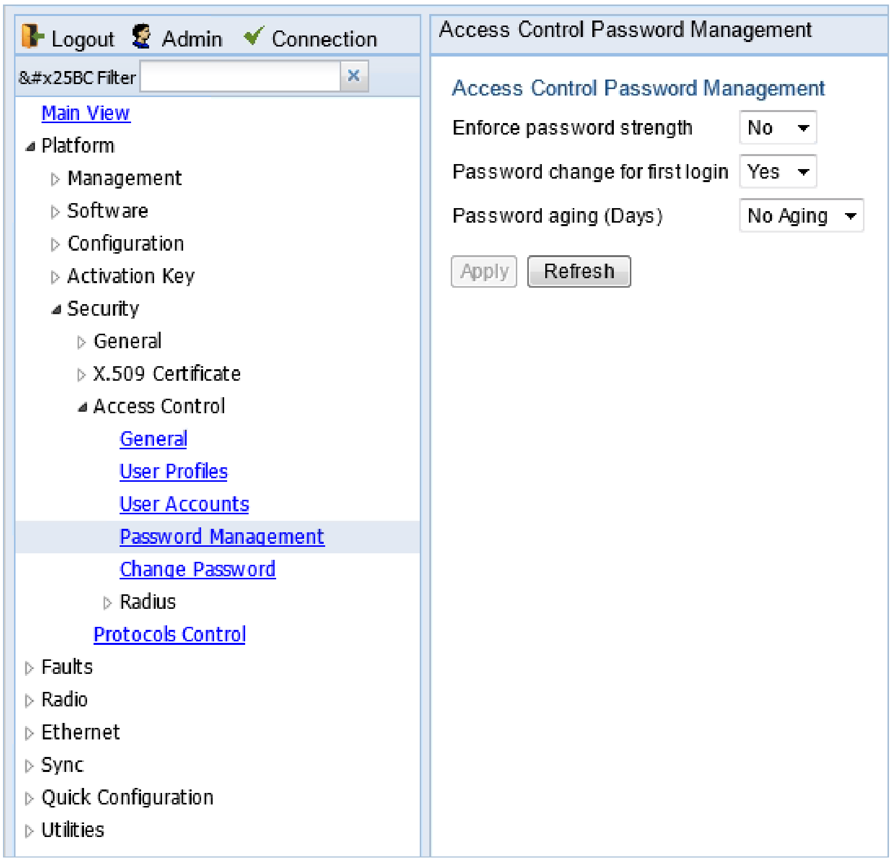
3 In the **Blocked** field, select **No**.
4 Click **Apply**, then **Close**.

10.2. 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 202: Access Control Password Management Page



Access Control Password Management

Access Control Password Management

Enforce password strength: No

Password change for first login: Yes

Password aging (Days): No Aging

2 In the **Enforce password strength** field, select **Yes** or **No**. When **Yes** is selected:

- Password length must be at least eight characters.
- Password must include characters of at least three of the following character types: lower case letters, upper case letters, digits, and special characters. For purposes of meeting this requirement, upper case letters at the beginning of the password and digits at the end of the password are not counted.
- The last five passwords you used cannot be reused.

3 In the **Password change for first login** field, select **Yes** or **No**. When **Yes** is selected, the system requires the user to change his or her password the first time the user logs in.

4 In the **Password aging (Days)** field, select the number of days that user passwords will remain valid from the first time the user logs into the system. You can enter 20-90, or **No Aging**. If you select **No Aging**, password aging is disabled and passwords remain valid indefinitely.

5 Click **Apply**.

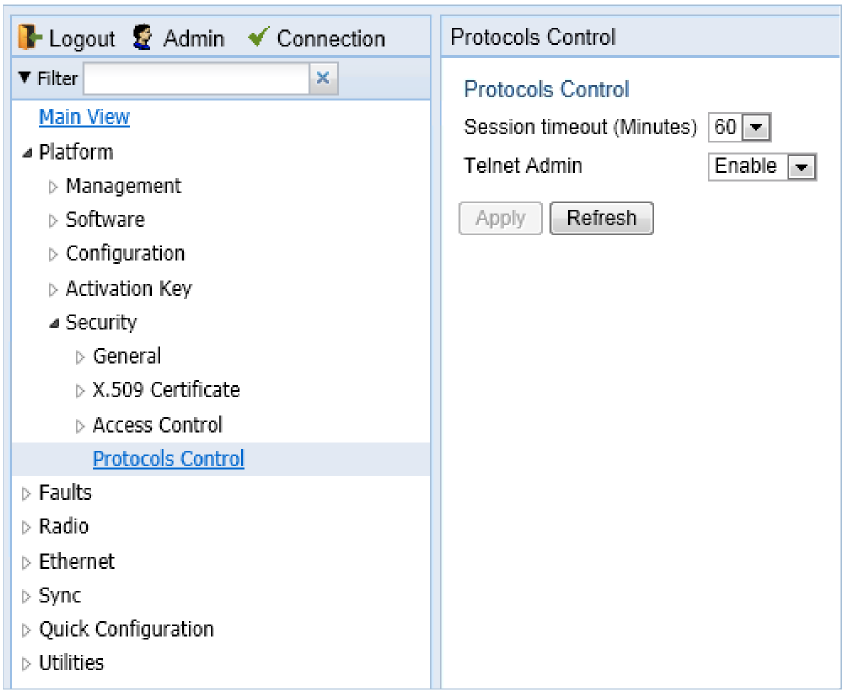
10.3. Configuring the Session Timeout

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 203: Protocols Control Page



Session timeout (Minutes) 60

Telnet Admin Enable

2 In the **Session timeout (Minutes)** field, select a session timeout, in minutes, from 1 to 60.

3 Click **Apply**.

10.4. Configuring Users

This section includes:

- *User Configuration Overview*
- *Configuring User Profiles*
- *Configuring Users*

Related topics:

- *Changing Your Password*

10.4.1. User Configuration Overview

User configuration is based on the Role-Based Access Control (RBAC) model. According to the RBAC model, permissions to perform certain operations are assigned to specific roles. Users are assigned to particular roles, and through those role assignments acquire the permissions to perform particular system functions.

In the NS Primo/Diplo 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.

10.4.2. Configuring User Profiles

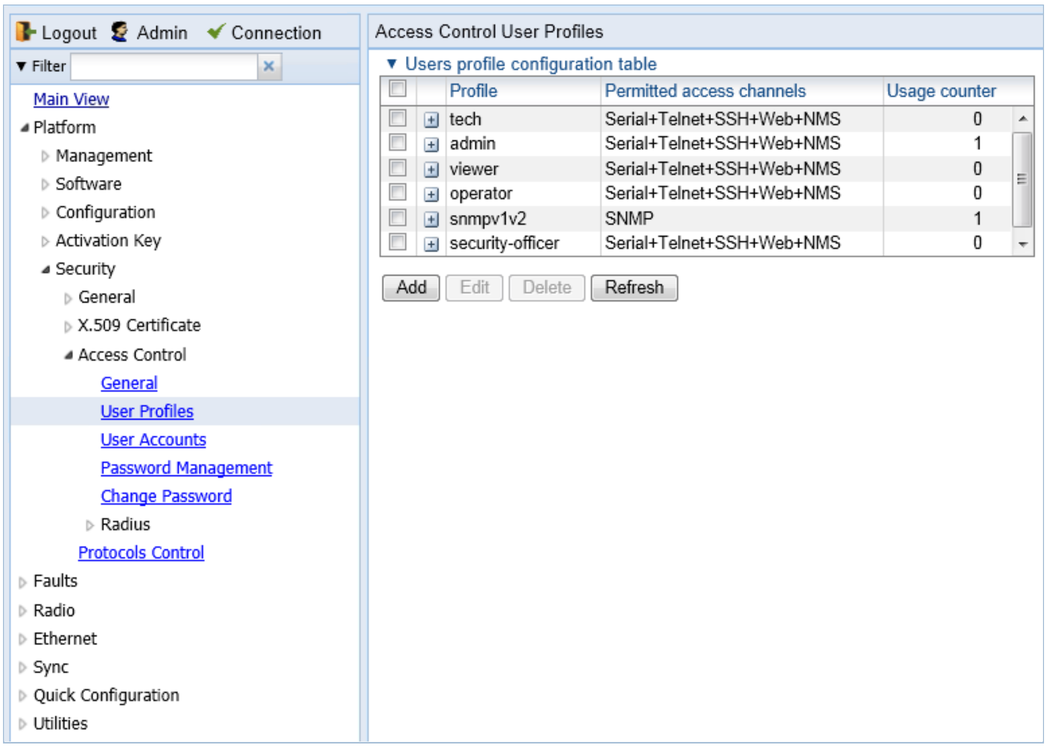
User profiles enable you to define system access levels. Each user must be assigned a user profile. Each user profile contains a detailed set of read and write permission levels per functionality group.

The system includes a number of pre-defined user profiles. You can edit these profiles, and add user profiles. Together, the system supports up to 50 user profiles.

To add a user profile:

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

Figure 204: Access Control User Profiles Page



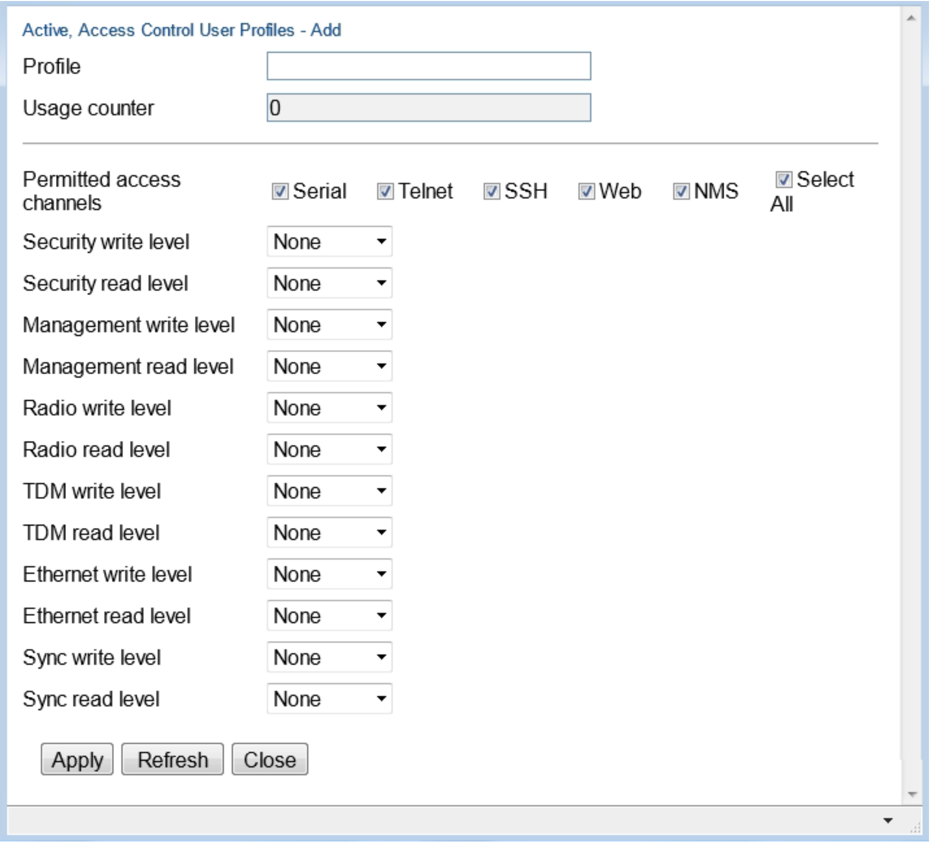
Access Control User Profiles

▼ Users profile configuration table

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

2 Click **Add**. The Access Control User Profiles - Add page opens.

Figure 205: Access Control User Profiles - Add Page



Active, Access Control User Profiles - Add

Profile	
Usage counter	0
Permitted access channels	☑ Serial ☑ Telnet ☑ SSH ☑ Web ☑ NMS ☑ Select All
Security write level	None
Security read level	None
Management write level	None
Management read level	None
Radio write level	None
Radio read level	None
TDM write level	None
TDM read level	None
Ethernet write level	None
Ethernet read level	None
Sync write level	None
Sync read level	None

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.

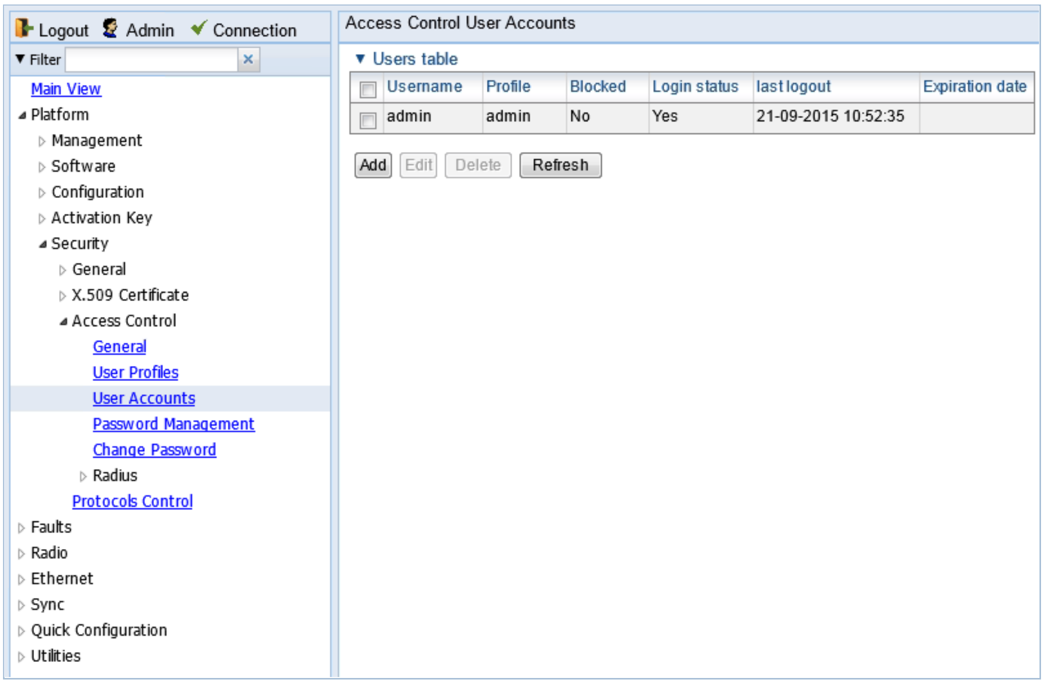
10.4.3. Configuring Users

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 206: Access Control User Accounts Page



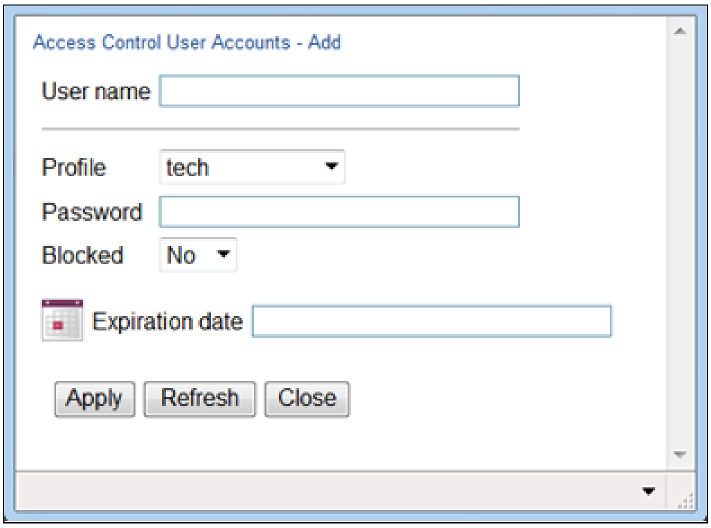
Access Control User Accounts

Users table

□	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 207: Access Control User Accounts - Add Page



Access Control User Accounts - Add

User name

Profile: tech

Password

Blocked: No

Expiration date

3 In the **User name** field, enter a user name for the user. The user name can be up to 32 characters.

4 In the **Profile** field, select a User Profile. The User Profile defines the user's access levels for functionality groups in the system. See *Configuring User Profiles*.

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

- ○ Password length must be at least eight characters.
- ○ Password must include characters of at least three of the following character types: lower case letters, upper case letters, digits, and special characters. For purposes of meeting this requirement, upper case letters at the beginning of the password and digits at the end of the password are not counted.
- ○ The last five passwords you used cannot be reused.

6 In the **Blocked** field, you can block or unblock the user. Selecting **Yes** blocks the user. You can use this option to block a user temporarily, without deleting the user from the system. If you set this option to **Yes** while the user is logged into the system, the user will be automatically logged out of the system within 30 seconds.

Note

Users can also be blocked by the system automatically. You can unblock the user by selecting **No** in the **Blocked** field. See *Configuring the General Access Control Parameters*.

7 Optionally, in the **Expiration date** field, you can configure the user to remain active only until a defined date. After that date, the user automatically becomes inactive. To set an expiration date, click the calendar icon and select a date, or enter a date in the format dd-mm-yyyy.

In addition to the configurable parameters described above, the Access Control User Accounts page displays the following information for each user:

- **Login Status** – Indicates whether the user is currently logged into the system.
- **Last Logout** – The date and time the user most recently logged out of the system.

To edit a user’s account details, select the user and click **Edit**. You can edit all of the user account parameters except the **User name** and **password**.

To add a user, click **Add**.

To delete a user, select the user and click **Delete**.

10.5. 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*

10.5.1. RADIUS Overview

The RADIUS protocol provides centralized user management services. NS Primo/Diplo 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 NS Primo/Diplo 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

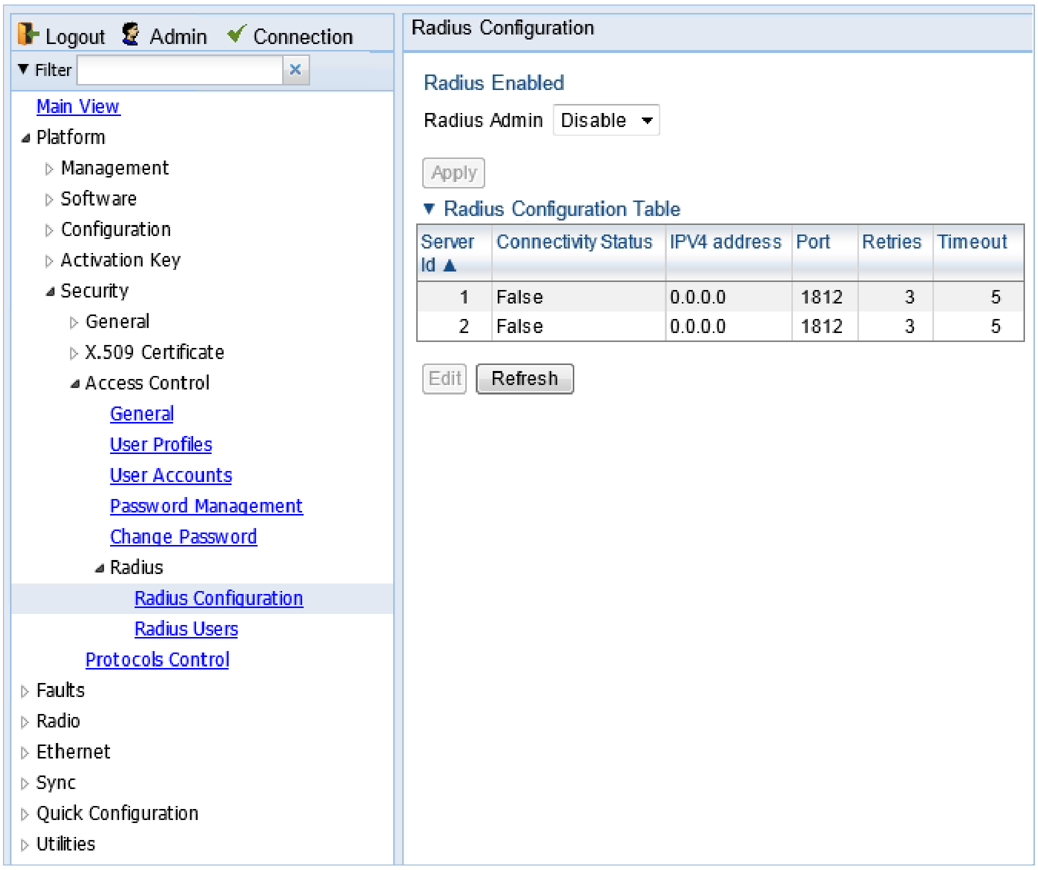
You can define up to two Radius servers. If you define two, one serves as the primary server and the other as the secondary server.

10.5.2. Activating RADIUS Authentication

To activate RADIUS authentication:

1 Select **Platform > Security > Access Control > Radius > Radius Configuration**. The Radius Configuration page opens.

Figure 208: Radius Configuration Page



Radius Configuration

Radius Enabled

Radius Admin: Disable

▼ 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

2 In the **Radius Admin** field, select **Enable**.

3 Click **Apply**.

10.5.3. Configuring the RADIUS Server Attributes

To configure the RADIUS server attributes:

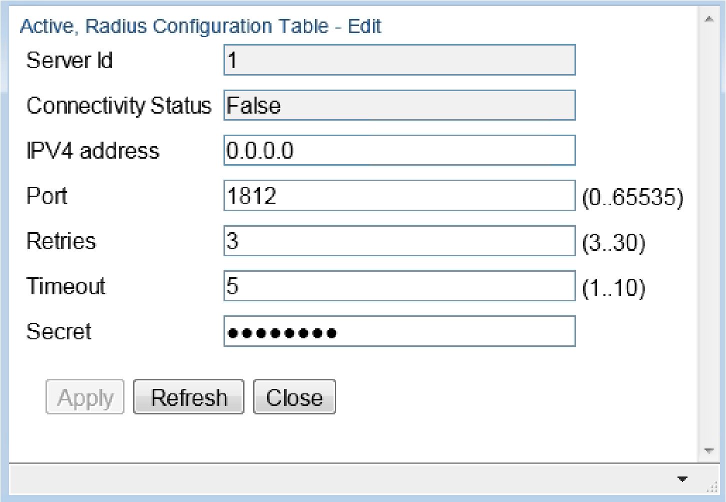
1 Select **Platform > Security > Access Control > Radius > Radius Configuration**. The Radius Configuration page opens (*Figure 208*).

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 209: 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	●●●●●●●●●	

4 In the **IPV4 address** field, enter the IP address of the RADIUS server.
5 In the **Port** field, enter the port of the RADIUS server.
6 In the **Retries** field, enter the number of times the unit will try to communicate with the RADIUS server before declaring the server to be unreachable.
7 In the **Timeout** field, enter the timeout (in seconds) that the agent will wait in each communication with the selected RADIUS server before retrying if no response is received.
8 In the **Secret** field, enter the shared secret of the RADIUS server. The string must be between 22-128 characters long.
9 Click **Apply**, then **Close**.

In addition to the configurable parameters described above, the 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.

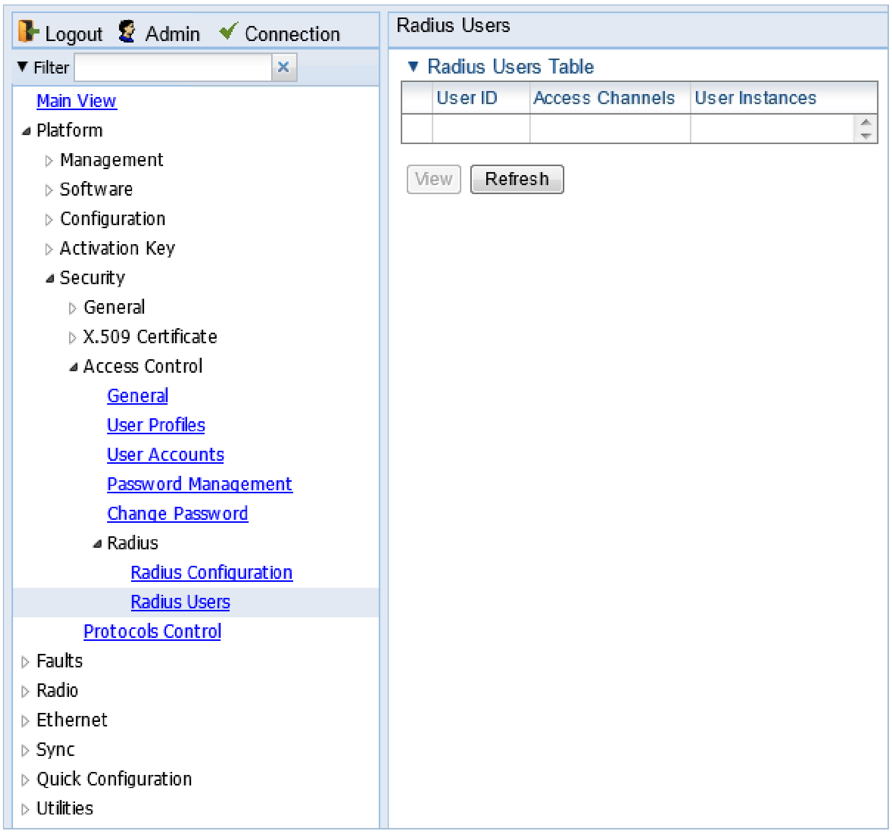
10.5.4. Viewing RADIUS User Permissions and Connectivity

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 210: Radius Users Page



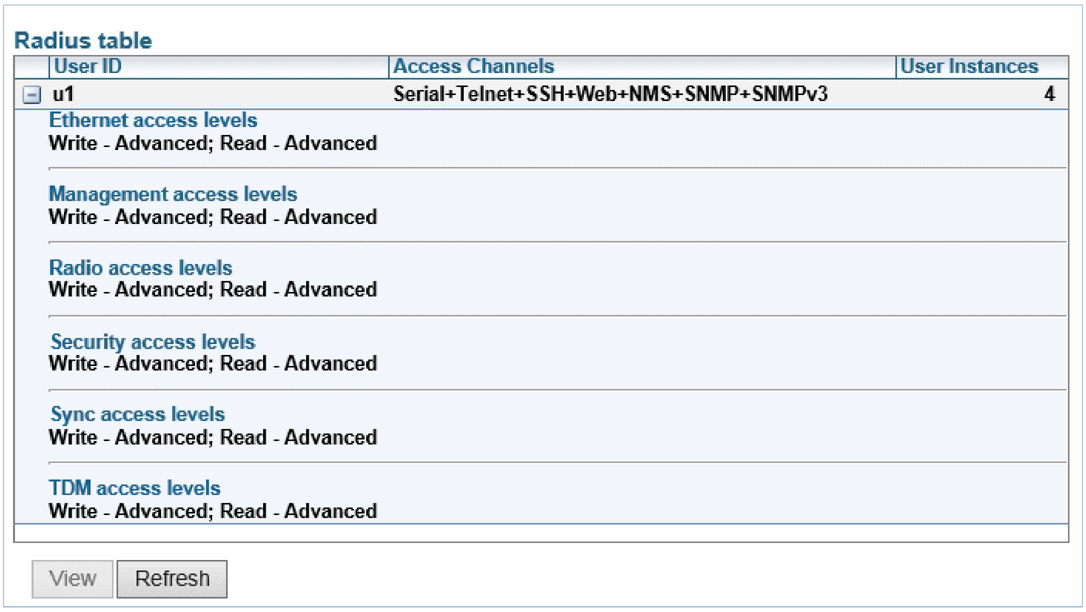
Radius Users Table

	User ID	Access Channels	User Instances

- 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 211: 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**).

10.5.5. Configuring a RADIUS Server

If you want to use the NS Primo/Diplo RADIUS feature, you must first install a RADIUS server and configure it to work with the NS Primo/Diplo device.

The following subsections describe how to configure a Win2008 RADIUS server and a Linux FreeRADIUS server to work with an NS Primo/Diplo. 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.

10.5.5.1. Configuring a Win 2008 RADIUS Server

The following sub-sections describe how to configure a Win 2008 RADIUS Server to work with an NS Primo/Diplo device.

Step 1 – Creating Groups and Users

To create groups and users:

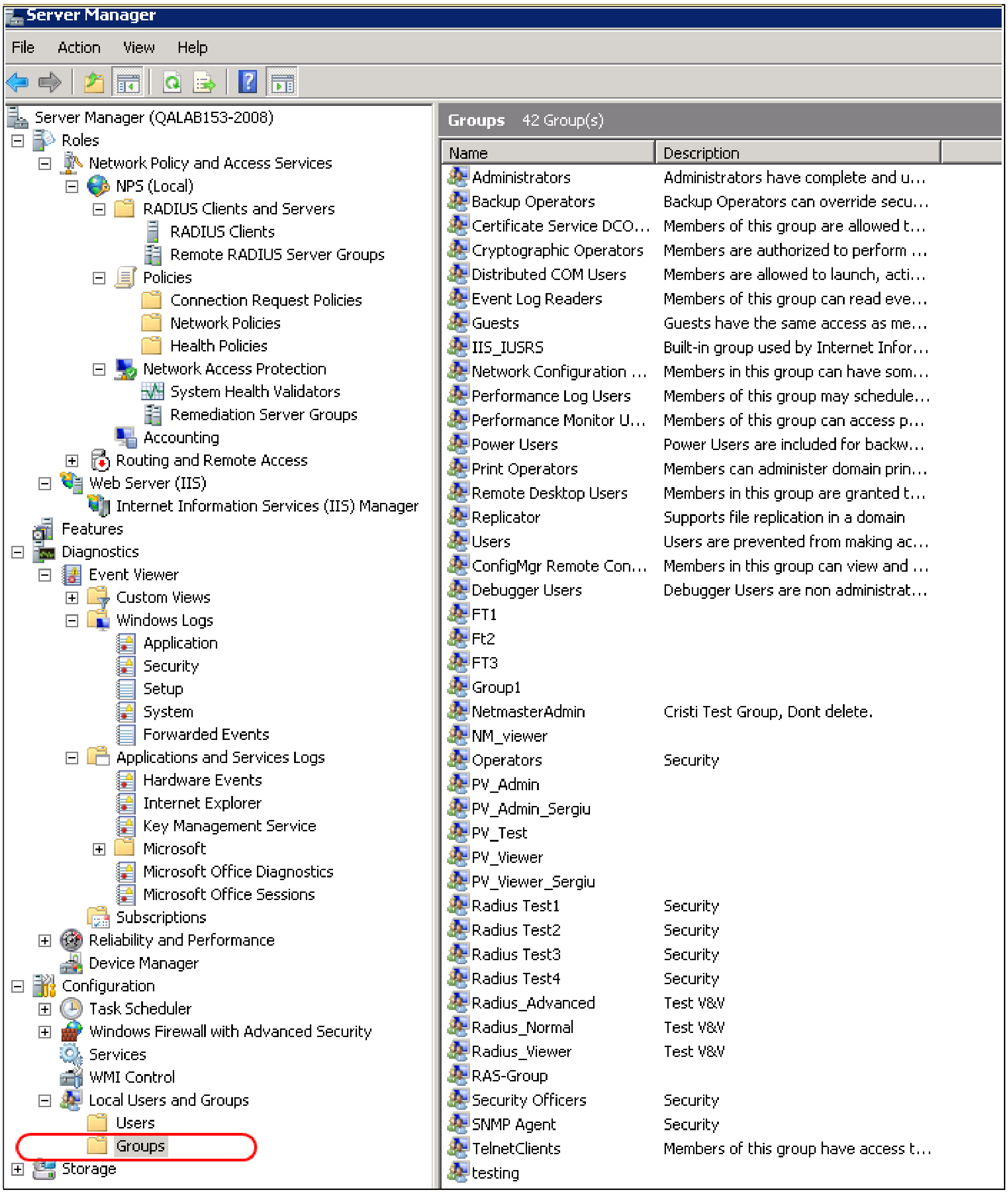
1 Create three user groups, as follows:

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 212: Server Manager – Creating User Groups



- Server Manager (QALAB153-2008)
  - Roles
    - Network Policy and Access Services
      - NPS (Local)
        - RADIUS Clients and Servers
          - RADIUS Clients
          - Remote RADIUS Server Groups
        - Policies
          - Connection Request Policies
          - Network Policies
          - Health Policies
        - Network Access Protection
          - System Health Validators
          - Remediation Server Groups
        - Accounting
      - Routing and Remote Access
    - Web Server (IIS)
      - Internet Information Services (IIS) Manager
  - Features
  - Diagnostics
    - Event Viewer
      - Custom Views
      - Windows Logs
        - Application
        - Security
        - Setup
        - System
        - Forwarded Events
      - Applications and Services Logs
        - Hardware Events
        - Internet Explorer
        - Key Management Service
        - Microsoft
        - Microsoft Office Diagnostics
        - Microsoft Office Sessions
      - Subscriptions
    - Reliability and Performance
    - Device Manager
  - Configuration
    - Task Scheduler
    - Windows Firewall with Advanced Security
    - Services
    - WMI Control
    - Local Users and Groups
      - Users
      - Groups
  - Storage

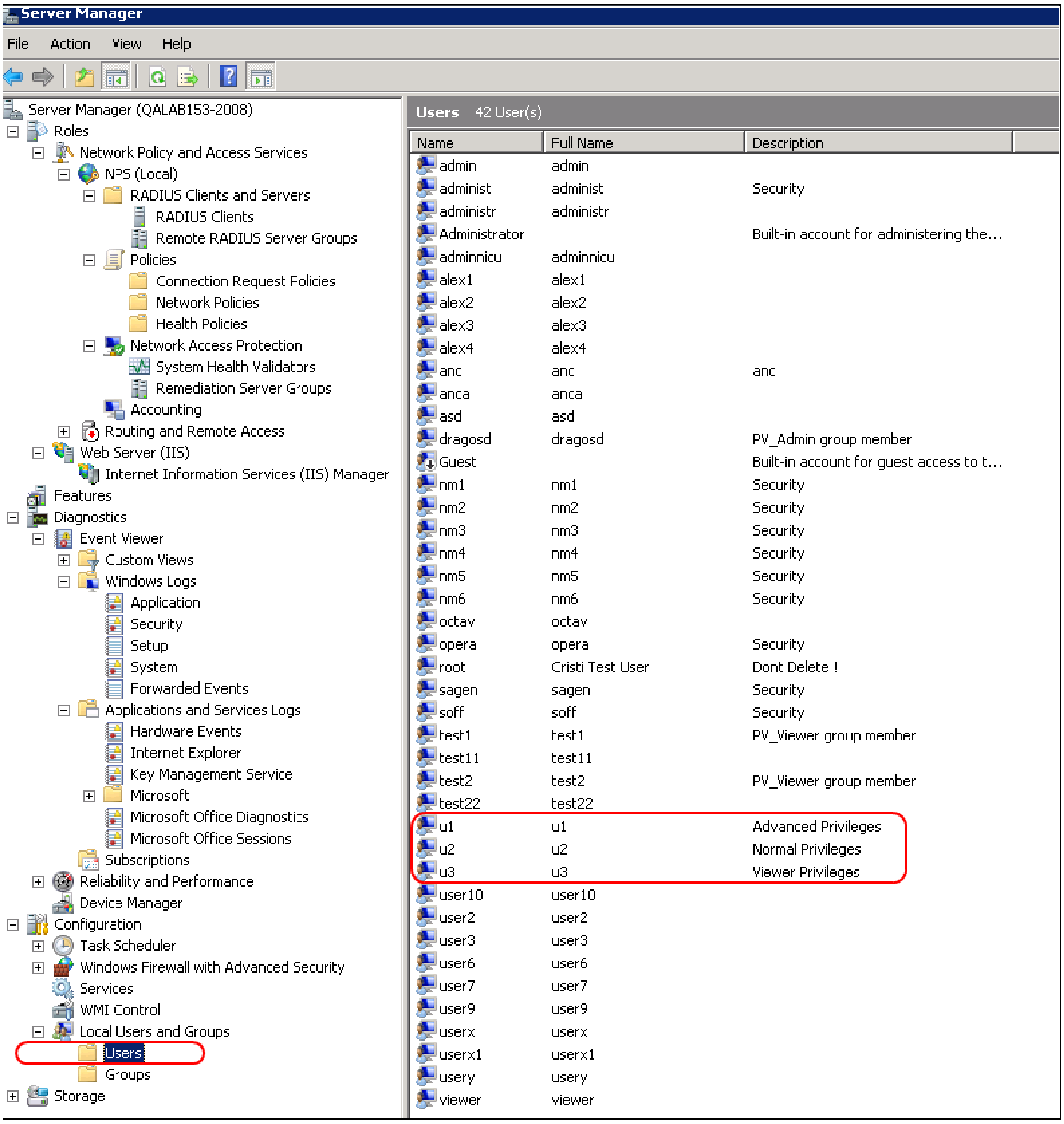
Groups 42 Group(s)

Name	Description
Administrators	Administrators have complete and u...
Backup Operators	Backup Operators can override secu...
Certificate Service DCO...	Members of this group are allowed t...
Cryptographic Operators	Members are authorized to perform ...
Distributed COM Users	Members are allowed to launch, acti...
Event Log Readers	Members of this group can read eve...
Guests	Guests have the same access as me...
IIS_IUSRS	Built-in group used by Internet Infor...
Network Configuration ...	Members in this group can have som...
Performance Log Users	Members of this group may schedule...
Performance Monitor U...	Members of this group can access p...
Power Users	Power Users are included for backw...
Print Operators	Members can administer domain prin...
Remote Desktop Users	Members in this group are granted t...
Replicator	Supports file replication in a domain
Users	Users are prevented from making ac...
ConfigMgr Remote Con...	Members in this group can view and ...
Debugger Users	Debugger Users are non administrat...
FT1	
Ft2	
FT3	
Group1	
NetmasterAdmin	Cristi Test Group, Dont delete.
NM_viewer	
Operators	Security
PV_Admin	
PV_Admin_Sergiu	
PV_Test	
PV_Viewer	
PV_Viewer_Sergiu	
Radius Test1	Security
Radius Test2	Security
Radius Test3	Security
Radius Test4	Security
Radius_Advanced	Test V&V
Radius_Normal	Test V&V
Radius_Viewer	Test V&V
RAS-Group	
Security Officers	Security
SNMP Agent	Security
TelnetClients	Members of this group have access t...
testing	

2 Create three users:

- u1
- u2
- u3

Figure 213: Server Manager – Creating Users



Name	Full Name	Description
admin	admin	
administ	administ	Security
administr	administr	
Administrator		Built-in account for administering the...
adminnicu	adminnicu	
alex1	alex1	
alex2	alex2	
alex3	alex3	
alex4	alex4	
anc	anc	anc
anca	anca	
asd	asd	
dragosd	dragosd	PV_Admin group member
Guest		Built-in account for guest access to t...
nm1	nm1	Security
nm2	nm2	Security
nm3	nm3	Security
nm4	nm4	Security
nm5	nm5	Security
nm6	nm6	Security
octav	octav	
opera	opera	Security
root	Cristi Test User	Dont Delete !
sagen	sagen	Security
soff	soff	Security
test1	test1	PV_Viewer group member
test11	test11	
test2	test2	PV_Viewer group member
test22	test22	
u1	u1	Advanced Privileges
u2	u2	Normal Privileges
u3	u3	Viewer Privileges
user10	user10	
user2	user2	
user3	user3	
user6	user6	
user7	user7	
user9	user9	
userx	userx	
userx1	userx1	
usery	usery	
viewer	viewer	

3 Attach each user to a group, as follows:

- Attach u1 to Radius_Advanced
- Attach u2 to Radius_Normal
- Attach u3 to Radius_Viewer

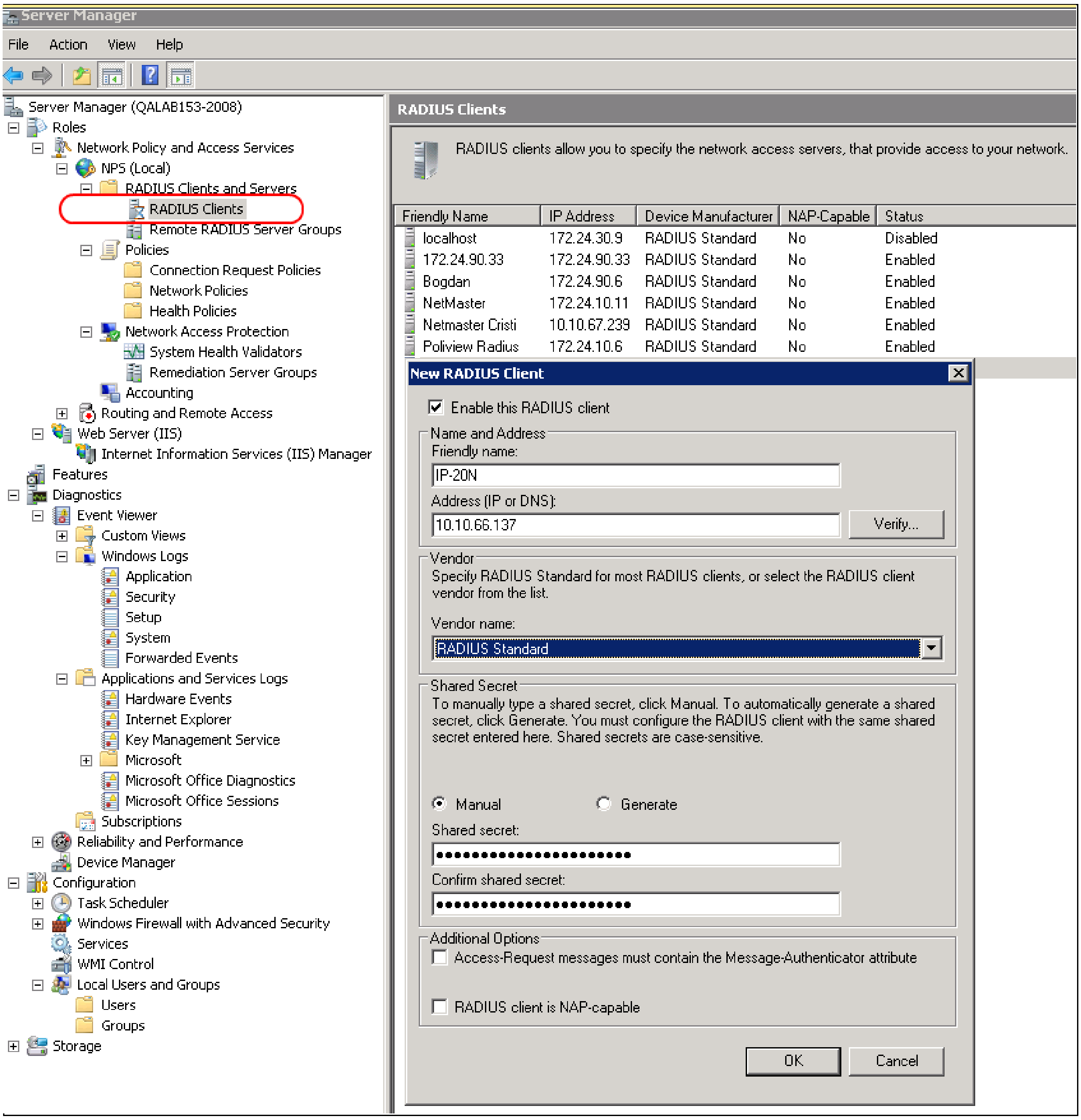
Step 2 – Creating a RADIUS Client

Define the NS Primo/Diplo 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 214: Server Manager – Creating a RADIUS Client



Server Manager

File Action View Help

Server Manager (QALAB153-2008)
- Roles
  - Network Policy and Access Services
    - NPS (Local)
      - RADIUS Clients and Servers
        - RADIUS Clients
        - Remote RADIUS Server Groups
      - Policies
        - Connection Request Policies
        - Network Policies
        - Health Policies
      - Network Access Protection
        - System Health Validators
        - Remediation Server Groups
      - Accounting
    - Routing and Remote Access
  - Web Server (IIS)
    - Internet Information Services (IIS) Manager
- Features
- Diagnostics
  - Event Viewer
    - Custom Views
    - Windows Logs
      - Application
      - Security
      - Setup
      - System
      - Forwarded Events
    - Applications and Services Logs
      - Hardware Events
      - Internet Explorer
      - Key Management Service
      - Microsoft
      - Microsoft Office Diagnostics
      - Microsoft Office Sessions
    - Subscriptions
  - Reliability and Performance
  - Device Manager
- Configuration
  - Task Scheduler
  - Windows Firewall with Advanced Security
  - Services
  - WMI Control
  - Local Users and Groups
    - Users
    - Groups
- Storage

RADIUS Clients

RADIUS clients allow you to specify the network access servers, that provide access to your network.

Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
localhost	172.24.30.9	RADIUS Standard	No	Disabled
172.24.90.33	172.24.90.33	RADIUS Standard	No	Enabled
Bogdan	172.24.90.6	RADIUS Standard	No	Enabled
NetMaster	172.24.10.11	RADIUS Standard	No	Enabled
Netmaster Cristi	10.10.67.239	RADIUS Standard	No	Enabled
Poliview Radius	172.24.10.6	RADIUS Standard	No	Enabled

New RADIUS Client

☑ Enable this RADIUS client

Name and Address

Friendly name: IP-20N

Address (IP or DNS): 10.10.66.137

Vendor

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name: RADIUS Standard

Shared Secret

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••••••••••••••••••••

Confirm shared secret: ••••••••••••••••••••••

Additional Options

□ Access-Request messages must contain the Message-Authenticator attribute

□ RADIUS client is NAP-capable

3 In the New RADIUS Client window:

i Select the **Enable this RADIUS client** check box.

ii Enter a descriptive **Friendly name** for the device, such as `NS Primo/DiploX`.

iii Enter the device IP **Address**.

iv Select **RADIUS Standard** as the **Vendor name**.

- In the **Shared Secret** section, select **Manual**, and enter a **Shared secret**, then enter it again in **Confirm shared secret**. Note down the secret because you will need to enter the same value in the **Secret** field of the Radius Configuration – Edit page (*Figure 209*).

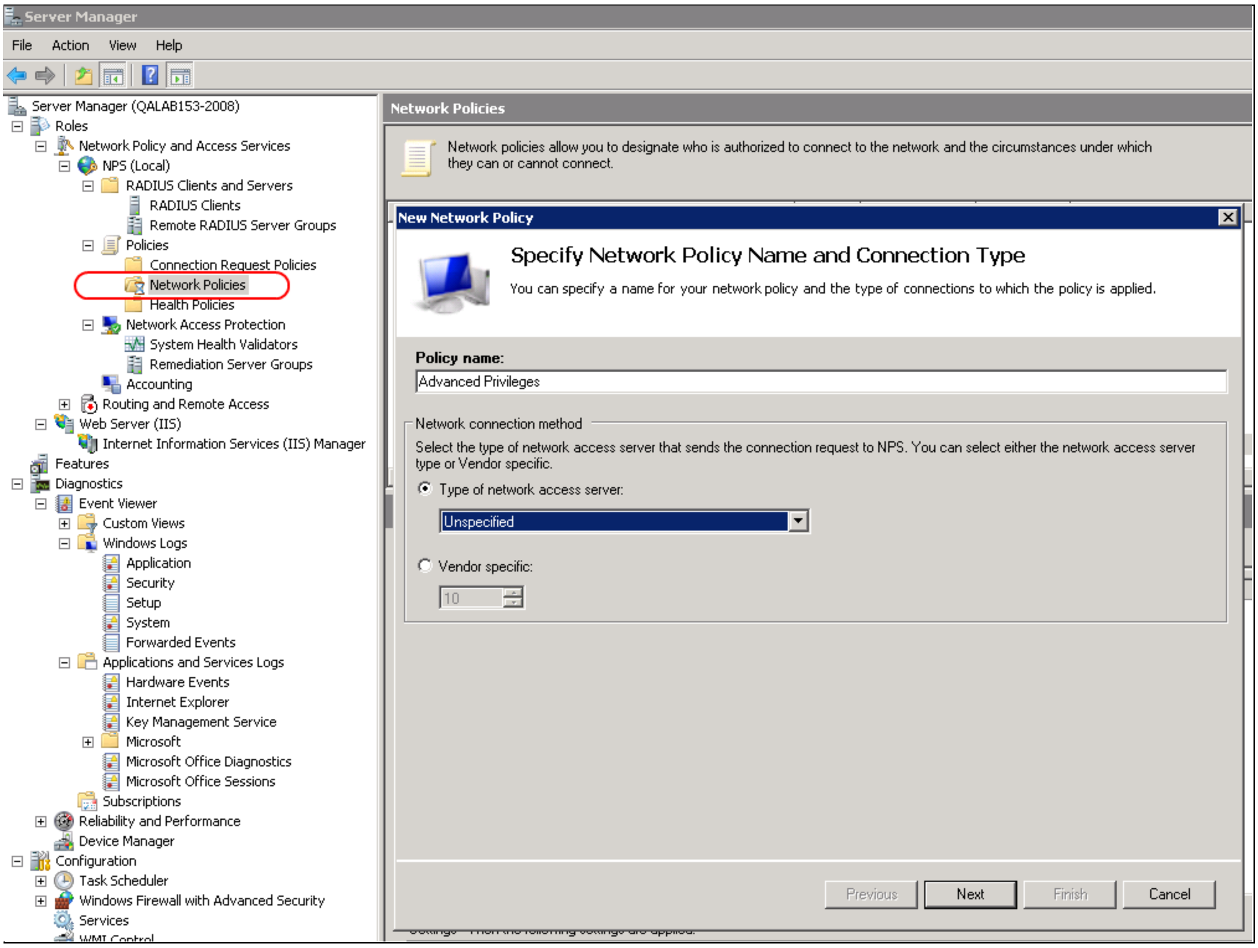
Step 3 – Creating a Network Policy

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 215: Create Network Policy – Specify Name and Connection Type



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name: Advanced Privileges

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.

● Type of network access server: Unspecified

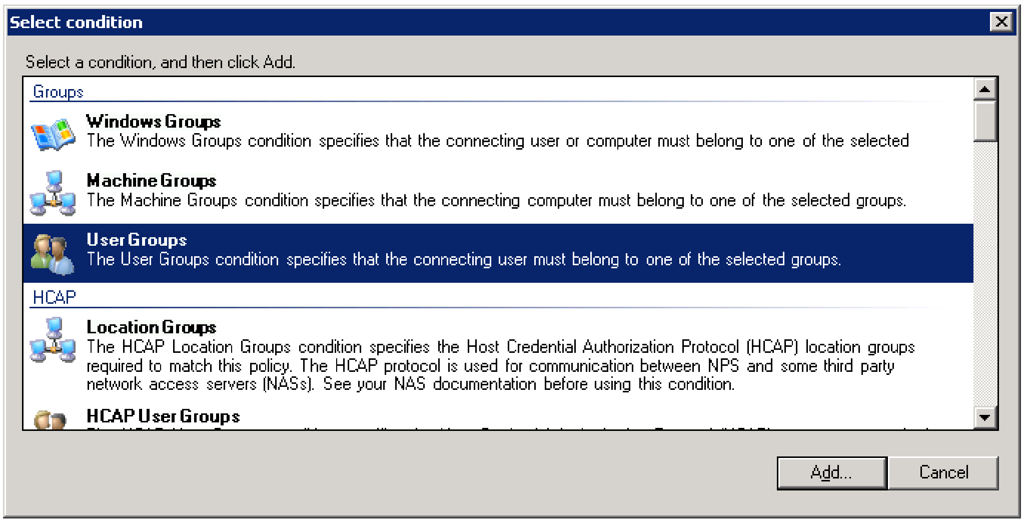
○ Vendor specific: 10

4 Click **Next**.

5 In the Specify Conditions window, click **Add.**

6 In the Select Condition window that appears, select the **User Groups** condition and click **Add**.

Figure 216: Create Network Policy – Select Condition



Select condition

Select a condition, and then click Add.

Groups

Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected

Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.

User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

HCAP

Location Groups
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.

HCAP User Groups

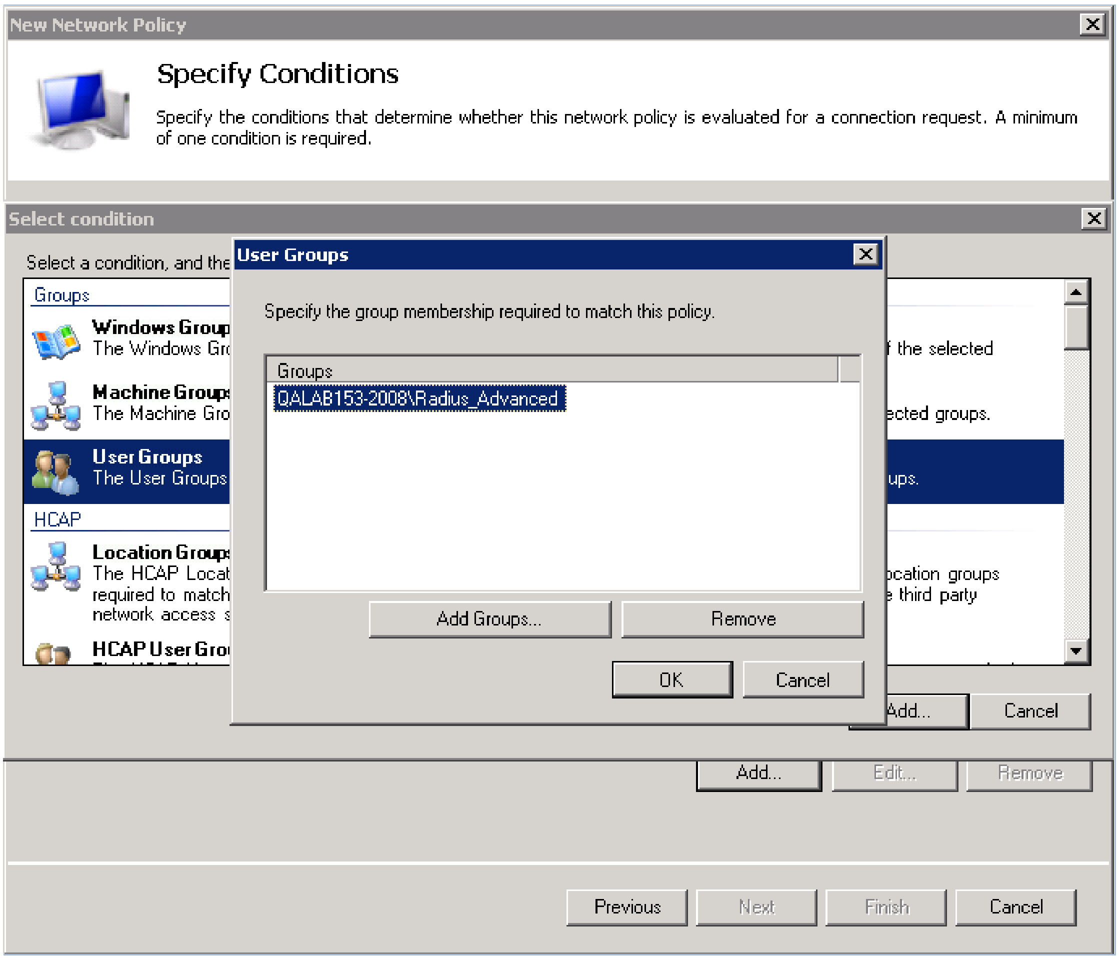
7 In the User Groups window that appears, click **Add Groups**.

8 In the Select Group window that appears, click **Advanced**.

9 In the Select Group window that appears, click **Find Now** to list all groups, and then select the appropriate group from the list: Radius_Advanced, Radius_Normal, or Radius_Viewer.

10 Click **OK**.

Figure 217: Create Network Policy – User Group added to Policy's Conditions



New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Select condition

User Groups

Specify the group membership required to match this policy.

Groups

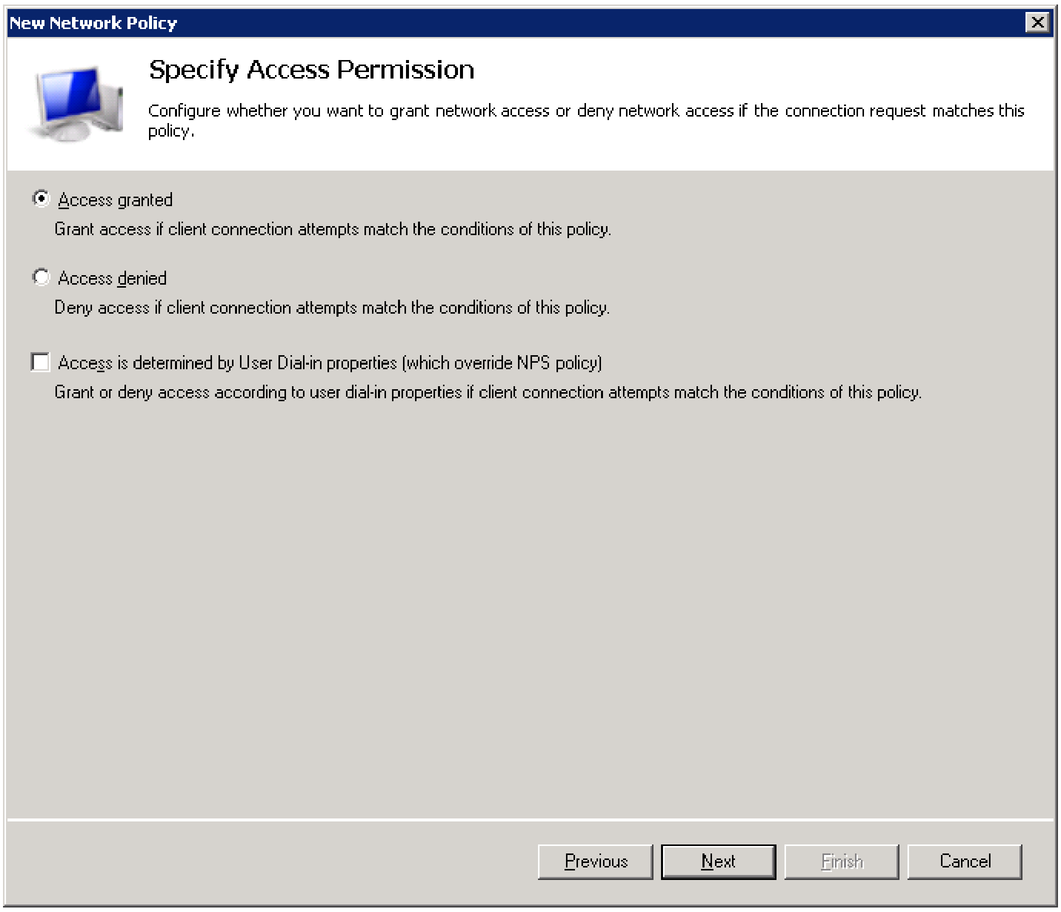
QALAB153-2008\Radius_Advanced

11 Click **OK** to save settings.

12 Click **Next**.

13 In the Specify Access Permission window that appears, select the **Access Granted** option.

Figure 218: Create Network Policy – Specifying Access Permission



New Network Policy

Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

● Access granted
Grant access if client connection attempts match the conditions of this policy.

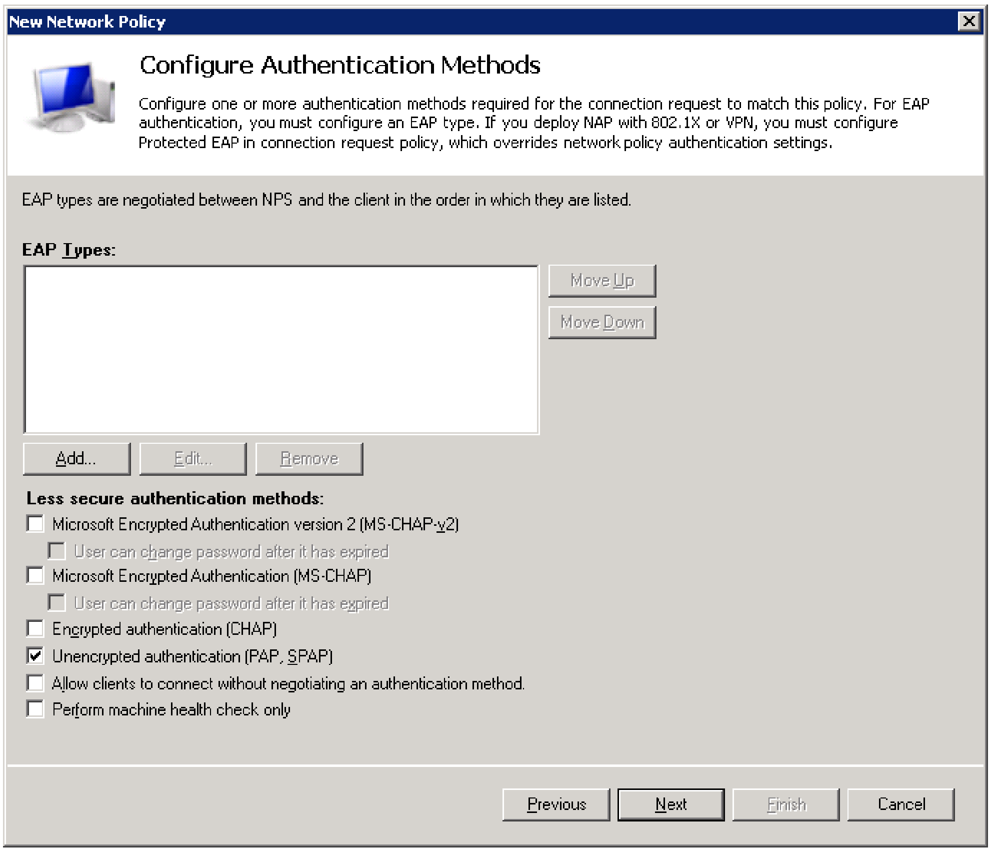
○ Access denied
Deny access if client connection attempts match the conditions of this policy.

□ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

14 Click **Next**.

15 In the Configure Authentication Methods window that appears, make sure only the **Unencrypted Authentication (PAP, SPAP)** option is selected.

Figure 219: Create Network Policy – Configuring Authentication Methods



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Less secure authentication methods:

□ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

□ User can change password after it has expired

□ Microsoft Encrypted Authentication (MS-CHAP)

□ User can change password after it has expired

□ Encrypted authentication (CHAP)

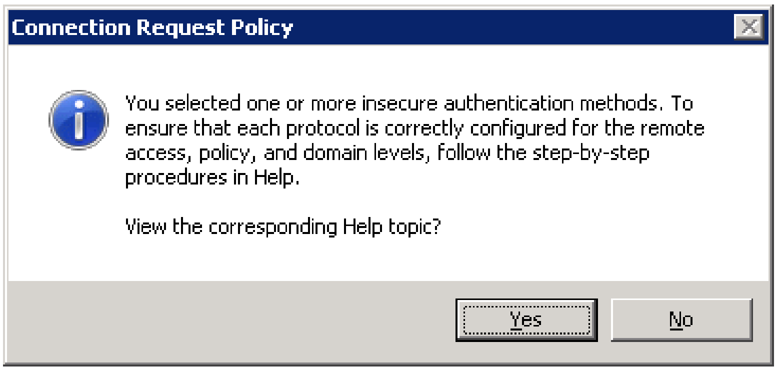
☑ Unencrypted authentication (PAP, SPAP)

□ Allow clients to connect without negotiating an authentication method.

□ Perform machine health check only

16 In the query window that appears, click **No**.

Figure 220: Create Network Policy – Insecure Authentication Method Query



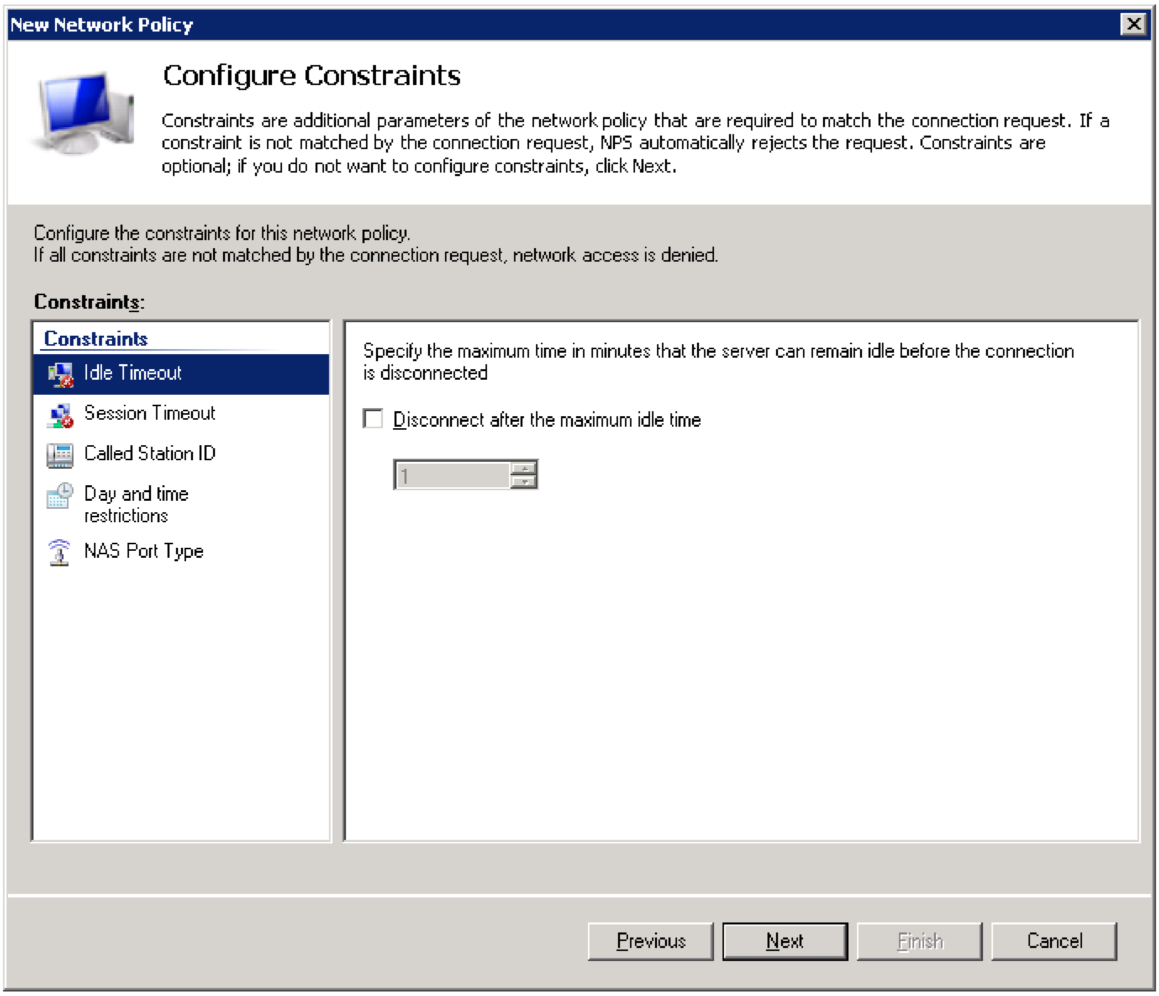
Connection Request Policy

You selected one or more insecure authentication methods. To ensure that each protocol is correctly configured for the remote access, policy, and domain levels, follow the step-by-step procedures in Help.

View the corresponding Help topic?

17 In the Configure Constraints window that appears, click **Next**.

Figure 221: Create Network Policy – Configuring Constraints



New Network Policy

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

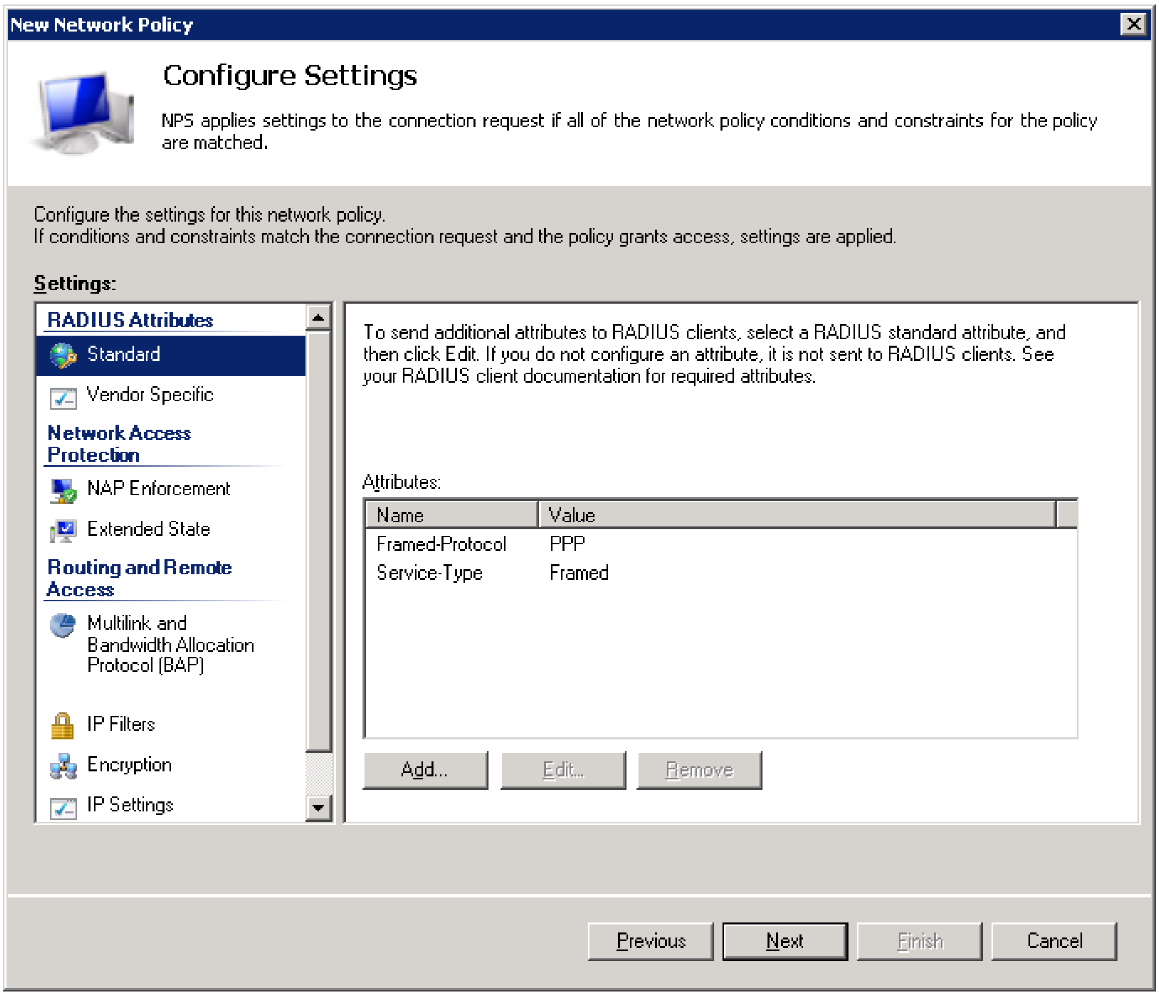
□ Disconnect after the maximum idle time

1

18 In the Configure Settings window that appears:

i Remove all **Standard** RADIUS attributes. Make sure the Attributes table is empty.

Figure 222: Create Network Policy – Configuring Settings



New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

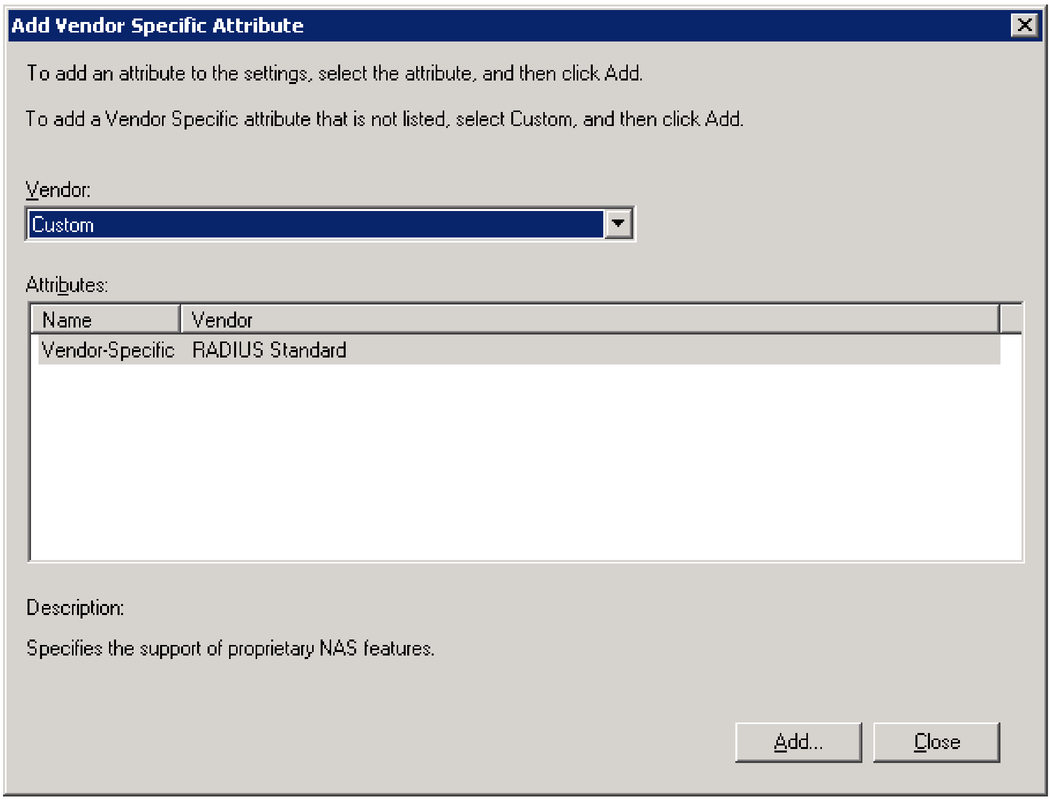
ii Select the **Vendor Specific** checkbox and click **Add** under the Attributes table.

19 In the Add Vendor Specific Attribute window that appears:

i Select **Custom** in the **Vendor** drop down field.

ii Click **Add**.

Figure 223: Create Network Policy – Adding Vendor Specific Attributes



Add Vendor Specific Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.

Vendor: Custom

Attributes:

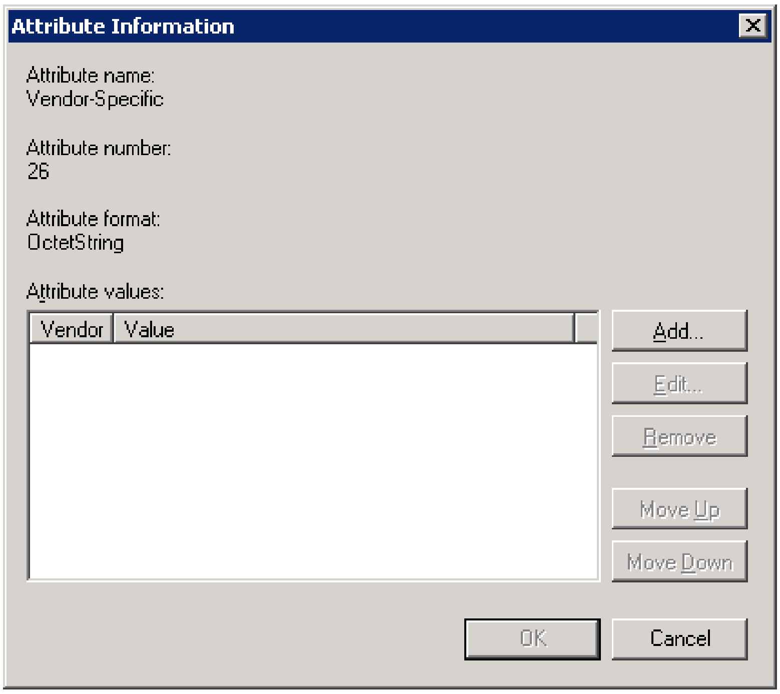
Name	Vendor
Vendor-Specific	RADIUS Standard

Description:

Specifies the support of proprietary NAS features.

20 In the Attribute Information window that appears, click **Add**.

Figure 224: Create Network Policy – Selecting to Add Attribute Information



Attribute Information

Attribute name:
Vendor-Specific

Attribute number:
26

Attribute format:
OctetString

Attribute values:

Vendor	Value

21 In the Vendor-Specific Attribute Information window that appears:

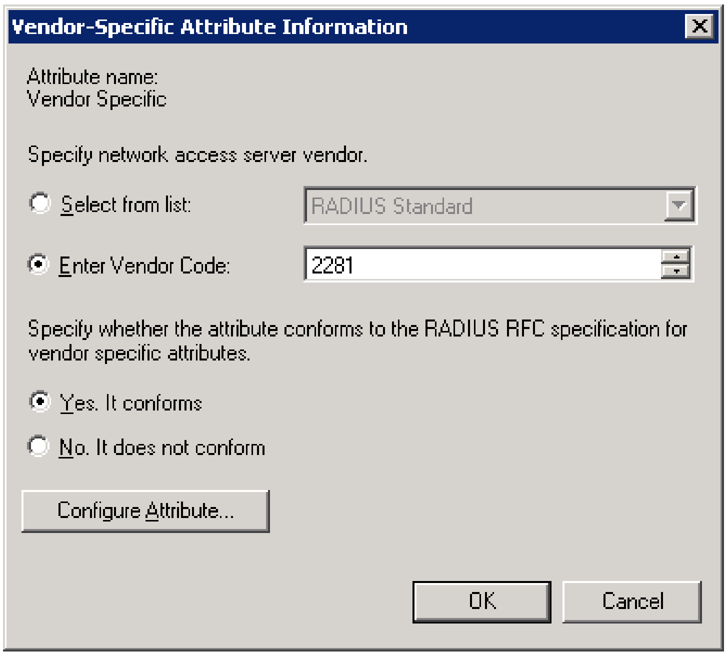
i Select **Enter Vendor Code**.

ii Enter **2281** in the **Enter Vendor Code** field.

iii Select the option **Yes. It conforms**.

iv Click **Configure Attribute**.

Figure 225: Create Network Policy – Specifying the Vendor



Vendor-Specific Attribute Information

Attribute name:
Vendor Specific

Specify network access server vendor.

○ Select from list: RADIUS Standard

● Enter Vendor Code: 2281

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

● Yes. It conforms

○ No. It does not conform

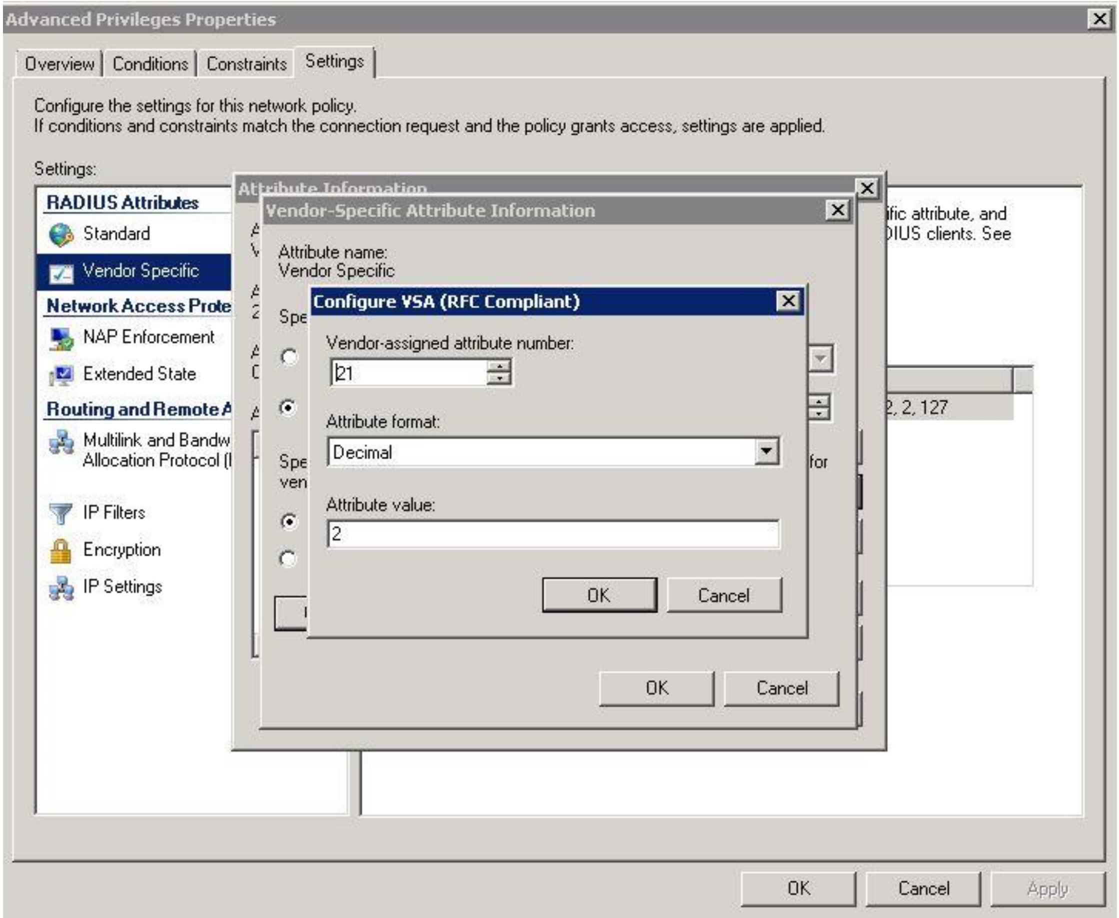
22 In the Configure VSA (RFC Compliant) window that appears, configure 13 attributes as follows:

i For **Vendor-assigned attribute number** from 21 till 32, select **Decimal** in the **Attribute format** field. These twelve attributes define the Read access level (None, Regular, or Advanced), and the Write access level (None, Regular, or Advanced) for each of the six functional groups (Ethernet, Management, Radio, Security, Sync, TDM). Therefore, in the **Attribute value** field enter the value corresponding to the access level you wish to permit to members of the group whose policy you are configuring, where:

- **2** = Advanced
- **1** = Regular
- **0** = None

Thus for example, enter **2** for all twelve attributes if you are configuring a policy for the Radius_Advanced group. This gives Advanced read permissions and Advanced write permissions, for all six functional groups, to the members of the Radius_Advanced group.

Figure 226: Create Network Policy – Configuring Vendor-Specific Attribute Information



Configure VSA (RFC Compliant)

Vendor-assigned attribute number: 21

Attribute format: Decimal

Attribute value: 2

Advanced Privileges Properties
Overview
Conditions
Constraints
Settings
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 Prote
NAP Enforcement
Extended State
Routing and Remote A
Multilink and Bandw Allocation Protocol (I
IP Filters
Encryption
IP Settings
Attribute Information
Vendor-Specific Attribute Information
Attribute name:
Vendor Specific
OK
Cancel
Apply

ii For **Vendor-assigned attribute number** 50, select **Decimal** in the **Attribute format** field. The **Attribute value** of this attribute defines the access channel(s) permitted to members of the group whose policy you are configuring. The **Attribute value** is the sum of the values corresponding to the access channels you wish to permit, where the value for each access channel is:

- none=0
- serial=1
- telnet=2
- ssh=4
- web=8
- nms=16
- snmp=32
- snmpV3=64

Thus for example, enter **127** to allow access from all channels:
Serial + Telnet + SSH + Web + NMS + SNMP +SNMPv3;

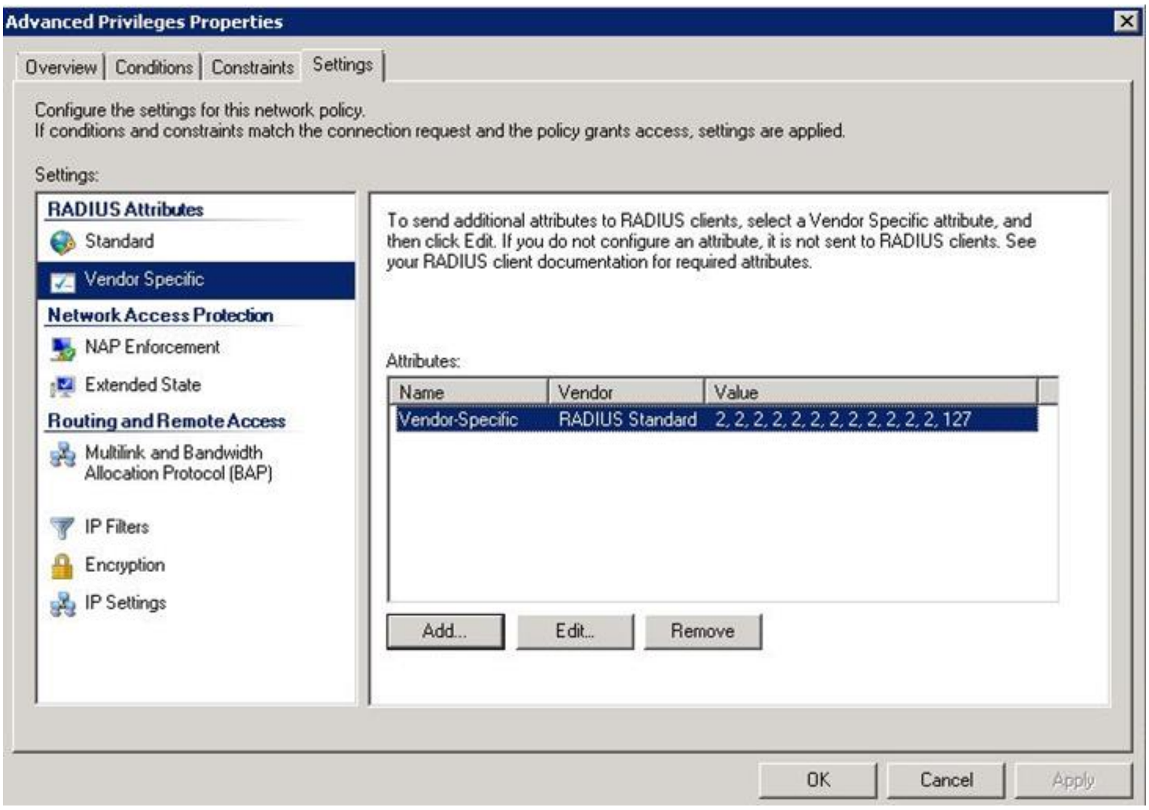
Or enter **24** to allow access only from NMS + SNMP channels.

iii Click **OK**.

23 Click **OK**.

The following figure shows the Attributes table for the Radius_Advanced group, where access to the device is allowed from all channels.

Figure 227: Create Network Policy – Example of Vendor-Specific Attribute Configuration



Advanced Privileges Properties

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
Vendor-Specific	RADIUS Standard	2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 127

24 Close all opened windows and click **Next**.

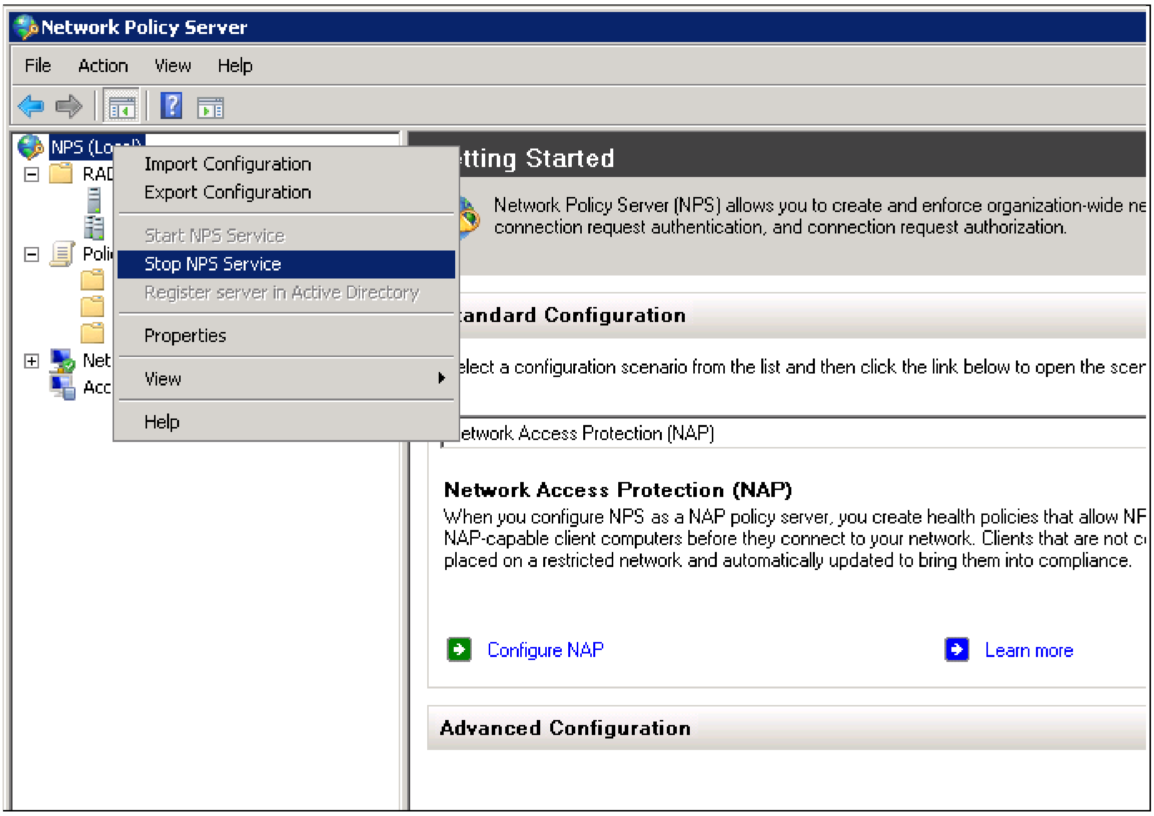
25 In the Completing New Network Policy window, click **Finish**.

26 Reset the Network Policy Server (NPS) by stopping and starting the NPS service as follows:

i Right click the **NPS (Local)** node, and select **Stop NPS Service**.

ii Right click the **NPS (Local)** node, and select **Start NPS Service**.

Figure 228: Create Network Policy – Stopping/Starting NPS Services


Network Policy Server
File Action View Help
NPS (Local)
RAD
Poli
Net
Acc
Import Configuration
Export Configuration
Start NPS Service
Stop NPS Service
Register server in Active Directory
Properties
View
Help
tting Started
Network Policy Server (NPS) allows you to create and enforce organization-wide ne
connection request authentication, and connection request authorization.
andard Configuration
elect a configuration scenario from the list and then click the link below to open the scer
etwork Access Protection (NAP)
Network Access Protection (NAP)
When you configure NPS as a NAP policy server, you create health policies that allow NF
NAP-capable client computers before they connect to your network. Clients that are not c
placed on a restricted network and automatically updated to bring them into compliance.
Configure NAP
Learn more
Advanced Configuration

10.5.5.2. Configuring a Linux FreeRADIUS Server

The following sub-sections describe how to configure a Linux FreeRADIUS server to work with an NS Primo/Diplo device.

To so do, you will need to modify the following three files:

- /etc/raddb/users
- /etc/raddb/clients.conf
- /usr/share/freeradius/dictionary.Netronics

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.Netronics` 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.Netronics` file.

Step 3 – Specifying the RADIUS client

This step describes how to define a device as a RADIUS client. The RADIUS server accepts attempts to connect to a device only if that is device is defined as a RADIUS client.

To define a device as a RADIUS client:

1 In the `/etc/raddb/clients.conf` file, add the device according to the following example.

The example shows how to add an NS Primo/Diplo device with IP address 192.168.1.118:

```
# NSPrimoDiplo
client 192.168.1.118 {
        secret          = default_not_applicable
        shortname       = NSPrimoDiplo
}
```

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 209*).
- 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 &`

10.6. Configuring X.509 CSR Certificates and HTTPS

The web interface protocol for accessing NS Primo/Diplo 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 NS Primo/Diplo 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 NS Primo/Diplo 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

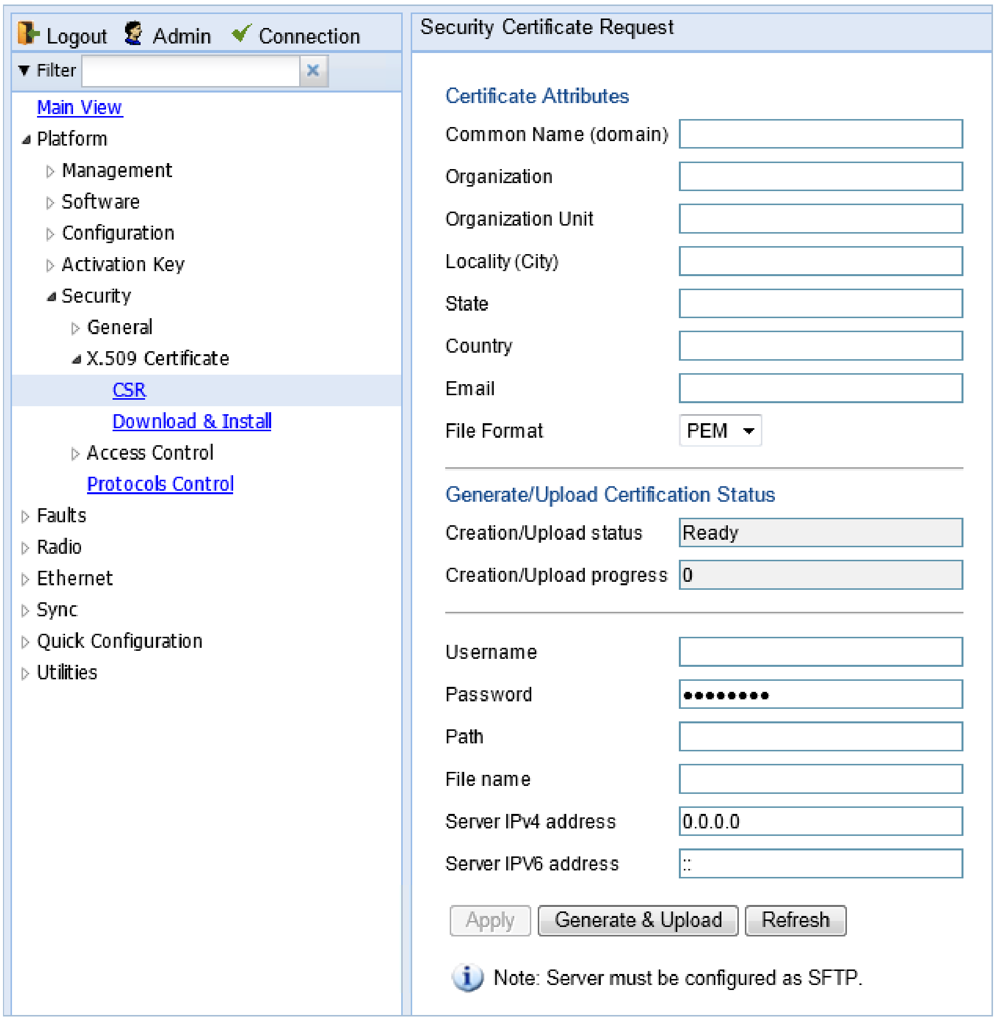
For these operations, SFTP must be used.

10.6.1. 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 229: Security Certificate Request Page



Security Certificate Request

Certificate Attributes

Common Name (domain)	
Organization	
Organization Unit	
Locality (City)	
State	
Country	
Email	
File Format	PEM

Generate/Upload Certification Status

Creation/Upload status	Ready
Creation/Upload progress	0

Username	
Password	••••••••
Path	
File name	
Server IPv4 address	0.0.0.0
Server IPV6 address	::

Note: Server must be configured as SFTP.

2 In the **Common Name** field, enter the fully–qualified domain name for your web server. You must enter the exact domain name.

3 In the **Organization** field, enter the exact legal name of your organization. Do not abbreviate.

4 In the **Organization Unit** field, enter the division of the organization that handles the certificate.

5 In the **Locality** field, enter the city in which the organization is legally located.

6 In the **State** field, enter the state, province, or region in which the organization is located. Do not abbreviate.

7 In the **Country** field, enter the two-letter ISO abbreviation for your country (e.g., US).

8 In the **Email** field, enter an e-mail address that can be used to contact your organization.

9 In the **File Format** field, select **PEM** or **DER** to determine the file format.

Note

In this version, only PEM is supported.

10 In the **Username** field, enter the user name you configured in the SFTP server.

11 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.
12 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. To leave the path blank, enter //.
13 In the **File Name** field, enter the name you want to give to the exported CSR.
14 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*.
15 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*.
16 Click **Apply** to save your settings.
17 Click **Generate & Upload**. The file is generated and uploaded.

The **Creation/Upload status** field displays the status of any pending CSR generation and upload. Possible values are:

- **Ready** – The default value, which appears when CSR generation and upload is in progress.
- **File-in-transfer** – The upload operation is in progress.
- **Success** – The file has been successfully uploaded.
- **Failure** – The file was not successfully uploaded.

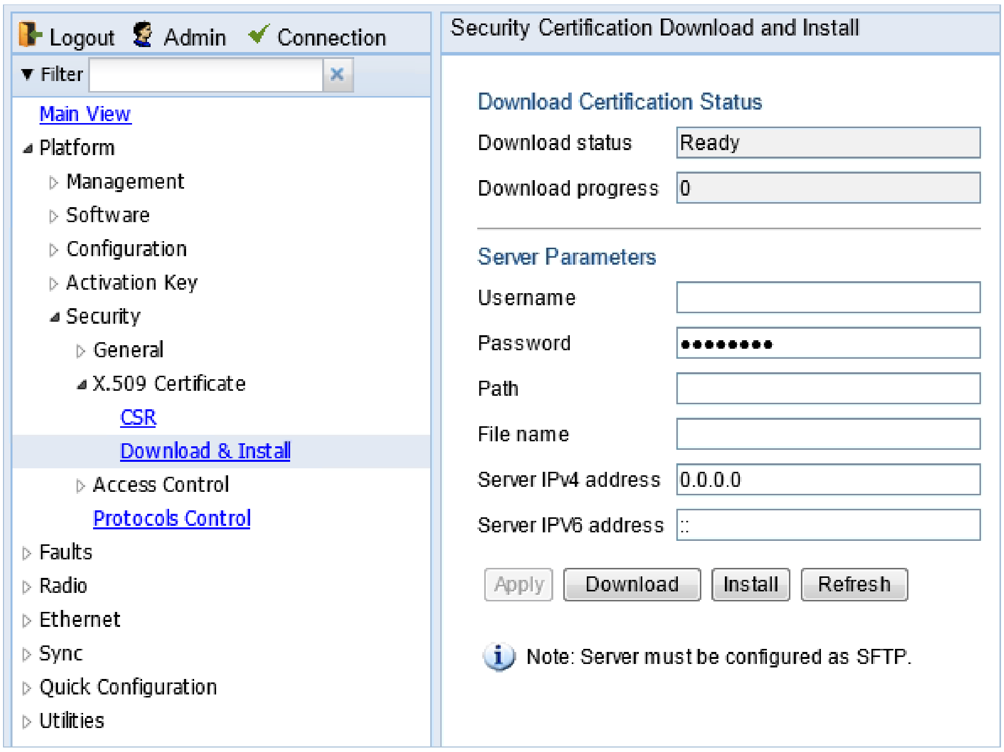
The **Creation/Upload progress** field displays the progress of any current CSR upload operation.

10.6.2. Downloading a Certificate

To download a certificate:

1 Select **Platform > Security > X.509 Certificate > Download & Install**. The Security Certification Download and Install page opens.

Figure 230: Security Certification Download and Install Page



Security Certification Download and Install

Download Certification Status

Download status: Ready

Download progress: 0

Server Parameters

Username:

Password: ●●●●●●●●

Path:

File name:

Server IPv4 address: 0.0.0.0

Server IPV6 address: ::

Note: Server must be configured as SFTP.

2 In the **Username** field, enter the user name you configured in the SFTP server.

3 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.

4 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. To leave the path blank, enter //.

5 In the **File Name** field, enter the certificate's file name in the SFTP server.

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 SFTP 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 SFTP server in the **Server IPv6 address** field. See *Defining the IP Protocol Version for Initiating Communications*.

8 Click **Apply** to save your settings.

9 Click **Download**. The certificate is downloaded.

10 Click **Install**. The certificate is installed on the NS Primo/Diplo.

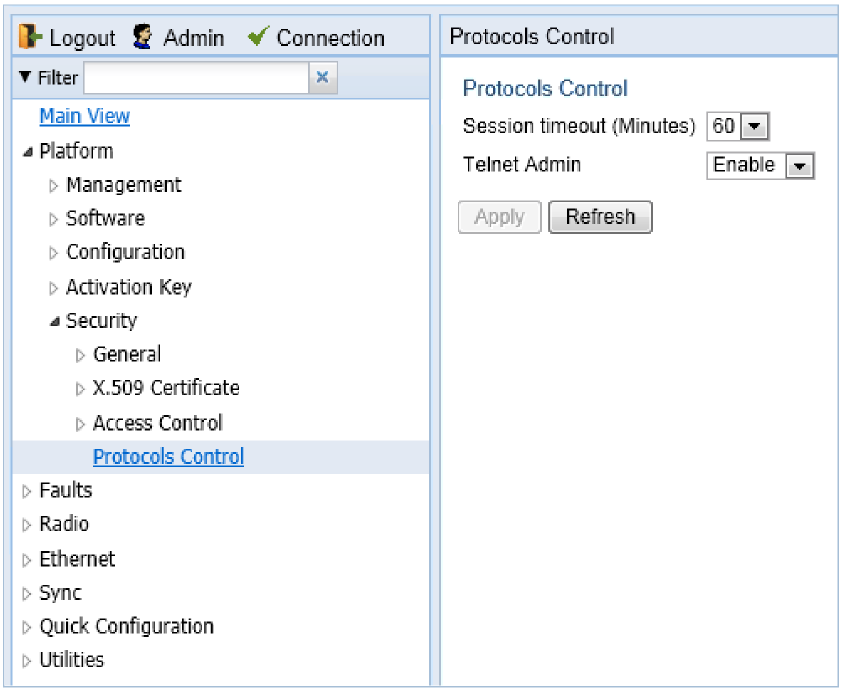
10.7. Blocking Telnet Access

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 231: Protocols Control Page



Protocols Control

Session timeout (Minutes) 60

Telnet Admin Enable

2 In the **Telnet Admin** field, select **Disable** to block telnet access. By default, telnet access is enabled (**Enable**).

3 Click **Apply**.

10.8. 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.

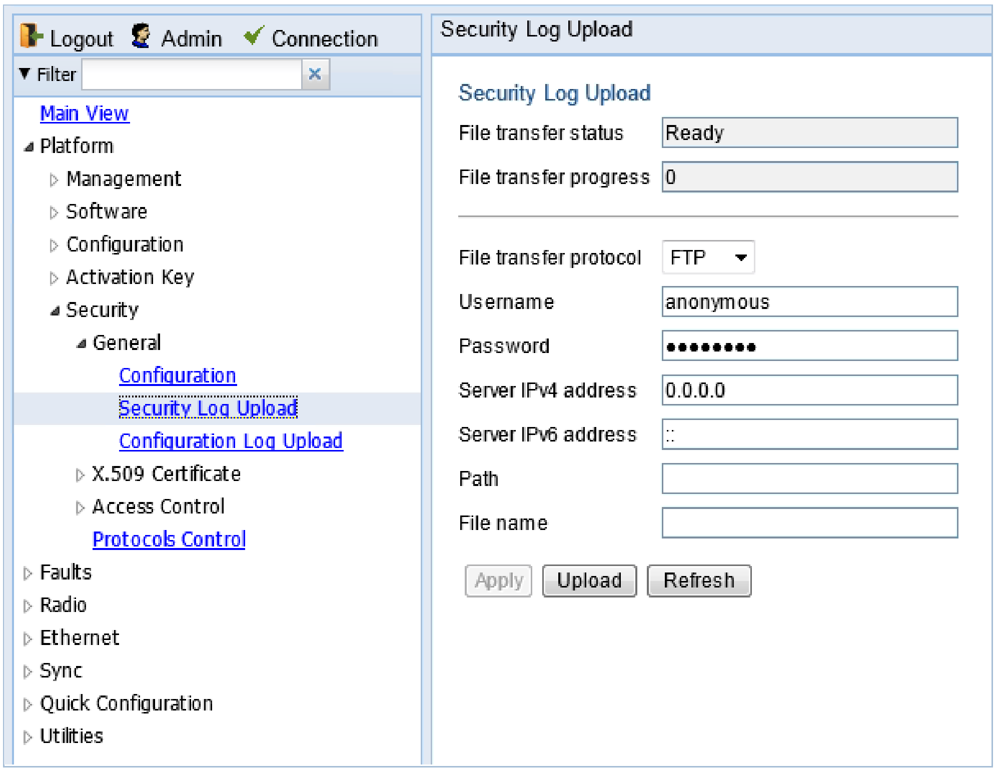
When uploading the security log, the NS Primo/Diplo functions as an FTP or SFTP client. You must install FTP or SFTP server software on the PC or laptop you are using to perform the import or export. For details, see *Installing and Configuring an FTP or SFTP Server*.

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 232: Security Log Upload Page



Security Log Upload

File transfer status: Ready

File transfer progress: 0

File transfer protocol: FTP

Username: anonymous

Password: ••••••••

Server IPv4 address: 0.0.0.0

Server IPv6 address: ::

Path:

File name:

3 In the **Protocol Type** field, select the file transfer protocol you want to use (**FTP** or **SFTP**).

4 In the **Server username** field, enter the user name you configured in the FTP server.

5 In the **Server 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. To leave the path blank, enter //.

9 In the **File Name** field, enter the name you want to give to the exported security log.

10 Click **Apply** to save your settings.

11 Click **Upload**. The upload begins.

The **File transfer status** field displays the status of any pending security log upload. Possible values are:

- **Ready** – The default value, which appears when no file transfer is in progress.
- **File-in-transfer** – The upload operation is in progress.

- **Success** – The file has been successfully uploaded.
- **Failure** – The file was not successfully uploaded.

The **File transfer progress** field displays the progress of any current security log upload operation.

10.9. 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.

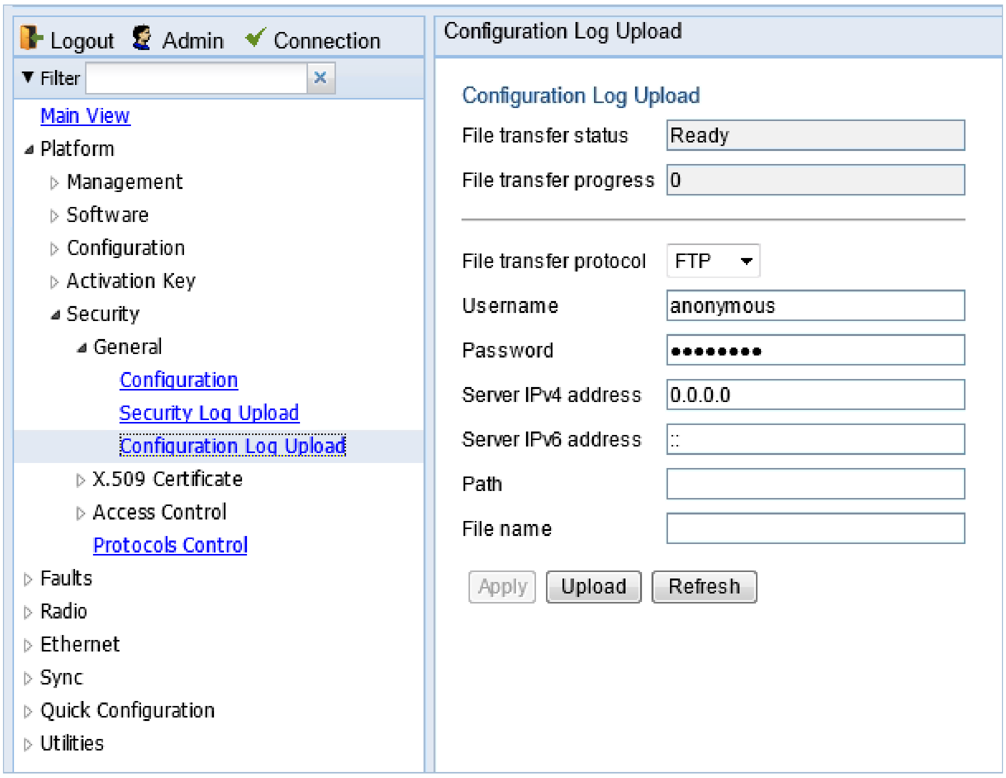
When uploading the configuration log, the NS Primo/Diplo functions as an FTP or SFTP client. You must install FTP or SFTP server software on the PC or laptop you are using to perform the upload. For details, see *Installing and Configuring an FTP or SFTP Server*.

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 Security Log Upload page opens.

Figure 233: Configuration Log Upload Page



Configuration Log Upload

File transfer status	Ready
File transfer progress	0
File transfer protocol	FTP
Username	anonymous
Password	••••••••
Server IPv4 address	0.0.0.0
Server IPv6 address	::
Path	
File name	

3 In the **File transfer protocol** field, select the file transfer protocol you want to use (**FTP** or **SFTP**).

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. To leave the path blank, enter //.

9 In the **File Name** field, enter the name you want to give to the exported configuration log.

Note

The directory path and fie name, together, cannot be more than:

If the IP address family is configured to be IPv4: 236 characters

If the IP address family is configured to be IPv6: 220 characters

10 Click **Apply** to save your settings.

11 Click **Upload**. The upload begins.

The **File transfer status** field displays the status of any pending configuration log upload. Possible values are:

- **Ready** – The default value, which appears when no file transfer is in progress.
- **File-in-transfer** – The upload operation is in progress.
- **Success** – The file has been successfully uploaded.
- **Failure** – The file was not successfully uploaded.

The **File transfer progress** field displays the progress of any current configuration log upload operation.

11. Alarm Management and Troubleshooting

This section includes:

- *Viewing Current Alarms*
- *Viewing the Event Log*
- *Editing Alarm Text and Severity*
- *Uploading Unit Info*
- *Performing Diagnostics*

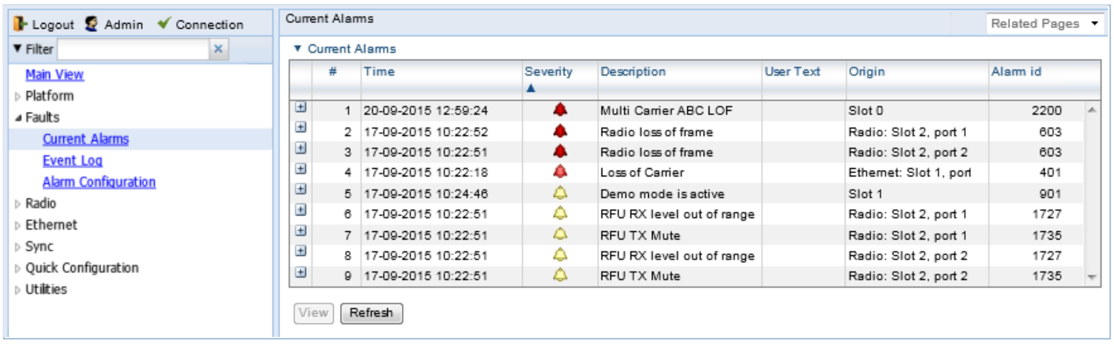
> ***Note:*** *CW mode, used* to transmit a single or dual frequency tones for debugging purposes, can be configured using the CLI. *See Working in CW Mode (Single or Dual Tone) (CLI).*

11.1. Viewing Current Alarms

To display a list of current alarms in the unit:

1 Select **Faults > Current Alarms**. The Current Alarms page opens. The Current Alarms page displays current alarms in the unit. Each row in the Current Alarms table describes an alarm and provides basic information about the alarm. For a description of the information provided in the Current Alarms page, see *Table 61: Alarm Information*.

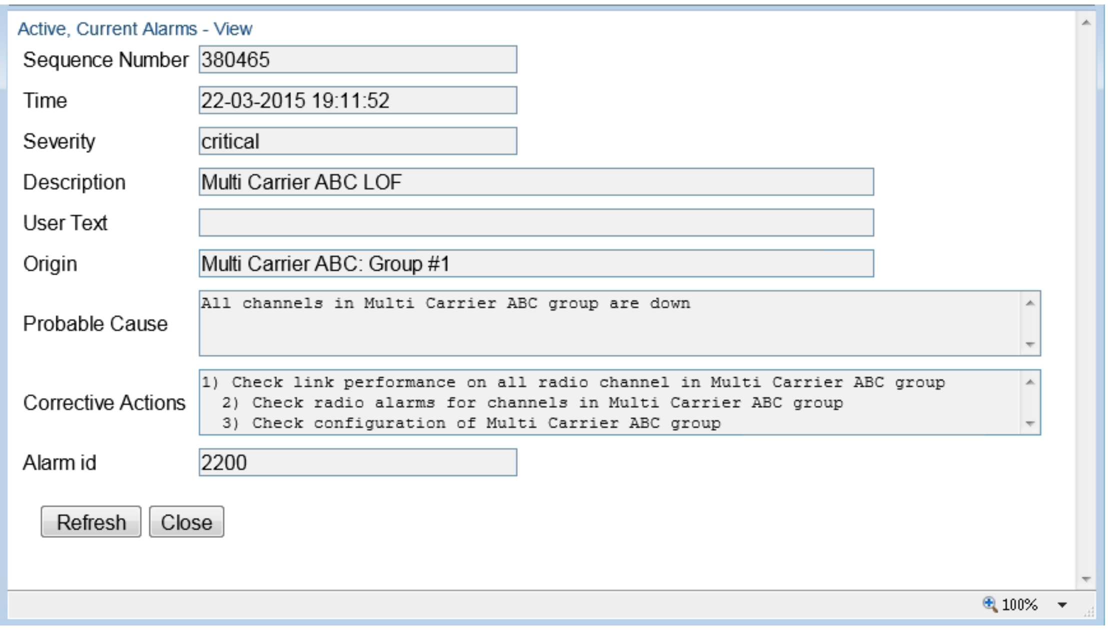
Figure 234: Current Alarms Page



	#	Time	Severity	Description	User Text	Origin	Alarm id
⊞	1	20-09-2015 12:59:24	🔴	Multi Carrier ABC LOF		Slot 0	2200
⊞	2	17-09-2015 10:22:52	🔴	Radio loss of frame		Radio: Slot 2, port 1	603
⊞	3	17-09-2015 10:22:51	🔴	Radio loss of frame		Radio: Slot 2, port 2	603
⊞	4	17-09-2015 10:22:18	🔴	Loss of Carrier		Ethernet: Slot 1, port	401
⊞	5	17-09-2015 10:24:46	🟡	Demo mode is active		Slot 1	901
⊞	6	17-09-2015 10:22:51	🟡	RFU RX level out of range		Radio: Slot 2, port 1	1727
⊞	7	17-09-2015 10:22:51	🟡	RFU TX Mute		Radio: Slot 2, port 1	1735
⊞	8	17-09-2015 10:22:51	🟡	RFU RX level out of range		Radio: Slot 2, port 2	1727
⊞	9	17-09-2015 10:22:51	🟡	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 235: Current Alarms - View Page



Active, Current Alarms - View

Sequence Number	380465
Time	22-03-2015 19:11:52
Severity	critical
Description	Multi Carrier ABC LOF
User Text	
Origin	Multi Carrier ABC: Group #1
Probable Cause	All channels in Multi Carrier ABC group are down
Corrective Actions	1) Check link performance on all radio channel in Multi Carrier ABC group 2) Check radio alarms for channels in Multi Carrier ABC group 3) Check configuration of Multi Carrier ABC group
Alarm id	2200

Table 61: Alarm Information

Parameter	Definition
Sequence Number (#)	A unique sequence number assigned to the alarm by the system.
Time	The date and time the alarm was triggered.
Severity	The severity of the alarm. In the Current Alarms table, the severity is indicated by a symbol. You can display a textual description of the severity by holding the cursor over the symbol. Note: You can edit the severity of alarm types in the Alarm Configuration page. See *Editing Alarm Text and Severity*.
Description	A system-defined description of the alarm.
User Text	Additional text that has been added to the system-defined description of the alarm by users. Note: You can add user text to alarms in the Alarm Configuration page. See *Editing Alarm Text and Severity*.
Origin	The module that generated the alarm.
Probable Cause	This field only appears in the Current Alarms - View page. One or more possible causes of the alarm, to be used for troubleshooting.
Corrective Actions	This field only appears in the Current Alarms - View page. One or more possible corrective actions to be taken in troubleshooting the alarm.
Alarm ID	A unique ID that identifies the alarm type.

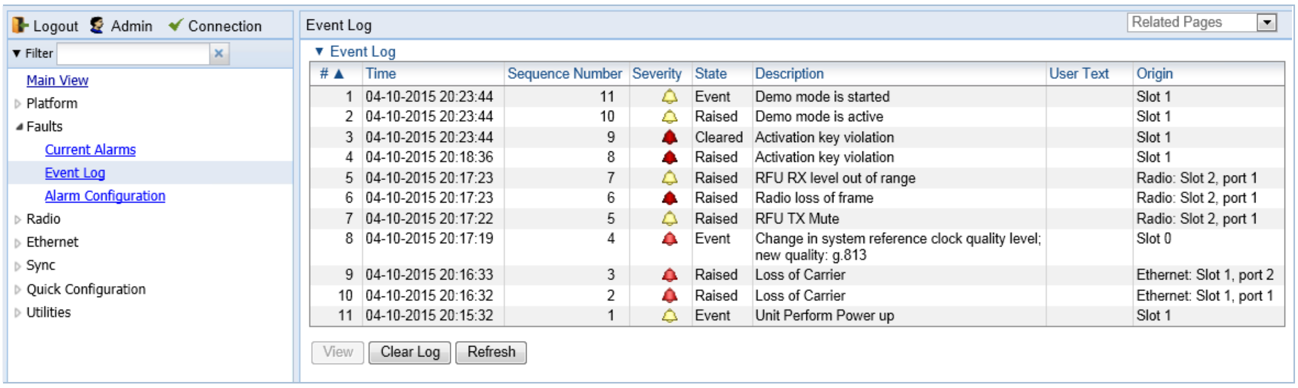
11.2. Viewing the Event Log

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 62: Event Log Information.*

Figure 236: Event Log



# ▲	Time	Sequence Number	Severity	State	Description	User Text	Origin
1	04-10-2015 20:23:44	11	🟨	Event	Demo mode is started		Slot 1
2	04-10-2015 20:23:44	10	🟨	Raised	Demo mode is active		Slot 1
3	04-10-2015 20:23:44	9	🟥	Cleared	Activation key violation		Slot 1
4	04-10-2015 20:18:36	8	🟥	Raised	Activation key violation		Slot 1
5	04-10-2015 20:17:23	7	🟨	Raised	RFU RX level out of range		Radio: Slot 2, port 1
6	04-10-2015 20:17:23	6	🟥	Raised	Radio loss of frame		Radio: Slot 2, port 1
7	04-10-2015 20:17:22	5	🟨	Raised	RFU TX Mute		Radio: Slot 2, port 1
8	04-10-2015 20:17:19	4	🟥	Event	Change in system reference clock quality level; new quality: g.813		Slot 0
9	04-10-2015 20:16:33	3	🟥	Raised	Loss of Carrier		Ethernet: Slot 1, port 2
10	04-10-2015 20:16:32	2	🟥	Raised	Loss of Carrier		Ethernet: Slot 1, port 1
11	04-10-2015 20:15:32	1	🟨	Event	Unit Perform Power up		Slot 1

Table 62: Event Log Information

Parameter	Definition
Time	The date and time the event was triggered.
Sequence Number (#)	A unique sequence number assigned to the event by the system.
Severity	The severity of the event. In the Event Log table, the severity is indicated by a symbol. You can display a textual description of the severity by holding the cursor over the symbol. Note You can edit the severity of event types in the Alarm Configuration page. See *Editing Alarm Text and Severity*.
State	Indicates whether the event is currently raised or has been cleared.
Description	A system-defined description of the event.
User Text	Additional text that has been added to the system-defined description of the event by users. Note You can add user text to events in the Alarm Configuration page. See *Editing Alarm Text and Severity*.
Origin	The module that generated the event.

11.3. 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*

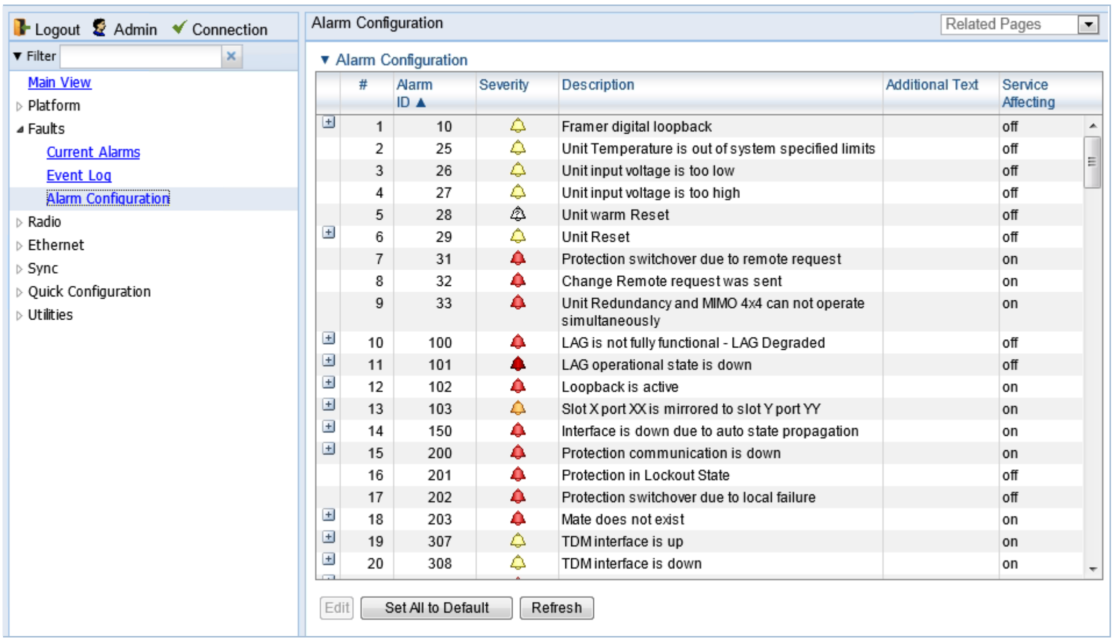
- *Editing an Alarm Type*
- *Setting Alarms to their Default Values*

11.3.1. Displaying Alarm Information

To view the list of alarms defined in the system:

1 Select **Faults > Alarm Configuration**. The Alarm Configuration page opens. For a description of the information provided in the Alarm Configuration page, see *Table 63: Alarm Configuration Page Parameters*.

Figure 237: Alarm Configuration Page



#	Alarm ID ▲	Severity	Description	Additional Text	Service Affecting
1	10	🔔	Framer digital loopback		off
2	25	🔔	Unit Temperature is out of system specified limits		off
3	26	🔔	Unit input voltage is too low		off
4	27	🔔	Unit input voltage is too high		off
5	28	🔔	Unit warm Reset		off
6	29	🔔	Unit Reset		off
7	31	🔔	Protection switchover due to remote request		on
8	32	🔔	Change Remote request was sent		on
9	33	🔔	Unit Redundancy and MIMO 4x4 can not operate simultaneously		on
10	100	🔔	LAG is not fully functional - LAG Degraded		off
11	101	🔔	LAG operational state is down		off
12	102	🔔	Loopback is active		on
13	103	🔔	Slot X port XX is mirrored to slot Y port YY		on
14	150	🔔	Interface is down due to auto state propagation		on
15	200	🔔	Protection communication is down		on
16	201	🔔	Protection in Lockout State		off
17	202	🔔	Protection switchover due to local failure		off
18	203	🔔	Mate does not exist		on
19	307	🔔	TDM interface is up		on
20	308	🔔	TDM interface is down		on

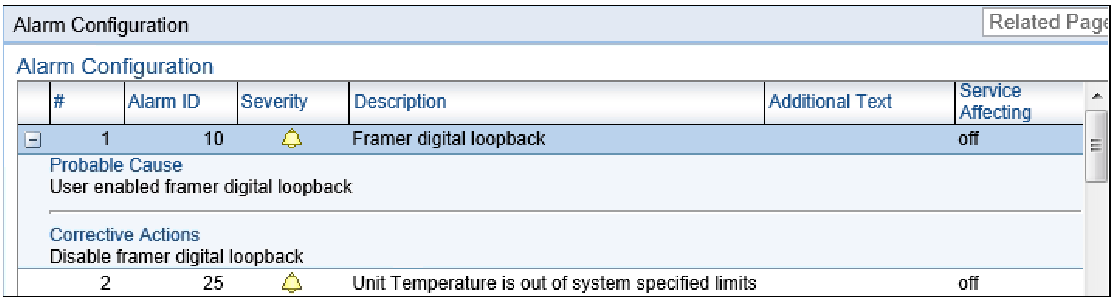
Table 63: Alarm Configuration Page Parameters

Parameter	Definition
Sequence Number (#)	A unique sequence number assigned to the row by the system.
Alarm ID	A unique ID that identifies the alarm type.
Severity	The severity assigned to the alarm type. You can edit the severity in the Alarm Configuration – Edit page. See *Editing an Alarm Type*.
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**).

11.3.2. Viewing the Probable Cause and Corrective Actions for an Alarm Type

Most alarm types include a system-defined probable cause and suggested corrective actions. To view an alarm type's probable cause and corrective actions, click + on the left side of the alarm type's row in the Alarm Configuration page. The Probable Cause and Corrective Actions appear underneath the alarm type's row, as shown below. If there is no +, that means no Probable Cause and Corrective Actions are defined for the alarm type.

Figure 238: Alarm Configuration Page – Expanded



Alarm Configuration

Alarm Configuration

	#	Alarm ID	Severity	Description	Additional Text	Service Affecting
⊟	1	10	🔔	Framer digital loopback		off

Probable Cause
User enabled framer digital loopback

Corrective Actions
Disable framer digital loopback

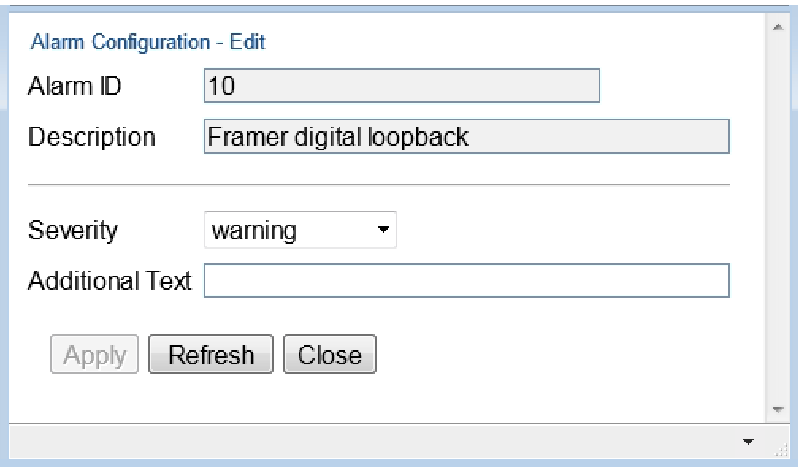
	#	Alarm ID	Severity	Description	Additional Text	Service Affecting
	2	25	🔔	Unit Temperature is out of system specified limits		off

11.3.3. 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 237*).
2 Click **Edit**. The Alarm Configuration - Edit page opens.

Figure 239: Alarm Configuration - Edit Page



Alarm Configuration - Edit

Alarm ID: 10

Description: Framer digital loopback

Severity: warning

Additional Text:

3 Modify the **Severity** and/or **Additional Text** fields.
4 Click **Apply**, then **Close**.

11.3.4. 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 237*).

11.4. 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.

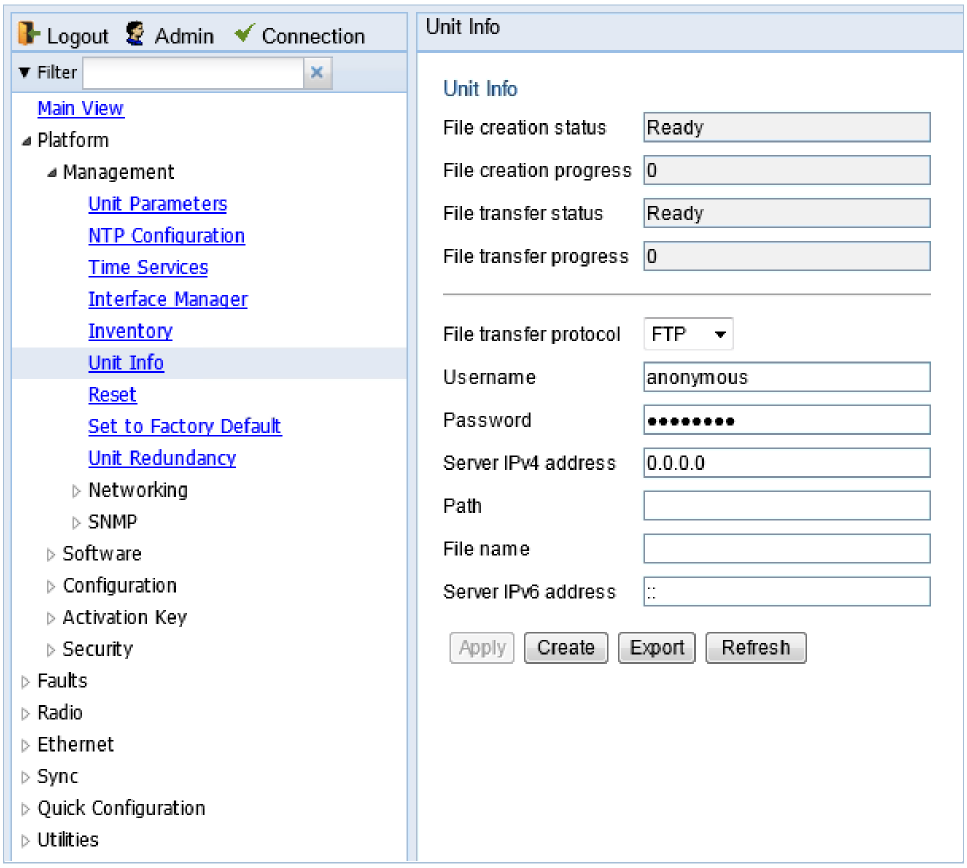
When uploading a Unit Information file, the NS Primo/Diplo functions as an FTP or SFTP client. You must install FTP or SFTP server software on the PC or laptop you are using to perform the upload. For details, see *Installing and Configuring an FTP or SFTP Server*.

To generate and upload a Unit Information file:

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 240: Unit Info Page



Unit Info

File creation status	Ready
File creation progress	0
File transfer status	Ready
File transfer progress	0
File transfer protocol	FTP
Username	anonymous
Password	••••••••
Server IPv4 address	0.0.0.0
Path	
File name	
Server IPv6 address	::

3 In the **File transfer protocol** field, select the file transfer protocol you want to use (**FTP** or **SFTP**).

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 file. Enter the path relative to the FTP user's home directory, not the absolute path. To leave the path blank, enter //.
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:
    - **File creation status** – Displays the file creation status. You must wait until the status is Success to upload the file. Possible values are:
        - **Ready** – The default value, which appears when no file is being created.
        - **Generating File** – The file is being generated.
        - **Success** – The file has been successfully created. You may now upload the file.
        - **Failure** – The file was not successfully created.
    - **File creation progress** – Displays the progress of the current Unit Information file creation operation.
12. Click **Export**. The upload begins. The following fields display the status of the upload process:
    - **File transfer status** – Displays the status of any pending Unit Information file upload. Possible values are:
        - **Ready** – The default value, which appears when no file transfer is in progress.
        - **File-in-transfer** – The upload operation is in progress.
        - **Success** – The file has been successfully uploaded.
        - **Failure** – The file was not successfully uploaded.

    If you try to export the file before it has been created, the following error message appears: **Error #3-Invalid set value**.

    If this occurs, wait about two minutes then click **Export** again.

    - **File transfer progress** – Displays the progress of the current Unit Information file upload operation.

11.5. Performing Diagnostics

This section includes:

- *Performing Radio Loopback*
- *Performing Ethernet Loopback*

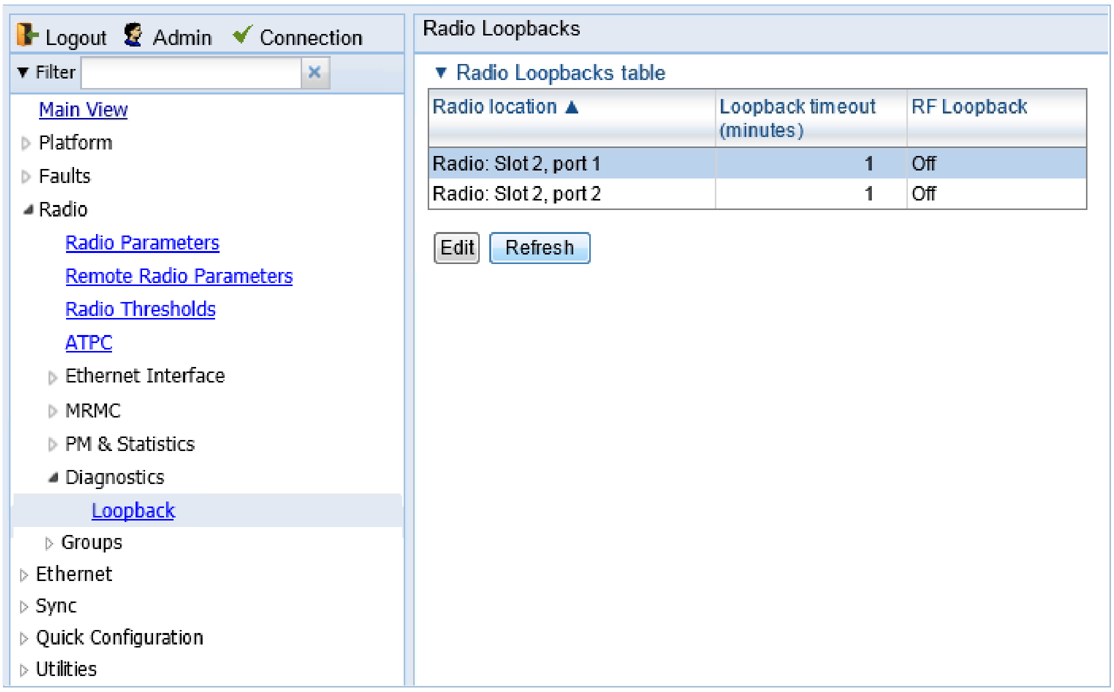
- *Configuring Service OAM (SOAM) Fault Management (FM)*

11.5.1. Performing Radio Loopback

To perform loopback on a radio:

1 Select **Radio > Diagnostics > Loopback**. The Radio Loopbacks page opens.

Figure 241: Radio Loopbacks Page

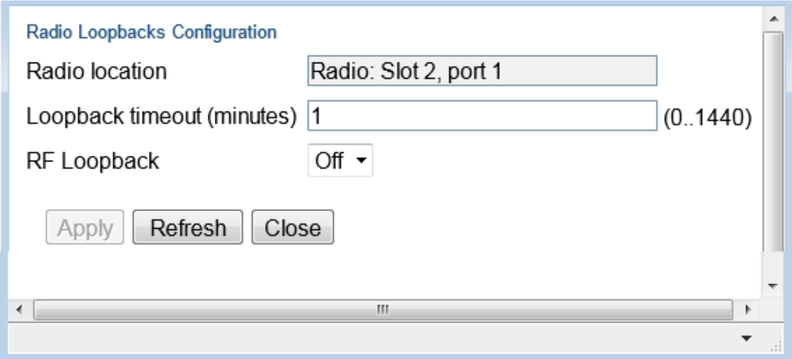


Radio location ▲	Loopback timeout (minutes)	RF Loopback
Radio: Slot 2, port 1	1	Off
Radio: Slot 2, port 2	1	Off

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 242: Radio Loopbacks – Edit Page



Radio location	Radio: Slot 2, port 1	
Loopback timeout (minutes)	1	(0..1440)
RF Loopback	Off	

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**.

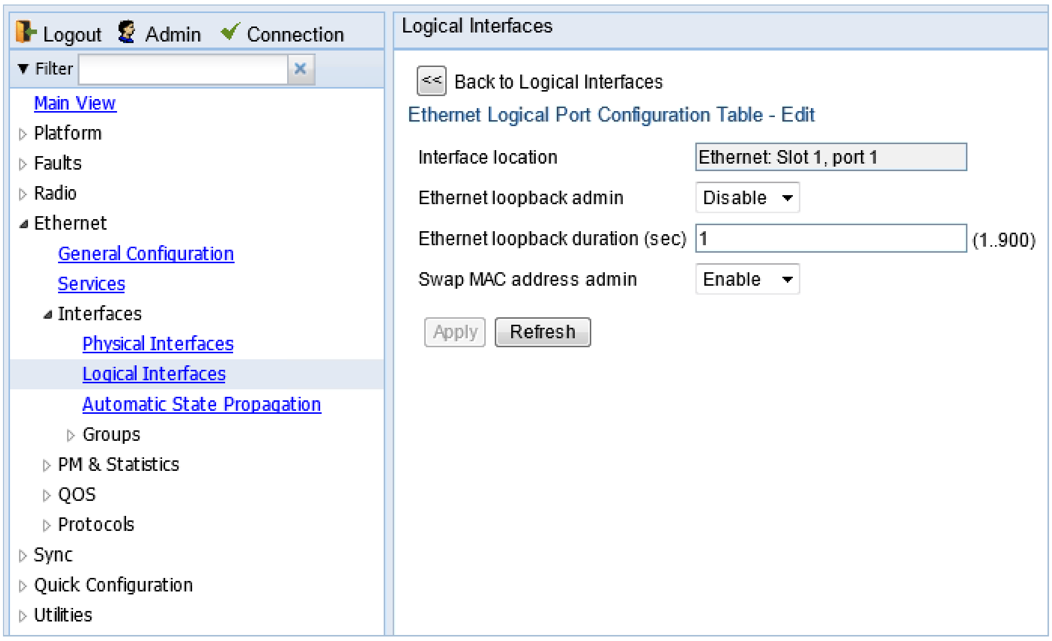
11.5.2. Performing Ethernet Loopback

Ethernet loopbacks can be performed on any logical Ethernet interface except a LAG. When Ethernet loopback is enabled on an interface, the system loops back all packets ingressing the interface. This enables loopbacks to be performed over the link from other points in the network.

To perform Ethernet loopback:

1 Select **Ethernet > Interfaces > Logical Interfaces**. The Logical Interfaces page opens (*Figure 140*).
2 Select an interface in the Ethernet Logical Port Configuration table and click **Loopback**. The Logical Interfaces – Loopback page opens.

Figure 243: Logical Interfaces – Loopback Page



Ethernet Logical Port Configuration Table - Edit

Interface location	Ethernet: Slot 1, port 1
Ethernet loopback admin	Disable
Ethernet loopback duration (sec)	1 (1..900)
Swap MAC address admin	Enable

3 In the **Ethernet loopback admin** field, select **Enable** to enable Ethernet loopback on the logical interface, or **Disable** to disable Ethernet loopback on the logical interface.
4 In the **Ethernet loopback duration (sec)** field, enter the loopback duration time (in seconds).
5 In the **Swap MAC address admin** field, select whether to swap DA and SA MAC addresses during the loopback. Swapping addresses prevents Ethernet loops from occurring. It is recommended to enable MAC address swapping if LLDP is enabled.
6 Click **Apply** to initiate the loopback.

11.5.3. Configuring Service OAM (SOAM) Fault Management (FM)

This section includes:

- *SOAM Overview*
- *Configuring MDs*
- *Configuring MA/MEGs*
- *Configuring MEPs*
- *Displaying Remote MEPs*
- *Displaying Last Invalid CCMS*

11.5.3.1. SOAM Overview

The Y.1731 and IEEE 802.1ag 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 and Loopback are planned for future release.

NS Primo/Diplo utilizes these protocols to maintain smooth system operation and non-stop data flow.

Note

Support for IEEE 802.1ag is planned for future release.

The following are the basic building blocks of FM:

- MD (Maintenance Domain) – An MD defines the network segment for which connectivity faults are managed via SOAM.
- MA/MEG (Maintenance Association/Maintenance Entity Group) – An MA/MEG contains a set of MEPs.
- MEP (Maintenance Association End Points) – Each MEP is located on a service point of an Ethernet service. 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.

Note

MIPs (Maintenance Association Intermediate Points) are not supported in the current release.

- 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.

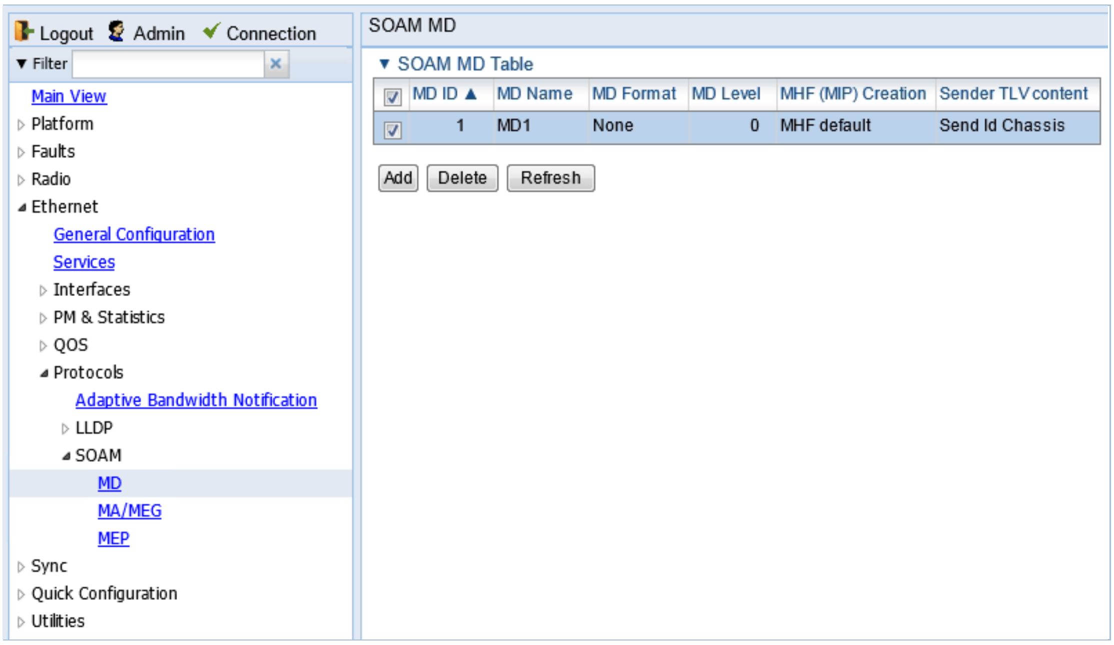
11.5.3.2. Configuring MDs

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 244: SOAM MD Page

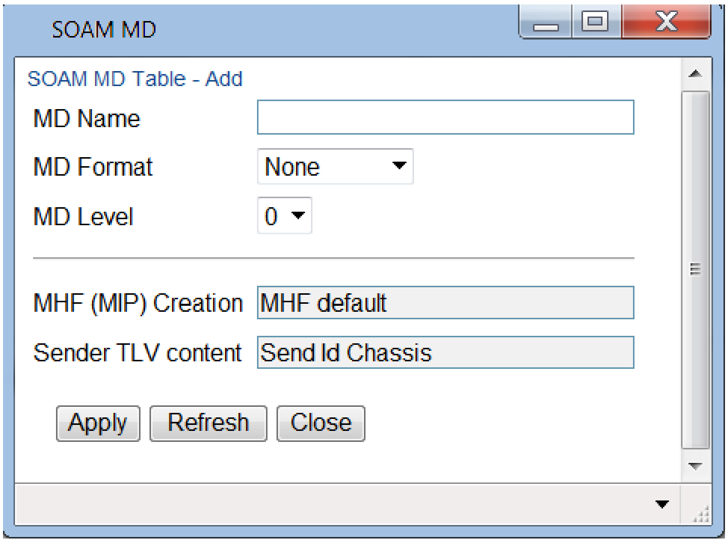


SOAM MD Table

☑	MD ID ▲	MD Name	MD Format	MD Level	MHF (MIP) Creation	Sender TLV content
☑	1	MD1	None	0	MHF default	Send Id Chassis

2 Click **Add**. The SOAM MD – Add page opens.

Figure 245: SOAM MD Page



SOAM MD Table - Add

MD Name	
MD Format	None
MD Level	0
MHF (MIP) Creation	MHF default
Sender TLV content	Send Id Chassis

3 In the **MD Name** field, enter an identifier for the MD (up to 43 alphanumeric characters). The MD Name should be unique over the domain.

4 In the **MD Format** field, select **None**.

Note

Support for MDs with the MD format Character String is planned for future release. In this release, the software enables you to configure such MDs, but they have no functionality.

5 In the **MD Level** field, select the maintenance level of the MD (0-7). The maintenance level ensures that the CFM frames for each domain do not interfere with each other. Where domains are nested, the encompassing domain must have a higher level than the domain it encloses. The maintenance level is carried in all CFM frames that relate to that domain. The **MD Level** must be the same on both sides of the link.

Note

In the current release, the MD level is not relevant to the SOAM functionality.

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

The **MHF (MIP) Creation** field displays the type of MHF format included in the CCMs sent in this MD (in the current release, this is **MHF Default**).

The **Sender TLV Content** field displays the type of TLVs included in the CCMs sent in this MD (in the current release, this is only **Send ID Chassis**).

11.5.3.3. Configuring MA/MEGs

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 64*):

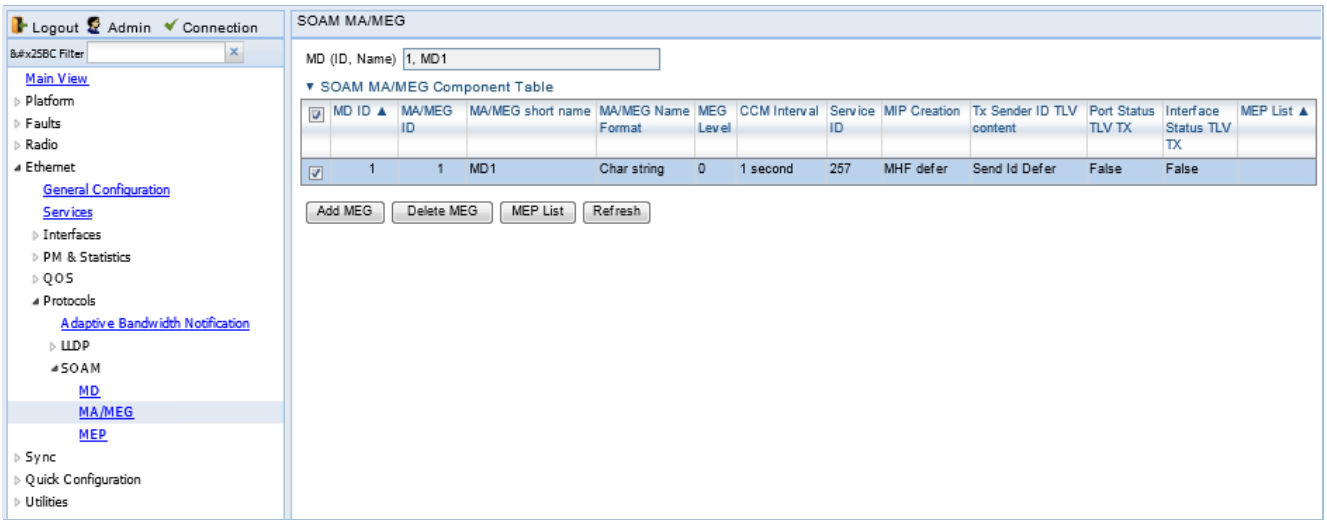
- Fast MEGs have a CCM interval of 1 second.
- Slow MEGs have a CCM interval of 10 seconds, 1 minute, or 10 minutes.

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:

1 Select **Ethernet > Protocols > SOAM > MA/MEG**. The SOAM MA/MEG page opens.

Figure 246: SOAM MA/MEG Page



SOAM MA/MEG

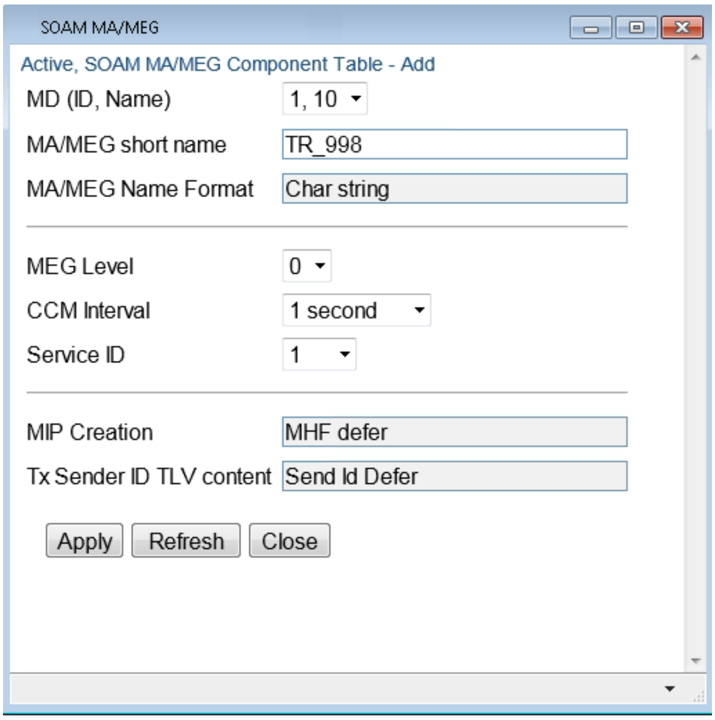
MD (ID, Name) 1, MD1

▼ SOAM MA/MEG Component Table

☑	MD ID ▲	MA/MEG ID	MA/MEG short name	MA/MEG Name Format	MEG Level	CCM Interval	Service ID	MIP Creation	Tx Sender ID TLV content	Port Status TLV TX	Interface Status TLV TX	MEP List ▲
☑	1	1	MD1	Char string	0	1 second	257	MHF defer	Send Id Defer	False	False	

2 Click **Add MEG**. The SOAM MA/MEG – Add page opens.

Figure 247: SOAM MA/MEG – Add Page



Active, SOAM MA/MEG Component Table - Add

MD (ID, Name)	1, 10
MA/MEG short name	TR_998
MA/MEG Name Format	Char string
MEG Level	0
CCM Interval	1 second
Service ID	1
MIP Creation	MHF defer
Tx Sender ID TLV content	Send Id Defer

3 Configure the fields described in *Table 64*.

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

Table 65 describes the status (read-only) fields in the SOAM MA/MEG Component table.

Table 64: 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).
MEG Level	Select a MEG level (0-7). The MEG level must be the same for MEGs on both sides of the link. Higher levels take priority over lower levels. If MEGs are nested, the OAM flow of each MEG must be clearly identifiable and separable from the OAM flows of the other MEGs. In cases where the OAM flows are not distinguishable by the Ethernet layer encapsulation itself, the MEG level in the OAM frame distinguishes between the OAM flows of nested MEGs. Eight MEG levels are available to accommodate different network deployment scenarios. When customer, provider, and operator data path flows are not distinguishable based on means of the Ethernet layer encapsulations, the eight MEG levels can be shared among them to distinguish between OAM frames belonging to nested MEGs of customers, providers and operators. The default MEG level assignment among customer, provider, and operator roles is: ● The customer role is assigned MEG levels 6 and 7. ● The provider role is assigned MEG levels 3 through 5. ● The operator role is assigned MEG levels: 0 through 2. The default MEG level assignment can be changed via a mutual agreement among customer, provider, and/or operator roles. The number of MEG levels used depends on the number of nested MEs for which the OAM flows are not distinguishable based on the Ethernet layer encapsulation.
CCM Interval	The interval at which CCM messages are sent within the MEG. Options are: ● 1 second (default) ● 10 seconds ● 1 minute ● 10 minutes It takes a MEP 3.5 times the CCM interval to determine a change in the status of its peer MEP. For example, if the CCM interval is 1 second, a MEP will detect failure of the peer 3.5 seconds after it receives the first CCM failure message. If the CCM interval is 10 minutes, the MEP will detect failure of the peer 35 minutes after it receives the first CCM failure message.
Service ID	Select an Ethernet service to which the MEG belongs. You must define the service before you configure the MEG.

Table 65: SOAM MA/MEG Status Parameters

Parameter	Definition
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.
MIP Creation	Reserved for future use.
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.

11.5.3.4. 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)*.

To configure a MEP, you must:

1 Add MEPs to the relevant MA/MEG. In this stage, you add both local and remote MEPs. The only thing you define at this point is the MEP ID. See *Adding Local and Remote MEPs*.

2 Configure the local MEPs. At this point, you determine which MEPs are local MEPs. The system automatically defines the other MEPs you configured in the previous step as remote MEPs. See *Configuring the Local MEPs*.

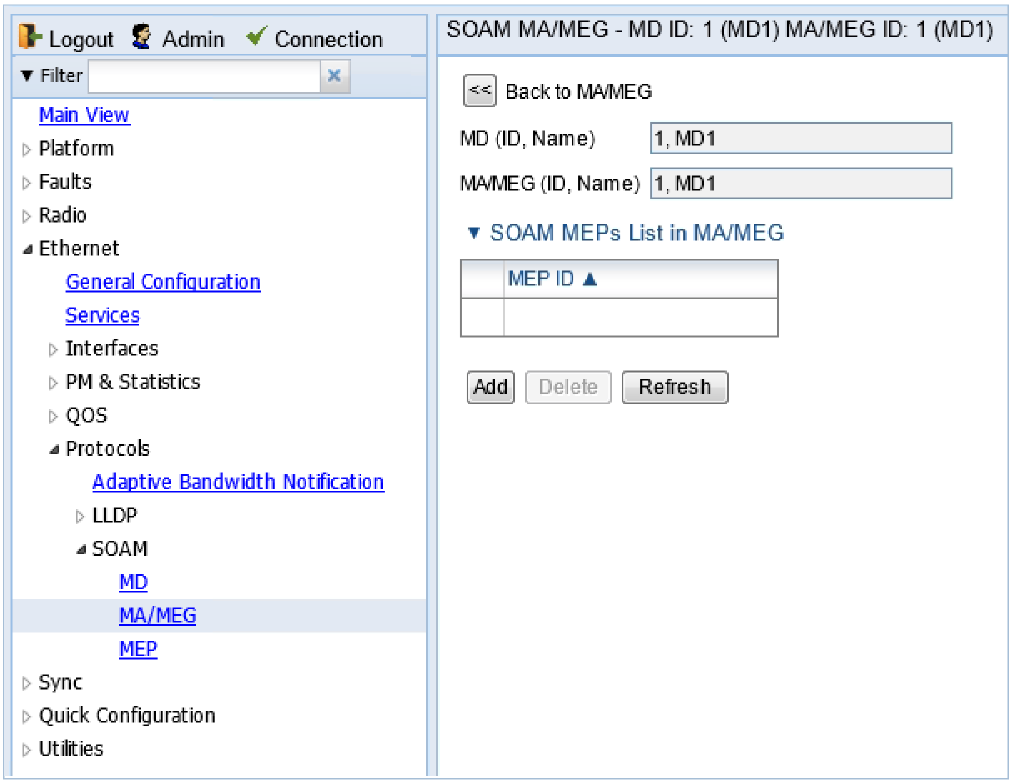
3 Enable the Local MEPs. See *Enabling Local MEPs*.

Adding Local and Remote MEPs

To add a MEP to the MA/MEG:

1 In the SOAM MA/MEG page, select a MA/MEG and click **MEP List**. The MEP List page opens.

Figure 248: MEP List Page



SOAM MA/MEG - MD ID: 1 (MD1) MA/MEG ID: 1 (MD1)

Back to MA/MEG

MD (ID, Name): 1, MD1

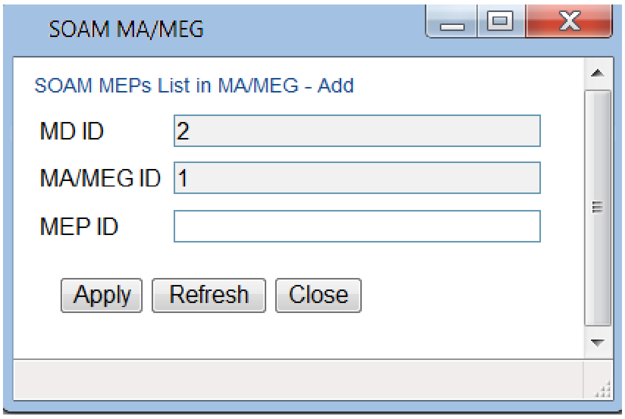
MA/MEG (ID, Name): 1, MD1

▼ SOAM MEPs List in MA/MEG

	MEP ID ▲

2 Click **Add**. The Add MEP page opens.

Figure 249: Add MEP Page



SOAM MEPs List in MA/MEG - Add

MD ID: 2

MA/MEG ID: 1

MEP ID:

3 In the **MEP ID** field, enter a MEP ID (1-8191).

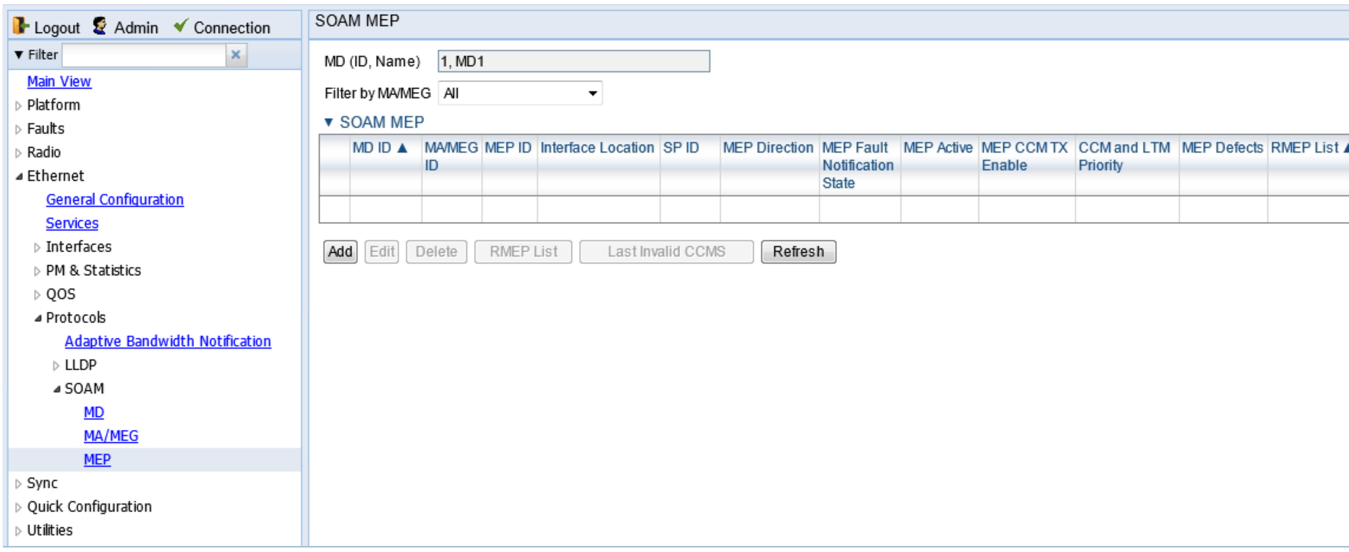
4 Click **Apply**, then **Close**.

Configuring the Local MEPs

Once you have added local and remote MEPs, you must define the MEPs and determine which are the local MEPs:

1 Select **Ethernet > Protocols > SOAM > MEP**. The SOAM MEP page opens. *Table 66* lists and describes the parameters displayed in the SOAM MEP page.

Figure 250: SOAM MEP Page



SOAM MEP

MD (ID, Name) 1, MD1

Filter by MA/MEG All

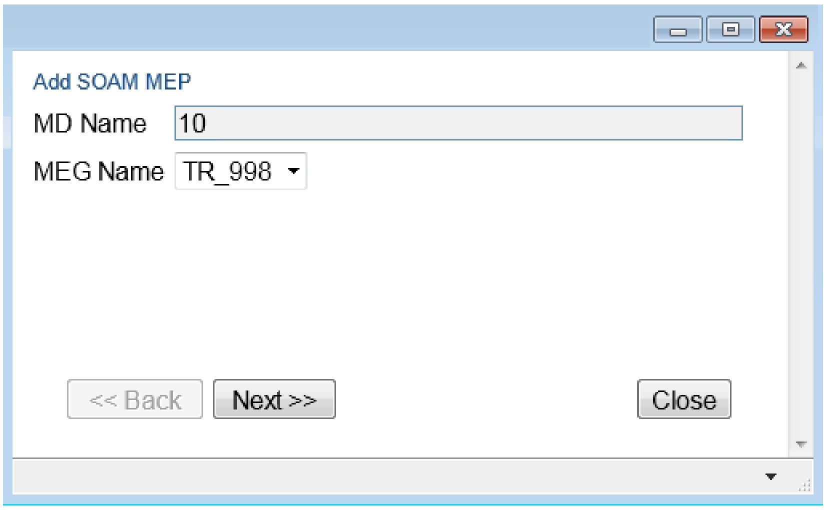
SOAM MEP

MD ID ▲	MA/MEG ID	MEP ID	Interface Location	SP ID	MEP Direction	MEP Fault Notification State	MEP Active	MEP CCM TX Enable	CCM and LTM Priority	MEP Defects	RMEP List

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 251: Add SOAM MEP Wizard – Page 1



Add SOAM MEP

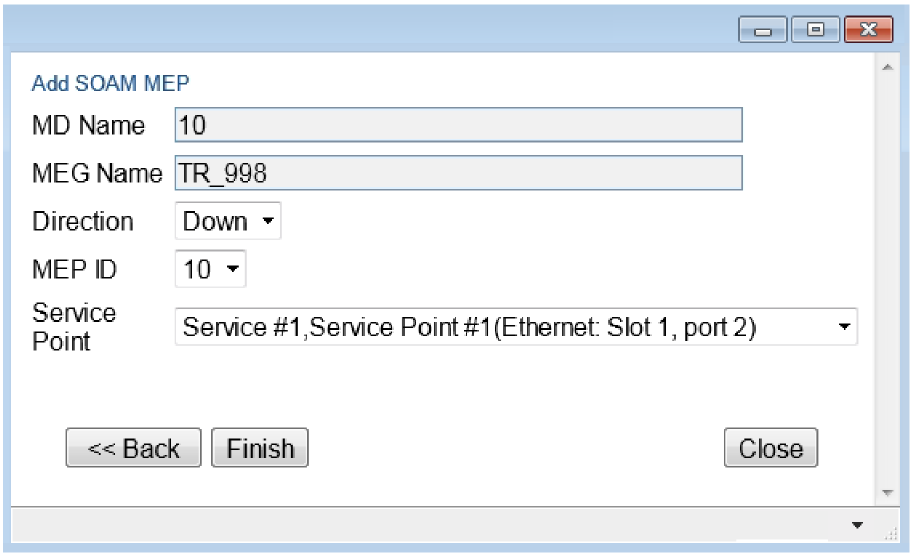
MD Name 10

MEG Name TR_998

3 In the **MEG Name** field, select an MA/MEG.

4 Click **Next**. Page 2 of the Add SOAM MEP wizard opens.

Figure 252: Add SOAM MEP Wizard – Page 2



Add SOAM MEP

MD Name: 10

MEG Name: TR_998

Direction: Down

MEP ID: 10

Service Point: Service #1,Service Point #1(Ethernet: Slot 1, port 2)

5 In the **Direction** field, select **Down**.

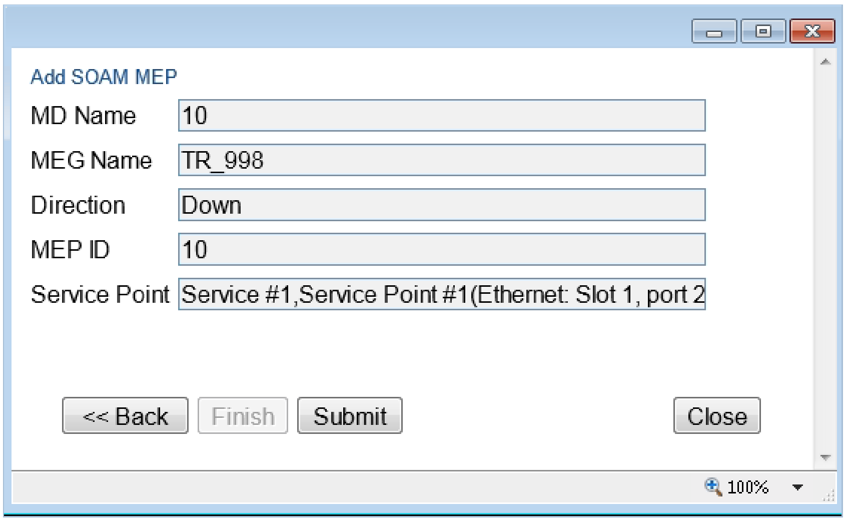
Note: In the current release, the Up direction is not supported.

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 253: Add SOAM MEP Wizard –Summary Page



Add SOAM MEP

MD Name: 10

MEG Name: TR_998

Direction: Down

MEP ID: 10

Service Point: Service #1,Service Point #1(Ethernet: Slot 1, port 2

9 Verify that you want to submit the displayed parameters and click **Submit**.

Table 66: SOAM MEP Parameters

Parameter	Definition
MD ID	An MD ID automatically generated by the system.
MA/MEG ID	An MA/MEG ID 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 **Down** is supported.
MEP Fault Notification State	The initial status of the SOAM state machine.
MEP Active	Indicates whether the MEP is enabled (**True**).
MEP CCM TX Enable	Indicates whether the MEP is sending CCMs (**True**).
CCM and LTM Priority	The p-bit included in CCMs sent by this MEP (0 to 7).
MEP Defects	Reserved for future use.
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.

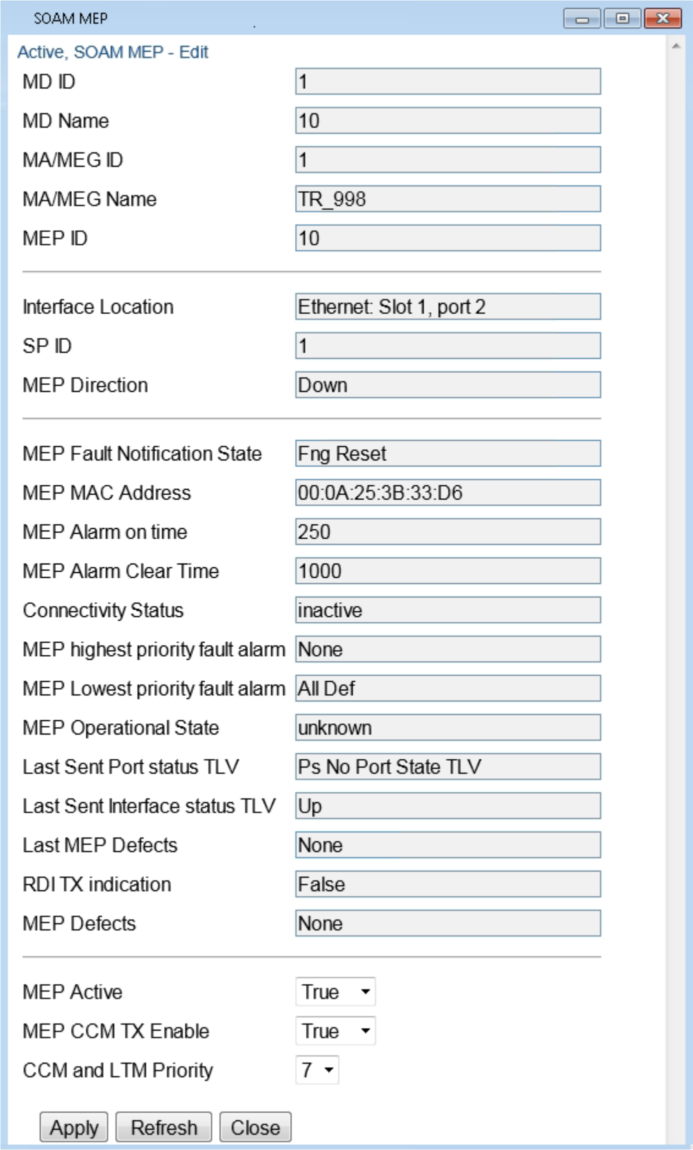
Enabling Local MEPs

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 250*), select the MEP you want to enable.
2 Click **Edit**. The SOAM MEP - Edit page opens.

Figure 254: SOAM MEP - Edit Page



SOAM MEP

Active, SOAM MEP - Edit

MD ID	1
MD Name	10
MA/MEG ID	1
MA/MEG Name	TR_998
MEP ID	10
Interface Location	Ethernet: Slot 1, port 2
SP ID	1
MEP Direction	Down
MEP Fault Notification State	Fng Reset
MEP MAC Address	00:0A:25:3B:33:D6
MEP Alarm on time	250
MEP Alarm Clear Time	1000
Connectivity Status	inactive
MEP highest priority fault alarm	None
MEP Lowest priority fault alarm	All Def
MEP Operational State	unknown
Last Sent Port status TLV	Ps No Port State TLV
Last Sent Interface status TLV	Up
Last MEP Defects	None
RDI TX indication	False
MEP Defects	None
MEP Active	True
MEP CCM TX Enable	True
CCM and LTM Priority	7

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**.

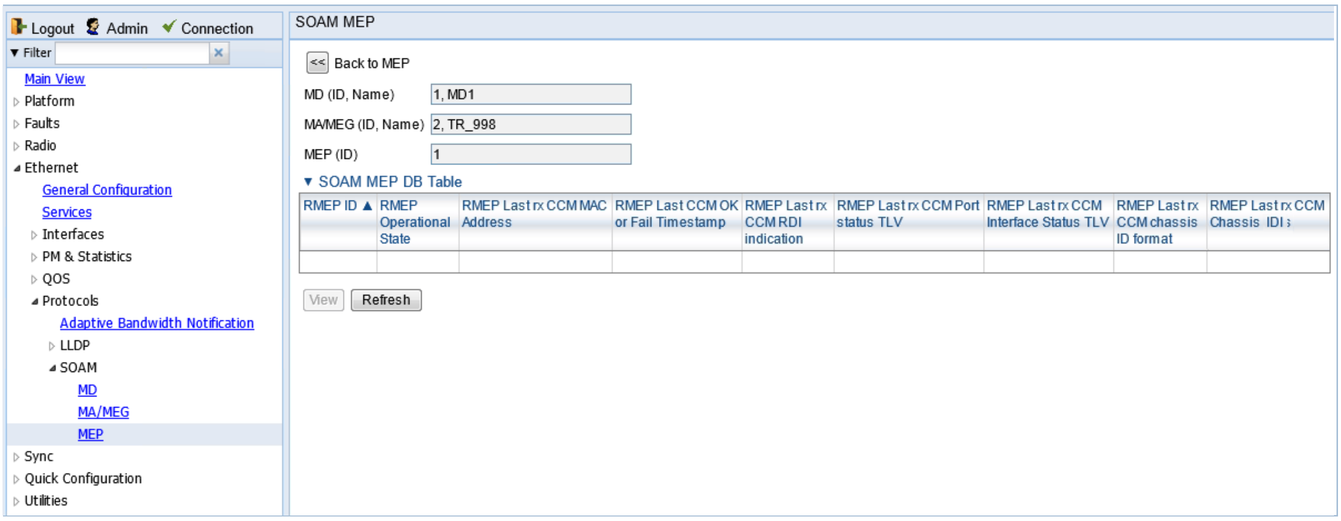
11.5.3.5. Displaying Remote MEPs

To display a list of remote MEPs (RMEPs) and their parameters:

1 Select **Ethernet > Protocols > SOAM > MEP**. The SOAM MEP page opens (*Figure 250*).

2 Select a MEP and click **RMEP List**. The SOAM MEP DB table is displayed.

Figure 255: SOAM MEP DB Table



MD (ID, Name) 1, MD1

MA/MEG (ID, Name) 2, TR_998

MEP (ID) 1

▼ SOAM MEP DB Table

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 IDI ;

Table 67 lists and describes the parameters displayed in the SOAM MEP DB table. To return to the SOAM MEP page, click **Back to MEP**.

Note

To display these parameters in a separate window for a specific remote MEP, select the RMEP ID and click **View**.

Table 67: SOAM MEP DB Table Parameters

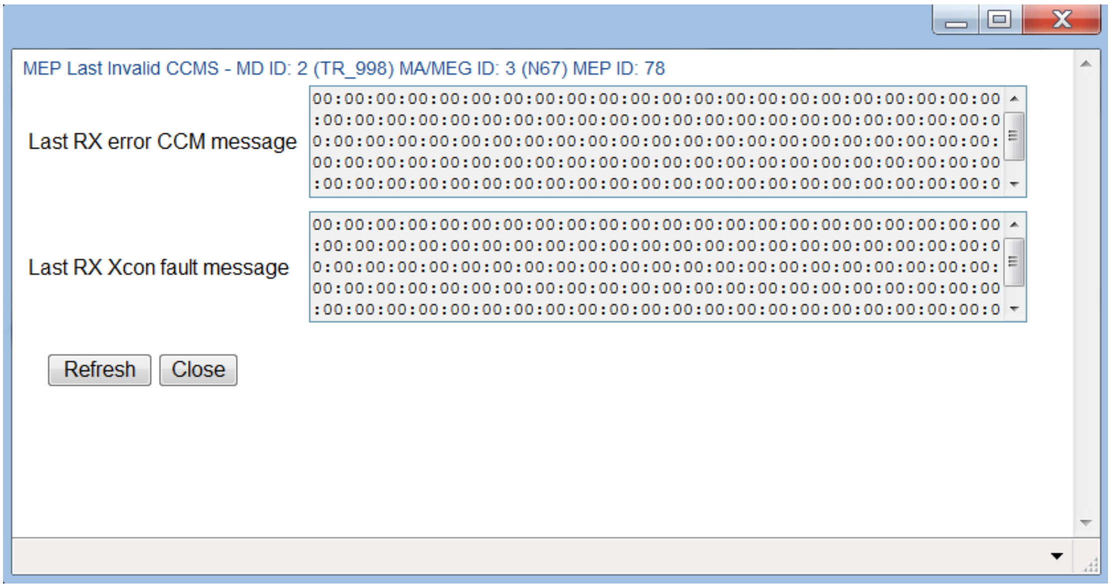
Parameter	Definition
RMEP ID	The remote MEP ID.
RMEP Operational State	The operational state of the remote MEP.
RMEP Last rx CCM MAC Address	The MAC Address of the interface on which the remote MEP is located.
RMEP Last CCM OK or Fail Timestamp	The timestamp marked by the remote MEP indicated the most 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 bit in the most recent CCM received by the remote MEP: ● **True** – RDI was received in the last CCM. ● **False** – No RDI was received in the last CCM.
RMEP Last rx CCM Port Status TLV	The Port Status TLV in the most recent CCM received from the remote MEP.
RMEP Last rx CCM Interface Status TLV	Reserved for future use.
RMEP Last rx CCM Chassis ID Format	Displays the MAC address of the remote unit.
RMEP Last rx CCM Chassis ID	Reserved for future use.

11.5.3.6. 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 250*).
2 Select a MEP and click **Last Invalid CCMS**. The MEP Last Invalid CCMS page opens.

Figure 256: MEP Last Invalid CCMS Page



MEP Last Invalid CCMS - MD ID: 2 (TR_998) MA/MEG ID: 3 (N67) MEP ID: 78

Last RX error CCM message

```
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0
0:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0
```

Last RX Xcon fault message

```
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0
0:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0
```

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.

12. Web EMS Utilities

This section includes:

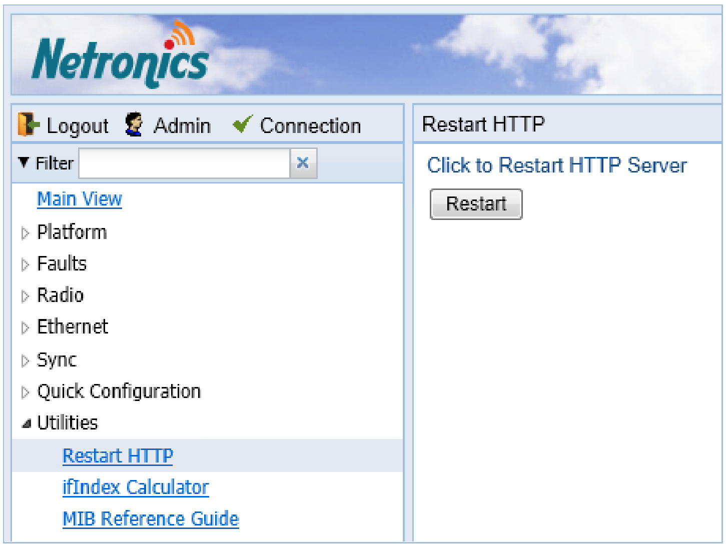
- *Restarting the HTTP Server*
- *Calculating an ifIndex*
- *Displaying, Searching, and Saving a list of MIB Entities*

12.1. Restarting the HTTP Server

To restart the unit's HTTP server:

1 Select **Utilities > Restart HTTP**. The Restart HTTP page opens.

Figure 257: 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.

12.2. Calculating an ifIndex

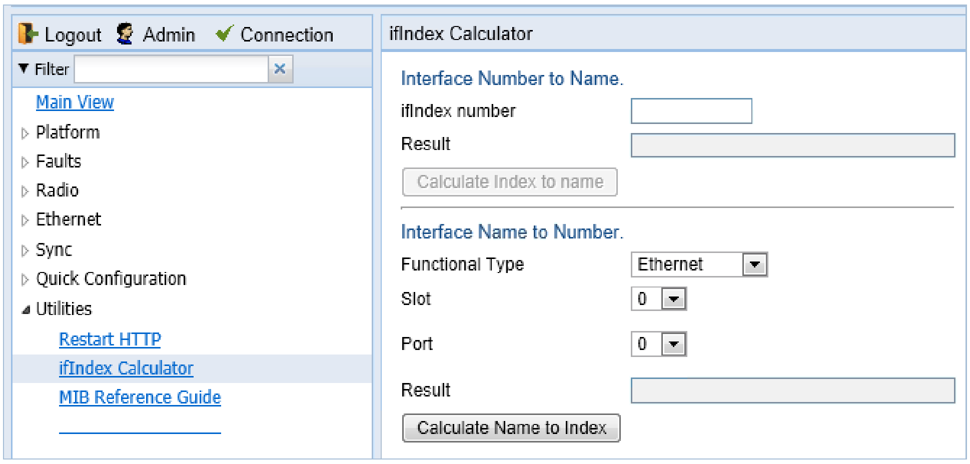
The ifIndex calculator enables you to:

- Calculate the ifIndex for any object in the system.
- Determine the object represented by any valid ifIndex.

To use the ifIndex calculator:

1 Select **Utilities > ifCalculator**. The ifIndex Calculator page opens.

Figure 258: ifIndex Calculator Page



ifIndex number

Result

Functional Type: Ethernet

Slot: 0

Port: 0

Result

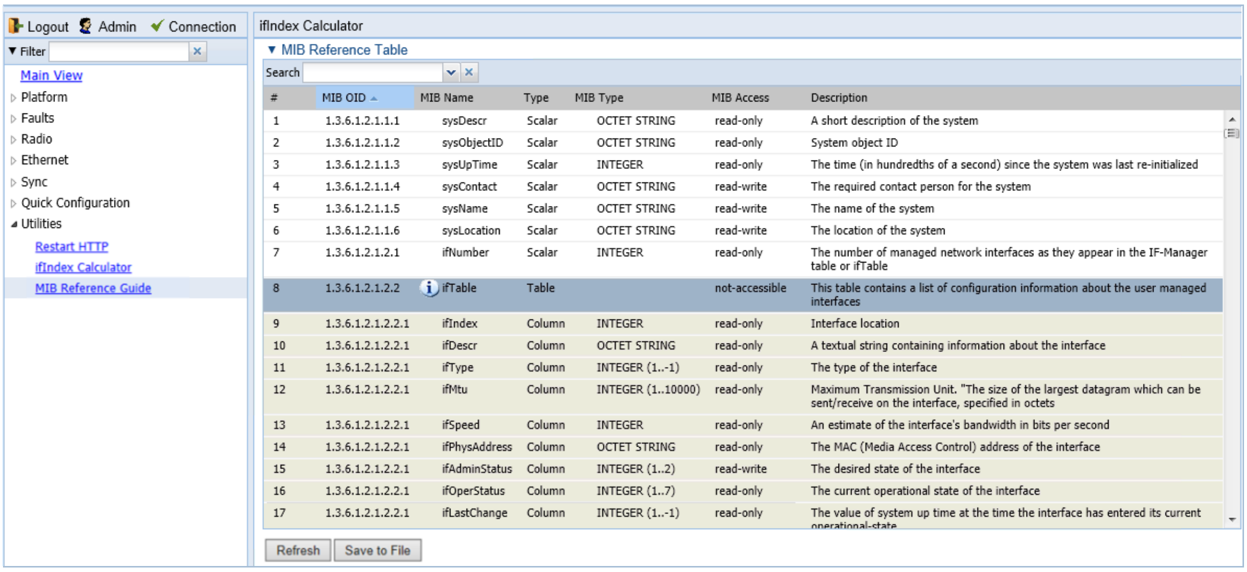
- If you have an ifIndex and you want to determine which hardware item in the unit it represents, enter the number in the **ifIndex number** field and click **Calculate Index to name**. A description of the object appears in the **Result** field.
- To determine the ifIndex of a hardware item in the unit, such as an interface, card, or slot, select the object type in the **Functional Type** field, select the **Slot** and **Port** (if relevant), and click **Calculate Name to Index**. The object's ifIndex appears in the **Result** field.

12.3. Displaying, Searching, and Saving a list of MIB Entities

To display a list of entities in the NS Primo/Diplo private MIB:

1 Select **Utilities > ifCalculator**. The ifIndex Calculator page opens.

Figure 259: 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 NS Primo/Diplo product you are using. There are three separate versions of the MIB Reference Table:

- NS Primo/DiploN/A/LH
- NS Primo/DiploG/GX
- NetStream Diplo/S/E

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. For example, the column *genEquipUnitShelfSlotConfigTable* is relevant to NS Primo/DiploGX but not to NS Primo/DiploG.

- 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**.

Section III:

CLI Configuration

13. Getting Started (CLI)

This section includes:

13.1. General (CLI)

Before connection over the radio hop is established, it is of high importance that you assign to the NS Primo/Diplo 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 NS Primo/Diplo unit has the following IP settings:

- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0

Warning

If the connection over the link is established with identical IP addresses, an IP address conflict will occur and remote connection to the element on the other side of the link may be lost.

13.2. Establishing a Connection (CLI)

Connect the NS Primo/Diplo unit to a PC by means of a TP cable. The cable is connected to the MGT port on the NS Primo/Diplo 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 NS Primo/Diplo IP address, as well as the password, should be changed before operating the system. See *Changing the Management IP Address (CLI)* and *Changing Your Password (CLI)*.

13.2.1. PC Setup (CLI)

To obtain contact between the PC and the NS Primo/Diplo unit, it is necessary to configure an IP address on the PC within the same subnet as the NS Primo/Diplo unit. The default NS Primo/Diplo 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 NS Primo/Diplo IP address, as well as the password, should be changed before operating the system. See *Changing the Management IP Address (CLI)* and *Changing Your Password (CLI)*.

13.3. Logging On (CLI)

Use a telnet connection to manage the NS Primo/Diplo 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:
```

```
Last login: Mon Apr 13 11:27:02 on console

NS Diplo

root>
```

13.4. General CLI Commands

To display all command levels available from your current level, press <TAB> twice. For example, if you press <TAB> twice at the root level, the following is displayed:

```
root>

auto-state-propagation    ethernet  exit   multi-carrier-abc

platform        quit        radio      radio-groups

switch-back    switch-to     wait
```

Some of these are complete commands, such as `quit` and `exit`. Others constitute the first word or phrase for a series of commands, such as `ethernet` and `radio`.

Similarly, if you enter the word "platform" and press <TAB> twice, the first word or phrase of every command that follows platform is displayed:

```
root> platform
activation-key     configuration   if-manager      management
security      software                 status
sync        unit-info      unit-info-file
root> platform
```

To auto-complete a command, press <TAB> once.

Use the up and down arrow keys to navigate through recent commands.

Use the ? key to display a list of useful commands and their definitions.

At the prompt, or at any point in entering a command, enter the word `help` to display a list of available commands. If you enter `help` at the prompt, a list of all commands is displayed. If you enter `help` after entering part of a command, a list of commands that start with the portion of the command you have already entered is displayed.

To scroll up and down a list, use the up and down arrow keys.

To end the list and return to the most recent prompt, press the letter `q`.

To ping another network device, enter one of the following commands:

```
root> ping ipv4-address <x.x.x.x> count <number of echo packets>
root> ping ipv6-address <ipv6> count < number of echo packets>
```

The count parameter is optional. This parameter can be an integer from 1 to 10. The default value is 4.

The ping command is available from all views (e.g., root, interface views, group views).

13.5. Changing Your Password (CLI)

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

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.
- The last five passwords you used cannot be reused.

See *Configuring the Password Security Parameters (CLI)*.

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 Netronics Customer Support. It is strongly recommended to change this password.

13.6. Configuring In-Band Management (CLI)

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

Each NS Primo/Diplo 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)*.

13.7. 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
```

13.8. 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 Demo Mode (CLI)*
- *Displaying a List of Activation-Key-Enabled Features (CLI)*

13.8.1. Activation Key Overview (CLI)

NS Primo/Diplo 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 NS Primo/Diplo 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.

Note

To obtain an activation key cipher, you may need to provide the unit's serial number. See *Displaying Unit Inventory (CLI)*.

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.

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

13.8.2. Viewing the Activation Key Status Parameters (CLI)

To display information about the currently installed activation key, enter the following command in root view:

```
root> platform activation-key show information
```

13.8.3. Entering the Activation Key (CLI)

To enter the activation key, enter the following command in root view.

```
root> platform activation-key set key string <key string>
```

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

13.8.4. Activating Demo Mode (CLI)

To activate demo mode, enter the following command in root view:

```
root> platform activation-key set demo admin enable
```

To display the current status of demo mode, enter the following command in root view:

```
root> platform activation-key show demo status
```

13.8.5. 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
```

13.9. Setting the Time and Date (Optional) (CLI)

Related Topics:

- *Configuring NTP (CLI)*

NS Primo/Diplo 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 NS Primo/Diplo unit holds the UTC offset and daylight savings time information for the location of the unit. Each management unit presenting the information uses its own UTC offset to present the information with the correct time.

Note

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

To set the UTC time, enter the following command in root view:

```
root> platform management time-services utc set date-and-time
<date-and-time>
```

To set the local time offset relative to UTC, enter the following command in root view:

```
root> platform management time-services utc set offset hours-
offset <hours-offset> minutes-offset <minutes-offset>
```

To display the local time configurations, enter the following command in root view:

```
root> platform management time-services show status
```

Table 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
```

13.9.1. 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
```

13.10. 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

NetStream Primo and NS Primo/DiploE units have 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: 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 (NetStream Diplo 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:

```
root> platform if-manager set interface-type radio slot 2 port
1 admin up
```

The following command disables radio interface 1:

```
root> platform if-manager set interface-type radio slot 2 port
1 admin down
```

The following command disables Ethernet port 3:

```
root> platform if-manager set interface-type ethernet slot 1
port 3 admin down
```

13.11. 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.

13.11.1. Entering Radio View (CLI)

To view and configure radio parameters, you must first enter the radio’s view level in the CLI.

To enter a radio’s view level, enter the following command in root view:

```
root> radio slot <slot> port <port>
```

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 (NetStream Diplo 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]>
```

13.11.2. Muting and Unmuting a Radio (CLI)

To mute or unmute the radio, enter the following command in radio view:

```
radio[x/x]>rf mute set admin <admin>
```

To display the mute status of a radio, enter the following command in radio view:

```
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 NetStream Diplo unit:

```
radio[2/2]>rf mute set admin off
```

13.11.3. Configuring the Transmit (TX) Level (CLI)

To set the transmit (TX) level of a radio, enter the following command in radio view:

```
radio[x/x]>rf set tx-level <tx-level>
```

To display the maximum transmit (TX) level of a radio, enter the following command in radio view:

```
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	NetStream Diplo and NetStream Primo units: -1 to 22 NS Primo/DiploE units: -1 to 12	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
```

13.11.4. Configuring the Transmit (TX) Frequency (CLI)

To set the transmit (TX) frequency of a radio, enter the following command in radio view. This command includes an option to set the remote RX frequency in parallel:

```
radio[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 NetStream Diplo or NetStream Primo 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 NetStream Diplo or NetStream Primo 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
```

The following command sets the TX frequency of the radio in an NS Primo/DiploE unit to 71000000 KHz, and sets the RX frequency of the remote unit to the same value.

```
radio[2/1]> rf set tx-frequency 71000000 local-remote enable
```

The following command sets the TX frequency of the radio in an NS Primo/DiploE unit to 71000000 KHz, but does not set the RX frequency of the remote unit.

```
radio[2/1]> rf set rx-frequency 71000000 local-remote disable
```

13.12. 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.

13.12.1. 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.
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 NetStream Diplo unit:

```
radio[2/2]>mrmc script show script-type normal acm-support yes
```

The following command displays available symmetrical (normal) scripts for an NS Primo/DiploE unit:

```
radio[2/2]>mrmc script show script-type normal acm-support yes
```

13.12.2. Assigning an MRMC Script to a Radio Carrier (CLI)

Once you have a list of valid scripts, you can assign a script to the radio carrier. The command syntax differs depending on whether you are assigning a script with ACM support or a script without ACM support.

Note

When you enter a command to change the script, a prompt appears informing you that changing the traffic will reset the unit and affect traffic. To continue, enter `yes`.

To assign a script with ACM enabled, enter the following command in radio view:

```
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 in radio view:

```
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 in radio view:

```
radio[x/x]>mrmc show script-configuration
```

Table 78: MRMC Script Assignation 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).
profile	Number	NetStream Diplo and NetStream Primo units: 0-10 NS Primo/DiploE units: 0-6	The maximum modulation profile. For NetStream Diplo and NetStream Primo, the options are: 0 – QPSK 1 – 8 PSK 2 – 16 QAM 3 – 32 QAM 4 – 64 QAM 5 – 128 QAM 6 – 256 QAM 7 – 512 QAM 8 – 1024 QAM (Strong FEC) 9 – 1024 QAM (Light FEC) 10 – 2048 QAM For NS Primo/DiploE, the options are: 0 – BPSK 1 – QPSK 2 – 8 QAM 3 – 16 QAM 4 – 32 QAM 5 – 64 QAM 6 – 128 QAM

Examples

The following command assigns MRMC script ID 1503, with ACM enabled and a maximum profile of 9, to radio carrier 1 in a NetStream Diplo and NetStream Primo unit:

```
radio[2/1]>mrmc set acm-support script-id 13 modulation
adaptive max-profile 9
```

The following command assigns MRMC script ID 1502, with ACM disabled and a maximum profile of 5, to radio carrier 2 in a NetStream Diplo unit:

```
radio[2/2]>mrmc set acm-support script-id 13 modulation fixed
profile 5
```

The following command assigns MRMC script ID 4701, with ACM disabled and a maximum profile of 5, to the radio carrier in an NS Primo/DiploE unit:

```
radio[2/1]>mrmc set acm-support script-id 4701 modulation fixed
profile 5
```

13.13. 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 NS Primo/Diplo 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 in radio view:

```
radio[x/x]>rf adaptive-power admin enable
```

To disable Adaptive TX Power for a radio, enter the following command in radio view:

```
radio[x/x]>rf adaptive-power admin disable
```

To display whether Adaptive TX Power is enabled, enter the following command in radio view:

```
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.

13.14. Operating in FIPS Mode (CLI)

Note

This feature is only relevant for NetStream Diplo and NetStream Primo units.

From NetStream OS version 8.3, NetStream Diplo and NetStream Primo can be configured to be FIPS 140-2-compliant in specific hardware and software configurations, as described in this section.

13.14.1. Requirements for FIPS Compliance (CLI)

For a full list of FIPS requirements, refer to the *Netronics NS Primo/Diplo FIPS 140-2 Security Policy*, available upon request. It is the responsibility of the customer to ensure that these requirements are met.

For details on hardware requirements for operating in FIPS mode, see *Requirements for FIPS Compliance*.

13.14.2. 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.

For a full list of FIPS requirements, including software configuration requirements, refer to the *Netronics NS Primo/Diplo FIPS 140-2 Security Policy*, available upon request.

13.15. 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)*.

13.16. Creating Service(s) for Traffic (CLI)

In order to pass traffic through the NS Primo/Diplo, you must configure Ethernet traffic services. For configuration instructions, see *Configuring Ethernet Services (CLI)*.

14. Configuration Guide (CLI)

14.1. System Configurations (CLI)

This section lists the basic system configurations and the NS Primo/Diplo 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)	NetStream Diplo	Configuring Multi-Carrier ABC (CLI)
Link Aggregation (LAG)	NetStream Diplo/S/E	Configuring Link Aggregation (LAG) (Optional) (CLI)
XPIC	NetStream Diplo	Configuring XPIC (CLI)
HSB Radio Protection	NetStream Diplo/S	Configuring HSB Radio Protection (CLI)
MIMO and Space Diversity	NetStream Diplo	Configuring MIMO and Space Diversity (CLI)
NetStream Diplo in Single Radio Carrier Mode	NetStream Diplo	Operating an NetStream Diplo in Single Radio Carrier Mode (CLI)

14.2. Configuring Multi-Carrier ABC (CLI)

Note: This option is only relevant for NetStream Diplo units.

This section includes:

- *Multi-Carrier ABC Overview (CLI)*
- *Configuring a Multi-Carrier ABC Group (CLI)*
- *Removing Members from a Multi-Carrier ABC Group (CLI)*
- *Deleting a Multi-Carrier ABC Group (CLI)*

14.2.1. 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.

14.2.2. Configuring a Multi-Carrier ABC Group (CLI)

Note

Radio slot 2 port 1 should always be configured on channel 1 while Radio slot 2 port 2 should always be configured on channel 2.

To configure a Multi-Carrier ABC group:

1 Create the group by entering the following command in root view:

```
root> multi-carrier-abc create group group_id 1
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
```

14.2.3. 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>
```

14.2.4. Deleting a Multi-Carrier ABC Group (CLI)

To delete a Multi-Carrier ABC group:

1 Remove the members from the group. See *Removing Members from a Multi-Carrier ABC Group (CLI)*.

2 Delete the group by entering the following command in root view:

```
root> multi-carrier-abc delete group group_id 1
```

14.3. Configuring Link Aggregation (LAG) (Optional) (CLI)

Link aggregation (LAG) enables you to group several physical Ethernet or radio interfaces into a single logical interface bound to a single MAC address. This logical interface is known as a LAG group. Traffic sent to the interfaces in a LAG group is distributed by means of a load balancing mechanism. NS Primo/Diplo 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)*
- *Viewing LAG Details (CLI)*
- *Editing and Deleting a LAG Group (CLI)*

14.3.1. LAG Overview (CLI)

Link aggregation (LAG) enables you to group several physical Ethernet or radio interfaces into a single logical interface bound to a single MAC address. This logical interface is known as a LAG group. Traffic sent to the interfaces in a LAG group is distributed by means of a load balancing mechanism. NS Primo/Diplo 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)*.

14.3.2. 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.

14.3.3. 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
```

14.3.4. 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 (NetStream Diplo 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
```

14.4. Configuring XPIC (CLI)

Note

This option is only relevant for NetStream Diplo units.

This section explains how to configure XPIC and includes the following topics:

- *XPIC Overview (CLI)*

- *Configuring the Antennas (CLI)*
- *Configuring the Radio Carriers for XPIC (CLI)*
- *Creating an XPIC Group (CLI)*

14.4.1. 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 antennas and then configure the carriers, as described below.

14.4.2. Configuring the Antennas (CLI)

To configure the antennas:

1 Align the antennas for one carrier. While you are aligning these antennas, mute the second carrier. See *Configuring the Radio Parameters (CLI)*.

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.

3 Record the RSL$_{wanted}$ and mute the first radio carrier at each end of the link.

4 Unmute the second (orthogonal) radio carrier which was muted during the antenna alignment process.

5 Determine the XPI, by either of the following two methods:

   ○ Measure the RSL of the second carrier (the “RSL$_{unwanted}$”). To calculate the XPI, subtract RSL$_{unwanted}$ from the RSL$_{wanted}$.

Note

To measure the second carrier, leave the Voltmeter connected to the BNC connector. In the Radio Parameters page of the Web EMS (*Figure 17*), change the **RSL Connector Source** field from **PHYS1** to **PHYS2** (or vice versa). The BNC connector will now measure RSL from the other carrier.

   ○ 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
```

6 The XPI should be at least 25dB. If it is not, you should adjust the OMT assembly on the back of the antenna at one side of the link until you achieve the highest 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. It is recommended to achieve XPI levels between 25dB and 30dB.

7 Enable all four radio carriers and check the XPI levels of both 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.

14.4.3. 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 NetStream Diplo/S/E Release Notes.

3 Create an XPIC group. See *Creating an XPIC Group (CLI)*.

14.4.4. Creating an XPIC Group (CLI)

To create an XPIC group, enter the following commands:

```
root> radio-groups
radio-groups>
radio-groups> xpic set admin enable
```

To disable XPIC, enter the following commands:

```
root> radio-groups
radio-groups>
radio-groups> xpic set admin disable
```

14.5. Configuring HSB Radio Protection (CLI)

This section explains how to configure HSB radio protection and includes the following topics:

- *HSB Radio Protection Overview (CLI)*
- *Configuring HSB Radio Protection (CLI)*
- *Configuring 2+2 HSB Protection on an NetStream Diplo 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)*

14.5.1. HSB Radio Protection Overview (CLI)

NetStream Diplo and NetStream Primo support 1+1 HSB radio protection. NetStream Diplo also supports 2+2 HSB radio protection. In HSB radio protection, one NS Primo/Diplo 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 NetStream Diplo, refer to the NetStream Diplo Technical Description.
- For a full explanation of 1+1 HSB radio protection support in NetStream Primo, refer to the NetStream Primo Technical Description.

14.5.2. 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 NetStream Diplo or NetStream Primo.

Ethernet traffic must be routed to each unit via an optical splitter cable.

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:

- 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.

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
```

14.5.3. Configuring 2+2 HSB Protection on an NetStream Diplo Unit (CLI)

In order to configure 2+2 HSB unit protection on an NetStream Diplo 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
```

14.5.4. Viewing the Configuration of the Standby unit (CLI)

You can view the settings of the standby unit any time.

To view the settings of the standby unit, you can run show commands in the standby unit. To do so, first enter the mate/root context, as described in *Performing CLI operations on the Standby unit (CLI)*, then run the relevant show command, and then switch back to the active unit.

14.5.5. Editing Standby Unit Settings (CLI)

Almost all settings of the standby unit are view-only. However, several settings are editable on the Standby unit. They must be configured separately for the Standby unit, and are not copied via copy-to-mate, nor do they trigger a configuration mismatch in the CLI.

In the Web EMS, failure to synchronize these configuration settings causes a configuration mismatch alarm.

The following settings must be configured separately on the standby unit:

- 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 *Configuring the Activation Key (CLI)* and *Activating Demo Mode (CLI)*.
- Defining user accounts. Refer to *Configuring User Accounts (CLI)*.
- Setting synchronization settings. Refer to *Configuring SyncE Regenerator (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.

14.5.5.1. Performing CLI operations on the Standby unit (CLI)

You can run CLI commands in the standby unit.

To run CLI commands in the standby unit:

1. Use the following command to enter view context for the standby unit:

```
root> switch-to mate

mate/root>
```

2. Enter the specific CLI command you want to run in mate/root context.
3. To switch back to the active unit, enter the following command:

```
mate/root> switch-back

root>
```

14.5.6. 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
```

14.5.7. 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
```

14.5.8. Disabling Automatic Switchover to the Standby Unit (CLI)

At any point, you can perform lockout, which disables automatic switchover to the standby unit.

To disable automatic switchover to the Standby unit, use the following command in root view:

```
root> platform management protection lockout set admin on
```

To re-enable automatic switchover to the standby unit, use the following command in root view:

```
root> platform management protection lockout set admin off
```

14.5.9. 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
```

14.6. Configuring MIMO and Space Diversity (CLI)

Note

This feature is only relevant for NetStream Diplo units.

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

- *MIMO and Space Diversity Overview (CLI)*
- *MIMO Mate Management Access (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)*

14.6.1. 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 an 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.

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

The same hardware configurations can also be used to implement BBS Space Diversity. NetStream Diplo supports 1+0 and 2+2 Space Diversity.

Note

Only one MIMO or Space Diversity group can be created per NetStream Diplo unit.

14.6.1.1. 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 NetStream Diplo units operating in dual core mode. In each NetStream Diplo unit, both radio carriers are connected to a single antenna. One optical GbE port on each NetStream Diplo is connected to an optical splitter. Traffic must be routed to an optical GbE port on each NetStream Diplo unit.

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

14.6.2. MIMO Mate Management Access (CLI)

For MIMO configurations using in-band management and an external switch operating in LAG mode, you must enable MIMO Mate Management Access in order to manage both units via in-band management. When MIMO Mate Management Access is enabled, the two units exchange incoming management packets, ensuring that all management data is received by both units.

Note that MIMO Mate Management Access should only be enabled if both of the following conditions exist:

- In-band management
- External switch using LAG

If either of these conditions is not present, MIMO Mate Management Access should be disabled, otherwise in-band management may be lost. By default, the feature is disabled.

To enable MIMO Mate Management Access, enter the following command:

```
root> radio mimo mate mng access set admin enable
```

To disable MIMO Mate Management Access, enter the following command:

```
root> radio mimo mate mng access set admin disable
```

To display whether MIMO Mate Management Access is enabled, enter the following command:

```
root> radio mimo mate mng access show
```

14.6.3. Creating a MIMO or Space Diversity Group (CLI)

Note

Only one MIMO or Space Diversity group can be created per NetStream Diplo 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).

14.6.4. 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>
```

14.6.5. 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 NetStream Diplo 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>
```

14.6.6. 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.

To reset MIMO, enter the following command in root view:

```
root > radio mimo reset group 1
```

14.6.7. 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 81: 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.

14.6.8. 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
```

14.7. Operating an NetStream Diplo in Single Radio Carrier Mode (CLI)

If you wish to operate an NetStream Diplo 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)*.

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)*
- *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)*

15.1. Defining the IP Protocol Version for Initiating Communications (CLI)

You can specify which IP protocol the unit will use when initiating communications, such as downloading software, sending traps, pinging, or exporting configurations. The options are IPv4 or IPv6.

To define which IP protocol the unit will use when initiating communications, enter the following command in root view:

```
root> platform management ip set ip-address-family <ipv4|ipv6>
```

To show the IP protocol version the unit will use when initiating communications, enter the following command in root view:

```
root> platform management ip show ip-address-family
```

15.2. Configuring the Remote Unit's IP Address (CLI)

You can configure the remote unit's IP address, subnet mask and default gateway in IPv4 format and/or in IPv6 format. The remote unit will receive communications whether they were sent to its IPv4 address or its IPv6 address.

15.2.1. Configuring the Remote Radio's IP Address in IPv4 format (CLI)

To set the remote radio's IP Address, enter the following command in radio view:

```
radio[x/x]>remote-unit set ip-address <ipv4-address>
```

To display the remote radio’s IP Address, enter the following command in radio view:

```
radio[x/x]>remote-unit show ip-address
```

To set the remote radio’s subnet mask, enter the following command in radio view:

```
radio[x/x]>remote-unit set subnet-mask IP <subnet-mask>
```

To display the remote radio’s subnet mask, enter the following command in radio view:

```
radio[x/x]>remote-unit show subnet-mask
```

To set the remote radio’s default gateway, enter the following command in radio view:

```
radio[x/x]>remote-unit set default-gateway IP <ipv4-address>
```

To display the remote radio’s default gateway, enter the following command in radio view:

```
radio[x/x]>remote-unit show default-gateway
```

Table 82: 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[2/1]>remote-unit set ip-address 192.168.1.1
radio[2/1]>remote-unit set subnet-mask IP 255.255.255.255
```

15.2.2. Configuring the Remote Radio's IP Address in IPv6 format (CLI)

To set the remote radio’s IP Address, enter the following command in radio view:

```
radio[x/x]>remote-unit set ip-address-ipv6 <ipv6-address>
```

To display the remote radio’s IP Address, enter the following command in radio view:

```
radio[x/x]>remote-unit show ip-address-ipv6
```

To set the remote radio’s prefix length , enter the following command in radio view:

```
radio[x/x]>remote-unit set prefix-length <prefix-length >
```

To display the remote radio's prefix-length , enter the following command in radio view:

```
radio[x/x]>remote-unit show prefix-length
```

To set the remote radio's default gateway, enter the following command in radio view:

```
radio[x/x]>remote-unit set default-gateway-ipv6 IPv6 <ipv6-
address>
```

To display the remote radio's default gateway, enter the following command in radio view:

```
radio[x/x]>remote-unit show default-gateway-ipv6
```

Table 83: 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.

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
```

15.3. Configuring SNMP (CLI)

NetStream Primo, and NS Primo/Diplo support SNMP v1, V2c, and v3. You can set community strings for access to NS Primo/Diplo units.

NetStream Diplo, NetStream Primo, and NS Primo/DiploE 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.

This section includes:

- *Configuring Basic SNMP Settings (CLI)*

- *Configuring SNMPv3 (CLI)*
- *Displaying the SNMP Settings (CLI)*
- *Configuring Trap Managers (CLI)*

15.3.1. 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 84: Basic SNMP CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin	Variable	enable disable	Select **enable** to enable SNMP monitoring, or **disable** to disable SNMP monitoring.
version	Variable	v1 v2 v3	Specifies the SNMP version.
read-community	Text String	Any valid SNMP read community.	The community string for the SNMP read community.
write-community	Text String	Any valid SNMP write community.	The community string for the SNMP write community.

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
```

15.3.2. Configuring SNMPv3 (CLI)

The following commands are relevant for SNMPv3.

To block SNMPv1 and SNMPv2 access so that only SNMPv3 access will be enabled, enter the following command in root view:

```
root> platform security protocols-control snmp v1v2-block set
<set-block>
```

To add an SNMPv3 user, enter the following command in root view:

```
root> platform security protocols-control snmp v3-
authentication add v3-user-name <v3-user-name> v3-user-password
<v3-user-password> v3-security-mode <v3-security-mode> v3-
encryption-mode <v3-encryption-mode> v3-auth-algorithm <v3-
auth-algorithm> v3-access-mode <v3-access-mode>
```

To remove an SNMP v3 user, enter the following command in root view:

```
root> platform security protocols-control snmp v3-
authentication remove v3-user-name <v3-user-name>
```

To display all SNMP v3 users and their authentication parameters, enter the following command in root view:

```
root> platform security protocols-control snmp v3-
authentication show
```

Table 85: 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		An SNMPv3 user name.
v3-user-password	Text String	Must be at least eight characters.	An SNMPv3 user password.
v3-security-mode	Variable	authNoPriv authPriv noAuthNoPriv	Defines the security mode to be used for this user.
v3-encryption-mode	Variable	None DES AES	Defines the encryption (privacy) protocol to be used for this user.
v3-auth-algorithm	Variable	None SHA 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
```

15.3.3. Displaying the SNMP Settings (CLI)

To display the general SNMP parameters, enter the following command in root view:

```
root> platform security protocols-control snmp show-all
```

To display all SNMP v3 users and their authentication parameters, enter the following command in root view:

```
root> platform security protocols-control snmp v3-
authentication show
```

To display the current MIB version used in the system, enter the following command in root view:

```
root> platform security protocols-control snmp show-mib-version
```

To display details about the current MIB version used in the system, enter the following command in root view:

```
root> platform security protocols-control snmp show-mib-
version-table
```

To display the SNMP read and write communities, enter the following command in root view:

```
root> platform security protocols-control snmpv1v2 show
```

15.3.4. Configuring Trap Managers (CLI)

To display the current SNMP trap manager settings, enter the following command in root view:

```
root> platform security protocols-control snmp trap-manager
show
```

To modify the settings of an SNMP trap manger, enter the following command in root view:

```
root> platform security protocols-control snmp trap-manager set
manager-id <manager-id> manager-admin <manager-admin> manager-
ipv4 <manager-ipv4> manager-ipv6<manager-ipv6> manager-port
<manager-port> manager-community <manager-community> manager-
v3-user <manager-v3-user> manager-description <manager-
description>
```

To enable an SNMP trap manger without modifying its parameters, enter the following command in root view:

```
root> platform security protocols-control snmp trap-manager
admin manager-id <manager-id> manager-admin <manager-admin>
```

To specify the number of minutes between heartbeat traps, enter the following command in root view:

```
root> platform security protocols-control snmp trap-manager
heartbeat manager-id <manager-id> manager-heartbeat <manager-
heartbeat>
```

Table 86: Trap Managers CLI Parameters

Parameter	Input Type	Permitted Values	Description
manager-id	Number.	1 – 4	Enter the Manager ID of the trap manager you want to modify.
manager-admin	Variable.	enable disable	Enter **enable** or **disable** to enable or disable the trap manager.
manager-ipv4	Dotted decimal format.	Any valid IPv4 address.	If the IP protocol selected in *platform management ip set ip-address-family* is IPv4, enter the destination IPv4 address. Traps will be sent to this IP address.
manager-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	If the IP protocol selected in platform management ip set ip-address-family is IPv6, enter the destination IPv6 address. Traps will be sent to this IP address.
manager-port	Number.	70 – 65535	Enter the number of the port through which traps will be sent.
manager-community	Text String.	Any valid SNMP read community.	Enter the community string for the SNMP read community.
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
```

15.4. Upgrading the Software (CLI)

NS Primo/Diplo 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)*

15.4.1. Software Upgrade Overview (CLI)

The NS Primo/Diplo 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 NS Primo/Diplo that are currently running an older version.

3 **Reset** – The NS Primo/Diplo 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 NS Primo/Diplo 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 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)*.

15.4.2. Viewing Current Software Versions (CLI)

To display all current software versions, enter the following command in root view:

```
root> platform software show versions
```

15.4.3. Configuring a Software Download (CLI)

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 87: Software Download CLI Parameters

Parameter	Input Type	Permitted Values	Description
server-ipv4	Dotted decimal format.	Any valid IPv4 address.	The IPv4 address of the PC or laptop you are using as the FTP server.
server-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The IPv6 address of the PC or laptop you are using as the FTP server.
directory	Text String.		The directory path from which you are downloading the files. Enter the path relative to the FTP user's home directory, not the absolute path. To leave the path blank, enter //.
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
```

15.4.4. Downloading a Software Package (CLI)

To initiate a software download, enter the following command in root view:

```
root> platform software download version protocol ftp
```

The following prompt appears:

```
You are about to perform a software management operation. This
may cause a system reset.
Are you sure? (yes/no)
```

Enter `Yes` at the prompt. When the prompt appears again, enter the following command to check the download status:

```
root> platform software download status show
```

Once the following message appears, proceed with the installation:

```
DOWNLOAD VERSION status: download success, process percentage:
100
```

If the software version on the FTP or SFTP server has already been downloaded to the unit, the following message appears:

```
DOWNLOAD VERSION status: all components exist, process
percentage: 0
```

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.

15.4.5. Installing and Upgrading Software (CLI)

To install or upgrade the software, enter the following command in root view after downloading the software bundle:

```
root> platform software install version
```

If you wish to delay the start of installation, enter instead the following command. The time you enter in HH:MM format is the amount of time to delay until the start of the installation process:

```
root> platform software install version timer-countdown <hh:mm>
```

The following prompt appears:

```
Software version to be installed:

Are you sure? (yes/no)
```

To display the status of a software installation or upgrade, enter the following command:

```
root> platform software install status show
```

Note

DO NOT reboot the unit during software installation process. As soon as the process is successfully completed, the unit will reboot itself.

Sometimes the installation process can take up to 30 minutes.

Only in the event that software installation was not successfully finished and more than 30 minutes have passed can the unit be rebooted.

If you configured delayed installation, you can do any of the following:

- Abort the current delayed installation. To do so, enter the following command:

```
root> platform software install abort-timer
```

- Show the time left until the installation process begins. To do so, enter the following command:

```
root> platform software install time-to-install
```

- Show the original timer as configured for a delayed installation. To do so, enter the following command:

```
root> platform software install show-time
```

15.5. Backing Up and Restoring Configurations (CLI)

You can import and export NS Primo/Diplo configuration files. This enables you to copy the system configuration to multiple NS Primo/Diplo units. You can also backup and save configuration files.

Configuration files can only be copied between units of the same type, i.e., NetStream Diplo to NetStream Diplo, NetStream Primo to NetStream Primo, and NS Primo/DiploE to NS Primo/DiploE.

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)*

15.5.1. Configuration Management Overview (CLI)

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

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

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

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

You must configure from 1 to 3 restore points:

- When you import a configuration file, the file is saved to the selected restore point, and overwrites whichever file was previously held in that restore point.
- When you export a configuration file, the file is exported from the selected restore point.
- When you 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.

15.5.2. Setting the Configuration Management Parameters (CLI)

When importing and exporting configuration files, the NS Primo/Diplo 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 88: Configuration Management CLI Parameters

Parameter	Input Type	Permitted Values	Description
server-ipv4	Dotted decimal format.	Any valid IPv4 address.	The IPv4 address of the PC or laptop you are using as the FTP server.
server-ipv6	Eight groups of four hexadecimal digits separated by colons.	Any valid IPv6 address.	The IPv6 address of the PC or laptop you are using as the FTP server.
directory	Text String.		The directory path to which you are exporting or from which you are importing the configuration file. Enter the path relative to the FTP user's home directory, not the absolute path. To leave the path blank, enter //.
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
```

15.5.3. Backing up and Exporting a Configuration File (CLI)

To save the current configuration as a backup file to one of the restore points, enter the following command in root view:

```
root> platform configuration configuration-file add <restore-
point>
```

To export a configuration from a restore point to the external server location, enter the following command in root view:

```
root> platform configuration configuration-file export
<restore-point>
```

Table 89: 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
```

15.5.4. Importing and Restoring a Configuration File (CLI)

You can import a configuration file from an external PC or laptop to one of the restore points. Once you have imported the file, you can restore the configuration. Restoring a saved configuration does not change the unit's FIPS mode.

Note

In order to import a configuration file, you must configure the FTP channel parameters and restore points, as described in *Setting the Configuration Management Parameters* and *Backing up and Exporting a Configuration File*.

To import a configuration file, enter the following command in root view:

```
root> platform configuration configuration-file import <restore-point>
```

To restore a configuration from a restore point to become the active configuration file, enter the following command in root view:

```
root> platform configuration configuration-file restore <restore-point>
```

Table 90: 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 NS Primo/Diplo, and restore the file to be the system configuration file for the NS Primo/Diplo:

```
root> platform configuration configuration-file import restore-point-2

root> platform configuration configuration-file restore restore-point-2
```

15.5.5. Editing CLI Scripts (CLI)

The configuration file package includes a text file that enables you to write CLI scripts in a backed-up configuration that are executed after restoring the configuration.

To edit a CLI script:

1 Back up the current configuration to one of the restore points. See *Backing up and Exporting a Configuration File (CLI)*.
2 Export the configuration from the restore point to a PC or laptop. See *Backing up and Exporting a Configuration File (CLI)*.
3 On the PC or laptop, unzip the file *Configuration_files.zip*.
4 Edit *the cli_script.txt* file using clish commands, one per line.
5 Save and close the *cli_script.txt* file, and add it back into the *Configuration_files.zip* file.
6 Import the updated Configuration_files.zip file back into the unit. See *Importing and Restoring a Configuration File (CLI)*.
7 Restore the imported configuration file. See *Importing and Restoring a Configuration File (CLI)*. The unit is automatically reset. During initialization, the CLI script is executed, line by line.

Note

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

15.6. 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.

15.7. 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.

15.8. 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 91: 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 NS Primo/Diplo:

```
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
```

15.9. Configuring NTP (CLI)

NS Primo/Diplo 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 92: 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
```

15.10. 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 : NS Primo/Diplo

Subtype : 350

part number : 22-0001-0|

serial number : F493606212

company name : Netronics Networks Ltd.

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>
```

16. Radio Configuration (CLI)

This section includes:

- *Viewing and Configuring the Remote Radio Parameters (CLI)*
- *Configuring ATPC (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) (Optional) (CLI)*
- *Configuring XPIC (CLI)*
- *Configuring HSB Radio Protection (CLI)*
- *Configuring MIMO and Space Diversity (CLI)*
- *Operating an NetStream Diplo in Single Radio Carrier Mode (CLI)*

Note that 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)*.

Note

For convenience, this User Guide generally shows the radio prompt as `radio[2/1]>`.

16.1. 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)*

16.1.1. Displaying Communication Status with the Remote Radio (CLI)

To display the communication status with the remote radio, enter the following command in radio view:

```
radio[x/x]>remote-unit communication status show
```

16.1.2. Displaying the Remote Radio's Link ID (CLI)

To display the remote radio's Link ID, enter the following command in radio view:

```
radio[x/x]>remote-unit show link-id
```

16.1.3. Muting and Unmuting the Remote Radio (CLI)

To mute or unmute the remote radio, enter the following command in radio view:

```
radio[x/x]>remote-unit mute set admin <admin>
```

To display the mute status of the remote radio, enter the following command in radio view:

```
radio[x/x]>remote-unit mute show status
```

Table 93: 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
```

16.1.4. Displaying the Remote Radio's RX Level (CLI)

To display the remote radio's RX level, enter the following command in radio view:

```
radio[x/x]>remote-unit show rx-level
```

16.1.5. Configuring the Remote Radio's TX Level (CLI)

To set the transmit (TX) level of the remote radio, enter the following command in radio view:

```
radio[x/x]>remote-unit set tx-level <tx-level>
```

To display the transmit (TX) level of the remote radio, enter the following command in radio view:

```
radio[x/x]>remote-unit show tx-level
```

Table 94: 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
```

16.1.6. Configuring Remote ATPC (CLI)

To set the RX reference level for ATPC on the remote radio, enter the following command in radio view:

```
radio[x/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 in radio view:

```
radio[x/x]>remote-unit atpc show ref-level
```

Table 95: 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
```

16.2. Configuring ATPC (CLI)

Automatic TX Power Control (ATPC) is a closed-loop mechanism by which each carrier adjusts its transmitted signal power according to the indication received across the link, in order to achieve a desired RSL on the other side of the link. Without ATPC, if loss of frame occurs the system automatically increases its transmit power to the configured maximum. This may cause a higher level of interference with other systems until the failure is corrected.

Note

You cannot use ATPC in MIMO mode. See *Configuring MIMO and Space Diversity (CLI)*.

To enable or disable ATPC, enter the following command in radio view:

```
radio[x/x]>atpc set admin <admin>
```

To display whether or not ATPC is enabled, enter the following command in radio view:

```
radio[x/x]>atpc show admin
```

To set the RX reference level for ATPC, enter the following command in radio view

```
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 in radio view:

```
radio[x/x]>atpc show rx-level
```

Table 96: 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.

The following commands enable ATPC mode for radio carrier 1 and set the RX reference level to -55:

```
radio[2/1]>atpc set admin enable
radio[2/1]>atpc set rx-level atpc_ref_rx_level -55
```

16.3. Configuring Header De-Duplication (CLI)

Note

Header De-Duplication is supported for NetStream Diplo and NetStream Primo. For NS Primo/DiploE, Header De-Duplication is planned for future release.

Header De-Duplication identifies traffic flows and replaces header fields with a flow ID. The Header De-Duplication module includes an algorithm for learning each new flow, and implements compression on the flow type starting with the next frame of that flow type.

You can determine the depth to which the compression mechanism operates, from Layer 2 to Layer 4. You must balance the depth of compression against the number of flows in order to ensure maximum efficiency. Multi-Layer (Enhanced) compression supports up to 256 flow types.

Note

The Header De-Duplication configuration must be identical on both sides of the link.

To configure Header De-Duplication, enter the following command in radio view:

```
radio[2/1]> compression header-compression set <mode>
```

Note

In this release, if two radio carriers in an NetStream Diplo 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 in radio view:

```
radio[x/x]>clear-ethernet-port-counters
```

Table 97: Header De-Duplication CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin	Variable	Enable disable	Enables or disables ATPC mode.
mode	Variable	Disabled Layer2 MPLS Layer3 Layer4 Tunnel Tunnel-Layer3 Tunnel-Layer4	Disabled - Header De-Duplication is disabled. Layer2 - Header De-Duplication operates on the Ethernet level. MPLS - Header De-Duplication operates on the Ethernet and MPLS levels. Layer3 - Header De-Duplication operates on the Ethernet and IP levels. Layer4 - Header De-Duplication operates on all supported layers up to Layer 4. Tunnel - Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel layer for packets carrying GTP or GRE frames. Tunnel-Layer3 - Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel and T-3 layers for packets carrying GTP or GRE frames. Tunnel-Layer4 - Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel, T-3, and T-4 layers for packets carrying GTP or GRE frames.

The following command enables Layer 2 Header De-Duplication on radio carrier 1:

```
root> radio slot 2 port 1
radio[2/1]> compression header-compression set Layer2
```

16.3.1. Displaying Header De-Duplication Information (CLI)

To display the current Header De-Duplication configuration, enter the following command in radio view:

```
radio[2/1]> compression show-configuration
```

To display counters for Header De-Duplication, enter the following command in radio view:

```
radio[2/1]> compression show-configuration
```

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.

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

Frame Cut-Through cannot be used together with 1588 Transparent Clock.

Note

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
```

16.5. Configuring AES-256 Payload Encryption (CLI)

Note

This feature is only relevant for NetStream Diplo and NetStream Primo units. This feature is not supported with MIMO links.

This feature requires:

- Requires an activation key. If no valid AES activation key has been applied to the unit, AES will not operate on the unit. See *Configuring the Activation Key (CLI)*.

Note

In order for the AES activation key to become active, you must reset the unit after configuring a valid AES activation key. Until the unit is reset, an alarm will be present if you enable AES. This is not the case for other activation keys.

NetStream Diplo and NetStream Primo 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.

NS Primo/Diplo uses a dual-key encryption mechanism for AES:

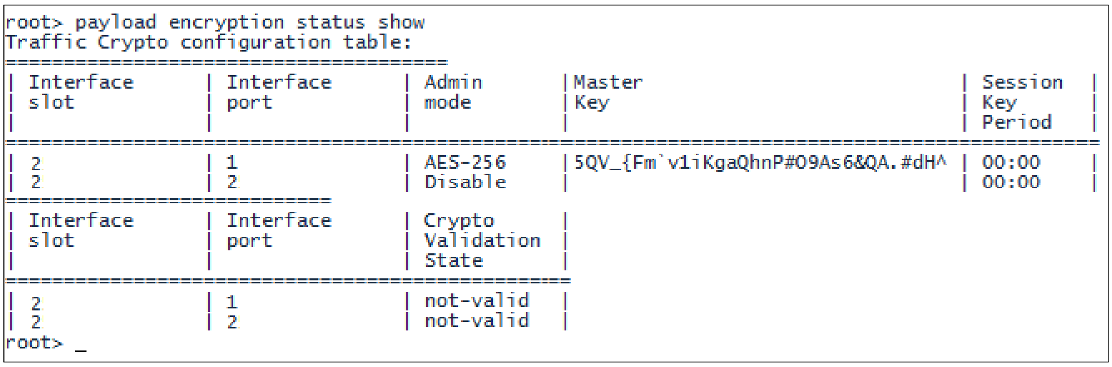
- The user provides a master key. The master key can also be generated by the system upon user command. The master key is a 32-byte symmetric encryption key. The same master key must be manually configured on both ends of the encrypted link.
- The session key is a 32-byte symmetric encryption key used 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      | Interface      | Admin       |Master                           | Session  |
| slot           | port           | mode        |Key                              | Key      |
|                |                |             |                                 | Period   |
==============================================================================================
| 2              | 1              | AES-256     |5QV_{Fm`v1iKgaQhnP#O9As6&QA.#dH^ | 00:00    |
| 2              | 2              | Disable     |                                 | 00:00    |
============================
| Interface      | Interface      | Crypto      |
| slot           | port           | Validation  |
|                |                | State       |
================================================
| 2              | 1              | not-valid   |
| 2              | 2              | not-valid   |
root> _
```

To configure AES on a radio carrier, you must first enter traffic encryption view for the specific radio. To enter traffic 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

Traffic Encryption [1/1]>
```

To display the payload encryption mode of the radio interface, enter the following command in Traffic Encryption view:

```
Traffic Encryption [2/x]> payload encryption mode show
```

The following display indicates that payload encryption is enabled on radio interface 1:

```
Traffic Encryption [2/1]> payload encryption mode show

Admin Mode: AES-256
```

The following display indicates that payload encryption is disabled on radio interface 1:

```
Traffic Encryption [2/1]> payload encryption mode show

Admin Mode: Disable
```

To enable payload encryption, enter the following command in Traffic Encryption view:

```
Traffic Encryption [2/x]> payload encryption mode admin AES-256
```

To disable payload encryption, enter the following command in Traffic Encryption view:

```
Traffic Encryption [2/x]> payload encryption mode admin Disable
```

Configure the master key by doing one of the following:

- Enter a master key manually.
- Generate the master key automatically.

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

To define the master key manually, enter the following command in Traffic Encryption view:

```
Traffic Encryption [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 Traffic Encryption view:

```
Traffic Encryption [2/x]> master key generate
```

A random master key is generated. You must copy and paste this key to the remote 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.

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 formats the unit's disk, and renders the unit non-operational. If it is necessary to use this command, contact Netronics Technical Support for instructions how to re-configure the unit.

The session key is automatically regenerated at defined intervals. To set the session key regeneration interval, enter the following command in Traffic Encryption view:

```
Traffic 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:

```
Traffic Encryption [2/1]> payload encryption session-key period
set 04:15
```

To display the session key regeneration interval, enter the following command in Traffic Encryption view:

```
Traffic Encryption [2/x]> payload encryption session-key period
show
```

Note

Any time payload encryption fails, the Operational status of the link is Down until payload encryption is successfully restored.

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.

To enable Frame Cut-Through on a radio carrier, go to radio view and enter the following command:

To clear Ethernet port counters, including both Frame Cut-Through and Header De-Duplication counters, go to radio view and enter the following command:

● Parameter	● Input Type	● Permitted Values	● Description
● mode	● Variable	● yes ● no	● yes - Enables Frame Cut-Through ● no - Disables Frame Cut-Through

The following command enables Frame Cut-Through for radio carrier 1 in an NetStream Diplo or NetStream Primo unit :

The following command enables Frame Cut-Through for the radio in an NS Primo/DiploE unit:

To display the current Frame Cut-Through mode for carrier, go to radio view and enter the following command:

To display counters for Frame Cut-Through for a carrier, go to radio view and enter the following command:

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:

16.6. 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)*

16.6.1. Displaying General Modem Status and Defective Block PMs (CLI)

To display the general status of the modem, enter the following command in radio view:

```
radio[x/x]>modem show status
```

The following is a sample output of the `modem show status` command:

```
MSE[db]: -99.00
Defective Blocks count: 0

Current Tx profile: 0
Current Tx QAM: 4
Current Tx rate(Kbps): 43389
Current Rx profile: 0
Current Rx QAM: 4
Current Rx rate(Kbps): 43389
radio [2/1]>modem show status
```

To clear all radio PMs in the system, enter the following command in root view:

```
root> radio pm clear all
```

To clear defective blocks counters for a radio, enter the following command in radio view:

```
radio[x/x]>modem clear counters
```

16.6.2. Displaying Excessive BER (Aggregate) PMs (CLI)

You can display modem BER (Bit Error Rate) PMs in either 15-minute or daily intervals.

To display modem BER PMs in 15-minute intervals, enter the following command in radio view:

```
radio [x/x]>framer pm-aggregate show interval 15min
```

The following is a partial sample output of the `framer pm-aggregate show interval 15min` command:

```
radio [2/1]>framer pm-aggregate show interval 15min
Modem BER PM table:
===================

Interval    Integrity    ES      SES       UAS        BBE
===========================================================
0           1            0       0         333         0
1           1            0       0         900         0
2           1            0       0         900         0
3           1            0       0         900         0
4           1            0       0         900         0
5           1            0       0         900         0
6           1            0       0         900         0
7           1            0       0         900         0
8           1            0       0         900         0

radio [2/1]>
```

To display modem BER PMs in daily intervals, enter the following command in radio view:

```
radio [x/x]>framer pm-aggregate show interval 24hr
```

The following is a sample output of the `framer pm-aggregate show interval 24hr` command:

```
radio [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 99: 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.

16.6.3. Displaying BER Level and Configuring BER Parameters (CLI)

To display the current BER level, enter the following command in radio view:

```
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 in radio view:

```
radio [x/x]>modem excessive-ber set threshold <threshold>
```

To display the excessive BER threshold, enter the following command in radio view:

```
radio [x/x]>modem excessive-ber show threshold
```

Table 100: Excessive BER CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin	Variable	enable disable	Enables or disables propagation of excessive BER as a fault.
threshold	Variable	1e -3 1e -4 1e -5	The level above which an excessive BER alarm is issued for errors detected over the radio link.

The following command enables `excessive-ber`:

```
root> radio excessive-ber set admin enable
```

The following command sets the excessive BER threshold to 1e-5:

```
radio [2/1]>modem excessive-ber set threshold 1e-5
```

16.6.4. Configuring RSL Thresholds (CLI)

You can set two RSL (RX Signal Level) thresholds. The number of seconds during which the RSL exceeds these thresholds are counted as RSL Exceed Threshold Seconds. See *Displaying RSL and TSL Levels (CLI)*.

To set the RSL thresholds, enter the following command in radio view:

```
radio [x/x]>rf pm-rsl set threshold1 <threshold1> threshold2
<threshold2>
```

Table 101: 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
```

16.6.5. Configuring TSL Thresholds (CLI)

The number of seconds during which the TX Signal Level exceeds the TSL threshold are counted as TSL Exceed Threshold Seconds. See *Displaying RSL and TSL Levels (CLI)*.

To set the TSL threshold, enter the following command in radio view:

```
radio [x/x]>rf pm-tsl set threshold -15
```

Table 102: TSL Thresholds CLI Parameters

Parameter	Input Type	Permitted Values	Description
threshold	Number	-10 - 34	The TSL threshold (dBm).

The following command sets the TSL threshold to 10 dBm:

```
radio [2/1]>rf pm-tsl set threshold 10
```

16.6.6. Displaying RSL and TSL Levels (CLI)

You can display the RSL (RX Signal Level) and TSL (TX Signal Level) PMs in either 15-minute or daily intervals.

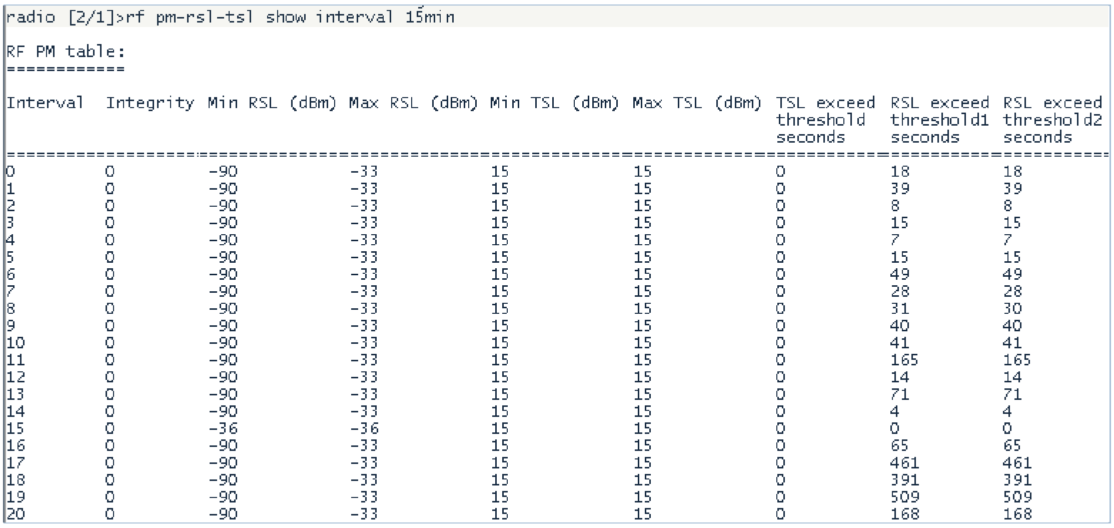
To display RSL and TSL PMs in 15-minute intervals, enter the following command in radio view:

```
radio [x/x]>rf pm-rsl-tsl show interval 15min
```

To display RSL and TSL PMs in daily intervals, enter the following command in radio view:

```
radio [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 103: 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)*.

16.6.7. Configuring the Signal Level Threshold (CLI)

To set the BER (Bit Error Rate) level above which a Signal Degrade alarm is issued for errors detected over the radio link, enter the following command in radio view:

```
radio [x/x]>modem signal-degrade set threshold 1e-7
```

To display the Signal Degrade BER threshold, enter the following command in radio view:

```
radio [x/x]>modem signal-degrade show threshold
```

Table 104: 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
```

16.6.8. Configuring the MSE Thresholds and Displaying the MSE PMs (CLI)

To configure the MSE (Mean Square Error) threshold, enter the following command in radio view:

```
radio [x/x]>modem set mse-exceed threshold <threshold>
```

To display the currently configured MSE threshold, enter the following command in radio view:

```
radio [x/x]>modem show threshold-mse-exceed
```

Table 105: MSE CLI Parameters

Parameter	Input Type	Permitted Values	Description
threshold	Number	-99 - -1	The MSE threshold.

To display MSE (Mean Square Error) PMs in 15-minute intervals, enter the following command in radio view:

```
radio [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 in radio view:

```
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 106: 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.
Min MSE (dB)	Indicates the minimum MSE in dB, measured during the interval.
Max MSE (dB)	Indicates the maximum MSE in dB, measured during the interval.
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
```

16.6.9. 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 in radio view:

```
radio[x/x]>modem set threshold-xpi-exceed threshold <threshold>
```

To display the currently configured XPI threshold, enter the following command in radio view:

```
radio[x/x]>modem show threshold-xpi-below
```

Table 107: XPI Threshold CLI Parameters

Parameter	Input Type	Permitted Values	Description
threshold	Number	0-99	The XPI threshold.

To display XPI PMs in 15-minute intervals, enter the following command in radio view:

```
radio[x/x]>modem pm-xpi show interval 15min
```

The following is a partial sample output of the `modem pm-xpi show interval 15min` command:

```
radio [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 in radio view:

```
radio[x/x]>modem pm-xpi show interval 24hr
```

The following is a partial sample output of the `modem pm-xpi show interval 24hr` command:

```
radio [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 108: 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
```

16.6.10. Displaying ACM PMs (CLI)

To display ACM PMs in 15-minute intervals, enter the following command in radio view:

```
radio [x/x]>mrmc pm-acm show interval 15min
```

The following is a partial sample output of the `modem pm-acm show interval 15min` command:

```
radio [2/1]>mrmc pm-acm show interval 15min


MRMC 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 in radio view:

```
radio [x/x]>mrmc pm-acm show interval 24hr
```

The following is sample output of the `modem pm-acm show interval 24hr` command:

```
radio [2/1]>mrmc pm-acm show interval 24hr

MRMC 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 109: 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.

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 (CLI)*
- *Viewing Ethernet PMs and Statistics (CLI)*

Related topics:

- Configuring Link Aggregation (LAG) (Optional) (CLI)
- *Quality of Service (QoS) (CLI)*
- *Ethernet Protocols (CLI)*
- *Performing Ethernet Loopback (CLI)*

17.1. Configuring Ethernet Services (CLI)

This section includes:

- *Ethernet Services Overview (CLI)*
- *General Guidelines for Provisioning Ethernet Services (CLI)*
- *Defining Services (CLI)*
- *Configuring Service Points (CLI)*
- *Defining the MAC Address Forwarding Table for a Service (CLI)*

17.1.1. 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 NS Primo/Diplo network element.

This version of NS Primo/Diplo supports the following service types:

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

In addition to user-defined services, NS Primo/Diplo 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 (CLI)*.

A service point is a logical entity attached to a physical or logical interface. Service points define the movement of frames through the service. Each service point includes both ingress and egress attributes. A Point-to-Point or Multipoint service can hold up to 32 service points. A Management service can hold up 30 service points.

For a more detailed overview of the NS Primo/Diplo service-oriented Ethernet switching engine, refer to the Technical Description for the NS Primo/Diplo product type you are using.

17.1.2. General Guidelines for Provisioning Ethernet Services (CLI)

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

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

17.1.3. Defining Services (CLI)

Use the commands described in the following sections to define a service and its parameters. After defining the service, you must add service points to the service in order for the service to carry traffic.

17.1.3.1. Adding a Service (CLI)

To add a service, enter the following command in root view:

```
root> ethernet service add type <service type> sid <sid> admin
<service admin mode> evc-id <evc-id> description <evc-
description>
```

Table 110: 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.

17.1.3.2. 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 111: 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]>
```

17.1.3.3. 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
```

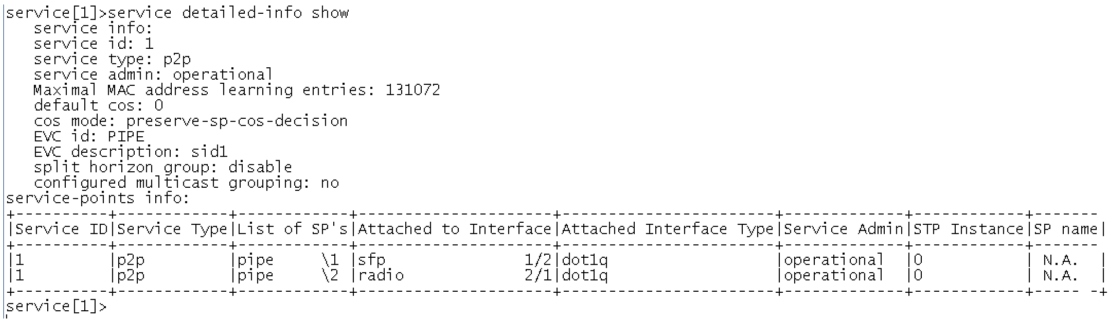
```
service info:
service id: 1
service type: p2p
service admin: operational
Maximal MAC address learning entries: 131072
default cos: 0
cos mode: preserve-sp-cos-decision
EVC id: N.A.
EVC description: N.A.
split horizon group: disable
configured multicast grouping: no
```

```
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]>
```

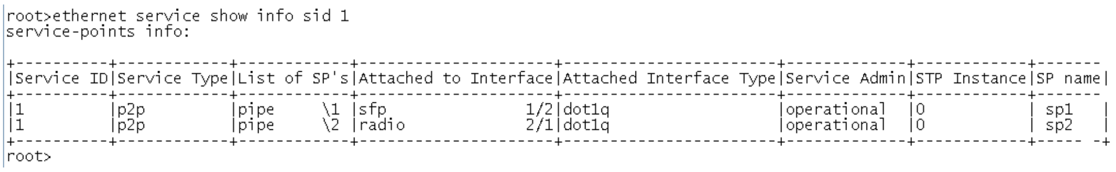
To display a list of service points and their attributes, enter the following command in root view:

```
root>ethernet service show info sid <sid>
```

Table 112: Displaying Ethernet Service Details CLI Parameters

Parameter	Input Type	Permitted Values	Default	Description
sid	Number	Any defined Service ID.	None	The Service ID.

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>
```

17.1.3.4. 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 113: 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
```

17.1.3.5. 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 114: 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
```

17.1.3.6. 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 115: 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
```

17.1.3.7. 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 116: 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
```

17.1.4. Configuring Service Points (CLI)

This section includes:

17.1.4.1. Service Points Overview (CLI)

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

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

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

Management services utilize Management (MNG) service points.

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

Table 117 summarizes the service point types available per service type.

Table 117: 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 118 shows which service point types can co-exist on the same interface.

Table 118: 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.

17.1.4.2. 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 119 and *Table 120* show which service point – Interface Type combinations can co-exist on the same interface.

Table 119: 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 120: 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

17.1.4.3. 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 121: Add Service Point CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-type	Variable	sap snp pipe mng	● SAP - Service Access Point ● SNP - Service Network Point ● PIPE - Pipe service point ● MNG - Management service point
int-type	Variable	all-to-one dot1q s-tag bundle-c-tag bundle-s-tag qinq	Determines which frames enter the service via this service point, based on the frame's VLAN tagging. Since more than one service point may be associated with a single interface, frames are assigned to the earliest defined service point in case of conflict. ● all-to-one - All C-VLANs and untagged frames that enter the interface are classified to the service point. Only valid for SAP service point types. ● dot1q - A single C-VLAN is classified to the service point. Valid for all service point types. ● s-tag - A single S- VLAN is classified to the service point. Valid for SNP and MNG service point types. ● bundle-c-tag - A set of multiple C-VLANs is classified to the service point. Only valid for SAP service point types. ● bundle-s-tag - A single S-VLAN and a set of multiple C-VLANs are classified to the service point. Only valid for SAP service point types. ● qinq - A single S-VLAN and C-VLAN combination is classified to the service point. Valid for SAP and MNG service point types.
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	This ID is unique within the service.
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 HSP protection are only relevant for NetStream Diplo units.
slot	Number	Ethernet: 1 Radio: 2	
port	Number	For an Ethernet interface: 1-3 For a radio interface in NetStream Diplo units: 1-2 For a radio interface in NetStream Primo and NS Primo/DiploE units: 1	The port or radio carrier on which the service point is located.
vlan	Number or Variable	1-4094 (except 4092 which is reserved for the default management service), or Untagged	Defines the VLAN classified to the service point. This parameter should not be included for service points with an interface type of bundle-C-tag. For instructions on attaching a bundled VLAN, refer to *Attaching a VLAN Bundle to a Service Point (CLI)*. This parameter is also not relevant for: Service points with an interface type of qinq and all-to-one. Pipe service points.
outer-vlan	Number	1-4094 (except 4092, which is reserved for the default management service), or Untagged	Defines the S-VLAN classified to the service point. This parameter is only relevant for service points with the interface type bundle-s-tag or qinq.
inner-vlan	Number	1-4094 (except 4092, which is reserved for the default management service), or Untagged	Defines the C-VLAN classified to the service point. This parameter is only relevant for service points with the interface type qinq.
sp-name	Text string	Up to 20 characters.	A descriptive name for the service point (optional).

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-c-tag. This service point is located on radio carrier 1.

```
service[37]>sp add sp-type sap int-type bundle-c-tag spid 10
interface radio slot 2 port 1 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 an NetStream Diplo 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 an NetStream Diplo 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 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 snp int-type dot1q spid 10 interface
radio slot 2 port 1 vlan 100 sp-name Radio
```

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 command adds a Pipe service point with Service Point ID 2 to Service 1, with interface type dot1q. This service point is located on radio carrier 1.

```
service[1]>sp add sp-type pipe int-type dot1q spid 2 interface
radio slot 2 port 1 sp-name pipe_dot1q_radio
```

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]>
```

17.1.4.4. 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 122: 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 123: 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 124: 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
```

17.1.4.5. Configuring Service Point Egress Attributes (CLI)

A service point's egress attributes are attributes that operate upon frames ingressing via the service point. This includes VLAN preservation and marking attributes.

This section includes:

- *Configuring VLAN and CoS Preservation (CLI)*
- *Configuring Service Bundles (CLI)*
- *Attaching a VLAN Bundle to a Service Point (CLI)*

Configuring VLAN and CoS Preservation (CLI)

CoS and VLAN preservation determines whether the CoS and/or VLAN IDs of frames egressing the service via the service point are restored to the values they had when the frame entered the service.

This section includes:

- *Configuring C-VLAN CoS Preservation (CLI)*
- *Configuring C-VLAN Preservation (CLI)*
- *Configuring S-VLAN CoS Preservation (CLI)*

Configuring C-VLAN CoS Preservation (CLI)

To configure CoS preservation for C-VLAN-tagged frames, go to service view for the service and enter the following command:

```
service[SID]>sp cvlan-cos-preservation-mode set spid <sp-id>
mode <c-vlan cos preservation mode>
```

Table 125: 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
```

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 126: 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
```

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 127: 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 128: 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 classify untagged frames to a bundle-c-tag or bundle s-tag service point, go to service view for the service and enter the following command:

```
service[SIP]>sp bundle attach untagged spid <sp-id>
```

To remove a VLAN Bundle from a bundle-c-tag or bundle-s-tag service point, go to service view for the service and enter the following command:

```
service[SIP]>sp bundle cvlan remove spid <sp-id> vlan <vlan>
to-vlan <to-vlan>
```

To removed untagged frames from a bundle-c-tag or bundle s-tag service point, go to service view for the service and enter the following command:

```
service[SIP]>sp bundle remove untagged spid <sp-id>
```

To display a service point’s attributes, including the VLANs classified to a bundle service point, go to service view for the service to which the service point belongs and enter the following command:

```
service[SID]>sp service-point-info show spid <sp-id>
```

Table 129: 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 classifies untagged frames to Service Point 1 in Service 37:

```
service[37]>sp bundle attach untagged spid 1
```

The following command removes C-VLANs 100 through 200 from Service Point 1 in Service 37:

```
service[37]>sp bundle cvlan remove spid 1 vlan 100 to-vlan 200
```

The following command removes untagged frames to Service Point 1 in Service 37:

```
service[37]>sp bundle remove untagged spid 1
```

17.1.4.6. 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 130: 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
```

17.1.4.7. 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 131: 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
```

17.1.5. Defining the MAC Address Forwarding Table for a Service (CLI)

This section includes:

- *MAC Address Forwarding Table Overview (CLI)*
- *Setting the Maximum Size of the MAC Address Forwarding Table (CLI)*
- *Setting the MAC Address Forwarding Table Aging Time (CLI)*
- *Adding a Static MAC Address to the Forwarding Table (CLI)*
- *Displaying the MAC Address Forwarding Table (CLI)*
- *Flushing the MAC Address Forwarding Table (CLI)*
- *Enabling MAC Address Learning on a Service Point (CLI)*

17.1.5.1. MAC Address Forwarding Table Overview (CLI)

NS Primo/Diplo performs MAC address learning per service. NS Primo/Diplo 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.

17.1.5.2. 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 132: 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
```

17.1.5.3. 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 133: 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
```

17.1.5.4. 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 134: 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
```

17.1.5.5. 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
```

17.1.5.6. 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
```

17.1.5.7. 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 135: Enabling MAC Address Learning CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32	The Service Point ID of the service point associated with the MAC address.
learning	Variable	Enable disable	Select enable or disable to enable or disable MAC address learning for frames that ingress via the service point. When enabled, the service point learns the source MAC addresses of incoming frames and adds them to the MAC address forwarding table.

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
```

17.2. Setting the MRU Size and the S-VLAN Ethertype (CLI)

The following parameters are configured globally for the NS Primo/Diplo 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. NS Primo/Diplo 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)*

17.2.1. Configuring the S-VLAN Ethertype (CLI)

To configure the S-VLAN Ethertype, enter the following command in root view:

```
root> ethernet generalcfg ethertype set svlan-value <ethertype>
```

To display the system S-VLAN ethertype, enter the following command in root view:

```
root> ethernet generalcfg ethertype show svlan
```

Table 136: Configure S-VLAN Ethertype CLI Parameters

Parameter	Input Type	Permitted Values	Description
ethertype	Hexadecimal	0x8100 0x88a8 0x9100 0x9200	Defines the ethertype recognized by the system as the S-VLAN ethertype.

Example

For example, the following command sets the system S-VLAN ethertype to 0x88a8:

```
root> ethernet generalcfg ethertype set svlan-value 0x88a8
```

17.2.2. Configuring the C-VLAN Ethertype (CLI)

The system C-VLAN Ethertype is set by the system as 0x8100.

To display the system C-VLAN ethertype, enter the following command in root view:

```
root> ethernet generalcfg ethertype show cvlan
```

17.2.3. Configuring the MRU (CLI)

To define the global size (in bytes) of the Maximum Receive Unit (MRU), enter the following command in root view:

```
root> ethernet generalcfg mru set size <size>
```

To display the system MRU, enter the following command in root view:

```
root> ethernet generalcfg mru show
```

Table 137: 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
```

17.3. Configuring Ethernet Interfaces (CLI)

Related Topics:

- *Enabling the Interfaces (CLI)*
- *Performing Ethernet Loopback (CLI)*
- *Configuring Ethernet Services (CLI)*
- *Quality of Service (QoS) (CLI)*

NetStream Primo/Diplo'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)*

17.3.1. Entering Interface View (CLI)

To view interface details and set the interface's parameters, you must enter the interface's view level in the CLI.

Use the following command to enter an Ethernet interface's view level:

```
root> ethernet interfaces eth slot <slot> port <port>
```

Use the following command to enter the radio interface's view level:

```
root> ethernet interfaces radio slot <slot> port <port>
```

Use the following command to enter the view level of a group, such as a Multi-Carrier ABC group, an HSB protection group, or a LAG:

```
root> ethernet interfaces group <group>
```

Table 138: 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: 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 (NetStream Diplo 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 NetStream Diplo.

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 an NetStream Diplo 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 an NetStream Primo or an NS Primo/DiploE unit:

```
root> ethernet interfaces radio slot 2 port 1
```

The following prompt appears:

```
radio [2/1]>
```

The following command enters interface view for LAG 1:

```
root> ethernet interfaces group lag1
```

The following prompt appears:

```
eth type group [64/1]>
```

Note

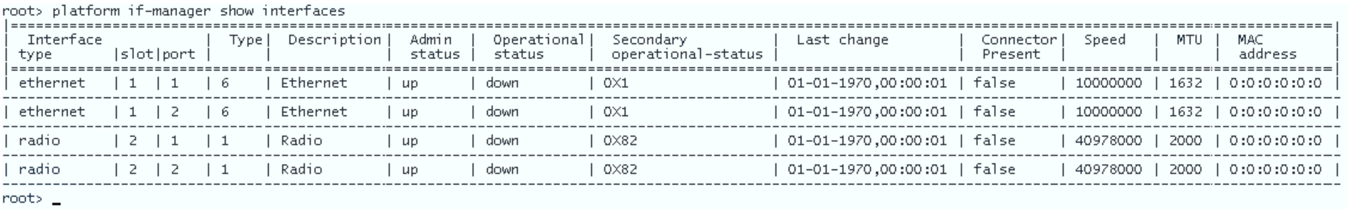
For simplicity, the examples in the following sections show the prompt for an Ethernet interface.

17.3.2. Displaying the Operational State of the Interfaces in the Unit (CLI)

To display a list of all interfaces in the unit and their operational states, enter the following command:

```
root> platform if-manager show interfaces
```

The following is a sample output of this command:



```
root> platform if-manager show interfaces
|=================================================================================================================================================================|
|  Interface             |  Type|  Description|  Admin  |  Operational|  Secondary              |  Last change          |  Connector|  Speed    |  MTU |  MAC          |
| type      |slot|port |      |             |  status |  status     |  operational-status     |                       |  Present  |           |      |  address      |
|=================================================================================================================================================================|
| 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> _
```

17.3.3. Viewing Interface Attributes (CLI)

To display an interface’s attributes, go to interface view for the interface and enter the following command:

```
eth type eth [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
```

17.3.4. 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 139: 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
```

17.3.5. 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 140: Interface Speed and Duplex State CLI Parameters

Parameter	Input Type	Permitted Values	Description
speed-and-duplex state	Variable	'10hd' '10fd' '100hd' '100fd' '1000fd'	This parameter sets the maximum speed and the duplex state of the interface. For RJ-45 interfaces, any of the permitted values 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'
```

17.3.6. 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 141: 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
```

17.3.7. 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 142: 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
```

17.3.8. 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 143: 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
```

17.3.9. 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 144: 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
```

17.3.10. Displaying Interface Statistics (RMON) (CLI)

NS Primo/Diplo 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 145: 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 an NetStream Diplo or NetStream Primo 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
```

17.4. Configuring Automatic State Propagation (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.

You must first configure automatic state propagation for a pair consisting of an Ethernet interface, on the one hand, and a radio interface, Multi-Carrier ABC group, or HSB protection group, on the other. You must then use a separate command to enable automatic state propagation on the selected pair and determine whether a failure on the remote side of the link is propagated to the local interface.

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

This section includes:

- *Configuring Automatic State Propagation to an Ethernet Port (CLI)*
- *Enabling Automatic State Propagation (CLI)*
- *Deleting Automatic State Propagation (CLI)*
- *Displaying Automatic State Propagation Parameters (CLI)*

17.4.1. Configuring Automatic State Propagation to an Ethernet Port (CLI)

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>
```

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>
```

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>
```

Table 146: 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 (NetStream Diplo only): 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 NetStream Diplo units.
protection-group	Number	1-4	The HSB-SD protection group failure of which is propagated to the defined interface. **Note**: Only relevant for NetStream Diplo units.

Example

The following commands configure and enable automatic state propagation to propagate faults from radio interface 1 to Ethernet port 1.

```
root> auto-state-propagation add eth-port-to-radio eth-slot 1
eth-port 1 radio-slot 2 radio-port 1
```

The following commands configure and enable automatic state propagation to propagate faults from Multi-Carrier ABC group 1 to Ethernet port 1 on an NetStream Diplo unit.

```
root> auto-state-propagation add eth-port-to-multi-radio-group
eth-slot 1 eth-port 1 multi-radio-group 1
```

The following commands configure and enable automatic state propagation to propagate faults from 1+1 HSB-SD protection group 1 to Ethernet port 1 on an NetStream Diplo unit.

```
root> auto-state-propagation add eth-port-to-protection-group
eth-slot 1 eth-port 1 protection-group 1
```

17.4.2. Enabling Automatic State Propagation (CLI)

To enable automatic state propagation on an Ethernet port and determine whether remote interface failures are also propagated, 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>
```

Table 147: Enable Automatic State Propagation 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.
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.

Example

The following command enables automatic state propagation to Ethernet port 1, and specifies that faults on the remote carrier are also propagated to Ethernet port 1. CSF mode is enabled.

```
root> auto-state-propagation configure eth-port eth-slot 1 eth-
port 1 asp-admin enable remote-fault-trigger-admin enable csf-
mode-admin enable
```

17.4.3. Deleting Automatic State Propagation (CLI)

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>
```

Table 148: Delete Automatic State Propagation 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 wanted to propagate faults from the selected radio or group.

17.4.4. Displaying Automatic State Propagation Parameters (CLI)

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 149: Display Automatic State Propagation 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 propagate faults from the selected radio or group.

17.5. Viewing Ethernet PMs and Statistics (CLI)

NS Primo/Diplo 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)*

17.5.1. 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 150: 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
```

17.5.2. Configuring Ethernet Port PMs and PM Thresholds (CLI)

To enable the gathering of PMs for an Ethernet interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm set admin <enable|disable>
```

You can configure thresholds and display the number of seconds these thresholds were exceeded during a specified interval.

To configure interface PM thresholds, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm set thresholds rx-layer1-rate-threshold
<0-4294967295> tx-layer1-rate-threshold <0-4294967295>
```

To display whether or not PM gathering is enabled for an Ethernet interface, as well as the configured thresholds, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show configuration
```

Table 151: Port PM Thresholds CLI Parameters

Parameter	Input Type	Permitted Values	Description
rx-layer1-rate-thershold	Number	0-4294967295	The exceed threshold for port RX PMs, in bytes per second.
tx-layer1-rate-thershold	Number	0-4294967295	The exceed threshold for port TX PMs, in bytes per second.

The following commands bring you to interface view for Ethernet port 1, enable PM gathering, and set the thresholds for RX and TX PMs at 850,000,000 bytes per second:

```
root> ethernet interfaces eth slot 1 port 1

eth type eth [1/1]>pm set admin enable

eth type eth [1/1]>pm set thresholds rx-layer1-rate-threshold
850000000 tx-layer1-rate-threshold 850000000
```

17.5.3. Displaying Ethernet Port PMs (CLI)

Note

The port PM results may be several pages long. Remember:

To view the next results page, press the space bar.
To end the list and return to the most recent prompt, press the letter q.

To display RX packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-packets interval 15min
```

To display RX packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-packets interval 24hr
```

To display RX broadcast packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bcast-packets interval 15min
```

To display RX broadcast packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bcast-packets interval 24hr
```

To display RX multicast packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-mcast-packets interval 15min
```

To display RX multicast packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-mcast-packets interval 24hr
```

To display Layer 1 RX PMs, in bytes per second, in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bytes-layer1 interval 15min
```

To display Layer 1 RX PMs, in bytes per second, in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bytes-layer1 interval 24hr
```

To display Layer 2 RX PMs, in bytes per second, in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bytes-layer2 interval 15min
```

To display Layer 2 RX PMs, in bytes per second, in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show rx-bytes-layer2 interval 24hr
```

To display TX packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-packets interval 15min
```

To display TX packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-packets interval 24hr
```

To display TX broadcast packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bcast-packets interval 15min
```

To display TX broadcast packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bcast-packets interval 24hr
```

To display TX multicast packet PMs in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-mcast-packets interval 15min
```

To display TX multicast packet PMs in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-mcast-packets interval 24hr
```

To display Layer 1 TX PMs, in bytes per second, in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bytes-layer1 interval 15min
```

To display Layer 1 TX PMs, in bytes per second, in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bytes-layer1 interval 24hr
```

To display Layer 2 TX PMs, in bytes per second, in 15-minute intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bytes-layer2 interval 15min
```

To display Layer 2 TX PMs, in bytes per second, in 24-hour intervals, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm show tx-bytes-layer2 interval 24hr
```

Table 152: Ethernet Port PMs

Parameter	Definition
Interval	For 24-hour intervals, displays the date of the interval. For 15-minute intervals, displays the date and ending time of the interval.
Invalid data flag	Indicates whether the values received during the measured interval are valid. An x in the column indicates that the values are not valid (for example, because of a power surge or power failure that occurred during the interval).
Peak RX Packets	The peak rate of RX packets per second for the measured time interval.
Average RX Packets	The average rate of RX packets per second for the measured time interval.
Peak RX Broadcast Packets	The peak rate of RX broadcast packets per second for the measured time interval.
Average RX Broadcast Packets	The average rate of RX broadcast packets per second for the measured time interval.
Peak RX Multicast Packets	The peak rate of RX multicast packets per second for the measured time interval.
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).

17.5.4. Clearing Ethernet Port PMs (CLI)

To clear all PMs for an Ethernet interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> pm clear-all
```

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)*

18.1. Configuring Classification (CLI)

This section includes:

- *Classification Overview (CLI)*
- *Configuring Ingress Path Classification on a Logical Interface (CLI)*
- *Configuring VLAN Classification and Override (CLI)*
- *Configuring 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)*

18.1.1. Classification Overview (CLI)

NS Primo/Diplo 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

18.1.2. Configuring Ingress Path Classification on a Logical Interface (CLI)

Logical interface-level classification enables you to configure classification on a single interface or on a number of interfaces grouped tougher, such as a LAG group.

The classifier at the logical interface level supports the following classification methods, listed from highest to lowest priority. A higher level classification method supersedes a lower level classification method:

- VLAN ID
- 802.1p bits.
- DSCP values.
- MPLS EXP field.
- Default CoS

NS Primo/Diplo 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.

18.1.3. Configuring VLAN Classification and Override (CLI)

You can specify a specific CoS and Color for a specific VLAN ID. In the case of double-tagged frames, the match must be with the frame's outer VLAN. Permitted values are CoS 0 to 7 and Color Green or Yellow per VLAN ID. This is the highest classification priority on the logical interface level, and overrides any other classification criteria at the logical interface level.

To configure CoS and Color override based on VLAN ID, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>vlan-cos-override set outer-vlan-id <outer-
vlan-id> inner-vlan-id <inner-vlan-id> use-cos <use-cos> use-
color <use-color>
```

To display configured VLAN-based CoS and Color override values, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>vlan-cos-override show outer-vlan-id <outer-
vlan-id> inner-vlan-id <inner-vlan-id>
```

To delete a set of VLAN-based CoS and Color override values, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>vlan-cos-override delete outer-vlan-id
<outer-vlan-id> inner-vlan-id <inner-vlan-id>
```

Table 153: 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.
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 `outer-vlan-id` and `inner-vlan-id` values, respectively, in order for the defined CoS and Color values to be applied to the frame.
use-cos	Number	0 – 7	The CoS value applied to matching frames.
use-color	Variable	green yellow	The Color applied to matching frames.

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
```

18.1.4. 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)*

18.1.4.1. 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 154: 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 ingressing 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
```

18.1.4.2. 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 155: 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 156: 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.

Example

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
```

18.1.4.3. 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 157: S-VLAN 802.1 UP and DEI Bit Classification Table Default Values

802.1 UP	DEI	CoS (Configurable)	Color (Configurable)
0	0	0	Green
0	1	0	Yellow
1	0	1	Green
1	1	1	Yellow
2	0	2	Green
2	1	2	Yellow
3	0	3	Green
3	1	3	Yellow
4	0	4	Green
4	1	4	Yellow
5	0	5	Green
5	1	5	Yellow
6	0	6	Green
6	1	6	Yellow
7	0	7	Green
7	1	7	Yellow

To modify the S-VLAN 802.1 UP and DEI bit classification table, enter the following command:

```
root> ethernet qos 802.1ad-up-bits-mapping-tbl set 802.1p
<802.1p> dei <dei> cos <cos> color <color>
```

To display the S-VLAN 802.1 UP and CFI bit classification table, enter the following command:

```
root> ethernet qos 802.1ad-up-bits-mapping-tbl show
```

Table 158: 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
```

18.1.5. 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)*

18.1.5.1. 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 159: Trust Mode for DSCP CLI Parameters

Parameter	Input Type	Permitted Values	Description
ip-dscp	Variable	trust un-trust	Select the interface's trust mode for DSCP classification: ● `trust` – The interface performs QoS and color classification according to a user-configurable table for DSCP to CoS and color classification. DSCP classification has priority over MPLS classification, so that if a match is found with the DSCP value of the ingressing frame, MPLS bits are not considered. ● `un-trust` – The interface does not consider DSCP during classification.

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
```

18.1.5.2. Modifying the DSCP Classification Table (CLI)

The following table shows the default values for the DSCP classification table.

Table 160: DSCP Classification Table Default Values

DSCP	DSCP (bin)	Description	CoS (Configurable)	Color (Configurable)
0 (default)	000000	BE (CS0)	0	Green
10	001010	AF11	1	Green
12	001100	AF12	1	Yellow
14	001110	AF13	1	Yellow
18	010010	AF21	2	Green
20	010100	AF22	2	Yellow
22	010110	AF23	2	Yellow
26	011010	AF31	3	Green
28	011100	AF32	3	Yellow
30	011110	AF33	3	Yellow
34	100010	AF41	4	Green
36	100100	AF42	4	Yellow
38	100110	AF43	4	Yellow
46	101110	EF	7	Green
8	001000	CS1	1	Green
16	010000	CS2	2	Green
24	011000	CS3	3	Green
32	100000	CS4	4	Green
40	101000	CS5	5	Green
48	110000	CS6	6	Green
56	111000	CS7	7	Green
51	110011	DSCP_51	6	Green
52	110100	DSCP_52	6	Green
54	110110	DSCP_54	6	Green
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 161: 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
```

18.1.6. 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)*

18.1.6.1. 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 162: 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
```

18.1.6.2. Modifying the MPLS EXP Bit Classification Table (CLI)

The following table shows the default values for the MPLS EXP bit classification table.

Table 163: 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 164: 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
```

18.1.7. Configuring a Default CoS (CLI)

You can define a default CoS value for frames passing through the interface. This value can be overwritten on the service point and service level. The Color is assumed to be Green.

To define a default CoS value for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>classification set default-cos <default-cos>
```

To display the default CoS value for an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]>classification show default-cos
```

Table 165: 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
```

18.1.8. Configuring Ingress Path Classification on a Service Point (CLI)

For instruction on configuring ingress path classification on a service point, see *CoS Preservation and Modification on a Service Point (CLI)*.

18.1.9. Configuring Ingress Path Classification on a Service (CLI)

For instruction on configuring ingress path classification on a service, see *Configuring a Service's CoS Mode and Default CoS (CLI)*.

18.2. Configuring Policers (Rate Metering) (CLI)

This section includes:

- *Overview of Rate Metering (Policing) (CLI)*
- *Configuring Rate Meter (Policer) Profiles (CLI)*
- *Displaying Rate Meter Profiles (CLI)*
- *Deleting a Rate Meter Profile (CLI)*
- *Attaching a Rate Meter (Policer) to an Interface (CLI)*
- *Configuring the Line Compensation Value for a Rate Meter (Policer) (CLI)*
- *Displaying Rate Meter Statistics for an Interface (CLI)*

18.2.1. Overview of Rate Metering (Policing) (CLI)

The NS Primo/Diplo 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 NS Primo/Diplo'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.

18.2.2. Configuring Rate Meter (Policer) Profiles (CLI)

To add a rate meter (policer) profile, enter the following command:

```
root> ethernet qos rate-meter add profile-id <profile-id> cir
<cir> cbs <cbs> eir <eir> ebs <ebs> color-mode <color-mode>
coupling-flag <coupling-flag> rate-meter-profile-name <rate-
meter-profile-name>
```

To edit an existing rate meter (policer) profile, enter the following command:

```
root> ethernet qos rate-meter edit profile-id <profile-id> cir
<cir> cbs <cbs> eir <eir> ebs <ebs> color-mode <color-mode>
coupling-flag <coupling-flag> rate-meter-profile-name <rate-
meter-profile-name>
```

Table 166: 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

18.2.3. Displaying Rate Meter Profiles (CLI)

You can display all configured rate meter (policer) profiles or a specific profile.

To display a specific profile, enter the following command:

```
root> ethernet qos rate-meter show profile-id <profile-id>
```

To display all configured profiles, enter the following command:

```
root> ethernet qos rate-meter show profile-id all
```

Example

The following command displays the parameters of Rate Meter Profile 50:

```
root> ethernet qos rate-meter show profile-id 50
```

18.2.4. Deleting a Rate Meter Profile (CLI)

You cannot delete a rate meter (policer) profile that is attached to a logical interface. You must first remove the profile from the logical interface, then delete the profile.

To delete a rate meter (policer) profile, use the following command:

```
root> ethernet qos rate-meter delete profile-id <profile-id>
```

Example

The following command deletes Rate Meter Profile 50:

```
root> ethernet qos rate-meter delete profile-id 50
```

18.2.5. Attaching a Rate Meter (Policer) to an Interface (CLI)

On the logical interface level, you can assign rate meter (policer) profiles as follows:

- Per frame type (unicast, multicast, and broadcast)
- Per frame ethertype

This section includes:

- *Assigning a Rate Meter (Policer) for Unicast Traffic (CLI)*
- *Assigning a Rate Meter (Policer) for Multicast Traffic (CLI)*
- *Assigning a Rate Meter (Policer) for Broadcast Traffic (CLI)*
- *Assigning a Rate Meter (Policer) per Ethertype (CLI)*

18.2.5.1. 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 167: 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
```

18.2.5.2. 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 168: 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
```

18.2.5.3. 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 169: 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
```

18.2.5.4. 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 170: Assigning Rate Meter per Ethertype CLI Parameters

Parameter	Input Type	Permitted Values	Description
ethertype#	Variable	ethertype1 ethertype2 ethertype3 I	Identifies which of three possible policer-per-Ethertype combinations you are defining.
ethertype-value	Hexadecimal	1-65535	Identifies the Ethertype to which the profile applies.
admin-state	Variable	enable disable	Enables or disables policing on broadcast traffic flows from the logical interface.
profile-id	Number	1 – 250	Select from the policer profiles defined in the system. For instructions on defining rate meter (policer) profiles, refer to *Configuring Rate Meter (Policer) Profiles (CLI).*

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
```

18.2.6. 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 171: 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
```

18.2.7. 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 172: 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
```

18.3. Configuring Marking (CLI)

This section includes:

- *Marking Overview (CLI)*
- *Configuring Marking Mode on a Service Point (CLI)*
- *Marking Table for C-VLAN UP Bits (CLI)*
- *Marking Table for S-VLAN UP Bits (CLI)*

18.3.1. Marking Overview (CLI)

When enabled, NS Primo/Diplo'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.

18.3.2. Configuring Marking Mode on a Service Point (CLI)

To enable or disable marking mode on a service point, go to service view for the service and enter the following command:

```
service[SID]>sp marking set spid <sp-id> mode <mode>
```

Table 173: Marking Mode on Service Point CLI Parameters

Parameter	Input Type	Permitted Values	Description
sp-id	Number	1-32 for P2P and MP services. 1-30 for MNG services.	The Service Point ID.
mode	Variable	enable disable	Determines whether re-marking of the outer VLAN (C-VLAN or S-VLAN) of tagged frames that pass through the service point is enabled. ● If `mode` is set to `enable`, and CoS preservation for the relevant outer VLAN is set to `disable`, the service point re-marks the C-VLAN or S-VLAN 802.1p UP bits of egress frames according to the calculated CoS and Color, and the user-configurable 802.1Q and 802.1AD marking tables. ● If `mode` is set to `enable` and CoS preservation for the relevant outer VLAN is also set to `enable`, re-marking is not performed. ● If `mode` is set to `disable` and CoS preservation for the relevant outer VLAN is also set to `disable`, re-marking is applied, but only according to the values defined for Green frames in the 802.1Q and 802.1AD marking tables. For information about configuring CoS Preservation, refer to *CoS Preservation and Modification on a Service Point (CLI)*.

Examples

The following command enables marking mode on Service Point 3 on Service 2:

```
service[2]>sp marking set spid 3 mode enable
```

The following command disables marking mode on Service Point 3 on Service 2:

```
service[2]>sp marking set spid 3 mode disable
```

18.3.3. Marking Table for C-VLAN UP Bits (CLI)

When marking is performed, the following table is used by the marker to decide which CoS and Color to use as the egress CoS and Color bits for C-VLAN-tagged frames.

Table 174: 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 175: 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
```

18.3.4. Marking Table for S-VLAN UP Bits (CLI)

When marking is performed, the following table is used by the marker to decide which CoS and Color to use as the egress CoS and Color bits for S-VLAN-tagged frames.

Table 176: 802.1ad UP Marking Table (S-VLAN)

CoS	Color	802.1ad UP (Configurable)	DEI Color (Configurable)
0	Green	0	0
0	Yellow	0	1
1	Green	1	0
1	Yellow	1	1
2	Green	2	0
2	Yellow	2	1
3	Green	3	0
3	Yellow	3	1
4	Green	4	0
4	Yellow	4	1
5	Green	5	0
5	Yellow	5	1
6	Green	6	0
6	Yellow	6	1
7	Green	7	0
7	Yellow	7	1

To modify the 802.1ad CoS and Color to UP and DEI bit mapping table, enter the following command in root view:

```
root> ethernet qos 802.1ad-up-bits-marking-tbl set cos <cos>
color <color> 802.1p <802.1p> dei <dei>
```

To display the 802.1q CoS and Color to UP and CFI bit mapping table, enter the following command in root view:

```
root> ethernet qos 802.1ad-up-bits-marking-tbl show
```

Table 177: 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
```

18.4. Configuring WRED (CLI)

This section includes:

- *WRED Overview (CLI)*
- *Configuring WRED Profiles (CLI)*
- *Assigning a WRED Profile to a Queue (CLI)*

18.4.1. WRED Overview (CLI)

Weighted Random Early Detection (WRED) enables differentiation between higher and lower priority traffic based on CoS. You can define up to 30 WRED profiles. Each profile contains a green traffic curve and a yellow traffic curve. These curves describe the probability of randomly dropping frames as a function of queue occupancy.

The system also includes two pre-defined read-only profiles. These profiles are assigned WRED profile IDs 31 and 32.

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.

18.4.2. Configuring WRED Profiles (CLI)

To configure a WRED profile, enter the following command in root view:

```
root> ethernet qos wred-profile-tbl add profile-id <profile-id>
green-min-threshold <green-min-threshold> green-max-threshold
<green-max-threshold> green-max-drop <green-max-drop> yellow-
min-threshold <yellow-min-threshold> yellow-max-threshold
<yellow-max-threshold> yellow-max-drop <yellow-max-drop>
```

To edit an existing WRED profile, enter the following command in root view:

```
root> ethernet qos wred-profile-tbl edit profile-id <profile-
id> green-min-threshold <green-min-threshold> green-max-
threshold <green-max-threshold> green-max-drop <green-max-drop>
yellow-min-threshold <yellow-min-threshold> yellow-max-
threshold <yellow-max-threshold> yellow-max-drop <yellow-max-
drop>
```

To display a WRED profile, enter the following command in root view:

```
root> ethernet qos wred-profile-tbl show profile-id <profile-
id>
```

To delete a WRED profile, enter the following command in root view:

```
root> ethernet qos wred-profile-tbl delete profile-id <profile
id>
```

You cannot delete a WRED profile that is assigned to a queue. You must first remove the WRED profile from the queue by replacing it with a different WRED profile. You can then delete the WRED profile.

Note

Each queue always has a WRED profile assigned to it. By default, WRED Profile 31 is assigned to every queue until a different profile is assigned.

Table 178: 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.
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%

18.4.3. Assigning a WRED Profile to a Queue (CLI)

To assign a WRED profile to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> wred set service-bundle-id <service-bundle-
id> cos <cos> profile-id <profile-id>
```

To display the WRED profile assigned to a queue, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> wred show profile-id service-bundle-id
<service-bundle-id> cos <cos>
```

Table 179: 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
```

18.5. Configuring Shapers (CLI)

This section includes:

- *Overview of Egress Shaping (CLI)*
- *Configuring Queue Shapers (CLI)*
- *Configuring Service Bundle Shapers (CLI)*
- *Configuring Egress Line Compensation for Shaping (CLI)*

18.5.1. Overview of Egress Shaping (CLI)

Egress shaping determines the traffic profile for each queue. NS Primo/Diplo 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.

18.5.2. Configuring Queue Shapers (CLI)

You can configure up to 32 single leaky bucket queue shaper profiles. The CIR value can be set to the following values:

- 16,000 – 32,000,000 bps – granularity of 16,000 bps
- 32,000,000 – 131,008,000 bps – granularity of 64,000 bps

Note

You can enter any value within the permitted range. Based on the value you enter, the software automatically rounds off the setting according to the granularity. If you enter a value below the lowest granular value (except 0), the software adjusts the setting to the minimum.

You can attach one of the configured queue shaper profiles to each priority queue. If no profile is attached to the queue, no egress shaping is performed on that queue.

This section includes:

- *Configuring Queue Shaper Profiles (CLI)*
- *Attaching a Shaper Profile to a Queue (CLI)*

18.5.2.1. 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 180: 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
```

18.5.2.2. 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 181: Attaching Shaper Profile to Queue CLI Parameters

Parameter	Input Type	Permitted Values	Description
service-bundle-id	Number	1 – 63 **Note:** In the current release, only Service Bundle 1 is supported.	The service bundle to which you are attaching the queue shaper profile.
cos	Number	0 – 7	The CoS queue ID of the queue to which you want to assign the shaper. Queues are numbered according to CoS value.
admin-state	Variable	enable disable	Select `enable` to enable egress queue shaping on the queue, or `disable` to disable egress queue shaping on the queue. If you set shaping to `disable`, the shaper profile remains attached to the queue, but does not affect traffic.
profile-id	Number	1 – 32	Enter the ID of one of the configured queue shaper profiles.

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
```

18.5.3. 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)*

18.5.3.1. 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 182: 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
```

18.5.3.2. 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 183: 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
```

18.5.4. 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 184: 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
```

18.6. Configuring Scheduling (CLI)

This section includes:

- *Overview of Egress Scheduling (CLI)*
- *Configuring Queue Priority (CLI)*
- *Configuring Interface Priority Profiles (CLI)*
- *Attaching a Priority Profile to an Interface (CLI)*
- *Configuring Weighted Fair Queuing (WFQ) (CLI)*

18.6.1. Overview of Egress Scheduling (CLI)

Egress scheduling is responsible for transmission from the priority queues. NS Primo/Diplo 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.

18.6.2. Configuring Queue Priority (CLI)

A priority profile defines the exact order for serving the eight priority queues in a single service bundle. When you attach a priority profile to an interface, all the service bundles under the interface inherit the profile.

The priority mechanism distinguishes between two states of the service bundle:

- **Green State** – Committed state
- **Yellow State** – Best effort state

Green State refers to any time when the service bundle rate is below the user-defined CIR. Yellow State refers to any time when the service bundle is above the user-defined CIR but below the PIR.

You can define up to four Green priority profiles, from 4 (highest) to 1 (lowest). An additional four Yellow priority profiles are defined automatically and cannot be changed or edited.

The following table provides a sample of an interface priority profile. This profile is also used as the default interface priority profile.

Table 185: 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.

18.6.3. Configuring Interface Priority Profiles (CLI)

To define an interface priority profile, enter the following command in root view:

```
root> ethernet qos port-priority-profile-tbl add profile-id
<profile-id> cos0-priority <cos0-priority> description
<description> cos1-priority <cos1-priority> description
<description> cos2-priority <cos2-priority> description
<description> cos3-priority <cos3-priority> description
<description> cos4-priority <cos4-priority> description
<description> cos5-priority <cos5-priority> description
<description> cos6-priority <cos6-priority> description
<description> cos7-priority <cos7-priority> description
<description>
```

To edit an existing interface priority profile, enter the following command in root view:

```
root> ethernet qos port-priority-profile-tbl edit profile-id
<profile-id> cos0-priority <cos0-priority> description
<description> cos1-priority <cos1-priority> description
<description> cos2-priority <cos2-priority> description
<description> cos3-priority <cos3-priority> description
<description> cos4-priority <cos4-priority> description
<description> cos5-priority <cos5-priority> description
<description> cos6-priority <cos6-priority> description
<description> cos7-priority <cos7-priority> description
<description>
```

To display the parameters of an interface priority profile, enter the following command in root view:

```
root> ethernet qos port-priority-profile-tbl show profile-id
<profile-id>
```

To delete an interface priority profile, enter the following command in root view:

```
root> ethernet qos port-priority-profile-tbl delete profile-id
<profile-id>
```

You can only delete an interface priority profile if the profile is not attached to any interface.

Table 186: Interface Priority Profile CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	1 – 8	A unique ID to identify the profile.
cos0-priority	Number	1 – 4	The Green priority for the CoS 0 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 0 egressing the service bundle to which the profile is assigned.
description	Text String	Up to 20 characters.	A description of the priority level.
cos1-priority	Number	1 – 4	The Green priority for the CoS 1 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 1 egressing the service bundle to which the profile is assigned.
cos2-priority	Number	1 – 4	The Green priority for the CoS 2 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 2 egressing the service bundle to which the profile is assigned.
cos3-priority	Number	1 – 4	The Green priority for the CoS 3 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 3 egressing the service bundle to which the profile is assigned.
cos4-priority	Number	1 – 4	The Green priority for the CoS 4 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 4 egressing the service bundle to which the profile is assigned.
cos5-priority	Number	1 – 4	The Green priority for the CoS 5 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 5 egressing the service bundle to which the profile is assigned.
cos6-priority	Number	1 – 4	The Green priority for the CoS 6 queue, from 4 (highest) to 1 (lowest). This priority is applied to Green frames with CoS 6 egressing the service bundle to which the profile is assigned.
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 187: Interface Priority Sample Profile Parameters

CoS	Green Priority (user defined)	Yellow Priority (read only)	Description
0	1	1	c0_p1
1	1	1	c1_p1
2	1	1	c2_p1
3	2	1	c3_p2
4	2	1	c4_p2
5	3	1	c5_p3
6	4	1	c6_p4
7	4	4	c7_p4

The following command edits the profile you created in the previous command so that CoS 6 queues have a Green priority of 3 instead of 4, and a description of "c6_p3".

```
root> ethernet qos port-priority-profile-tbl edit profile-id 1
cos0-priority 1 description c0_p1 cos1-priority 1 description
c1_p1 cos2-priority 1 description c2_p1 cos3-priority 2
description c3_p2 cos4-priority 2 description c4_p2 cos5-
priority 3 description c5_p3 cos6-priority 3 description c6_p3
cos7-priority 4 description c7_p4
```

18.6.4. Attaching a Priority Profile to an Interface (CLI)

To attach a priority profile to an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> priority set profile-id <profile-id>
```

To display which priority profile is attached to an interface, go to interface view for the interface and enter the following command:

```
eth type eth [x/x]> port-priority show profile-id
```

Table 188: 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]>
```

18.6.5. 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)*

18.6.5.1. 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 189: 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
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.

18.6.5.2. 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 a WFQ profile if the profile is not attached to any interface.

Table 190: WFQ Profile CLI Parameters

Parameter	Input Type	Permitted Values	Description
profile-id	Number	2 – 6	A unique ID to identify the profile.
cos0-weight	Number	1 - 20	The relative weight for the CoS 0 queue.
cos1- weight	Number	1 - 20	The relative weight for the CoS 1 queue.
cos2- weight	Number	1 - 20	The relative weight for the CoS 2 queue.
cos3- weight	Number	1 - 20	The relative weight for the CoS 3 queue.
cos4- weight	Number	1 - 20	The relative weight for the CoS 4 queue.
cos5- weight	Number	1 - 20	The relative weight for the CoS 5 queue.
cos6- weight	Number	1 - 20	The relative weight for the CoS 6 queue.
cos7- weight	Number	1 - 20	The relative weight for the CoS 7 queue.

Examples

The following command configures a WFQ profile with Profile ID 2:

```
root> ethernet qos wfq-weight-profile-tbl add profile-id 2
cos0-weight 15 cos1-weight 15 cos2-weight 15 cos3-weight 15
cos4-weight 15 cos5-weight 15 cos6-weight 15 cos7-weight 20
```

This profile has the parameters listed in the following table. Note that the yellow queue weight is constant and cannot be changed. This means that all best effort traffic (yellow) will always have the same weight, regardless of CoS.

Table 191: 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
```

18.6.5.3. 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 192: 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]>
```

18.7. Displaying Egress Statistics (CLI)

NS Primo/Diplo collects egress PMs at the queue level and the service bundle level.

18.7.1. Displaying Queue-Level PMs (CLI)

NS Primo/Diplo 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 193: Egress Queue Level PMs CLI Parameters

Parameter	Input Type	Permitted Values	Description
service-bundle-id	Number	1 – 63 **Note**: In the current release, only Service Bundle 1 is supported.	The service bundle for which you want to display PMs.
cos	Number	0 - 7	The queue for which you want to display PMs.
clear-on-read	Boolean	yes no	If you enter yes, the statistics are cleared once you display them.
layer-1	Boolean	yes no	• yes – Statistics are represented as Layer 1 statistics, including preamble and IFG. • no – Statistics are represented as Layer 2 statistics.

The following command displays PMs for the CoS 0 queue in Service Bundle 1, on GbE 2. The PMs are cleared after they are displayed:

```
eth type eth [1/2]> tm-queue show statistics service-bundle-id
1 cos 0 clear-on-read yes layer-1 yes
```

The following command clears PMs for all queues in Service Bundle 1, on GbE 2:

```
eth type eth [1/2]> tm-queue clear statistics service-bundle-id
1
```

18.7.2. Displaying Service Bundle-Level PMs (CLI)

NS Primo/Diplo 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 194: 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.

Example

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
```

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)*

19.1. Configuring Adaptive Bandwidth Notification (ABN) (CLI)

This section includes:

- *Adaptive Bandwidth Notification Overview (CLI)*
- *Configuring an ABN Entity (CLI)*

19.1.1. 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.

19.1.2. 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 195: 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.
monitored-slot	Number	2	
monitored-port	Number	Radio Carrier 1: 1 Radio Carrier 2 (NetStream Diplo 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 NetStream Diplo 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.
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 - rp-4), 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 NetStream Diplo 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 an NetStream Diplo 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 an NetStream Diplo 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 an NetStream Diplo 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
```

19.2. 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)*

19.2.1. Configuring the General LLDP Parameters (CLI)

This section explains how to define the general LLDP parameters for the unit. For instructions on defining port-specific parameters, see *Configuring LLDP Port Parameters (CLI)*.

To define the Transmit Interval, which is the interval at which LLDP frames are transmitted, enter the following command in root view:

```
root> ethernet lldp tx-interval-set tx-interval <tx-interval>
```

The time-to-live (TTL) determines the length of time LLDP frames are retained by the receiving device. The TTL is determined by multiplying the Transmit Interval by the TTL Multiplier.

To define the TTL Multiplier, enter the following command in root view:

```
root> ethernet lldp tx-hold-multiplier-set hold-multiplier
<hold-multiplier>
```

To define the interval between transmission of LLDP notifications during normal transmission periods, enter the following command in root view:

```
root> ethernet lldp notif-interval-set notif-interval <notif-
interval>
```

Table 196: 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
```

19.2.2. 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.

19.2.3. 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 197: 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.
agent-admin	Variable	txOnly rxOnly txAndRx disabled	Defines how the LLDP protocol operates for this port: ● `txOnly` - The LLDP agent transmits LLDP frames on this port but does not update information about its peer. ● `rxOnly` - The LLDP agent receives but does not transmit LLDP frames on this port. ● `txAndRx` - The LLDP agent transmits and receives LLDP frames on this port (default value). ● `disabled` - The LLDP agent does not transmit or receive LLDP frames on this port.
agent-notif-enable	Variable	true false	● `true` - The agent sends a Topology Change trap to the NMS whenever the system information received from its peer changes. ● `false` - Notifications to the NMS are disabled (default value).

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:

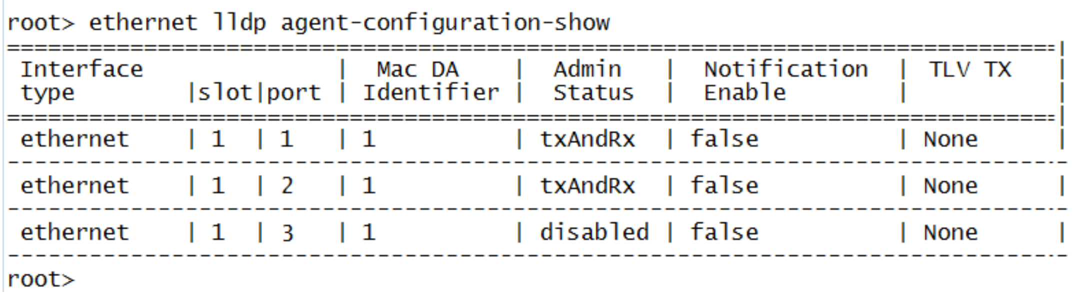
```
root> ethernet lldp agent-admin-set interface eth slot 1 port 2
agent-admin txAndRx

root> ethernet lldp agent-notif-enable interface eth slot 1
port 2 agent-notif-enable true
```

19.2.4. Displaying LLDP Port Parameters (CLI)

To display the LLDP agent configuration on all ports, enter the following command in root view:

```
root> ethernet lldp agent-configuration-show
```

The following is a sample output of the command:



```
root> ethernet lldp agent-configuration-show
==========================================================================|
 Interface            |  Mac DA    |  Admin    |  Notification    |  TLV TX   |
 type       |slot|port | Identifier |  Status   |  Enable          |           |
==========================================================================|
 ethernet   | 1  | 1   | 1          | txAndRx   | false            | None      |
--------------------------------------------------------------------------
 ethernet   | 1  | 2   | 1          | txAndRx   | false            | None      |
--------------------------------------------------------------------------
 ethernet   | 1  | 3   | 1          | disabled  | false            | None      |
--------------------------------------------------------------------------
root>
```

19.2.5. 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)*

19.2.5.1. 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

19.2.5.2. 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.

19.2.5.3. 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.

19.2.5.4. 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.

19.2.5.5. 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.

19.2.6. 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.

19.2.6.1. 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 198: 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 hardware unit.
- **Remote Chassis ID** – An octet string used to identify the peer hardware unit.
- **Rem Port ID subType** – The type of port identifier encoding used in the peer's Port ID.
- **Rem Port ID** – An octet string used to identify the port component associated with the peer.
- **Rem Port Description** – A description of the peer's port.
- **Rem System Name** – The peer's system name.
- **Rem System Description** – The peer's system description.

Note

The Rem Port Description, Rem System Name, and Rem System Description fields are not used in the current version.

- **Rem System Cap Supported** - The bitmap value used to identify which system capabilities are supported on the peer. The bitmap is defined by the following parameters:

  - 0 - other
  - 1 - repeater
  - 2 - bridge
  - 3 - wlanAccessPoint
  - 4 - router
  - 5 - telephone
  - 6 - docsisCableDevice
  - 7 - stationOnly
  - 8 - cVLANComponent
  - 9 - sVLANComponent
  - 10 - twoPortMACRelay

- **Rem System Cap Enabled** - The bitmap value used to identify which system capabilities are enabled on the peer. The bitmap is defined by the following parameters:
  - 0 - other
  - 1 - repeater
  - 2 - bridge
  - 3 - wlanAccessPoint
  - 4 - router
  - 5 - telephone
  - 6 - docsisCableDevice
  - 7 - stationOnly
  - 8 - cVLANComponent
  - 9 - sVLANComponent
  - 10 - twoPortMACRelay
- **Remote Changes** - Indicates whether there are changes in the peer's MIB, as determined by the variable **remoteChanges**. Possible values are:
  - **True** - Changes have taken place in the peer's MIB since the defined agent-start-time.
  - **False** - No changes have taken place in the peer's MIB since the defined agent-*start-time*.

19.2.6.2. 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 199: 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.

19.2.7. 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)*

19.2.7.1. 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.

19.2.7.2. 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.

19.2.7.3. 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.

20. Synchronization (CLI)

This section includes:

- *Configuring SyncE Regenerator (CLI)*

20.1. Configuring SyncE Regenerator (CLI)

Note

SyncE Regenerator is supported for NetStream Diplo and NetStream Primo. For NS Primo/DiploE, SyncE Regenerator support is planned for future release.

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.
When working with Transparent Clock, Sync Regenerator is only supported with optical interfaces.

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 200: 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.
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 (NetStream Diplo 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 by 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
```

NetStream Diplo, NetStream Primo, and NS Primo/DiploE use 1588v2-compliant Transparent Clock to counter the effects of delay variation. Transparent Clock measures and adjusts for delay variation, enabling the NetStream Diplo/S/E 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 G8.0.7:

Before configuring Transparent Clock:

1. Make sure that synchronization is properly configured for the radio on which you are configuring Transparent Clock.
2. Configure a service and service points to carry the PTP packets that will be passing between the master and slave nodes. See . It is recommended to:

To enable Transparent Clock, enter the following command in root view:

To disable Transparent Clock, enter the following command in root view:

To assign the radio that will carry the PTP packets and determine the direction of the PTP packet flow, enter the following command in root view:

The parameter must be set to on one side of the 1588 link and on the other.

To display the Transparent Clock settings, enter the following command in root view:

The following commands enable Transparent Clock on radio carrier 1 and configure the radio to send PTP packets downstream:

Parameter	Input Type	Permitted Values	Description
slot	Number	NetStream Diplo or NetStream Primo: 2 NS Primo/DiploE: 16	
port	Number	1	

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)*
- *Blocking Telnet Access (CLI)*
- *Uploading the Security Log (CLI)*
- *Uploading the Configuration Log (CLI)*

Related Topics:

- *Logging On (CLI)*
- *Operating in FIPS Mode (CLI)*
- *Configuring AES-256 Payload Encryption (CLI)*

21.1. 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)*

21.1.1. Configuring the Inactivity Timeout Period (CLI)

A system management session automatically times out after a defined period (in minutes) with no user activity. To configure the session timeout period, enter the following command in root view:

```
root> platform security protocols-control session inactivity-timeout set <inactivity-timeout>
```

To display the currently configured session timeout period, enter the following command in root view:

```
root> platform security protocols-control session inactivity-timeout show
```

Table 202: 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
```

21.1.2. Configuring Blocking Upon Login Failure (CLI)

Upon a configurable number of failed login attempts, the system blocks the user from logging in for a configurable number of minutes.

To configure the number of failed login attempts that will temporarily block the user from logging into the system, enter the following command in root view:

```
root> platform security access-control block-failure-login
attempt set <attempt>
```

To define the period (in minutes) for which a user is blocked after the configured number of failed login attempts, enter the following command in root view:

```
root> platform security access-control block-failure-login
period set <period>
```

To display the current failed login attempt blocking parameters, enter the following command in root view:

```
root> platform security access-control block-failure-login show
```

Table 203: 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
```

21.1.3. Configuring Blocking of Unused Accounts (CLI)

You can configure a number of days after which a user is prevented from logging into the system if the user has not logged in for the configured number of days. You can also manually block a specific user.

To configure the blocking of unused accounts period, enter the following command in root view:

```
root> platform security access-control block-unused-account
period set <period>
```

Once the user is blocked, you can use the following command to unblock the user:

```
root> platform security access-control user-account block user-
name <user-name> block no
```

To manually block a specific user, enter the following command in root view:

```
root> platform security access-control user-account block user-
name <user-name> block yes
```

To display the currently configured blocking of unused account period, enter the following command in root view:

```
root> platform security access-control block-unused-account
show
```

Table 204: 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
```

21.2. 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)*

21.2.1. Configuring Password Aging (CLI)

Passwords remain valid from the first time the user logs into the system for the number of days (20-90) set by this command. If you set this parameter to 0, password aging is disabled, and passwords remain valid indefinitely.

To configure password aging, enter the following command in root view:

```
root> platform security access-control password aging set
<password aging>
```

Table 205: 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
```

21.2.2. Configuring Password Strength Enforcement (CLI)

To set password strength enforcement, enter the following command in root view:

```
root> platform security access-control password enforce-
strength set <enforce-strength>
```

Table 206: 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 passwords you used cannot be reused.

Example

The following command enables password strength enforcement:

```
root> platform security access-control password enforce-
strength set yes
```

21.2.3. Forcing Password Change Upon First Login (CLI)

To determine whether the system requires users to change their password the first time they log into the system, enter the following command in root view.

```
root> platform security access-control password first-login set
<first-login>
```

To require users to change their password the first time they log in, enter the following command in root view:

```
root> platform security access-control password first-login set
yes
```

Table 207: 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.

21.2.4. Displaying the System Password Settings (CLI)

Use the following command to display the system password settings:

```
root> platform security access-control password show-all
```

21.3. Configuring Users (CLI)

This section includes:

- *User Configuration Overview (CLI)*
- *Configuring User Profiles (CLI)*
- *Configuring User Accounts (CLI)*

Related topics:

- *Logging On (CLI)*

21.3.1. User Configuration Overview (CLI)

User configuration is based on the Role-Based Access Control (RBAC) model. According to the RBAC model, permissions to perform certain operations are assigned to specific roles. Users are assigned to particular roles, and through those role assignments acquire the permissions to perform particular system functions.

In the NS Primo/Diplo 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.

21.3.2. Configuring User Profiles (CLI)

User profiles enable you to define system access levels. Each user must be assigned a user profile. Each user profile contains a detailed set of read and write permission levels per functionality group.

The system includes a number of pre-defined user profiles. You can edit these profiles, and add user profiles. Together, the system supports up to 50 user profiles.

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 208: 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
```

21.3.2.1. 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 209: 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
```

21.3.3. Configuring User Accounts (CLI)

You can configure up to 2,000 users. Each user has a user name, password, and user profile. The user profile defines a set of read and write permission levels per functionality group (see *Configuring User Profiles (CLI)*).

To create a new user account, enter the following command:

```
root> platform security access-control user-account add user-
name <user-name> profile-name <profile-name> expired-date
<expired-date>
```

When you create a new user account, the system will prompt you to enter a default password. If Enforce Password Strength is activated (refer to *Configuring Password Strength Enforcement (CLI)*), the password must meet the following criteria:

- Password length must be at least eight characters.

- Password must include characters of at least three of the following character types: lower case letters, upper case letters, digits, and special characters. For purposes of meeting this requirement, upper case letters at the beginning of the password and digits at the end of the password are not counted.
- The last five passwords 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 210: User Accounts CLI Parameters

Parameter	Input Type	Permitted Values	Description
user-name	Text String	Up to 32 characters	The name of the user profile.
profile name	Text String	Up to 49 characters	The name of the User Profile you want to assign to the user. The User Profile defines the user’s access permissions per functionality group.
expired-date	Date	Use the format: YYYY-MM-DD	Optional. The date on which the user account will expire. On this date, the user automatically becomes inactive.
block	Variable	yes no	yes - blocks the account. no - unblocks the account.

Example

The following command creates a user account named Tom_Jones, with user profile “operator”. This user’s account expires on February 1, 2014.

```
root> platform security access-control user-account add user-
name Tom_Jones profile-name operator expired-date 2014-02-01
```

21.4. 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)*

Note

For instructions on configuring a RADIUS server, see *Configuring a RADIUS Server*.

21.4.1. RADIUS Overview (CLI)

The RADIUS protocol provides centralized user management services. NS Primo/Diplo 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 NS Primo/Diplo 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.

21.4.2. Activating RADIUS Authentication (CLI)

To enable or disable Radius access control, enter the following command:

```
root> platform security radius-admin set <admin>
```

Table 211: Activate RADIUS CLI Parameters

Parameter	Input Type	Permitted Values	Description
admin	Variable	enable disable	Enables or disables Radius access control.

21.4.3. 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 212: Configure RADIUS Server CLI Parameters

Parameter	Input Type	Permitted Values	Description
server-id	Number	1 2	● 1 - The primary Radius server ● 2 - The secondary Radius server.
ip-address	Dotted decimal format	Any valid IP address	The IP address of the Radius server.
radius-port	Number	0-65535	The port ID of the RADIUS server.
retries	Number	3-30	The number of times the device will try to communicate with the RADIUS server before declaring the server to be unreachable.
timeout	Number	1-10	The timeout (in seconds) that the agent will wait in each communication with the selected RADIUS server before retrying if no response is received.
shared-secret	String	Between 22-128 characters	The shared secret of the RADIUS server.

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
```

21.4.4. 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
```

21.4.5. 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.

21.5. Configuring X.509 CSR Certificates and HTTPS (CLI)

The web interface protocol for accessing NS Primo/Diplo 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 NS Primo/Diplo 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 NS Primo/Diplo 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)*

21.5.1. Generating a Certificate Signing Request (CSR) File (CLI)

To set the CSR parameters, enter the following command in root view:

```
root> platform security csr-set-parameters common-name <common-
name> country <country> state <state> locality <locality>
organization <organization> org-unit <org-unit> email <email>
file-format <file-format>
```

To display the currently-configured CSR parameters, enter the following command in root view:

```
root> platform security csr-show-parameters
```

If the IP address family is configured to be IPv4, enter the following command in root view to configure the SFTP server parameters for the CSR file upload:

```
root> platform security csr-set-server-parameters server-ipv4
<server-ipv4> server-path <server-path> filename <filename>
server-username <username> server-password <password>
```

If the IP address family is configured to be IPv6, enter the following command in root view to configure the SFTP server parameters for the CSR file upload:

```
root> platform security csr-set-server-parameters server-ipv6
<server-ipv6> server-path <server-path> filename <filename>
server-username <username> server-password <password>
```

To display the currently-configured SFTP parameters for CSR upload, enter the following command in root view:

```
root> platform security csr-show-server-parameters
```

To generate and upload a CSR, enter the following command in root view:

```
root> platform security csr-generate-and-upload
```

To display the status of a pending CSR generation and upload operation, enter the following command in root view:

```
root> platform security csr-generate-and-upload-show-status
```

Table 213: 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.
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. To leave the path blank, enter //.
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.

21.5.2. Downloading a Certificate (CLI)

If the IP address family is configured to be IPv4, enter the following command in root view to configure the SFTP server parameters for downloading a certificate:

```
root> platform security certificate-set-download-parameters
server-ipv4 <server-ipv4> server-path <server-path> filename
<filename> server-username <username> server-password
<password>
```

If the IP address family is configured to be IPv6, enter the following command in root view to configure the SFTP server parameters for downloading a certificate:

```
root> platform security certificate-set-download-parameters
server-ipv6 < server-ipv6> server-path <server-path> filename
<filename> server-username <username> server-password
<password>
```

To display the currently-configured SFTP parameters for downloading a certificate, enter the following command in root view:

```
root> platform security certificate-show-download-parameters
```

To download a certificate, enter the following command in root view:

```
root> platform security certificate-download
```

To display the status of a pending certificate download, enter the following command in root view:

```
root> platform security certificate-download-show-status
```

To install a certificate, enter the following command in root view:

```
root> platform security certificate-install
```

Table 214: 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. To leave the path blank, enter //.
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.

21.5.3. Enabling HTTPS (CLI)

By default, HTTP is used by NS Primo/Diplo 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 NS Primo/Diplo 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
```

21.6. 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.

21.7. 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. NS Primo/Diplo 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 215: 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. To leave the path blank, enter //.
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
```

21.8. 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. NS Primo/Diplo 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 216: 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. To leave the path blank, enter //.
file-name	Text String		The name you want to give the file you are exporting. **Note:** You must add the suffix .zip to the file name. Otherwise, the file import may fail. You can export the file using any name, then add the suffix .zip manually. For example: UnitInfo.zip If the Unit Information file is exported several times consecutively, the file itself will not be replaced. Instead, the filename will be updated by time stamp. For example: UnitInfo.zip.11-05-14 03-31-04
ip-address	Dotted decimal format.	Any valid IP address.	The IP address of the PC or laptop you are using as the FTP or SFTP server.
protocol	Variable	ftp sftp	The file transfer protocol.
username	Text String		The user name for the FTP or SFTP session.
password	Text String		The password for the FTP or SFTP session. To configure the FTP or SFTP settings without a password, simply omit this parameter.

Note

The path and fie name, together, cannot be more than:

If the IP address family is configured to be IPv4: 236 characters
If the IP address family is configured to be IPv6: 220 characters

Examples

The following commands configure an FTP channel for configuration log export to IP address 192.168.1.99, in the directory “current”, with file name “cfg_log”, user name “anonymous”, and password “12345.”

```
root> platform security configuration-log-upload-params set
path \file-name cfg_log ip-address 192.168.1.99 protocol ftp
username anonymous password 12345

root> platform unit-info channel set protocol frp
```

The following command exports the configuration log to the external server location:

```
root> platform security configuration-log upload
```

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)*

22.1. Viewing Current Alarms (CLI)

To display all alarms currently raised on the unit, enter the following command in root view:

```
root> platform status current-alarm show module unit
```

To display the most severe alarm currently raised in the unit, enter the following command in root view:

```
root> platform status current-alarm show most-severe-alarm
module unit
```

22.2. Viewing the Event Log (CLI)

The Event Log displays a list of current and historical events and information about each event.

To display the event log, enter the following command in root view:

```
root> platform status event-log show module unit
```

To clear the event log, enter the following command in root view:

```
root> platform status event-log clear module unit
```

22.3. Editing Alarm Text and Severity (CLI)

You can view a list of alarm types, edit the severity level assigned to individual alarm types, and add additional descriptive text to individual alarm types.

This section includes:

- *Displaying Alarm Information (CLI)*
- *Editing an Alarm Type (CLI)*
- *Setting Alarms to their Default Values (CLI)*

22.3.1. Displaying Alarm Information (CLI)

To display a list of all alarm types and their severity levels and descriptions, enter the following command in root view:

```
root> platform status alarm-management show alarm-id all
```

22.3.2. Editing an Alarm Type (CLI)

To edit an alarm type's severity level, enter the following command in root view:

```
root> platform status alarm-management set alarm-id <alarm-id>
severity-level <severity-level>
```

To add descriptive information to an alarm type, enter the following command in root view:

```
root> platform status alarm-management set alarm-id <alarm-id>
additional-text <additional-text>
```

Table 217: 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 (Loss of Carrier) to minor:

```
root> platform status alarm-management set alarm-id 401
severity-level minor
```

22.3.3. Setting Alarms to their Default Values (CLI)

To restore an alarm type's severity level and description to their default values, enter the following command in root view:

```
root> platform status alarm-management set alarm-id <alarm-id>
restore default
```

To restore the severity levels and descriptions of all alarm types to their default values, enter the following command in root view:

```
root> platform status alarm-management set all default
```

Table 218: 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 (Loss of Carrier) to its default severity level:

```
root> platform status alarm-management set alarm-id 401 restore
default
```

22.4. 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.

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. NS Primo/Diplo 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 219: 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. To leave the path blank, enter //.
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
```

22.5. Performing Diagnostics (CLI)

This section includes:

- *Performing Radio Loopback (CLI)*
- *Performing Ethernet Loopback (CLI)*

22.5.1. Performing Radio Loopback (CLI)

You can perform loopback on a radio.

To set the timeout for a radio loopback, enter the following command in radio view:

```
radio[x/x]> radio loopbacks-timeout set duration <duration>
```

To display the radio loopback timeout, enter the following command in radio view:

```
radio[x/x]>radio loopbacks-timeout show
```

To activate an RF loopback, enter the following command in radio view:

```
radio[x/x]>rf loopback-rf set admin <admin>
```

Table 220: 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
```

The following command cancels an RF loopback on radio carrier 1:

```
radio[2/1]>rf loopback-rf set admin off
```

22.5.2. Performing Ethernet Loopback (CLI)

Ethernet loopbacks can be performed on any logical Ethernet interface except a LAG. When Ethernet loopback is enabled on an interface, the system loops back all packets ingressing the interface. This enables loopbacks to be performed over the link from other points in the network.

To configure loopback on an Ethernet interface, go to interface view for the interface and enter the following command:

```
eth type eth[x/x]> loopback admin <loopback-admin-state>
```

To configure the loopback duration time, go to interface view for the interface and enter the following command:

```
eth type eth[x/x]> loopback set duration <loopback-duration>
```

You can select whether to swap DA and SA MAC addresses during the loopback. Swapping addresses prevents Ethernet loops from occurring. It is recommended to enable MAC address swapping if LLDP is enabled.
To configure MAC address swapping, go to interface view for the interface and enter the following command:

```
eth type eth[x/x]> loopback swap-mac-address admin <MAC_swap-
admin-state>
```

To view loopback status, go to interface view for the interface and enter the following command:

```
eth type eth[x/x]> loopback status show
```

Table 221: 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
```

22.6. Working in CW Mode (Single or Dual Tone) (CLI)

CW mode enables you to transmit a single or dual frequency tones, for debugging purposes.

To work in CW mode, enter the following command in radio view:

```
radio[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 in radio view:

```
radio[x/x] modem tx-source set admin disable
```

Table 222: 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 on an NetStream Diplo or NetStream Primo unit, 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
```

The following commands set a single-tone transmit frequency of 6010 KHz on the radio interface of an NS Primo/DiploE unit, then exit CW mode and return the interface to normal operation:

```
root> radio slot 16 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 6010
radio[2/1] modem tx-source set admin disable
```

Section IV

Maintenance

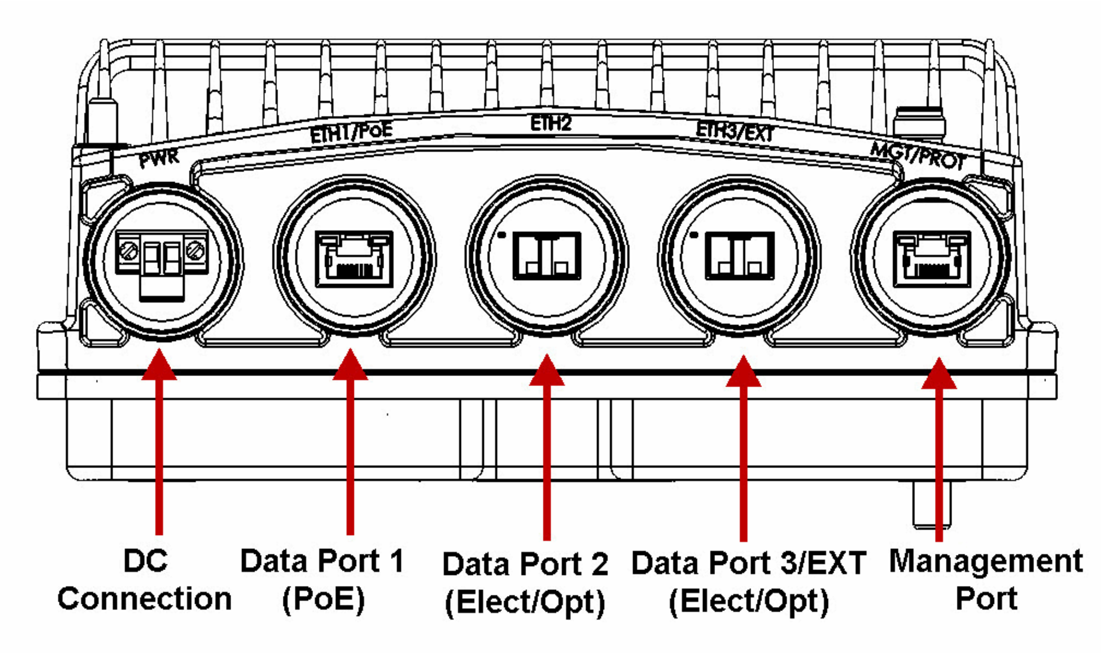
23. Maintenance

This section includes:

- *NetStream Diplo Connector Pin-outs*
- *NetStream Diplo LEDs*
- *NetStream Primo Connector Pin-outs*
- *NetStream Primo LEDs*
- *NS Primo/DiploE Connector Pin-outs*
- *NS Primo/DiploE LEDs*
- *PoE Injector Pin-outs*

23.1. NetStream Diplo Connector Pin-outs

Figure 260: NetStream Diplo Interfaces



23.1.1. Eth1/PoE - GbE Electrical+PoE/Optical

Table 223: NetStream Diplo 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)

23.1.2. Eth2 - GbE Electrical/Optical

Table 224: NetStream Diplo 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)

23.1.3. Eth3/EXP - GbE Electrical/Optical/Expansion

Table 225: NetStream Diplo 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)

23.1.4. MGT/PROT - Management (FE-Standard) and Protection (FE-Non-Standard)

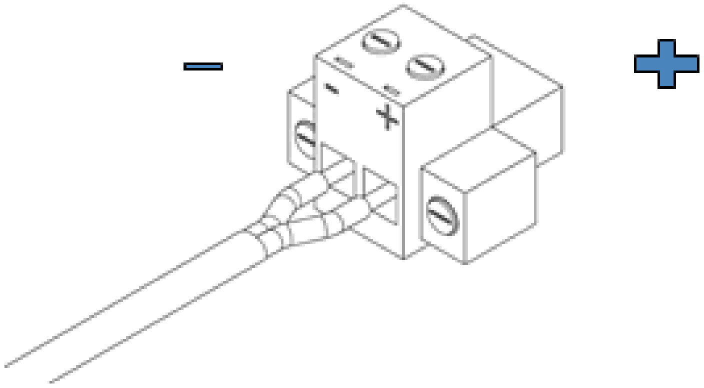
Table 226: NetStream Diplo MGT/PROT Interface - RJ-45 Pinouts

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-

23.1.5. DC

The DC port is UL-60950 compliant, with a 2-pin connector.

Figure 261: NetStream Diplo DC Port Connector



23.1.6. RSL Interface

NetStream Diplo uses a weather-proof BNC connector

23.1.7. Source Sharing

NetStream Diplo uses a TNC connector for source sharing. This connector is marked EXT/REF.

23.2. NetStream Diplo LEDs

The NetStream Diplo 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*

23.2.1. 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.

23.2.2. 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.

23.2.3. 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** – The interface is operational, and there is traffic on the interface (Tx, Rx, or both).

23.2.4. Radio LED

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).
- **Yellow** - 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.

23.2.5. Status LED

The Status LED is a three-color LED that indicates the status of the radio link:

- **Off** – The power is off.
- **Green** - The power is on, and no alarms are raised on the motherboard.
- **Yellow** - The power is on, and one or more minor alarms or warnings are raised on the motherboard.
- **Red** - The power is on, and one or more major or critical alarms are raised on the motherboard.

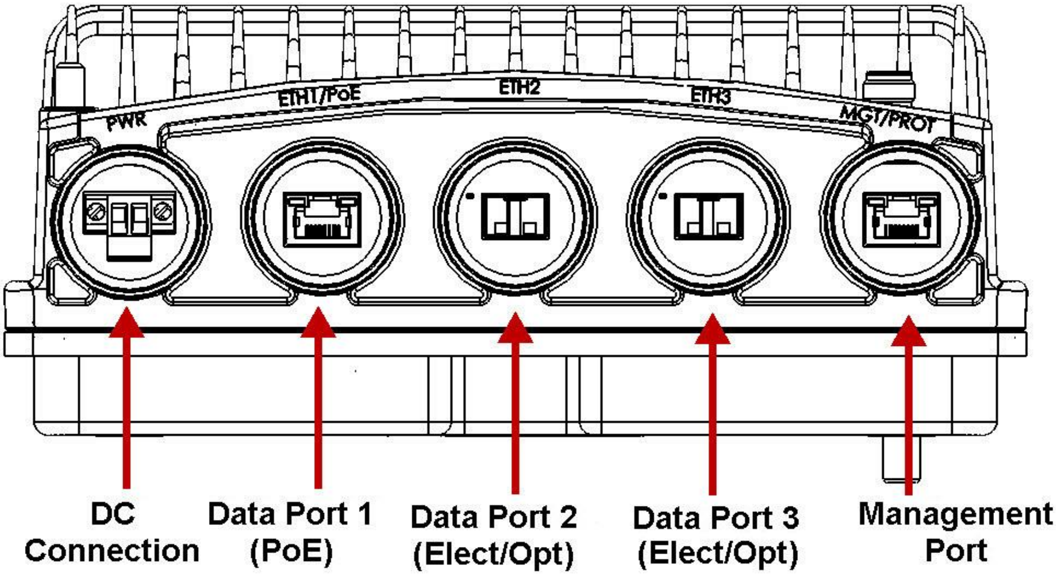
23.2.6. Protection LED

The Protection LED is a three-color LED that operates in a protected configuration to indicate the protection status:

- **Red** – A protection alarm exists (cable disconnected, etc.)
- **Yellow** - Protection is enabled, and the unit is in standby mode.
- **Green** - Protection is enabled, and the unit is in active mode.
- **Off** - Protection is not enabled.

23.3. NetStream Primo Connector Pin-outs

Figure 262: NetStream Primo Interfaces



23.3.1. Eth1/PoE - GbE Electrical+PoE/Optical

Table 227: NetStream Primo 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)

23.3.2. Eth2 - GbE Electrical/Optical

Table 228: NetStream Primo 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)

23.3.3. Eth3 - GbE Electrical/Optical

Table 229: NetStream Primo 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)

23.3.4. MGT/PROT - Management (FE-Standard) and Protection (FE-Non-Standard)

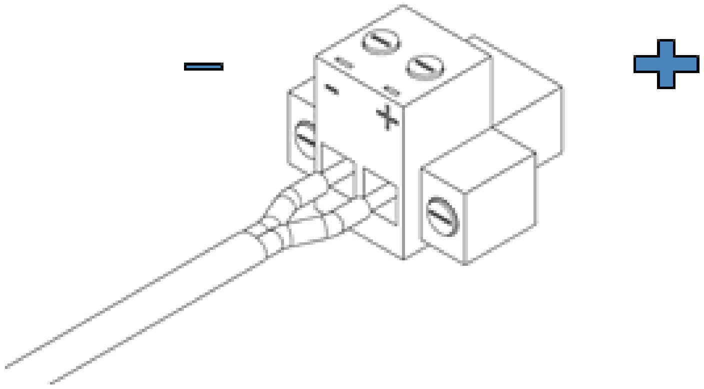
Table 230: NetStream Primo MGT/PROT Interface - RJ-45 Pinouts

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-

23.3.5. DC

The DC port is UL-60950 compliant, with a 2-pin connector.

Figure 263: NetStream Primo DC Connector



23.3.6. RSL Interface

NetStream Primo uses a weather-proof BNC connector.

23.4. NetStream Primo LEDs

The NetStream Primo 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*

23.4.1. 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.

23.4.2. 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.

23.4.3. 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** - 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.

23.4.4. Radio LED

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).
- **Yellow** - 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.

23.4.5. Status LED

The Status LED is a three-color LED that indicates the status of the radio link:

- **Off** – The power is off.
- **Green** - The power is on, and no alarms are raised on the motherboard.
- **Yellow** - The power is on, and one or more minor alarms or warnings are raised on the motherboard.
- **Red** - The power is on, and one or more major or critical alarms are raised on the motherboard.

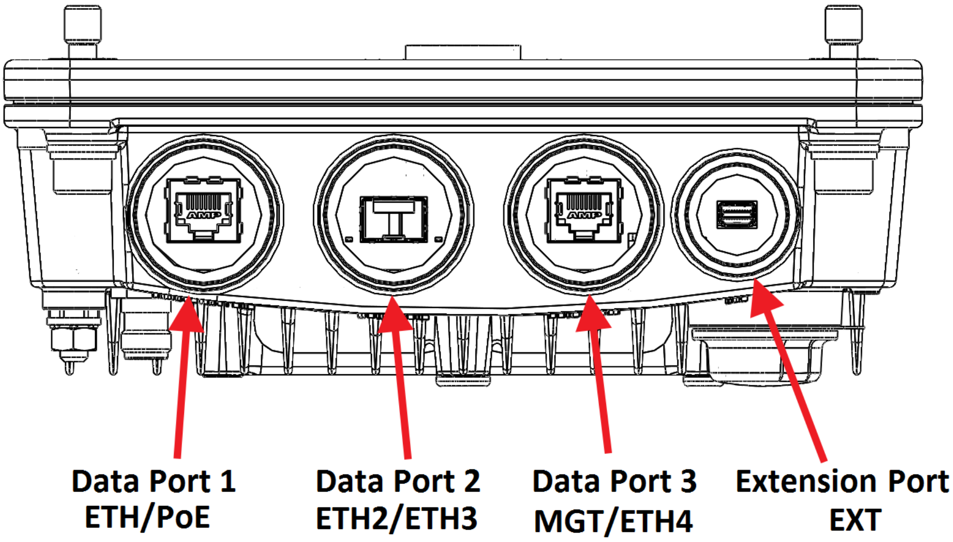
23.4.6. Protection LED

The Protection LED is a three-color LED that operates in a protected configuration to indicate the protection status:

- **Red** – A protection alarm exists (cable disconnected, etc.)
- **Yellow** - Protection is enabled, and the unit is in standby mode.
- **Green** - Protection is enabled, and the unit is in active mode.
- **Off** - Protection is not enabled.

23.5. NS Primo/DiploE Connector Pin-outs

Figure 264: NS Primo/DiploE Interfaces



Eth1/PoE GbE Interface (RJ-45)

Table 231: NS Primo/DiploE Eth1/PoE Interface- RJ-45/

Pin no.	Description
1	BI_DA+ (Bi-directional pair +A)
2	BI_DA- (Bi-directional pair -A)
3	BI_DB+ (Bi-directional pair +B)
4	BI_DC+ (Bi-directional pair +C)
5	BI_DC- (Bi-directional pair -C)
6	BI_DB- (Bi-directional pair +B)
7	BI_DD+ (Bi-directional pair +D)
8	BI_DD- (Bi-directional pair -D)

23.5.1. Eth2/Eth3 GbE Optical Interface (SFP/CSFP)

Eth2/Eth3 is an SFP cage that supports regular and CSFP standards.

23.5.2. MGT/Eth4 GbE Electrical Interface (RJ-45)

Table 232: NS Primo/DiploE MGT/Eth4 Interface - RJ-45/ Pinouts

Pin no.	Description
1	BI_DA+ (Bi-directional pair +A)
2	BI_DA- (Bi-directional pair -A)
3	BI_DB+ (Bi-directional pair +B)
4	BI_DC+ (Bi-directional pair +C)
5	BI_DC- (Bi-directional pair -C)
6	BI_DB- (Bi-directional pair +B)
7	BI_DD+ (Bi-directional pair +D)
8	BI_DD- (Bi-directional pair -D)

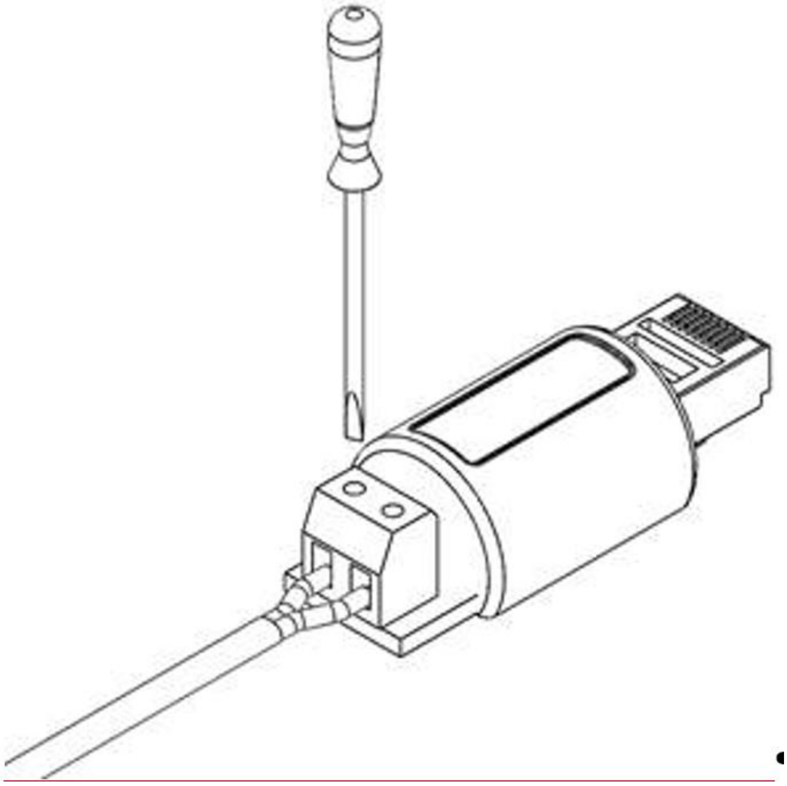
23.5.3. EXT Port

This port is reserved for future use.

23.5.4. Power Adaptor

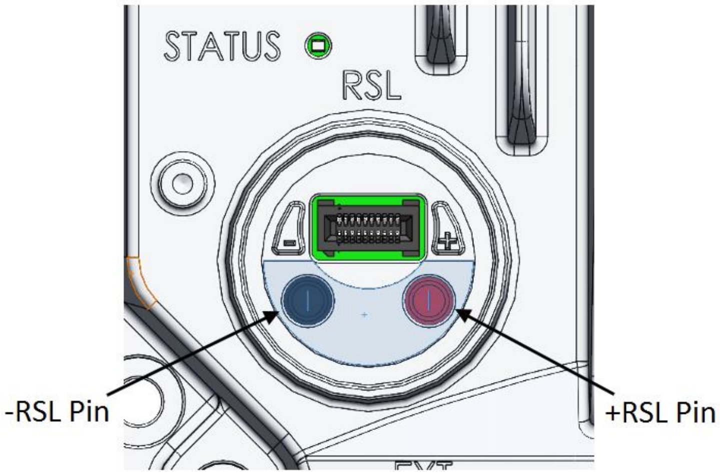
For configurations in which power is not provided via PoE, a special adaptor (NS Primo/Diplo_Mini_Power_Adaptor) is available that enables users to connect a two-wire power connector to the PoE port. This adaptor is located inside of the gland. In such configurations, only one electrical GbE interface is available (MGT/ETH4).

Figure 265: Two-Wire to PoE Port Power Adaptor



23.5.5. RSL Interface

NS Primo/DiploE uses a two-pin connection to measure the RSL level using standard voltmeter test leads:



23.6. NS Primo/DiploE LEDs

The NS Primo/DiploE provides the following LEDs to indicate the status of the unit's interfaces, and the unit as a whole:

- *Eth1/PoE GbE Interface (RJ-45) LEDs*
- *Eth2/Eth3 GbE Optical Interface (SFP/CSFP) LEDs*
- *MGT/Eth4 GbE Electrical Interface (RJ-45) LEDs*
- *Radio LED*
- *Status LED*
- *Protection LED*

23.6.1. Eth1/PoE 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 interface’s Admin status:

- **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.

23.6.2. Eth2/Eth3 GbE Optical Interface (SFP/CSFP) LEDs

Eth2/Eth3 is an SFP cage that supports regular and CSFP standards.

- When Eth2/Eth3 is used with a regular SFP, it provides Ethernet port 2.
- When Eth2/Eth3 is used with CSFP, it provides two Ethernet ports: Ethernet port 2 and Ethernet port 3.
- *NetStream Diplo Connector Pin-outs*
- *NetStream Diplo LEDs*
- *NetStream Primo Connector Pin-outs*
- *NetStream Primo LEDs*
- *NS Primo/DiploE Connector Pin-outs*
- *NS Primo/DiploE LEDs*
- *PoE Injector Pin-outs*

Note

The Web EMS displays Ethernet port 3 even if a regular SFP is used, and there is no Ethernet port 3. You must avoid configuring Ethernet port 3 in this case.

There is one Green LED to the left of the interface and one Green LED to the right of the interface. The LED to the left is for Eth2. When CSFP is used, the LED to the right is for Eth3; otherwise, it is inactive

Each LED indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

- **Off** - Admin is Disabled *or* no cable is connected to the interface.
- **Green** - Admin is Enabled and a cable is connected to the interface.
- **Blinking Green** - Admin is Enabled and a cable is connected to the interface, *and* there is traffic on the interface.

23.6.3. MGT/Eth4 GbE Electrical Interface (RJ-45) LEDs

There are two LEDs next to the MGT/Eth4 interface, a Green LED to the left of the interface and an Orange LED to the right of the interface.

The Orange LED indicates the interface's Admin and cable connection status, and whether there is traffic on the interface:

- **Off** - Admin is Disabled *or* no cable is connected to the interface.
- **Green** - Admin is Enabled and a cable is connected to the interface.
- **Blinking Green** - Admin is Enabled and a cable is connected to the interface, *and* there is traffic on the interface.

The Green LED is not functional in this release.

23.6.4. Radio LED

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).
- **Yellow** - 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.

23.6.5. Status LED

The Status LED is a three-color LED that indicates the status of the radio link:

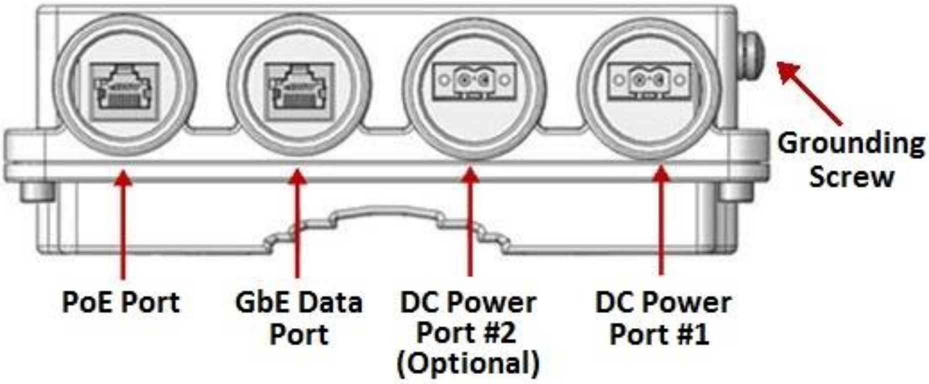
- **Off** – The power is off.
- **Green** - The power is on, and no alarms are raised on the motherboard.
- **Yellow** - The power is on, and one or more minor alarms or warnings are raised on the motherboard.
- **Red** - The power is on, and one or more major or critical alarms are raised on the motherboard.

23.6.6. Protection LED

Reserved for future use.

23.7. PoE Injector Pin-outs

Figure 266: PoE Injector Connectors



23.7.1. PoE Port

Table 233: 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)

23.7.2. Data Port

Table 234: PoE Injector RJ-45 Data Port Supporting 10/100/1000Base-T

Pin no.	Description
1	BI_DA+ (Bi-directional pair +A)
2	BI_DA- (Bi-directional pair -A)
3	BI_DB+ (Bi-directional pair +B)
4	BI_DC+ (Bi-directional pair +C)
5	BI_DC- (Bi-directional pair -C)
6	BI_DB- (Bi-directional pair +B)
7	BI_DD+ (Bi-directional pair +D)
8	BI_DD- (Bi-directional pair -D)

23.7.3. DC

One or two DC ports, depending on the PoE Injector model:

Two models of the PoE Injector are available:

- **PoE_Inj_AO_2DC_24V_48V** – Includes two DC power ports with power input ranges of ±(18-60)V each.
- **PoE_Inj_AO** – Includes one DC power port (DC Power Port #1), with a power input range of ±(40-60)V.

These ports are UL-60950 compliant, with a 2-pin connector.

23.8. 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.

23.8.1. Radio LED

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).
- **Yellow** - 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.

Section V

Appendices

24. Alarms List

The following table lists all alarms used in the NetStream Diplo/S/E products.

Alarms List

Alarm ID	Name	Type	Description	Severity	Probable Cause	Corrective Action	Notes
10	radio-digital-loopback	Alarm	Framer digital loopback	Warning	User enabled framer digital loopback.	Disable framer digital loopback.	
25	main-board-extreme-temperature-alarm	Alarm	Unit Temperature is out of system specified limits.	Warning			
28	main-board-warm-reset	Event	Unit warm reset.	Indeterminate			
29	main-board-cold-reset	Event	Unit reset.	Warning			
30	main-board-poe-low-voltage-alarm	Alarm	POE input voltage is too low	Warning			
31		Event	Change Remote request was sent	Major			(1)
32		Event	Protection switchover due to remote request	Major			(1)
33	protection-mimo-misconfiguration-alarm	Alarm		Major	Unit Redundancy and MIMO 4x4 cannot operate simultaneously.		(2)
100	lag-degraded	Alarm	LAG is not fully functional - LAG Degraded.	Major			
101	lag-down	Alarm	LAG operational state is down	Critical			
102	ethernet-loopback-active-alarm	Alarm	Loopback is active	Major	Ethernet loopback is active.	Wait till loopback timeout expires or disable loopback.	
103	port-mirroring-is-active	Alarm	Slot X port XX is mirrored to slot Y port YY	Minor	Mirroring is enabled by user configuration.	Disable mirroring.	
150	auto-state-propagation-interface-down-alarm	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	protection-communication-down-alarm	Alarm	Protection communication is down	Major	1. Mate unit is absent/failure. 2. Protection cable is disconnected. 3. Unit failure.	1. Check existence of mate unit. 2. Check protection cable connection between units. 3. Reset mate unit. 4. Replace mate unit.	

Alarms List

Alarm ID	Name	Type	Description	Severity	Probable Cause	Corrective Action	Notes
201	protection-lockout-alarm	Alarm	Protection in Lockout State	Major			
202	protection-switch-command	Event	Protection switchover due to local failure	Major			
203	protection-mate-not-present-alarm	Alarm	Mate does not exist	Major	Mate does not exist or cable unplugged.		
401	TrafficPhyLocAlarm	Alarm	Loss of Carrier	Major	1. Cable disconnected. 2. Defective cable.	1. Check connection of cable 2. Replace cable.	
407	ethernet-link-up	Event	Ethernet interface is up	Warning			
408	ethernet-link-down	Event	Ethernet interface is down	Warning			
601	radio-excessive-ber	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	remote-link-id-mismatch	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	radio-lof	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.	
604	radio-signal-degrade	Alarm	Radio signal degrade	Minor	1. Fade in the link. 2. Defective IF cable. 3. Fault in RFU. 4. Fault in RMC (Radio Modem Card).	1. Check link performance. 2. Check IF cable and replace if required. 3. Replace RFU. 4. Replace RMC (Radio Modem Card).	
605	radio-link-up	Event	Radio interface is up	Warning			
606	radio-link-down	Event	Radio interface is down	Warning			

Alarms List

Alarm ID	Name	Type	Description	Severity	Probable Cause	Corrective Action	Notes
801	corrupted-file	Alarm	Corrupted inventory file	Warning	The inventory file is corrupted	1. Reset the system. 2. Reinstall the software.	
802	file-not-found	Alarm	Inventory file not found	Warning	The inventory file is missing	1. Reset the system. 2. Reinstall the software.	
901	demo-license-alarm	Alarm	Demo mode is active	Warning	Demo mode has been activated by the user	Disable demo mode.	
902	license-demo-expired	Event	Demo mode is expired	Warning			
903	license-demo-start-by-user	Event	Demo mode is started	Warning			
904	license-demo-stop-by-user	Event	Demo mode is stopped	Warning			
905	license-load-fail	Event	Activation key loading failure	Major			
906	license-load-successful	Event	Activation key loaded successfully	Warning			
907	license-violation-alarm	Alarm	Activation key violation	Critical	The current configuration does not match the activation-key-enabled feature set. 48 hours after a "activation key violation" alarm is raised, sanction mode is activated in which all alarms except the activation key violation alarm are cleared and no new alarms are raised.	1. Get the list of features' configurations that are violated via the "activation key information report". 2. Install a new activation key that allows the use of all required features.	
908	demo-license-about-to-expire-alarm	Alarm	Demo mode is about to expire	Major	Demo mode allowed period is about to end within 10 days	Disable demo mode and install a new valid activation key.	
910	license-signature-failed-alarm	Alarm	Activation key signature failure	Major	Activation key validation has failed due to invalid product serial number	Replace the IDU	
911	license-violation-runtime-counter-expired	Event	Activation key violation sanction is enforced	Major			
913	license-bad-xml-file-alarm	Alarm	Activation key components are missing or corrupted	Major	Essential internal activation key components are missing or corrupted.	Reinstall software	
1102	software-installation-status	Event	Software installation status:	Warning			

Alarms List

Alarm ID	Name	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1105	software-new-version-installed	Event	New version installed	Warning	A software version has been installed but system has not been reset.		
1111	software-user-confirmation-for-version	Event	User approved download of software version file	Warning			
1112	software-download-status	Event	Software download status:	Warning			
1113	software-download-missing-components	Event	Missing components:	Warning			
1114	software-management-incomplete-bundle	Event	Incomplete file set; missing components	Warning	Software bundle is missing components.	Get a complete software bundle	
1150	backup-started	Event	Configuration file backup generation started	Warning	User command		
1151	backup-succeeded	Event	Configuration file backup created	Warning	Backup file creation finished successfully		
1152	backup-failure	Event	Failure in configuration file backup generation	Warning	System failed in attempt to create backup configuration file		
1153	restore-succeeded	Event	Configuration successfully restored from file backup	Warning	Configuration restore finished successfully		
1154	restore-failure	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	restore-canceled	Event	Configuration restore operation cancelled	Warning	Restore operation cancelled because of user command or execution of another configuration management operation	Try again	
1156	file-transfer-issued	Event	User issued command for transfer of configuration file	Warning	User command		
1157	file-transfer-succeeded	Event	Configuration file transfer successful	Warning	Configuration file transfer successful		
1158	file-transfer-failure	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.	

Alarm ID	Name	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1159	file-transfer-in-progress	Event	Configuration file transfer in progress	Warning	File transfer started		
1163	cli-script-activation-started	Event	CLI configuration script activation started	Warning	User command		
1164	cli-script-activation-succeeded	Event	CLI Configuration script executed successfully	Warning			
1165	cli-script-activation-failure	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	unit-info-file-transfer-status-changed	Event	Unit info file transfer status:	Warning			
1167	unit-info-file-creation-status-changed	Event	Unit info file creation status:	Warning			
1169	restore-started	Event	Configuration restore operation started	Warning	Restore operation started because of user command		
1201	file-missed	Alarm	Modem firmware file not found	Critical	Modem file is missing	1. Download software package. 2. Reset the system.	
1202	load-failed	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	modem-wd-reset	Event	Modem watch-dog reset event	Warning			
1312	script-loading-failed	Alarm	Radio MRMC script loading failed	Major	Damaged hardware module	Replace the radio hardware module	
1401	incompatible-rfu-tx-calibration	Alarm	Incompatible RFU TX calibration	Major	RFU calibration tables require SW upgrade	Upgrade IDU SW	
1501	remote-communication-failure	Alarm	Remote communication failure	Critical	Fade in the link	Check the link performance	
1601	if-loopback	Alarm	IF loopback	Warning	User enabled IF loopback	Disable IF loopback	

Alarm ID	Name	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1602	lock-detect	Alarm	IF synthesizer is unlocked.	Critical	1. Extreme temperature condition. 2. HW failure.	1. Check installation. 2. Reset the RMC (Radio Modem Card) module. 3. Replace the RMC (Radio Modem Card).	
1701	cable-open	Alarm	Cable open	Major	Cable is not connected to RMC (Radio Modem Card) or RFU	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.	
1702	cable-short	Alarm	Cable short	Major	Physical short at the IF cable	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	communication-failure	Alarm	RFU communication failure	Warning	3. Defective IF cable. 4. IF cable not connected properly. 5. Defective RMC (Radio Modem Card). 6. Defective RFU. 7. RFU software download in progress.	1. 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. For a high power RF Unit: 1. Check BMA connector on OCB 2. Check BMA connector on RFU.	
1704	delay-calibration-failure-1	Alarm	RFU delay calibration failure 1	Warning	Defective RFU	1. Reset the RMC (Radio Modem Card) / RFU. 2. Replace RFU.	
1705	delay-calibration-failure-2	Alarm	RFU delay calibration failure 2	Warning	Calibration cannot be completed due to notch detection	Enter delay calibration value manually.	
1706	extreme-temp-cond	Alarm	RFU extreme temperature	Warning	1. Installation conditions. 2. Defective RFU.	1. Check installation conditions. 2. Verify operation as per product's specs. 3. Replace RFU.	

Alarm ID	Name	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1708	freq-set-automatically	Event	RFU frequency was set automatically	Warning	Defective RFU	1. Check if problem repeats and if errors/alarms reported. 2. Replace RFU.	
1709	hardware-failure-1	Alarm	RFU hardware failure 1	Critical	Defective RFU.	Replace RFU.	
1710	hardware-failure-2	Alarm	RFU hardware failure 2	Critical	Defective RFU.	Replace RFU.	
1711	low-if-signal-to-rfu	Alarm	Low IF signal to RFU	Major	1. IF cable connection. 2. Defective RFU. 3. Defective RMC (Radio Modem Card).	1. Check IF cable connectors. 2. Verify that N-Type connector inner pin is not spliced. 3. Replace RMC (Radio Modem Card). 4. Replace RFU.	
1712	no-signal-from-rfu	Alarm	Low IF signal from RFU	Warning	Low RX IF signal (140 MHz) from RFU.	1. Check IF cable and connectors. 2. Verify that N-Type connector inner pin is not spliced. 3. Replace RMC (Radio Modem Card). 4. Replace RFU.	
1713	pa-extreme-temp-cond	Alarm	RFU PA extreme temperature	Warning	1. Installation conditions. 2. Defective RFU.	1. Check installation conditions. 2. Replace RFU.	
1721	reset-occurred	Event	RFU reset	Major			
1722	rfu-loopback-active	Alarm	RFU loopback is active	Major	User has activated RFU loopback.	Disable RFU loopback.	
1723	rfu-mode-changed-to-combined	Event	RFU mode changed to Combined	Indeterminate			
1724	rfu-mode-changed-to-diversity	Event	RFU mode changed to Diversity	Indeterminate			
1725	rfu-mode-changed-to-main	Event	RFU mode changed to Main	Indeterminate			
1726	rfu-power-supply-failure	Alarm	RFU power supply failure	Major	At least one of the RFU's power supply voltages is too low.	Replace RFU.	

Alarm ID	Name	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1727	rx-level-out-of-range	Alarm	RFU RX level out of range	Warning	RSL is very low, link is down.	1. Check antenna alignment & link planning. 2. Check link settings (TX power, TX frequency). 3. Check antenna connections. 4. Replace local/remote RFU.	
1728	rx-level-path1-out-of-range	Alarm	RFU RX level path1 out of range	Warning	1. Improper installation. 2. Fading event. 3. Defective RFU.	1. Check that the fault is not due to rain/multi-path fading or lack of LOS. 2. Check link settings (TX power, TX frequency). 3. Check antenna alignment. 4. Check antenna connections. 5. Replace local/remote RFU.	
1729	rx-level-path2-out-of-range	Alarm	RFU RX level path2 out of range	Warning	1. Improper installation. 2. Fading event. 3. Defective RFU.	1. Check that the fault is not due to rain/multi-path fading or lack of LOS. 2. Check link settings (TX power, TX frequency). 3. Check antenna alignment. 4. Check antenna connections. 5. Replace local/remote RFU.	
1733	synthesizer-unlocked	Alarm	RFU synthesizer unlocked	Major	At least one of the RFU synthesizers is unlocked	1. Replace RFU. 2. In XPIC mode, replace mate RFU as well.	
1734	tx-level-out-of-range	Alarm	RFU TX level out of range	Minor	Defective RFU (the RFU cannot transmit the requested TX power)	1. Replace RFU. 2. Intermediate solution - reduce TX power.	
1735	tx-mute	Alarm	RFU TX Mute	Warning	RFU Transmitter muted by user	Unmute the RFU transmitter	
1736	unknown-rfu-type	Alarm	IDU SW does not support this type of RFU	Major	IDC SW does not support the RFU	Upgrade IDC SW	
1769	unit-cold-reset-event	Event	Unit Perform Power up	Warning			

Alarm ID	Name	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1770	cable-lof-rfu	Event	Unit performing power-up.	Major			
1771	cable-error-rfu	Alarm	RFU cable error.	Major	Errors in signal from IDU to XCVR.	1. Check the IF cable and connectors. 2. Verify that the N-Type/TNC connector inner pin is not spliced. 3. Replace RMC. 4. Replace XCVR.	
1772	xpic-data-los	Alarm	Radio XPIC sync loss	Major	Signaling between RMCs (Radio Modem Cards) for XPIC functionality has failed	1. Check that the RMCs are in allowed slots. 2. Populate the RMCs in different allowed location in the chassis. 3. Replace RMC/s. 4. Replace chassis.	
1773	early-warning	Alarm	Radio early warning.	Warning	The estimated radio BER (Bit Error Rate) is above 10E-12.	5. Check link performance. 6. Check IF cable, and replace if required. 7. Replace XCVR. 8. Replace RMC.	
1774	sw-download-incompatible-rfu	Alarm	RFU software download cannot be initiated.	Critical	The hardware of the XCVR is OK, but is it running with METRO radio application.	1. Upgrade the XCVR software application via XPAND-IP and then reinitiate software download.	
1775	hw-incompatible-rfu	Alarm	RFU software download is not possible.	Critical	Wrong type of XCVR, the XCVR hardware is METRO.	Replace the XCVR	
1776	pll-rmc	Alarm	RMC hardware failure.	Major	RMC hardware failure of the clock distributor.	Replace the RMC.	
1780	mrmc-running-script-deleted	Event	MRMC running script is deleted	Warning	New installed software package does not include the running MRMC radio script	1. Make sure the required software package include the running MRMC radio script. 2. Download and install the correct software package.	

Alarm ID	Name	Type	Description	Severity	Probable Cause	Corrective Action	Notes
1781	mrmc-running-script-updated	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	
1790	np-hw-failure	Alarm	Hardware failure	Critical	An internal hardware failure has been detected by the system.	Replace the card or unit reporting the hardware failure.	
2100	STM-1-OC-3-IN-LOS	Alarm	Loss of Signal on Line Interface (LOS) on STM-1/OC-3 port.	Critical	1. Line is not properly connected. 2. External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment.	
2101	STM-1-OC-3-IN-LOF	Alarm	Loss of Frame on Line Interface (LOF) on STM-1/OC-3 port.	Major	1. Line is not properly connected. 2. External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment.	
2102	STM-1-OC-3-IN-MSAIS	Alarm	Alarm Indication Signal on Line Interface (MS-AIS/AIS-L) received.	Minor	1. Line is not properly connected. 2. External equipment is faulty.	1. Reconnect line. 2. Check line cables. 3. Check external equipment.	
2103	STM-1-OC-3-IN-MSRDI	Alarm	Remote Defect Indication on Line Interface (MS-RDI/RDI-L) received.	Minor	External equipment is faulty.	Check external equipment.	
2104	STM-1-OC-3-RX-LOS	Alarm	Loss of STM-1/OC-3 Frame on Radio Interface.	Major	1. All channels in Multi Carrier ABC group are down. 2. Incorrect configuration on remote side.	1. Check link performance. 2. Check radio alarms for channel. 3. Check configuration.	
2105	STM-1-OC-3-RX-MSAIS	Alarm	MS-AIS/AIS-L on Radio Interface detected.	Minor	1. Remote STM-1/OC-3 signal is missing (LOS/LOF/MS-AIS/AIS-L on remote STM-1/OC-3 interface). 2. STM-1/OC-3 Channel removed due to reduced radio capacity on remote side.	Check remote equipment.	
2106	STM-1-OC-3-RX-RDI	Alarm	MS-RDI/RDI-L on Radio Interface detected.	Minor	External equipment is faulty.	Check remote equipment.	
2107	STM-1-OC-3-LOOPBACK	Alarm	Loopback	Warning	Looping.	Remove looping.	

Alarm ID	Name	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2108	STM-1/OC-3-CHANNEL-1-REMOVED	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.	
2109	STM-1-OC-3-PBRS-INSERTION	Alarm	PBRS insertion.	Warning	PRBS insertion on STM-1/OC-3 card.	Remove PRBS insertion.	
2110	STM-1-OC-3-SFP-NOT-DETECTED	Alarm	SFP absent on STM-1/OC-3 port.	Critical	1. SFP is not properly installed. 2. SFP is faulty.	1. Install SFP properly. 2. Replace the card.	
2111	STM-1-OC-3-SFP-TX-FAILURE	Alarm	SFP Transmit Failure on STM-1/OC-3 port.	Critical	1. SFP is faulty.	1. Replace SFP or insert SFP if it is not inserted correctly. 2. Replace the card.	
2112	STM-1-OC-3-SFP-TX-MUTED	Alarm	SFP is muted on STM-1/OC-3 port.	Warning	SFP is muted by configuration.	Remove muting.	
2113	STM-1/OC-3-CHANNEL-2-REMOVED	Alarm	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for channel.	
2114	STM-1/OC-3-CHANNEL-3-REMOVED	Alarm	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for channel.	
2115	STM-1/OC-3-CHANNEL-4-REMOVED	Alarm	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for channel.	
2116	STM-1/OC-3-CHANNEL-5-REMOVED	Alarm	STM-1/OC-3 Channel Removed alarm (due to reduced radio capacity).	Warning	1. Reduced capacity. 2. Fading.	1. Check link performance. 2. Check radio alarms for channel.	
2117	STM-1/OC-3-CHANNEL-6-REMOVED	Alarm	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	STM-1/OC-3-CHANNEL-7-REMOVED	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	STM-1/OC-3-CHANNEL-8-REMOVED	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	Name	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2200	MC-ABC-Local-LOF	Alarm	Multi Carrier ABC LOF.	Critical	All channels in Multi Carrier ABC group are down.	1. Check link performance on all radio channels in Multi Carrier ABC group. 2. Check radio alarms for channels in Multi Carrier ABC group. 3. Check configuration of Multi Carrier ABC group.	
2203	MC-ABC-Lvds-Error-Sl2	Alarm	LVDS RX Error Slot 2.	Major	Hardware failure between RMC and TCC cards.	1. Replace RMC. 2. Replace TCC. 3. Replace chassis.	
2204	MC-ABC-Lvds-Error-Sl3	Alarm	LVDS RX Error Slot 3.	Major	Hardware failure between RMC and TCC cards.	1. Replace RMC. 2. Replace TCC. 3. Replace chassis.	
2205	MC-ABC-Lvds-Error-Sl4	Alarm	LVDS RX Error Slot 4.	Major	Hardware failure between RMC and TCC cards.	1. Replace RMC. 2. Replace TCC. 3. Replace chassis.	
2206	MC-ABC-Lvds-Error-Sl5	Alarm	LVDS RX Error Slot 5.	Major	Hardware failure between RMC and TCC cards.	1. Replace RMC. 2. Replace TCC. 3. Replace chassis.	
2207	MC-ABC-Lvds-Error-Sl6	Alarm	LVDS RX Error Slot 6.	Major	Hardware failure between RMC and TCC cards.	1. Replace RMC. 2. Replace TCC. 3. Replace chassis.	
2208	MC-ABC-Lvds-Error-Sl7	Alarm	LVDS RX Error Slot 7.	Major	Hardware failure between RMC and TCC cards.	1. Replace RMC. 2. Replace TCC. 3. Replace chassis.	
2209	MC-ABC-Lvds-Error-Sl8	Alarm	LVDS RX Error Slot 8.	Major	Hardware failure between RMC and TCC cards.	1. Replace RMC. 2. Replace TCC. 3. Replace chassis.	

Alarm ID	Name	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2210	MC-ABC-Lvds-Error-Sl9	Alarm	LVDS RX Error Slot 9.	Major	Hardware failure between RMC and TCC cards.	1. Replace RMC. 2. Replace TCC. 3. Replace chassis.	
2211	MC-ABC-Lvds-Error-Sl10	Alarm	LVDS RX Error Slot 10.	Major	Hardware failure between RMC and TCC cards.	1. Replace RMC. 2. Replace TCC. 3. Replace chassis.	
2212	MC-ABC-Lvds-Error-Sl12	Alarm	LVDS RX Error Slot 12.	Major	Hardware failure between RMC and TCC cards.	1. Replace RMC. 2. Replace TCC. 3. Replace chassis.	
2219	MC-ABC-Ch-Id-Mismatch-Ch1	Alarm	Multi Carrier ABC Channel Id Mismatch Ch1.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.	
2220	MC-ABC-Ch-Id-Mismatch-Ch2	Alarm	Multi Carrier ABC Channel Id Mismatch Ch2.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.	
2221	MC-ABC-Ch-Id-Mismatch-Ch3	Alarm	Multi Carrier ABC Channel Id Mismatch Ch3.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.	
2222	MC-ABC-Ch-Id-Mismatch-Ch4	Alarm	Multi Carrier ABC Channel Id Mismatch Ch4.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.	
2223	MC-ABC-Ch-Id-Mismatch-Ch5	Alarm	Multi Carrier ABC Channel Id Mismatch Ch5.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.	
2224	MC-ABC-Ch-Id-Mismatch-Ch6	Alarm	Multi Carrier ABC Channel Id Mismatch Ch6.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.	
2225	MC-ABC-Ch-Id-Mismatch-Ch7	Alarm	Multi Carrier ABC Channel Id Mismatch Ch7.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.	
2226	MC-ABC-Ch-Id-Mismatch-Ch8	Alarm	Multi Carrier ABC Channel Id Mismatch Ch8.	Warning	Configuration failure.	Compare Channel ID configuration with remote side.	
2235	MC-ABC-Ch-Id-Disabled-Ch1	Alarm	Multi Carrier ABC Channel Id Manual Disabled Ch1.	Warning	Admin state for channel is down.	Enable admin state for channel.	
2236	MC-ABC-Ch-Id-Disabled-Ch2	Alarm	Multi Carrier ABC Channel Id Manual Disabled Ch2.	Warning	Admin state for channel is down.	Enable admin state for channel.	

Alarm ID	Name	Type	Description	Severity	Probable Cause	Corrective Action	Notes
2237	MC-ABC-Ch-Id-Disabled-Ch3	Alarm	Multi Carrier ABC Channel Id Manual Disabled Ch3.	Warning	Admin state for channel is down.	Enable admin state for channel.	
2238	MC-ABC-Ch-Id-Disabled-Ch4	Alarm	Multi Carrier ABC Channel Id Manual Disabled Ch4.	Warning	Admin state for channel is down.	Enable admin state for channel.	
2239	MC-ABC-Ch-Id-Disabled-Ch5	Alarm	Multi Carrier ABC Channel Id Manual Disabled Ch5.	Warning	Admin state for channel is down.	Enable admin state for channel.	
2240	MC-ABC-Ch-Id-Disabled-Ch6	Alarm	Multi Carrier ABC Channel Id Manual Disabled Ch6.	Warning	Admin state for channel is down.	Enable admin state for channel.	
2241	MC-ABC-Ch-Id-Disabled-Ch7	Alarm	Multi Carrier ABC Channel Id Manual Disabled Ch7.	Warning	Admin state for channel is down.	Enable admin state for channel.	
2242	MC-ABC-Ch-Id-Disabled-Ch8	Alarm	Multi Carrier ABC Channel Id Manual Disabled Ch8.	Warning	Admin state for channel is down.	Enable admin state for channel.	
2300	protection-configuration-mismatc	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	protection-copytomate-started	Event	Copy to mate started	Indeterminate	The copy-to-mate command has just begun!	This is a notification	All
2302	protection-copytomate-completed	Event	Copy to mate completed	Indeterminate	The copy-to-mate command was completed.	This is a notification	All
5000	failure-login-event	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	g8032-protection-switching-alarm	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	g8032-failure-of-protocol-pm-alarm	Alarm	More than a single RPL is configured in a ring	Warning	User configuration	Reconfigure the RPL	
5003	lldp-topology-change	Event	LLDP topology change	Warning	New neighbor	None	
5004	security-log-upload-started-event	Event	Security log upload started	Indeterminate	Security log upload started		

Alarm ID	Name	Type	Description	Severity	Probable Cause	Corrective Action	Notes
5005	security-log-upload-failed-event	Event	Security log upload failed	Indeterminate	Security log upload failed		
5006	security-log-upload-succeeded-event	Event	Security log upload succeeded	Indeterminate	Security log upload succeeded		
5010	force-mode-alarm	Alarm	System is in sync force mode state	Warning	User command		
5011	sync-quality-change-event	Event	The sync-source quality level was changed	Major			
5012	system-clock-in-holdover-mode	Alarm	System Synchronization Reference in Holdover Mode	Critical			
5013	sync-T0-quality-change-event	Event	The system's reference-quality changed	Major			
5014	sync-pipe-invalid-interface-clock-source	Alarm	The pipe interface clock-source in signal-interface table is not system-clock	Major			
5015	sync-pipe-missing-edge	Alarm	The pipe is missing an edge interface	Major	Regenerator contains less than 2 interfaces	Accomplish configuration by assigning second interface	
5016	sync-pipe-interface-op-state-down	Alarm	Pipe interface operational state is down	Major	At least one of Regenerator Interfaces status is down	Checking regenerator Admin status	
5017	sync-pipe-invalid-pipe	Alarm	Pipe is invalid	Major	Interfaces has Configuration or Operation fails	Configuration not accomplished	
5030	soam-connectivity-failure	Alarm	A connectivity failure in MA/MEG	Minor	Specific defect dependent: User configuration , connectivity loss.	Reconfigure the RPL.	
5100	mkey-mismatch	Alarm	Master key mismatch cross over the link	Critical	Master Key was not set correctly.	Verify the Master Key.	(1)
5101	mkey-no-exist	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	general-encryption-failure	Alarm	Payload Encryption failure	Critical	1. Radio LOF on Tx/Rx direction. 2. The session key does not match across the link. 1. The AES admin setting does not match across the link.	1. Validate the MSE on both sides of the link. 2. Validate the session key on both sides of the link. 1. Validate the AES admin setting on both sides of the link.	(1)

Alarm ID	Name	Type	Description	Severity	Probable Cause	Corrective Action	Notes
5103	kep-finished	Event	Key Exchange Protocol successfully finished	Indeterminate			(1)
5104	kep-initiated	Event	Key Exchange Protocol initiated	Indeterminate			(1)
5105	kep-remote-initiated	Event	Key Exchange Protocol initiated by remote side	Indeterminate			(1)
5106	kep-zeroized	Event	Key Zeroization command executed	Indeterminate			(1)
5107	bypass-self-test-alarm	Alarm	FIPS Bypass Self-Test failed	Critical	Disk failure		(1)
5108	post-fail-alarm	Alarm	Power On Self-Test Failed	Critical	System failure	Reboot the unit.	(1)
30007	Clock-source-sharing-failure-event	Event	Clock source sharing failure	Critical	1. Faulty coaxial cable between master and slave RFUs. 2. Hardware failure in Master RFU. 3. Hardware failure in Slave RFU.	1. Try re-initiation of MIMO. If still fails: 2. Replace faulty coaxial cable and reset Master RFU. 3. Replace faulty RFU.	(2)
31000	Insufficient-conditions-for-MIMO-alarm	Alarm	Insufficient conditions for MIMO	Critical	1. Insufficient conditions for MIMO. 2. Hardware failure.	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	Unsuitable-hardware-for-MIMO-alarm	Alarm	Unsuitable hardware for MIMO	Critical	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	Name	Type	Description	Severity	Probable Cause	Corrective Action	Notes
31004	Unsuitable-software-configuration-for-MIMO-alarm	Alarm	Unsuitable software configuration for MIMO	Critical	1. Not all MIMO carriers are set to same radio script or script is not compatible for MIMO. 2. Radio TX and RX frequency is not identical on all MIMO carriers. 3. XPIC or Multi radio or ATPC features are enabled.	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	Clock-source-sharing-failure-alarm	Alarm	Clock source sharing cable unplugged	Critical	2. Faulty coaxial cable between master and slave RFUs 3. Mate does not exist	2. Replace faulty coaxial cable and reset Master RFU. 3. Replace faulty RFU.	(2)
5100	mkey-mismatch	Alarm	Master key mismatch cross over the link	Critical	Master Key was not set correctly.	Verify the Master Key.	(1)
5101	mkey-no-exist	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	general-encryption-failure	Alarm	Payload REncryption failure	Critical	3. Radio LOF on Tx/Rx direction. 4. The session key does not match across the link. 4. The AES admin setting does not match across the link.	3. Validate the MSE on both sides of the link. 4. Validate the session key on both sides of the link. 4. Validate the AES admin setting on both sides of the link.	(1)
5103	kep-finished	Event	Key Exchange Protocol successfully finished	Indeterminate			(1)
5104	kep-initiated	Event	Key Exchange Protocol initiated	Indeterminate			(1)
5105	kep-remote-initiated	Event	Key Exchange Protocol initiated by remote side	Indeterminate			(1)
5106	kep-zeroized	Event	Key Zeroization command executed	Indeterminate			(1)
5107	bypass-self-test-alarm	Alarm	FIPS Bypass Self-Test failed	Critical	Disk failure		(1)
5108	post-fail-alarm	Alarm	Power On Self-Test Failed	Critical	System failure	Reboot the unit.	(1)

(1) Supported by NetStream Diplo and NetStream Primo only

(2) Supported by NetStream Diplo only

25. Abbreviations

The following table lists the abbreviations used in this guide.

Abbreviations

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
AGC	Automatic Gain Control
AIS	Alarm Indicating Signal
ALC	Automatic Level Control
ANSI	American National Standards Institute
ASIC	Application Specified Integrated Circuit
ATPC	Automatic Transmit Power Control
AUX	Auxiliary Unit
B	
BB	Baseband
BBS	Baseband Switching
BER	Bit Error Rate
BLSR	Bidirectional Line Switch Ring
BPDU	Bridge Protocol Data Units
BWA	Broadband Wireless Access
C	
CBS	Committed Burst Size
CCDP	Co-Channel Dual Polarization
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
ETSI	European Telecommunications Standards Institute
F	
FCC	Federal Communications Commission
FCS	Frame Check Sequence
FTP	File Transfer Protocol
G	
GbE	Gigabit Ethernet
GFP	Generic Framing Procedure (Procedure for mapping of Ethernet traffic over a transport network)
GND	Ground
GRE	Generic Routing Encapsulation
GTP	GPRS Tunneling Protocol
H	
HBER	High Bit Error Rate
HDLC	High-level Data Link Control
HF	High Frequency (3-30 MHz)
HSB	Hot-Standby
HTTP	Hypertext Transfer Protocol
HTTPS	Secured Hypertext Transfer Protocol
I	
IDC	Indoor Controller
IF	Intermediate Frequency
IFC	IF Combining
ISO	International Organization for Standardization
ITU	International Telecom. Union
ITU-R	International Telecom. Union (former CCIR)
ITU-T	International Telecom. Union (former CCITT)
IVM	Inventory Module
L	
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group

LAN	Local Area Network
LBER	Low Bit Error Rate
LCAS	Link Capacity Adjustment Scheme
LED	Light Emitting Diode
LIU	Line Interface Unit
LLDP	Link Layer Discovery Protocol
LLF	Link Loss Forwarding
LMS	License Management System
LO	Local Oscillator
LOC	Loss of Carrier
LOF	Loss of Frame
LOS	Loss of Signal
LSI	Large Scale Integration
LTE	Long-Term Evolution
M	
MAID	Maintenance Association Identifier
MPLS	Multi Protocol Label Switching
MSP	Multiplex Section Protection
MUX	Multiplexer
N	
NE	Network Element
NMS	Network Management System
NTP	Network Time Protocol
O	
OAM	Operation Administration & Maintenance (Protocols)
OCB	Outdoor Circulator Box
OHC	OverHead Connections
OMT	Orthogonal Mode Transducer
OOF	Out of Frame
OPEX	Operational Expenditure
P	
PBB-TE	Provider Backbone Bridge Traffic Engineering
PBS	Peak Burst Rate
PC	Personal Computer
PCB	Printed Circuit Board
PDV	Packed Delay Variation
PIR	Peak Information Rate
PLL	Phase Locked Loop
PM	Performance Monitoring
PN	Provider Network

PROM	Programmable Read Only Memory
PSN	Packet Switched Network
PTP	Precision Timing Protocol
PWR	Power
Q	
QoE	Quality of Experience
QoS	Quality of Service
R	
RBAC	Role Based Access Control
RCVR	Receiver
RDI	Reverse Defect Indication
RF	Radio Frequency
RIP	Routing Information Protocol
RMON	Ethernet Statistics
RPS	Radio Protection Switching
RSL	Received Signal Level
RSSI	Received Signal Strength Indicator
RSTP	Rapid Spanning Tree Protocol
S	
SAP	Service Access Point
SDH	Synchronous Digital Hierarchy
SDWRR	Shaped Deficit Weighted Round Robin
SETS	Synchronous Equipment Timing Source
SFTP	Secure FTP
SLA	Service Level Agreements
SNCP	Simple Network Connection Protection
SNMP	Simple Network Management Protocol
SNP	Service Network Point
SNR	Signal to Noise Ratio
SNTP	Simple Network Time Protocol
SOH	Section OverHead (ETSI)
SONET	Synchronous Optical NETwork
SP	Service Point
SSH	Secured Shell (Protocol)
SSM	Synchronization Status Message
STP	Spanning Tree Protocol
SyncE	Synchronous Ethernet
SVCE	Service Channel Equipment
T	
TC	Traffic Class

TIM	Trace Identifier Mismatch
TOH	Transport OverHead (ANSI)
TOS	Type Of Service
V	
VC	Virtual Container
VCO	Voltage Controlled Oscillator
VCXO	Voltage Controlled crystal Oscillator
VLSI	Very Large Scale of Integration
W	
WAN	Wide Area Network
Web EMS	Web-Based Element Management System
WFQ	Weighted Fair Queue
WG	Waveguide
WRED	Weighted Random Early Detection
WRR	Weighted Round Robin
X	
XCVR	Transceiver (Transmitter/Receiver)
XMTR	Transmitter
XO	Crystal Oscillator
XPD	Cross Polar Differentiation
XPIC	Cross Polarization Interference Cancellation