



Service Aware Operating System®
SAOS

System Software Configuration Guide

Software Release 6.5.0



LEGAL NOTICES

THIS DOCUMENT CONTAINS CONFIDENTIAL AND TRADE SECRET INFORMATION OF CIENA CORPORATION AND ITS RECEIPT OR POSSESSION DOES NOT CONVEY ANY RIGHTS TO REPRODUCE OR DISCLOSE ITS CONTENTS, OR TO MANUFACTURE, USE, OR SELL ANYTHING THAT IT MAY DESCRIBE. REPRODUCTION, DISCLOSURE, OR USE IN WHOLE OR IN PART WITHOUT THE SPECIFIC WRITTEN AUTHORIZATION OF CIENA CORPORATION IS STRICTLY FORBIDDEN.

EVERY EFFORT HAS BEEN MADE TO ENSURE THAT THE INFORMATION IN THIS DOCUMENT IS COMPLETE AND ACCURATE AT THE TIME OF PRINTING; HOWEVER, THE INFORMATION CONTAINED IN THIS DOCUMENT IS SUBJECT TO CHANGE.

Copyright 2009 Ciena Corporation

Unpublished All Rights Reserved

The material contained in this document is also protected by copyright laws of the United States of America and other countries. It may not be reproduced or distributed in any form by any means, altered in any fashion, or stored in a data base or retrieval system, without express written permission of the Ciena Corporation.

Security

Ciena® cannot be responsible for unauthorized use of equipment and will not make allowance or credit for unauthorized use or access.

Contacting Ciena

Corporate Headquarters	410-694-5700 or 800-921-1144	www.ciena.com
Customer Technical Support/Warranty		
In North America	1-800-CIENA24 (243-6224) 410-865-4961	E-mail: CIENA24@ciena.com
In Europe, Middle East, and Africa	800-CIENA-24-7 (800-243-6224-7) +44-207-012-5508	E-mail: CIENA24@ciena.com
In Asia-Pacific	800-CIENA-24-7 (800-243-6224-7) +81-3-3248-4743	E-mail: CIENA24@ciena.com
Sales and General Information	410-694-5700	E-mail: sales@ciena.com
In North America	410-694-5700 or 800-207-3714	E-mail: sales@ciena.com
In Europe	+44-207-012-5500 (UK)	E-mail: sales@ciena.com
In Asia	+81-3-3248-4680 (Japan)	E-mail: sales@ciena.com
In Latin America	011-5255-1719-0220 (Mexico City)	E-mail: sales@ciena.com
Training and Documentation		
Training	877-CIENA-TD (243-6283) or 410-865-8996	E-mail: techtng@ciena.com
Documentation	877-CIENA-TD (243-6283) or 410-694-8125	E-mail: techpubs@ciena.com

For additional office locations and phone numbers, please visit the Ciena web site at www.ciena.com.



IMPORTANT: PLEASE READ THIS LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE INSTALLING OR USING CIENA COMMUNICATIONS, INC. ("Ciena") SOFTWARE, HARDWARE OR DOCUMENTATION (COLLECTIVELY, THE "EQUIPMENT").

BY INSTALLING OR USING THE EQUIPMENT, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. Right to Use License; Restrictions. Subject to these terms, and the payment of all applicable license fees, Ciena grants to you, as end user, a non-exclusive license to use the Ciena software excluding open source components (the "Software") in object code form solely in connection with, and as embedded within, the Equipment,. You shall have the right to use the Software solely for your own internal use and benefit. You may make one copy of the Software and documentation solely for backup and archival purpose, however you must reproduce and affix all copyright and other proprietary rights notices that appear in or on the original. You may not, without Ciena's prior written consent, (i) sublicense, assign, sell, rent, lend, lease, transfer or otherwise distribute the Software; (ii) grant any rights in the Software or documentation not expressly authorized herein; (iii) modify the Software nor provide any third person the means to do the same; (iv) create derivative works, translate, disassemble, recompile, reverse engineer or attempt to obtain the source code of the Software in any way; or (v) alter, destroy, or otherwise remove any proprietary notices or labels on or embedded within the Software or documentation. You acknowledge that this license is subject to Section 365 of the U.S. Bankruptcy Code and requires Ciena's consent to any assignment related to a bankruptcy proceeding. Sole title to the Software and documentation, to any derivative works, and to any associated patents and copyrights, remains with Ciena or its licensors. Ciena reserves to itself and its licensors all rights in the Software and documentation not expressly granted to you. You shall preserve intact any notice of copyright, trademark, logo, legend or other notice of ownership from any original or copies of the Software or documentation. Ciena does not place any restrictions on the open source components that may be distributed along with the Software. Any applicable open source licenses will be distributed to recipient separately.

2. Audit: Upon Ciena's reasonable request, but not more frequently than annually without reasonable cause, you shall permit Ciena to audit the use of the Software at such times as may be mutually agreed upon to ensure compliance with this Agreement.

3. Confidentiality. You agree that you will receive confidential or proprietary information ("Confidential Information") in connection with the purchase, deployment and use of the Equipment. You will not disclose Confidential Information to any third party without prior written consent of Ciena, will use it only for purposes for which it was disclosed, use your best efforts to prevent and protect the contents of the Software from unauthorized disclosure or use, and must treat it with the same degree of care as you do your own similar information, but with no less than reasonable care. You acknowledge that the design and structure of the Software constitute trade secrets and/or copyrighted materials of Ciena and agree that the Equipment is Confidential Information for purposes of this Agreement.

4. U.S. Government Use. The Software is provided to the Government only with restricted rights and limited rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in FAR Sections 52-227-14 and 52-227-19 or DFARS Section 52.227-7013(C)(1)(ii), as applicable. The Equipment and any accompanying technical data (collectively "Materials") are commercial within the meaning of applicable Federal acquisition regulations. These Materials were developed fully at private expense. U.S. Government use of the Materials is restricted by this Agreement, and all other U.S. Government use is prohibited. In accordance with FAR 12.212 and DFAR Supplement 227.7202, software delivered to you is commercial computer software and the use of that software is further restricted by this Agreement.

5. Term of License. This license is effective until terminated. Customer may terminate this license at any time by giving written notice to Ciena and destroying or erasing all copies of Software including any documentation. Ciena may terminate this Agreement and your license to the Software immediately by giving you written notice of termination in the event that either (i) you breach any term or condition of this Agreement or (ii) you are wound up other than voluntarily for the purposes of amalgamation or reorganization, have a receiver appointed or enter into liquidation or bankruptcy or analogous process in your home country. Termination shall be without prejudice to any other rights or remedies Ciena may have. In the event of any termination Customer will have no right to keep or use the Software or any copy of the Software for any purpose and Customer shall destroy and erase all copies of such Software in its possession or control, and forward written certification to Ciena that all such copies of Software have been destroyed or erased.



6. Compliance with laws. You agree to comply with all applicable laws, including all import regulations, and to obtain all required licenses and permits related to installation and use of Equipment. Software, including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software.

7. Limitation of Liability. ANY LIABILITY OF Ciena SHALL BE LIMITED IN THE AGGREGATE TO THE AMOUNTS PAID BY YOU FOR THE SOFTWARE. THIS LIMITATION APPLIES TO ALL CAUSES OF ACTION, INCLUDING WITHOUT LIMITATION BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS. THE LIMITATIONS OF LIABILITY DESCRIBED IN THIS SECTION ALSO APPLY TO ANY THIRD-PARTY SUPPLIER OF Ciena. NEITHER Ciena NOR ANY OF ITS THIRD-PARTY SUPPLIERS SHALL BE LIABLE FOR ANY INJURY, LOSS OR DAMAGE, WHETHER INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL INCLUDING WITHOUT LIMITATION ANY LOST PROFITS, CONTRACTS, DATA OR PROGRAMS, AND THE COST OF RECOVERING SUCH DATA OR PROGRAMS, EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

8. General. Ciena may assign this Agreement to any Ciena affiliate or to a purchaser of the intellectual property rights in the Software, but otherwise neither this Agreement nor any rights hereunder may be assigned nor duties delegated by either party, and any attempt to do so will be void. This Agreement shall be governed by the laws of the State of Maryland (without regard to the conflict of laws provisions) and shall be enforceable in the courts of Maryland. The U.N. Convention on Contracts for the International Sale of Goods shall not apply hereto. This Agreement constitutes the complete and exclusive statement of agreement between the parties relating to the license for the Software and supersedes all proposals, communications, purchase orders, and prior agreements, verbal or written, between the parties. If any portion hereof is found to be void or unenforceable, the remaining provisions shall remain in full force and effect. The source code for open source components distributed to an end user is available upon request.

Rev. May 14, 2009



In accordance with our policy to continually enhance the Ciena Corporation family of products, the specifications and information contained in this guide are subject to change at anytime without notice. All statements, information, and recommendations in this guide are believed to be accurate but are presented without warranty of any kind, expressed or implied. Ciena Corporation will not be liable for any damages of any kind arising from the use of this guide, including but not limited to direct, indirect, incidental punitive, and consequential damages. Users must take full responsibility for the application of the products.

This guide contains information protected by copyright. No part of this publication may be photocopied or reproduced in any form without prior written consent from Ciena Corporation.

The software provided with Ciena Corporation hardware and described in this guide is furnished under and is subject to a license and nondisclosure agreement.

Ethernet to the Subscriber, Fiber to the Subscriber, True Carrier Ethernet, and Ciena are all trademarks of Ciena Corporation.

Other specific product names mentioned herein are trademarks of their respective companies.

System Software Configuration Guide 6.5.0

Document Number: MAN-0157-001

Publication Date: June 2009

© 2009 Ciena Corporation

All Rights Reserved

Copyright and Trademark Guidelines

These copyright and trademark guidelines provide information concerning the proper usage and protection of Ciena Corporation trademarks, registered trademarks, service marks, registered service marks, tradenames, and/or registered tradenames.

Copyright

All content in this guide, including words, names, text, graphics, symbols, logos, icons, images, devices, and/or software, is the property of Ciena Corporation or its content suppliers and is protected by U.S. and international copyright laws. The compilation (meaning the collection, arrangement, and assembly) of all content in this guide is the exclusive property of Ciena Corporation and is protected by U.S. and international copyright laws. All software mentioned in this guide is the property Ciena Corporation or its software suppliers and protected by U.S. and international copyright laws. The content in this guide may be used as a resource. Any other use, including the reproduction, modification, distribution, transmission, republication, display, or performance, of the content in this guide is strictly prohibited.

Trademarks

Ciena Corporation trademarks may not be used in connection with any product or service that does not belong to Ciena Corporation. Furthermore, Ciena Corporation trademarks may not be used in any manner that is likely to cause confusion among customers or in such a way that it disparages or discredits Ciena Corporation.

Definitions

A trademark is often categorized as a word, name, text, graphic, symbol, logo, icon, image, device, and/or software or any combination used by a corporation to identify their products and distinguish those products from other corporations.

A service mark is typically used to identify a corporation's services rather than tangible products.

A tradename is commonly used as the name of a corporation or an abbreviation of that name under which normal business activity is conducted. Some tradenames might be used in more than one category; therefore, it is important that the reader be aware of the context for which the tradename is used.

Categories

Trademarks, service marks, and tradenames generally fall into two categories:

1. Those that are registered with the United States Patent and Trademark Office¹ (USPTO).
2. Those that are being used, but have not yet completed the registration process.

Both categories are protected, although those that are registered provide visible notice of the corporation's rights and stronger enforcement provisions.

The registration process may take a long period of time before it is finalized, thus pending trademarks, service marks, and tradenames may be in use by the corporation.

Trademarks, service marks, and tradenames must be used with the first mention or most prominent appearance in a publication, but need not be used with each subsequent appearance. If there are multiple uses of trademarks, service marks, and tradenames throughout the publication, an explanatory note on the cover sheet is sufficient.

1. Full information regarding the United States Patent and Trademark Office (USPTO) may be found online at <http://www.uspto.gov>

ISO Compliance



Important Safety Information



WARNING: This equipment is to be installed and maintained by qualified service personnel only. Refer to the **Regulatory Compliance and Safety** appendix of the User Guide for additional safety information.

AVERTISSEMENT: Cet équipement doit être installé et entretenu uniquement par un personnel de service qualifié.

WARNUNG: Dieses Gerät darf nur von qualifiziertem Wartungspersonal installiert und gewartet werden.

UPOZORNENIE: Toto zariadenie môže inštalovať a vykonávať na ňom údržbu len kvalifikovaný servisný personál.



Chapter 1: Introduction	1
Intended Audience	1
Overview	1
Structure	2
Document Conventions	4
Chapter 2: Chassis Setup	7
Enabling the Switch	7
Configuring the Serial Console Port	9
Configuring the Remote Management Interface	10
Configuring the Local Management Interface	11
Chapter 3: Managing Configuration	13
Overview	13
Access Levels	13
Accessing the CLI	14
Managing Configuration Files	15
Configuring Telnet	18
Managing Software License Keys	20
Configuring DHCP	23
Configuring NTP	27
DNS	32
SSHv2	33
SFTP	36
Customizing the System Shell	36
Retrieving System Information	39
Chapter 4: VLAN Management	43
Overview	43
VLANs and Traffic Flow	43
Behavior Summary	46
VLAN/Port Configuration	47
Port Mirroring	55
Port Loopback	56
Port Statistics	56
Chapter 5: Configuring CPU Rate Limiting	63
Overview	63
Benefits	63
Configuration	63
Troubleshooting	68
Chapter 6: Configuring IEEE 802.1x Security	71
802.1x Overview	71
Deployment Example	73
Using 802.1x with LACP	74
Configuring 802.1x	74
Using 802.1x to Authenticate a PC	77
Troubleshooting 802.1x Operation	79
Chapter 7: Link Aggregation and LACP	81
Overview	81
Link Aggregation Group	81
Manual Link Aggregation	82
LACP	82

Configuring Link Aggregation	85
Chapter 8: Monitoring System Status	89
Environmental Overview	89
Monitoring Temperature and Status.	89
Monitoring Power Supply Status	90
Monitoring Power On Self Tests	91
Managing Device Archives	92
Displaying Device Identification Attributes	93
Displaying Platform Capabilities	93
Displaying the Chassis MAC address	94
Chapter 9: OAM.	95
Overview	95
Principles of Operation	95
Feature Benefits	97
Configuring OAM	97
Chapter 10: Configuring and Identifying Transceivers	103
Overview	103
Compliance	103
Identification	103
Diagnostics	104
Displaying Transceiver Information	105
Determining Transceiver Speed	107
Disabling and Enabling Transceivers	108
Setting the Port Connector Mode	108
Chapter 11: Port State Mirroring	111
Overview	111
Principles of Operation	111
Feature Benefits	112
Bi-directional Port State Mirroring	112
Configuring Port State Mirroring	112
Chapter 12: Security	117
Overview	117
Service Access Control	117
User Management	122
RADIUS	125
TACACS+	128
IP Access Control Lists	130
Chapter 13: Configuring Broadcast Containment	133
Overview	133
Benefits	133
Configuring Broadcast Containment.	134
Troubleshooting	137
Chapter 14: Quality of Service	139
Overview	139
Ingress Resolved CoS Mapping	140
Traffic Profiling.	142
Ingress R-CoS to Egress CoS Queue Mapping	151
Congestion Avoidance.	152
Egress Scheduling	158

Egress Shaping	159
Configuring Frame Bandwidth Calculation	160
Chapter 15: Configuring Multicast Services	161
Overview	161
IGMP Snooping	161
Unknown Multicast Filtering	167
Configuring Multicast	167
Chapter 16: Layer 2 VPNs	181
Overview	181
Principles of Operation	181
Q-in-Q Encapsulation	183
Ethernet Virtual Private Line	186
Ethernet Private Line/LAN	187
EVPL Bundling	188
Chapter 17: Configuring Connectivity Fault Management	189
Overview	189
Benefits	194
Maintenance Association Examples	195
Configuring CFM Globally	198
Configuring CFM Services	200
Configuring MEPs	209
Configuring Remote MEPs	214
Configuring MIPs	219
Configuring CFM Services for a VLAN Service	221
Configuring CFM Services for a Virtual Switch	222
CFM Over Q-in-Q	223
Troubleshooting	225
Chapter 18: Configuring L2 Control Frame Tunneling	235
Overview	235
Benefits	239
Configuration	239
Troubleshooting	245
Chapter 19: Configuring TWAMP	249
Overview	249
Benefits	254
Configuring TWAMP	254
Troubleshooting	262
Chapter 20: Configuring MSTP	265
Overview	265
Benefits	269
Configuration	270
Troubleshooting	276
Chapter 21: Event Logging	283
Overview	283
Principles of Operation	283
Syslog	286
Flash Log	290
RAM Log	297

Command Log	302
Troubleshooting	306
Chapter 22: Configuring SNMP	307
Overview	307
Benefits	319
Configuring Global Attributes	319
Configuring SNMPv1/v2c Community Based Security	321
Configuring Port Traps and Servers	323
Configuring SNMPv3	324
Configuring RMON	334
Troubleshooting	340
Chapter 23: Provider Backbone Transport	341
Overview	341
Connectivity Fault Management	346
Benefits	348
Configuration	349
Chapter 24: Link Layer Discovery Protocol	359
Overview	359
Principles of Operation	359
Feature Benefits	362
Configuring Link Layer Discovery Protocol	363
Troubleshooting	366
Chapter 25: System Software Management	367
Overview	367
Network connectivity	367
Release Compatibility	367
Preparing Files for Upgrade	368
Upgrading from a Previous Version of SAOS	372
Backup Software Images	376
Appendix A: Command Line Interface	377
Overview	377
Access Levels	377
Accessing the CLI	378
Navigating the CLI	379
Deprecated Commands	385
Global Commands	385
Protocol/Manager Commands	387
Internet Site	539
E-mail Address	539
Telephone and Fax	539
Mailing Address	540

Glossary

Chapter Introduction

1

At a Glance:

- **Intended Audience**
- **Overview**
- **Structure**
- **Document Conventions**

This manual describes how to configure system software on the supported Service Delivery Switches. This system software is based on a common Service Aware Operating System (SAOS) code base designed to deliver consistent benefits across all Ethernet deliver, aggregation, and distribution configurations. This system software cannot be installed on other Service Delivery Switches, Service Concentration Switches or Service Aggregation Switches.

Intended Audience

This publication is intended for users, such as network technicians and system administrators, who will configure system software. It assumes that the intended user(s) possess basic knowledge of, but not limited to:

- Proper Hardware Installation
- Proper Hardware Diagnostics
- Ethernet Concepts
- IEEE 802 Standards
- Open Systems Interconnection (OSI) Seven Layer Model
- Optical Fiber Distribution and Monitoring
- Local Area Networks (LAN)
- Virtual Local Area Networks (VLAN)

Overview

This manual provides information and examples for use in configuring system software on any platform that it is installed. It includes an explanation of the key features supported by the devices and provides example configurations for these features. Although these examples are useful in configuration, they are not meant to be used as a configuration template.

Structure

In addition to this Introduction, this manual includes the following chapters:

Chapter 2 Chassis Setup

- Provides details for enabling the Service Delivery Switch and setting up interfaces.

Chapter 3 Managing Configuration

- Describes various tools for accessing the system and managing its configuration.

Chapter 4 VLAN Management

- Instructs how to configure VLANs and the ports associated with them.

Chapter 5 Configuring CPU Rate Limiting

- Explains the purpose and configuration of Central Processing Unit (CPU) rate limiting.

Chapter 6 Configuring IEEE 802.1x Security

- Discusses IEEE 802.1x security.

Chapter 7 Link Aggregation and LACP

- Discusses the differences between Link Aggregation and LACP. It also explains how to configure them.

Chapter 8 Monitoring System Status

- Explains how to monitor system components, including temperature, power, and device archive information.

Chapter 9 OAM

- Explains how to configure Operations, Administrations, and Maintenance (OAM).

Chapter 10 Configuring and Identifying Transceivers

- Explains the compliance, identification, and diagnostics requirements for transceivers. Instructs how to display vendor, diagnostic, and speed information.

Chapter 11 Port State Mirroring

- Explains Port State Mirroring groups and how to configure them.

Chapter 12 Security

- Describes methods for preventing unauthorized access to network resources and services.

Chapter 13 Configuring Broadcast Containment

- Describes how to prevent disruption of services from broadcast storms using broadcast containment.

Chapter 14 Quality of Service

- Describes the features for managing network resources.

Chapter 15 Configuring Multicast Services

- Describes the operation and configuration of multicast services.

Chapter 16 Layer 2 VPNs

- Details the operation and configuration of Virtual Private Networks (VPNs).

Chapter 17 Configuring Connectivity Fault Management

- Describes the configuration of Connectivity Fault Management (CFM) the operation and configuration of Virtual Private Networks (VPNs).

Chapter 18 Configuring L2 Control Frame Tunneling

- Describes configure the treatment of Layer 2 (L2) control frames.

Chapter 19 Configuring TWAMP

- Describes the implementation and configuration of Two-Way Active Measurement Protocol (TWAMP) for bi-directional IP performance testing.

Chapter 20 Configuring MSTP

- Explains the implementation of the Multiple Spanning Tree Protocol (MSTP).

Chapter 21 Event Logging

- Explains how to configure filters for managing system event logs and display log files.

Chapter 22 Configuring SNMP

- Describes the operation and configuration of Simple Network Management Protocol (SNMP) and remote monitoring (RMON) tools.

Chapter 23 Provider Backbone Transport

- Details the implementation of Provider Backbone Transport (PBT) in the core of a Ciena network.

Chapter 24 Link Layer Discovery Protocol

- Provides an overview of the Link Layer Discovery Protocol (LLDP) and describes how to configure 802.1AB LLDP on devices running SAOS.

Chapter 25 System Software Management

- Instructs how to upgrade and downgrade software.

Command Line Interface

- Describes how to access and navigate the CLI and provides an alphabetical lists of global (industry standard) commands and protocol/manager commands.

Service and Support

- Provides contact information for product support.

Glossary

Defines various networking terms.

Document Conventions

This section describes content, style, and usage conventions that outline specific categories of information throughout this manual.

Symbols

Symbols denote text that requires special attention. The information contained alongside a symbol corresponds to one of three levels:



WARNING: This symbol is used to highlight information so the user can avoid personal injury.



CAUTION: This symbol is used to highlight information so the user can avoid equipment damage or data loss.



NOTE: This symbol is used to highlight additional information.

Understanding Command Syntax

A variety of symbols are used to indicate CLI command syntax. These symbols describe how to enter a command. They are not entered as part of the command itself.

Table 1-1, in this chapter summarizes command syntax symbols.

Table 1-1: SAOS Command Syntax Symbols

Symbol	Description
< >	Encloses a variable or literal value that must be specified. Some examples include: <pre>server <IpHost> priority <NUMBER: 1-7> dns <on off> description <String[31]></pre> For <code>server <IpHost></code> , the attribute could be entered as <code>server 10.10.11.100</code> or <code>server www.ciena.com</code> . With <code>priority <NUMBER: 1-7></code> the text within <> indicates that 1 - 7 are valid values. In the example of <code>dns <on off></code> , either the literal value of on or off is valid, such as <code>dns on</code> . For <code>description <String[31]></code> , any string of up to 31 characters is entered.
{ }	Encloses a required value or list of required arguments. One or more values or arguments can be specified. For example, in the syntax: <pre>module create {slot <SlotListAll>} {model <3000-2P10L1 3000-24PLM1>} [description <String [1-32]>]</pre> The slot and module are required. The description is optional.
	Separates mutually exclusive items in a list, only one of which can be entered. For example, in the syntax: <pre>dhcp client options set subnet <on off></pre> either on or off must be specified, for example: <pre>dhcp client options set subnet on</pre>
[]	Encloses an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the syntax: <pre>arp show [interface <Interface>]</pre> you can enter a value for <code>interface <Interface></code> or not for example: <pre>arp show</pre>
{[], [], []}	Specifies a list of optional items where at least one must be specified.
...	Indicates the example has been abbreviated and that the actual display contains more information.
*	Indicates zero or more occurrences of what is preceding.

At a Glance:

- Enabling the Switch
- Configuring the Serial Console Port
- Configuring the Remote Management Interface
- Configuring the Local Management Interface

This chapter provides information on setting up switches so that they can be enabled for configuration over an IP connection.

Enabling the Switch

Switches can be enabled for configuration using either of the following methods:

- Enabling the switch manually
- Enabling the switch using Dynamic Host Configuration Protocol (DHCP)

Enabling the Switch Manually

Follow these steps to enable the switch manually:

1. Ensure that the chassis is properly mounted, grounded, and installed.
2. Power on the switch.
3. Connect a terminal or PC running terminal emulation software to the serial console port using an RJ-45 cable.
4. Configure the connected terminal with the following settings:
 - Character size = 8
 - Parity = None
 - Stop Bit = 1
 - Baud Rate = 9600 bps
 - Control = None
5. Enter the default user name and password:
 - username = su
 - password = wwp
6. The switch is now ready for manual configuration.

Enabling the Switch using DHCP

DHCP is enabled on the remote interface for all devices by default. Devices with a local interface also support DHCP on the local interface. Follow these steps to enable the switch using DHCP:

1. Ensure that the chassis is properly mounted, grounded, and installed.
2. Power on the switch.
3. Connect a terminal or PC running terminal emulation software to the serial console port using an RJ-45 cable.
4. Configure the connected terminal with the following settings:
 - Character size = 8
 - Parity = None
 - Stop Bit = 1
 - Baud Rate = 9600 bps
 - Control = None
5. Enter the default user name and password:
 - username = su
 - password = wwp
6. Enable DHCP using the `dhcp client enable` command.
7. Enter `config save` to complete the process. The switch is now ready for DHCP configuration.

Configuring the Serial Console Port

By default, the serial console port is enabled with the following configuration:

- Parity = None
- Stop Bit = 1
- Baud Rate = 9600 bps
- Flow Control = None

Currently, this configuration cannot be changed, but you can disable, enable, and display the status of the serial console port.

To disable the serial console port:

```
> interface serial-console disable
```

To enable the serial console port:

```
> interface serial-console enable
```

To display the status of the serial console port:

```
> interface serial-console show
+-----serial console-----+
| Parameter                | Value                |
+-----+-----+
| serial login              | enabled              |
+-----+-----+
```

Configuring the Remote Management Interface

The factory default IP address is 0.0.0.0 with subnet 0.0.0.0 for the remote interface. These values will be entered if the system is reset to factory defaults. You can modify the remote management interface, including:

- IP address.
- Subnet mask.
- Management VLAN.
- Gateway.



NOTE: The default priority for the remote management interface defaults to 7, and it is not configurable.



NOTE: The local and remote management interfaces cannot be configured to the same IP subnet.

To modify the remote management interface configuration:

```
interface remote set {[ip <IpAddress>], [subnet <SubnetMask>], [vlan <Vlan>], [gateway <IpAddress>]}
```

To disable the remote management interface:

```
> interface remote disable
```

To enable the remote management interface:

```
> interface remote enable
```

To display the remote management interface configuration:

```
> interface remote show
```

remote				
Parameter	Operational	User	DHCP	
IP Address	172.26.0.26	0.0.0.0	172.26.0.26	
Subnet Mask	255.255.0.0	0.0.0.0	0.0.0.0	
Index	2			
Admin State	Enabled			
Oper State	Enabled			
Broadcast Address	172.26.255.255			
MAC Address	00:02:a1:07:a4:a0			
VLAN	127			
Priority	7			
MTU	1500			

Configuring the Local Management Interface

The local management interface accepts untagged packets only; all tagged packets are dropped. The factory default IP address is 172.16.233.214 with subnet 255.255.255.0 for the local interface. You can configure the local management interface settings via DHCP or directly, including:

- IP address.
- Subnet mask.



NOTE: The CN 3911 does not support the local management interface.



NOTE: The local and remote management interfaces cannot be configured to the same IP subnet.

To modify the local management interface configuration:

```
interface local set {[ip <IpAddress>], [subnet <SubnetMask>]}
```

To disable the local management interface:

```
> interface local disable
```

To enable the local management interface:

```
> interface local enable
```

To display the local management interface configuration:

```
> interface local show
```

local				
Parameter	Operational	User	DHCP	
IP Address	10.10.120.165	172.16.233.214	10.10.120.165	
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	
Index	3			
Admin State	Enabled			
Oper State	Enabled			
Broadcast Address	10.10.120.255			
MAC Address	00:02:a1:07:ef:1e			
VLAN	0			
Priority	0			
MTU	1500			

Chapter Managing Configuration



At a Glance:

- Overview
- Access Levels
- Accessing the CLI
- Managing Configuration Files
- Managing Software License Keys
- Configuring DHCP
- Configuring NTP
- DNS
- SSHv2
- SFTP
- Customizing the System Shell
- Retrieving System Information

This chapter provides explanations for implementing the basic switch set up and describes the various options available to configure it.

Overview

The purpose of this chapter is to present the different tools for managing a Ciena switch. Following these guidelines will help to streamline network operations by installing and managing the device in the network and help to simplify the troubleshooting process.

Access Levels

When a user account is created, it is assigned an access level. The CLI provides three access levels, including:

- **Limited User** (lu) - able to execute commands that do not change the state of the system in a significant way or change the configuration of the device.
- **Super User** (su) - includes all the privileges of the limited user and can make significant system state changes, modify the device configuration, and perform execute commands including creating user accounts.

The CLI provides two default user names/passwords:

User Name	Access Level	Password	Access Rights
su	Super User	wwp	Read/Write
user	Limited User	<empty>	Read-Only

Accessing the CLI

To access CLI commands, a session must first be established with the device by establishing a Telnet session or through direct connection to the serial console port.



NOTE: A maximum of 6 Telnet sessions can be connected at the same time.

Accessing the CLI Using Telnet

To access the device through Telnet, the device must have an IP address, the Telnet client must have a route set up to allow access to the device, and the user must have a valid user name and password to log into the system.

To access the CLI using Telnet:

1. Determine the IP address for the device.
2. Obtain a valid user name and logon password.
3. Configure default gateway setup to access the device.
4. Use a Telnet client to connect to the device.
5. At the logon prompt, enter a user name and then a password to access the prompt, for example:

```
CN 3920 00:02:A1:07:B0:80
SAOS is True Carrier Ethernet TM software.
```

```
CN 3920 login: su
Password:
```

```
SAOS is True Carrier Ethernet TM software.
```

```
Welcome to the shell.
```

Accessing the CLI Using the Serial Console Port

By default, the serial console port is enabled.

1. Connect a terminal or PC running terminal emulation software to the serial console port using an RJ-45 cable.
2. Configure the connected terminal with the following settings:
 - Character size = 8
 - Parity = None
 - Stop Bit = 1
 - Baud Rate = 9600 bps
 - Control = None
3. At the logon prompt, enter a user name and then a password to access the prompt.

Managing Configuration Files

A device can store multiple device configuration files at one time. However, only one configuration file can be active at a time. By default, configuration information is saved to a file called `startup-config`. The `startup-config` file is also the default load file. The parameters defined in `startup-config` are applied when the device reboots (unless an alternate file is specified). The current configurations on a device are not saved to a configuration file unless specifically saved. This includes configuration changes made using the CLI. If a device is rebooted without saving the configuration, all changes will be lost.

In order to permanently save configuration changes, you must save the current device configurations to a configuration file. To save the current configuration, use the `configuration save` command. If you do not specify a file name, the current configuration is written to the default configuration file, `startup-config`. To save configuration to the default configuration file:

```
> configuration save
```

You can use the `configuration save` command to save the current configuration to an alternate file. To save configuration to an alternate file:

```
> configuration save filename <FileName>
```

By saving alternate versions of command files, you can store multiple configuration files for running different configurations of the system. For example, you can save configuration to an alternate file as a backup to restore to a previous configuration or you can store a configuration file for configuring another device of the same family. To activate an alternate command file, use the `configuration reset-to-user-config` command:

```
> configuration reset-to-user-config filename <FileName>
```

You can set alternate configuration files as the default save file so that when a configuration save is performed, the changes will be saved to the alternate configuration file. For example:

```
> configuration set default-save-filename <FileName>
```

When the device is rebooted, it will load the default-load file, which may or may not be the same file. However, when the device is rebooted it will load the `startup-config` file. To set the alternate command file as the default load file:

```
> configuration set default-load-filename <FileName>
```

To display the default save and load files, use the `configuration list` command:

```
> configuration list
```

```
+-----+
|      Configuration Files      |
+-----+
| startup-config                |
| test                          |
+-----+
| Default Save File: test       |
| Default Load File: test       |
+-----+
```

Configuration files are stored in the `/mnt/sysfs/config/` directory. You can delete configuration files from that directory using the `rm` command.

```
> rm /mnt/sysfs/config/<FileName>
```

Configuration File Format

When you save the configuration, each configuration command you have run during the session is written to the configuration file. The commands are saved in different sections based upon the feature and software manager process. You can display the entire configuration file or filter based on the software manager process. Alternately, you can search for a keyword and only display the lines in the configuration containing those keywords.

To display the entire configuration file:

```
> configuration show
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! NETWORK CONFIG:  vlans
!
vlan create vlan 100,200
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! CHASSIS CONFIG:
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! SYSTEM CONFIG:
!
system set host-name MyHostName
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! INTERFACE CONFIG:
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! PORT CONFIG: ports
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! NETWORK CONFIG:  vlan members and attributes
!
vlan remove vlan 127 port 1
vlan remove vlan 127 port 2
vlan remove vlan 127 port 3
vlan remove vlan 127 port 4
vlan remove vlan 127 port 5
vlan remove vlan 127 port 6
vlan remove vlan 127 port 7
vlan remove vlan 127 port 8
!
!
port set port 1 acceptable-frame-type all
port set port 2 acceptable-frame-type all
port set port 3 acceptable-frame-type all
port set port 4 acceptable-frame-type all
port set port 5 acceptable-frame-type all
port set port 6 acceptable-frame-type all
port set port 7 acceptable-frame-type all
port set port 8 acceptable-frame-type all
port set port 10 acceptable-frame-type all
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! PORT STATE GROUP CONFIG:
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! AGING and LEARNING CONFIG:
!
!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! SERVICE ACCESS CONTROL CONFIG:
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! STATIC MAC CONFIG:
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! LLDP CONFIG:
!
!
```

To display sections of the configuration file for a specific keyword:

```
configuration search [file <FileName>] [lines <NUMBER: 0-40>] {string <String [255]>}
```

Example:

```
> configuration search string aging lines 5
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! AGING and LEARNING CONFIG:
!
flow aging set time 1800
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! STATIC MAC CONFIG:
!
!
```

To manually edit a configuration file:

You can transfer a configuration file to a TFTP server, edit it manually, and then transfer it back to the device. When manually editing files, it is recommended that you follow these guidelines:

- Start with a system created configuration file. Creating a configuration file from scratch can cause unexpected results.
- Always use a plain text editor rather than a word processing program.
- Preface lines with an exclamation point (!) to add user comments.
- Do not modify any system generated lines, as it may cause syntax errors. This rule applies even to system generated comments, such as the header information and section delimiters, such as:

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! EXAMPLE MANAGER CONFIG:
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
...
```

These headers are synchronization points for the merge process that occurs upon re-boot. If they are modified, the merge process may fail. Usually, this failure results in a loss of user comments.

- While the system software attempts to preserve all user comments, it is possible for them to be removed during the merge process.

Configuring Telnet

By default, Telnet server is enabled and supports a maximum of 10 simultaneous sessions. You can configure Telnet to allow up to 9 limited users, 9 admin users, and 10 super users to log on simultaneously. By default, the maximum number of simultaneous sessions for limited users is 4, admin users is 4, and super users is 5. You can adjust the number of allowed connections per user to ensure proper management and utilization of the device.

To set the maximum number of simultaneous sessions per user access level:

```
telnet-server set {[max-limited-users <NUMBER:0-9>], [max-super-users <NUMBER:0-10>]}
```

Example:

```
> telnet-server set max-limited-users 3 max-super-users 6
```

To display the configuration and status of active users:

```
> telnet-server show
+----TELNET GLOBAL CONFIGURATION--++
| Parameter          | Value          |
+-----+-----+
| Server              | enable         |
| Max Limited User    | 5              |
| Max Super User      | 5              |
| Max System Logins   | 10             |
+-----+-----+

+-----TELNET GLOBAL STATUS-----+
| Attribute           | Value          |
+-----+-----+
| Active Limited Users | 0              |
| Active Super Users   | 1              |
+-----+-----+
```

To disable Telnet:

```
> telnet-server disable
```

To enable Telnet:

```
> telnet-server enable
```

In addition to the Telnet server, devices support a Telnet client for establishing Telnet connections to other Telnet servers specified by a host name or IP address. Optionally, you can log in with the specified user. If left unspecified, the remote system prompts for the user name. Also, you can specify a TCP port other than the default, 23.

To run the Telnet client:

```
telnet [-l <UserName>] [<IpAddress>] [<port>]
```


Example:

```
> telnet 10.10.121.19
```

```
Entering character mode  
Escape character is '^['.
```

```
3940 00:02:A1:24:0E:30  
SAOS is True Carrier Ethernet TM software.
```

```
3940 login: su  
Password:
```

```
SAOS is True Carrier Ethernet TM software.
```

```
Welcome to the shell.  
> exit
```

```
Goodbye.  
>
```

Managing Software License Keys

A license is a permit to use a premium feature. A license is considered installed or uninstalled based on the presence of one or more license keys. SAOS comes with the base features with no licensing and premium features that require advanced feature licensing. SAOS software supports premium features that require an installed license. A premium feature may consist of a portion of an existing feature, or it may consist of multiple features. Contact your Ciena Sales Rep to obtain advanced feature licensing.

The following software license keys are available:

- PBB-TE (not available on the CN 3911 and CN 3920 platforms)
- Advanced Security
- Advanced Ethernet (AE)
- Advanced OAM (AOAM)

Base features are available with no additional license required, as shown in **Table 3-2**.

A license key is a data object generated by the Ciena license administrator and installed by an operator. A license key is intended to be used in a single module within a specific chassis. License keys are encrypted and contain no human readable information.

When displaying the status of licenses, a premium feature license shows one of the following statuses:

- Not Installed. Also referred to as an invalid license. This means that none of the operationally enabled modules has a key installed for this license.
- Installed. Also referred to as a valid license. This means that all of the operationally enabled modules have a key installed for this license and all conditional requirements (described in separate requirements) for such license installation have been satisfied.
- Partial License. This means that one or more, but not all, operationally enabled modules have a key installed for this license.

Table 3-2 provides a list of features and software license requirements.

Table 3-1: Software License Details

Premium Feature Description	Software License Required
802.1ad Provider Backbone Bridging (not available on the CN 3911 and CN 3920 platforms)	PBB-TE
Broadcast Containment	Advanced Ethernet
Configurable per-port RED Egress Queuing	Advanced Ethernet
Configurable Metering Burst Size	Advanced Ethernet
Configurable L2 Frame Bandwidth Calculation	Advanced Ethernet
EPL Ethernet Private Line and LAN	Advanced Ethernet
EVPL Ethernet Virtual Private Line	Advanced Ethernet
IGMP Groups - max 128 without a license	Advanced Ethernet
Layer-2 Control Frame Tunneling (L2CFT)	Advanced Ethernet
802.1x LACP	Advanced Ethernet
MAC table size - max 4,000 without a license, 16,000 with a license (32000 on the CN 3960)	Advanced Ethernet
Multicast	Advanced Ethernet
Traffic Profiling - Per port QoS with CIR/EIR per Port - Per-port-per-vlan QoS with CIR/EIR per VLAN - Ingress CoS Classification 802.1p/.1D - Ingress CoS Classification IPP, DSCP, Ingress Port ID - L2 Priority mapping from IP DSCP/TOS - IP DSCP/TOS mapping from L2 Priority - Traffic Profile on Port/CVID/CPRI - Named Traffic Profiles	Advanced Ethernet
Non-conforming ARP Discard Mode	Advanced Ethernet
Port State Mirror Groups	Advanced Ethernet
MSTP	Advanced Ethernet
Statistics	Advanced Ethernet
VLAN create/delete (max 500 VLANs without an AE license max 4094 with a license)	Advanced Ethernet
802.3ah EFM (EOAM)	Advanced OAM
CFM	Advanced OAM
NTP Hardware Timestamping	Advanced OAM

Hardware-assisted TWAMP	Advanced OAM
Full TWAMP Responder	Advanced OAM
TWAMP Sender	Advanced OAM
Y.1731	Advanced OAM
SFTP	Advanced Security
SNMPv3	Advanced Security
SSHv2	Advanced Security
TACACS+	Advanced Security

Base Feature Description

DHCP	No license required
DNS	No license required
Dying Gasp	No license required
Eight CoS Queues with Default CoS Mapping	No license required
Full VLAN Range per Port	No license required
Line Rate Switching	No license required
MAC Learning and Aging	No license required
NTP	No license required
RADIUS	No license required
RMON	No license required
Strict Priority Scheduling	No license required

To install a license key:

```
software license install
```

Example:

```
> software license install license-key W1SSH2D3E4FGH5
```

One or more license keys can be stored in a single license file. There is no restriction on the number of keys stored in a license file.

To install license keys from a file:

```
software license install
```

Example:

```
> software license install file license.txt server 172.16.172.100
```

```
WORKING: downloading file remote license.txt local /tmp/temp2
```

To install a license key with the device's XML boot files:

The device will look for the license file tag in the XML file and it will download and process all licenses specified in the license file. A sample XML file is shown below.

```
<XmlWwpCommandFile>
  <XmlCmdPlatformClass name="CN3911"
    version="saos-%VERSION%"
    operation="upgrade"
    serviceAffecting="yes">
  </XmlCmdPlatformClass>
  <XmlCmdPlatformClass name="brego"
    configFilePath="myFolder/my-config-file.txt"
    configFileRule="activate"
    welcomeBanner="myBannerFile.txt"
    licenseFile="myLicenseFile.txt"
    <SshKeyFile name="user1.pk2"></SshKeyFile>
    <SshKeyFile name="user2.pk2"></SshKeyFile>
    <SshKeyFile name="user3.pk2"></SshKeyFile>
    version="saos-%VERSION%"
    packagePath="folder1/folder2/folder3"
    operation="install"
    serviceAffecting="no" >
  </XmlCmdPlatformClass>
</XmlWwpCommandFile>
```

To uninstall a license key:

```
software license uninstall feature-name <String[32]>
```

Example:

```
> software license uninstall security
```

To display the status of licenses:

```
> software license show
```

Configuring DHCP

SAOS supports IETF RFC 2131 Dynamic Host Configuration Protocol (DHCP) client on the active and direct control module interfaces for IP address assignment and other IP configuration through DHCP options. By default, DHCP is enabled on the remote management interface.



NOTE: DHCP can only be enabled on one interface at a given time.

DHCP interfaces to the following protocols and managers

- Software Management
- NTP
- Interface Config
- SYSLOG
- DNS
- ARP

When you enable DHCP on an interface, it creates a query and sends it to the DHCP server to receive IP configuration. If the interface has an assigned IP address, it creates a request query to renew the current IP address and obtain the configured DHCP options. Otherwise, it creates a discover query to obtain an IP address and the configured DHCP options. The server replies with the IP address and any configured DHCP options.

The DHCP client checks to see if the IP address is already in use by sending a gratuitous ARP. If it is in use, it sends a decline and re-starts the discover process. When DHCP is disabled, any configuration set through DHCP options are deleted. The configuration and options applied as a result of DHCP are not saved in the configuration file. A reboot requires a new DHCP transaction with the server.

The DHCP client supports the DHCP options as summarized in **Table 3-2**. A complete list of DHCP options is defined in RFC 1533.

Table 3-2: Supported DHCP Options

Option #	Name	Description
1	subnet	Specifies the subnet mask for the interface. Default is on.
2	time-offset	Specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC). Default is on.
3	router	Specifies a list of IP addresses for routers on the client's subnet (gateways). Routers should be listed in order of preference. Default is on.
6	dns	Specifies a list of five Domain Name System (STD 13, RFC 1035 [8]) name servers available to the client. Servers should be listed in order of preference. Default is on.
7	log-server	Specifies a list of MIT-LCS UDP log servers available to the client. Servers should be listed in order of preference. Used by Syslog. Note that this DHCP option provides no mechanism to configure the UDP port for a syslog server. Any syslog servers configured by DHCP will use the default UDP port for syslog. Default is on.
12	host-name	Specifies the name of the client. The name may or may not be qualified with the local domain name. Default is on.
15	domain-name	Specifies the domain name that the client should use when resolving host names via the Domain Name System (DNS). Default is on.
42	ntp	Specifies a list of IP addresses indicating Network Time Protocol (NTP) [18] servers available to the client. Servers should be listed in order of preference. Default is on.
51	lease-time	Request the lease time for the IP address. The default client lease-time is 1 hour and the default for this option is off.
66	tftp-server	Used to identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options. The TFTP address is only used to retrieve the command file and then is discarded. Default is on. If Option 66 is received in the DHCP reply and the option is On, then that IP address is used for the TFTP server, otherwise the value in 'siaddr' is used.
-1	boot-file	Specifies to use the boot image specified by the DHCP server.

To set DHCP options:

```
dhcp client options set [subnet <on|off>] [time-offset <on|off>] [router <on|off>]  
[dns <on|off>] [log-server <on|off>] [host-name <on|off>] [domain-name <on|off>] [ntp  
<on|off>] [lease-time <on|off>] [tftp-server <on|off>] [boot-file <on|off>]
```

To enable or disable the DHCP client:

```
dhcp client [enable | disable]
```

To renew the leased IP address:

```
dhcp client lease renew
```

To set the interface and discovery interval (1 to 60 seconds):

```
dhcp client set interface {[<remote>], [discovery-interval <NUMBER: 1-60>]}
```

To display the current DHCP configuration:

```
> dhcp client show
```

```
+----- DHCP CLIENT STATE -----+  
| Parameter                               | Value                               |  
+-----+-----+  
| Interface Name                         | tap1                               |  
| Admin State                           | Enabled                           |  
| Oper State                            | Enabled                           |  
| DHCP State                            | Disabled                           |  
| Discovery Interval                     | 30                                |  
| Lease Time (days hh:mm:ss)           | 0:00:00:00                        |  
| Lease Remaining (seconds)             | 0                                  |  
| Renewal (T1) Time (seconds)           | 0                                  |  
| Rebinding (T2) Time (seconds)         | 0                                  |  
| DHCP Server                           | 0.0.0.0                           |  
+-----+-----+  

```

```
+----- DHCP/BOOTP OPTIONS STATE -----+  
| Option | Description                               | State |  
+-----+-----+  
| 1       | Subnet Mask Option                       | On    |  
| 2       | Time Offset Option                      | On    |  
| 3       | Router Option                           | On    |  
| 6       | Domain Name Server Option               | On    |  
| 7       | Log Server Option                       | On    |  
| 12      | Host Name Option                        | On    |  
| 15      | Domain Name Option                      | On    |  
| 42      | Network Time Protocol Servers Option    | On    |  
| 51      | Lease Time Option                       | Off   |  
| 66      | Tftp Server Name Option                 | On    |  
| -1      | Bootfile Name Option                    | On    |  
+-----+-----+  

```


Configuring NTP

With the Network Time Protocol (NTP) client, you can configure a device to automatically synchronize its time and date to a remote NTP server running Coordinated Universal Time (UTC). By default, the NTP client is disabled, and you can manually configure the date and time. When you enable the NTP client, date and time configuration received from an NTP server will override any values manually set on the device. MD5 authentication support allows the NTP client to verify that the server is in fact known and trusted.

In broadcast mode, you do not need to configure the NTP client to use a specific server. Instead, the NTP client waits for broadcast servers on the same subnet to broadcast their current time. When the NTP client receives the first message, it will interact with that server to retrieve reliable time. When additional broadcast messages are received from that server, the NTP client will calculate the time difference and adjust the clock accordingly. If broadcast messages are received from several broadcast servers, the client will select the most accurate server to use.

With polling mode (default), you need to specify the host names or IP addresses of NTP servers along with a time interval to request for date and time information. SAOS supports up to 10 NTP servers and a range between 16 - 4096 seconds for the polling interval with 16 seconds as the default.

As the NTP client communicates with the server, the server status is updated. **Table 3-3** shows the status values you will see when displaying NTP configuration while the NTP client communicates with NTP servers.

Table 3-3: Server Status

Status Displayed	Description
Reject	Rejected or initial state.
Insane	Failed sanity check. Client has yet to be synchronized with the server.
Correct	Passed correctness check. Culled from the end of the candidate list.
Standby	Discarded by the clustering algorithm.
Candidate	Included in the final selection test.
Selected	Selected for synchronization; but distance exceeds maximum.
SysPeer	Selected for synchronization
PPSPeer	Selected for synchronization, PPS signal in use.
Reaching	Communicating with a potential candidate.
ERROR*	Error occurred with communication.

To set the mode to broadcast:

```
> ntp-client set mode broadcast
```



NOTE: When the device is set in broadcast mode, setting a polling-interval will be ignored by the device.

To set the mode to polling and specify a polling interval:

```
ntp-client set mode polling polling-interval <NUMBER: 16,32,64,128,256,512,1024,2048,4096>
```



NOTE: Any number can be entered for the interval value, but the system will round the number down to the nearest allowed value, as shown in the following example.

Example:

```
> ntp-client set polling-interval 1000  
Polling time has been adjusted to 512 seconds
```

To enable the NTP client:

```
> ntp-client enable
```

To disable the NTP client:

```
> ntp-client disable
```

To add an NTP server:

You can add a list of NTP servers directly or with a DHCP server using option 42 as shown in the **Configuring DHCP** section. To add directly:

```
ntp-client add server <IpHost>
```

To remove an NTP server:

```
ntp-client remove server <IpHost>
```

To display NTP state and configured servers:

```
> ntp-client show
```

NTP CLIENT STATE						
Parameter	Value					
Admin State	Enabled					
Mode	Polling					
Polling Interval (sec)	512					
Config State	user					
DHCP NTP Option State	Enabled					

NTP CLIENT SERVER CONFIGURATION						
IP Address	HostName	Config State	Admin State	Oper State	Server Status	
132.236.56.250		user	Enabled	Enabled	SysPeer	
192.83.249.31		user	Enabled	Enabled	Candidate	

To display operational servers:

```
> ntp-client show oper
```

OPER NTP SERVERS		
IP Address	Status	
132.236.56.250	SysPeer	
192.83.249.31	Candidate	

To display NTP state only:

```
> ntp-client show state
```

NTP STATE	
Parameter	Value
Admin State	Enabled
Mode	Polling
Polling Interval (sec)	16
Config State	user
DHCP NTP Option State	Enabled

To display a specific server configuration:

```
> ntp-client show server 132.236.56.250
```

NTP CLIENT SERVER CONFIGURATION	
Parameter	Value
Host Name	
IP Address	172.25.0.2
Admin State	Enabled
Oper State	Enabled
Config State	both
Server Status	SysPeer

Configuring MD5 Authentication

To prevent an unwanted network intruder from masquerading as an NTP server, you can configure authentication for the NTP client. Authentication provides a way for the NTP client to verify that a server is a known and trusted NTP source. The authentication

method supported for the NTP client is RSA Message Digest 5 (MD5) with a private key called keyed-MD5. NTP authentication keys are codes that are encrypted on both the server and client that are used to identify the NTP time server. Each authentication key consists of a key ID and the key itself. MD5 authentication works with both polling and broadcast modes.



NOTE: MD5 authentication is not supported for NTP servers configured with DHCP option 42. When the NTP servers are configured with DHCP, any user configured NTP settings are overridden.

The authentication key number acts as a reference to the specified authentication key. The actual keys must be identical on both the NTP client and the NTP server. The client may use a subset of the authentication keys specified on the NTP server, and the keys are case sensitive.

In polling mode, the NTP client configuration must specify the association of the key number to a server. When configured, the NTP client sends a request for time to the NTP Server with corresponding Key and Authentication code. The NTP server, after validating the client's authentication, replies with an encrypted response along with timestamp information. Upon receipt of the timestamp, the NTP client validates the Server's authentication, if valid, time configuration is updated. Otherwise, the time configuration is rejected.

In broadcast mode, since the server is auto-detected by the client, association of the key number to a server cannot be configured at the client. However, the corresponding key number and key values must be configured at the client. The NTP Server will broadcast timestamp information along with the key number and Authentication code encoded in the packet. Upon receipt of the timestamp, the NTP Client decrypts the key and verifies it against a list of trusted keys. If the key matches one of the list of trusted keys, the NTP Client starts synchronizing with that NTP Server using the same key number and Authentication code as the Server.

Enabling and Disabling MD5 Authentication

By default, MD5 authentication is disabled for the NTP client.

To enable MD5 authentication:

```
ntp-client md5-auth enable
```

Example:

```
> ntp-client md5-auth enable
```

To disable MD5 authentication:

```
ntp-client md5-auth disable
```

Example:

```
> ntp-client md5-auth disable
```

Adding MD5 Keys

You can add up to 32 MD5 keys. The key ID is a U32 value between 1 and 4294967295. If a key ID is entered or displayed as 0, this value implies there is no key. The MD5 key is a 1 to 31 ASCII character string, and cannot be any of the following characters:

- Space ()
- Double quote (")
- Number sign (#)
- TAB (\t)
- Return (\n)
- \0

There are three ways to add a key:

- **Plain text** - Entered directly.
- **Encrypted key** - Enter a key from an MD5 encrypted key generator.
- **Import from a key file** - Transfer a simple tag readable format file to the system and then import keys from it.

When importing from a file, the importing key-file should be in the following format:

<key-id> <type> <encrypted-key-value>

An example key-file that is ready to import is shown below:

```
1 MD5 !ZS,@S~(\D&1k0V'   # MD5 key
2 MD5 yz30$2*>oS(>o2Mf   # MD5 key
3 MD5 T/oI/Hqa!,|NQYgq   # MD5 key
```

Keys imported from a file will be subsequently saved in the config file, when a "configuration save" is executed.

To add an MD5 key in plain text:

```
ntp-client md5-auth add key-id <NUMBER:0-4294967295> md5 <MD5AuthKey>
```

Example:

```
> ntp-client md5-auth add key-id 1 md5 Key1
```

To add an MD5 key in encrypted form:

```
ntp-client md5-auth secret key-id <NUMBER:0-4294967295> md5 <MD5AuthKeyEncrypt>
```

Example:

```
ntp-client md5-auth add key-id 1 md5 3bf313a5
```

To import an MD5 key from a file:

```
ntp-client md5-auth import filename <FileName>
```

Example:

```
> tget 10.25.41.68 ntp_simple_tag.key ntp_simple_tag.key
Received 46 bytes in 0.0 seconds.
Received 2000 bytes/second.
> ntp-client md5-auth import filename ntp_simple_tag.key
```

Removing an MD5 Key

To remove an MD5 key:

```
ntp-client md5-auth remove key-id <NUMBER:1-4294967295>
```

Example:

```
ntp-client md5-auth remove key-id 1
```

Displaying MD5 authentication configuration

To display MD5 configuration:

```
ntp-client md5 show
```

Example:

```
> ntp-client md5-auth show
```

NTP CLIENT STATE	
Parameter	Value
Admin State	Enabled
MD5 Auth Admin State	Disabled
Mode	Polling
Polling Interval (sec)	16
Config State	user
DHCP NTP Option State	Enabled

NTP MD5 AUTH KEYS	
Key ID	MD5 (Encrypted Value)
11	1def01f15eef65
12	1def01f15eef66
266	1def01f15eec6214
267	1def01f15eec6215

NTP SERVER CONFIGURATION						
IP Address/HostName	MD5 Key ID	Config State	Admin State	Oper State	Server Status	
192.83.249.31	0	user	Ena	Ena	Reject	
132.236.56.250	0	user	Ena	Ena	SysPeer	

DNS

The system supports up to three domain name servers that can be prioritized by the administrator. This functionality resolves Hostnames to IP addresses. By default the DNS client is enabled, although no servers are configured.

DNS servers can be configured via DHCP. When both DHCP and the user configure a set of DNS servers, the servers configured by DHCP will be active (operationally enabled), and the other servers will be inactive.

The following IP addresses cannot be specified as DNS servers:

- 0.0.0.0
- 224.0.0.0 -> 255.255.255.255
- 127.0.0.0 -> 127.255.255.255

An error is returned if an IP address is not resolved.

To add a DNS server to the DNS list:

```
> dns-client add server <server ip address>
```

To resolve an IP address or hostname:

```
> dns-client resolve ip ciena.com
Hostname: ciena.com
IP Address: 192.168.75.20
```

To define the default domain name that is appended to unqualified host names:

```
> dns-client set domain-name ciena.com
```

SSHv2

Secure Shell (SSH) provides remote login and SFTP file transfers. Intended as a more secure replacement of Telnet, SSH verifies and grants access to log in requests by encrypting user ID and passwords. It also supports public key based authentication. In public key based authentication, a password is not required, instead a key pair consisting of a private key and a public key is generated, then encrypted and stored on the server. The public key must be distributed to the client machine.



NOTE: To enable SSHv2 commands, the Advanced Security feature license must be installed with the software license install command.

Setting Up SSH Server

To set up SSH with the default configuration:

1. Generate the public/private key pair.

```
>ssh-server key generate
```

This command generates, encrypts, and then stores the public/private key pair as follows:

```
> cd /mnt/sysfs/ssh
> ls
ssh_host_rsa_key
ssh_host_rsa_key.pub
```

SSH user keys can be provisioned using the device's XML file:

```
<XmlWwpCommandFile>
  <XmlCmdPlatformClass name="CN3911"
    version="saos-%VERSION%"
    operation="upgrade"
    serviceAffecting="yes">
  </XmlCmdPlatformClass>
  <XmlCmdPlatformClass name="brego"
    configFilePath="myFolder/my-config-file.txt"
    configFileRule="activate"
    welcomeBanner="myBannerFile.txt"
    licenseFile="myLicenseFile.txt"
    <SshKeyFile name="user1.pk2"></SshKeyFile>
    <SshKeyFile name="user2.pk2"></SshKeyFile>
    <SshKeyFile name="user3.pk2"></SshKeyFile>
    version="saos-%VERSION%"
    packagePath="folder1/folder2/folder3"
    operation="install"
    serviceAffecting="no" >
  </XmlCmdPlatformClass>
</XmlWwpCommandFile>
```

2. Display the current configuration to verify it is correct.

```
>ssh-server-server show
```

3. Enable SSH server.

```
>ssh enable
```

4. Save the configuration.

```
>configuration save
```

Modifying SSH Server

To modify the SSH server settings:

- Add an IP address for each client.

```
>ssh-server add [ client <IpAddress> ]
```

The default configuration allows any IP address to connect. Adding clients restricts access to the IP addresses in the client list.

- Change the maximum number of authentication retries and which port listens for SSH requests.

```
>ssh-server set {[authentication-retries <NUMBER: 1-3>] [listener-port] <NUMBER: 22 - 65535>}]
```

The authentication-retries setting determines how many times the SSH server will prompt for a username and password validation if public key encryption fails. The authentication retry counter is incremented when an authentication method fails, even within the same login cycle. For example, with authentication-retries set to 3, when the SSH client fails to authenticate using an RSA public key, and then a DSA public key, each attempt increments the authentication-retries counter and only one prompt for a username and password occurs for that login cycle.

- Remove any clients from which you do not want to accept a connection.

```
>ssh-server remove [client <IpAddress>]
```

- Disable SSH server.

```
>ssh-server disable
```


Accessing SSH Server

To access SSH Server, you need to install an SSH version 2 client. **Table 3-4** shows a list of tested SSH clients. Other SSH clients may also be compatible but have not been explicitly tested with SAOS.

Table 3-4: Tested SSH Clients

Client	Version	Operating System
Bitvise Tunnelier	Version 4.19	Windows
Esh Client	Version 3.2 for Windows	Windows
JellyfiSSH	Version 4.4	MAC OS X
OpenSSH	4.5	Windows
OpenSSH	OpenSSH_3.9p1, OpenSSL 0.9.7a Feb. 19 2003	RedHat Enterprise Linux
OpenSSH	OpenSSH_4.3p2, OpenSSL 0.9.8b 04 May 2006	Fedora Core 6
Putty SSH	Release .58	Windows
SecureCRT	Version 5.1.4 (build 285) - Official Release - September 14, 2006	Windows
SSH Tectia	Version 5.0.1.79	Windows

Public Key Authentication

Public key authentication relies on copying the public keys (RSA or DSA) of a user on a remote host to the right location on the device (in this case, the CN 3911). The `command.xml` file is used to simplify the process of copying the key files, and the file name can contain a path relative to the TFTP directory of the server.

The 'SshKeyFile' tag in the `command.xml` file can be used to specify the SSH key file for a user. Multiple files can be specified in the `command.xml` file (one for each user), and all of the public keys for a single user need to be in one file. The format for the key file name should be `username.pk2`; for example, the key file name for user `gss` should be `gss.pk2`.

The key file does not have to be present when SSH is enabled, but it should be in place before the user logs in or the system will resort to password based authentication.

The following is a sample command file:

```
<XmlWwpCommandFile>
    ...
    ...
    ...
    ...
    ...
    <SshKeyFile name="gss.pk2"/>
    <SshKeyFile name="su.pk2"/>
    ...
</XmlWwpCommandFile>
```

</XmlWwpCommandFile>

The format of the key files should be as specified in <http://www.openbsd.org/cgi-bin/man.cgi?query=sshd&sektion=8> under the section AUTHORIZED_KEYS FILE FORMAT. The keyfile is stored as /mnt/sysfs/ssh/users/<username>/keyfile.

SFTP

After setting up the SSH server, you can transfer files with an SFTP client. SFTP uses standard file transfer commands, such as get and put for transferring files. SFTP encrypts the user ID, password, and the file and then transfers the information over the SSH server port number.

Table 3-5 shows a list of tested SFTP clients. Other SFTP clients may also be compatible but have not been explicitly tested with SAOS.

Table 3-5: Tested SFTP Clients

Client	Version	Operating System
Bitvise Tunnelier	Version 4.19	Windows
Esh Client	Version 3.2 for Windows	Windows
JellyfiSSH	Version 4.4	MAC OS X
OpenSSH	Version 4.5	Windows
Putty SSH	Release .58	Windows
SecureCRT	Version 5.1.4 (build 285) - Official Release - September 14, 2006	Windows
SSH Tectia	Version 5.0.1.79	Windows

Customizing the System Shell

Configuring the Host Name

The default host name is the model number of the device, such as CN 3940. The host name is displayed in the command prompt. You can set a custom host name to identify the device. The host name length is 2-63 characters without any spaces. At least one character must be alpha (a-z) or a dash (-). IP addresses are not allowed. The host name is not case sensitive. The following special characters are not allowed:

“
%
*
?
!

To set the host name:

```
system set [host-name <String>]
```

Example:

```
>system set host-name myHostName
```

To reset the host name to default:

```
> system unset host-name
```

Setting the Date and Time

If desired, you can manually set the date and time. However, if NTP is enabled, all manual time and date settings will be overridden by the NTP settings. Date and time settings include:

- **Date** - Accepted formats are yyyy-mm-dd, yy-mm-dd, or mm-dd. If the yy-mm-dd format is used the two digits will be added to a base of 2000. For example, 03-01-07 will become 2007-01-01. If you enter a date prior to 01-01-2004, the system will automatically set the date to 01-01-2004 on startup.
- **Time** - Accepted formats are hh:mm:ss or hh:mm.
- **Time offset** - Value range is -2147483648 to 2147483648 seconds from UTC. Positive numbers are east of the UTC; negative numbers are west of the UTC.
- **Timestamp** - Sets the timestamp for system logging entries. When set to 'local,' any system timestamps will use the configured time-offset. When set to 'UTC,' system timestamps will be based on UTC.

To set the date and time:

```
system set [date <yyyy-mm-dd>|<yy-mm-dd>|<mm-dd>] [time <hh:mm:ss>|<hh:mm>] [time-offset  
<NUMBER: -2147483648...2147483648>] [timestamp <local|UTC>
```

Example of setting the date and time:

```
> system set date 2007-06-18 time 09:33
```

Example of setting the time for Pacific Daylight Time (PDT):

```
> system set time 09:33 time-offset -25200
```

Example of setting the time for Pacific Standard Time (PST):

```
> system set time 09:33 time-offset -28800
```

Example of setting the time for Eastern Daylight Time (EDT) USA:

```
> system set time 09:33 time-offset -14400
```

Example of setting the time for Eastern Standard Time (EST) USA:

```
> system set time 09:33 time-offset -18000
```

Ending Inactive Connections

To free up inactive Telnet or SSH connections, you can configure the device to automatically end inactive connections by setting a global inactivity time-out and timer. By default, the time-out is 10 minutes, and the timer is turned off.

To automatically end inactive connections after a period of inactivity:

```
>system shell set [global-inactivity-timeout <NUMBER: 1-1500>] [global-inactivity-timer  
<on|off>]
```

To reset the global inactivity time-out and timer to defaults:

```
>system shell set global-inactivity-timeout global-inactivity-timer
```

Configuring Lines to Display

By default, when you run a command, all lines are displayed and you are returned to a prompt. When the command displays several lines of information, the first lines can scroll beyond the viewable window. You can configure how many lines to display at a time before the system pauses and prompts for an action to display more lines. For example, setting “more” to on and the number of lines to 5 results in:

```
> system shell set more on more-lines 5  
> system ?  
ps                               information about system processes  
set                               set system attributes  
shell                             shell configuration  
show                             show system attributes  
[more 36%] (q,g,space,enter)
```

To configure more lines for all sessions:

```
system shell set global-more <on|off> global-more-lines <NUMBER: 0-999>
```

To reset more lines for all sessions to the defaults:

```
system shell unset global-more global-more-lines
```

To configure more lines for your current session:

```
system shell set more <on|off> more-lines <NUMBER: 0-999>
```

To reset more lines for your current session to the defaults:

```
system shell unset more more-lines
```

Configuring the Welcome Banner

You can create a customized welcome banner in a text file, and set your devices to use the file when Telnet or SSH client sessions are established.

To set the welcome banner:

1. Create a text file with the banner text. For example, the file named myBannerFile.txt has the following text:

```
*****  
*                               *  
*               Welcome        *  
*                               *  
*****
```



NOTE: Be sure each line ends with a carriage return. If a line does not end with a carriage return, it will not display.

2. Transfer the file to the device to the /flash0 directory.

```
> tget xxx.xxx.xx.xx myBannerFile.txt /flash0/myBannerFile.txt
Received 23 bytes in 0.0 seconds.
Received 958 bytes/second.
```

3. Verify the file is stored.

```
> ls
Directory '/flash0/'
config/
archive/
myBannerFile.txt
```

4. To set the device to use your welcome banner:

```
> system shell set welcome-banner-file /flash0/myBannerFile.txt
```

To reset the welcome banner to the defaults:

```
system shell unset welcome-banner-file
```

Retrieving System Information

Displaying System Settings

You can display time and CPU load by default or individual system settings, including

- Date
- Host name
- Load query
- Time
- Time offset
- Up time from last re-boot

To display all system settings:

```
system show [date] [host-name] [load-query] [time-offset] [uptime]
```

Example:

```
> system show date host-name load-query time time-offset uptime
Friday December 31, 1999
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+
| Oper | CN 3940 |
| User | CN 3940 |
| DHCP |         |
+-----+-----+-----+-----+-----+-----+-----+-----+
|
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+
| Interval | Load (%) |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Last 15 minutes | 9 |
| Last 5 minutes | 5 |
| Last 1 minute | 8 |
+-----+-----+-----+-----+-----+-----+-----+-----+
|
```

```
MemTotal:      60664 kB
MemFree:       3420 kB
```

```
+----- Global Service Mode -----+
| Service Mode      | None                |
+-----+-----+
+----- TIME Settings -----+
| Parameter          | Value               |
+-----+-----+
| Local date and time | Fri Dec 31 17:38:42 1999 |
| Greenwich Mean Time (GMT) | Sat Jan 01 00:38:42 2000 |
| Time Offset (seconds east) | -25200              |
+-----+-----+
```

```
+----- TIME OFFSET (sec) -----+
| Operational | User      | DHCP      |
+-----+-----+
| -25200      | -25200    | 0         |
+-----+-----+
```

System uptime: 0d 5h 37m 59s

Displaying the System Shell Attributes

To display the system shell attributes:

system shell show

Example:

```
> system shell show
+----- Shell Settings -----+
| Parameter          | Value               |
+-----+-----+
| Global more         | on                  |
| Global more lines   | 0                   |
| Global inactivity timer | off                 |
| Global inactivity timeout | 10 min              |
| Global login timer   | on                  |
| Global login timeout | 60 sec              |
| Session more        | on                  |
| Session more lines   | 0                   |
| Welcome banner file  | (none)              |
+-----+-----+
```

Displaying System Processes

To display system process information:

system ps show [blockId <String>] [format <wide>]

Example of all processes:

```
> system ps show
PID USER      VSZ STAT COMMAND
  1 root        3808 S   init
  2 root         0 SWN  [ksoftirqd/0]
  3 root         0 SW<  [events/0]
  4 root         0 SW<  [khelper]
  5 root         0 SW<  [kthread]
  6 root         0 SW<  [kblockd/0]
 27 root         0 SW   [pdflush]
 28 root         0 SW   [pdflush]
 30 root         0 SW<  [aio/0]
 29 root         0 SW   [kswapd0]
546 root         0 SW<  [kseriod]
553 root         0 SW   [mtdblockd]
583 root         0 SWN  [jffs2_gcd_mtd5]
664 root       1900 S   /sbin/monitor -t /tmp/fifo/mon/saos /sbin/start-saos
669 root       1900 S   /sbin/monitor -p -t /tmp/fifo/mon/saos.loader /mnt/ap
670 root       4112 S   /usr/sbin/inetd -f
671 su        20428 S   -saos
672 root       3872 S   /bin/sh /sbin/corewatch.sh
892 root      36968 S   /mnt/apps/bin/saos -s
1223 root       3876 S   telnetd -i
1224 su        20428 S   -saos
1436 root       3876 S   telnetd -i
1437 su        20428 S   -saos
1810 root       3676 S   sleep 15
1811 su        3808 S   /bin/sh -l -c ps
1830 su        4176 R   ps
```

Generating a System State Dump File

For troubleshooting purposes, you can generate a system state dump file to a TFTP server. The state dump file contains configuration and status information for major device components all in one file, including:

- System configuration
- Interface configuration
- Chassis device identification, device archives, and power supplies
- Module configuration, temperature, CPU load, and POST
- Port configuration and status
- System process information
- Configuration file
- Log files

To generate a system state dump file:

```
system state-dump tftp-server <IpAddress> file-name <FileName>
```

Example:

```
> system state-dump tftp-server 192.168.75.100 file-name StateDump.txt
Writing system info
Writing interface info
Writing chassis info
Writing module info
Writing port info
Writing device ID info
Writing fan info
Writing power info
Writing archive info
Writing alarm info
Writing system config
Writing log files
File StateDump.txt transferred to tftp server 192.168.75.100
```


Chapter VLAN Management

4

At a Glance:

- Overview
- VLANs and Traffic Flow
- Behavior Summary
- VLAN/Port Configuration
- Port Mirroring
- Port Loopback
- Port Statistics

This chapter details the function of VLANs. It also details how to configure port settings to switch traffic properly through the network.

Overview

Virtual Local Area Networks (VLANs) are a key element within the system software. A VLAN is used to group resources that have a common set of requirements, regardless of where they are located physically. They also allow ports on a device to be grouped in order to limit the distribution of unicast, multicast, and broadcast traffic. For example, flooded traffic originating from a particular VLAN can be limited to only other ports belonging to that VLAN. VLANs allow traffic on the same physical connection to be divided into separate services. These services can then be further divided into groups within each service.

VLANs and Traffic Flow

VLANs determine how traffic is forwarded within a device. The ingress and egress behavior of each port must be taken into account. Five basic rules govern traffic forwarded through the device:

- Port VLAN Membership
- Acceptable Frame Types (ingress rule)
- Port VLAN ID (PVID) (ingress rule)
- Ingress Filtering (ingress rule)
- Ingress Untagged Frames (ingress rule)
- Egress Untagged VLAN (egress rule)

Acceptable Frame Types

When a frame arrives at a port on a device with SAOS operating system, it is first examined to determine whether it is a tagged (contains a VLAN ID) or untagged frame. This is referred to as the frame type. Each port of the device has an associated Acceptable Frame Types (AFT) parameter that controls whether or not the port will accept untagged frames. A port can be configured to admit ONLY tagged frames or to admit ALL Frames.

The default value of the Acceptable Frame Types parameter is set to "VLAN tagged-only" on ports 9 and 10. In other words, by default, tagged frames are allowed to ingress while untagged or priority-tagged frames (i.e., a frame with no tag header, or a frame with a tag header that carries the null VLAN ID) received on the port are discarded. Tagged frames are then further processed according to the additional ingress rules set on the port. In contrast, if the Acceptable Frame Types parameter is set to "all", which is the default for ports 1-8, all frames are allowed to ingress, regardless of their tag status.

Port VLAN ID

The full VLAN address range from 1 to 4094 can be supported per port. For untagged or priority-tagged frames, the next ingress rule applied is the Port VLAN ID (PVID). Each port on the device has an associated PVID. By default, the PVID value is the default VLAN ID (VLAN 1). When an untagged frame arrives at an ingress port (assuming that the port is set to accept all frame types) it may be forwarded to all ports that are members of the configured PVID (depending on additional ingress parameters set on the device). If an ingress frame is not tagged with the VLAN specified by the port's PVID, then the setting on the port's Ingress Filter will apply.

Similarly, if a port is removed from a VLAN that is also its PVID, the PVID value remains the same and the port's Ingress Filter setting is therefore applied (refer to the **VLAN Ingress Filter** section).

The PVID assignment for aggregated ports is slightly different. When a physical port is added to an aggregation, it inherits the PVID setting of the aggregation group. However, when the port is removed from the aggregation, its own PVID setting becomes valid again.



NOTE: PVIDs can only be set to the VLAN ID of configured VLANs, therefore the VLAN must exist before the corresponding PVID can be assigned. The port does not however, have to be a member of the VLAN in order to assign the PVID.

VLAN Ingress Filter

The last parameter applied to ingress frames is the VLAN Ingress Filter. The VLAN Ingress Filter forwards or discards a frame based on the VLAN tag. When VLAN Ingress Filtering is enabled on a port (VLAN Ingress Filtering is enabled by default), an ingress frame that is tagged with a VLAN to which the ingress port does not belong, will be discarded. For example, assuming that VLAN 200 is configured on the device, if the ingress frame is tagged with VLAN 200, but the port is not a member of VLAN 200, the frame is discarded.

If VLAN Ingress Filtering is disabled, ports do not consider the VLAN membership of ingress frames. In the above example, with VLAN Ingress Filtering disabled, the frame tagged with VLAN 200 may be forwarded to all port members of VLAN 200, regardless of whether the ingress port belongs to VLAN 200. However, if VLAN 200 has not been configured on the device, the frame is then dropped.

Ingress Untagged Frames

When you have a port set to accept all frame types, untagged data frames and untagged control frames are allowed to ingress.

You can configure a port's untagged-data-vid attribute to add (push) a tag containing a Customer VLAN ID (CVID) on untagged data frames on ingress. In addition to the CVID, the tag will include the port's ingress fixed .1d priority (ingress-fixed-dot1dpri) setting.

Egress Untagged VLAN

Once a frame reaches its egress port on the device, one final VLAN operation is performed. The Egress Untagged VLAN (EUV) parameter determines whether the egressing frame will be forwarded tagged or untagged. As a frame egresses the device, its VLAN ID is compared to the EUV. If the VLAN ID is the same as the EUV, then the VLAN tag is stripped from the egressing frame and it is sent untagged. If the VLAN ID is not the same as the port's EUV, then the frame is sent out with its tag intact. By default, the EUV is VLAN 1, as is the PVID. When the PVID is changed, the EUV value automatically updates to match the PVID, until it is explicitly set.

For example, the default PVID and EUV are set to 1. If you set port's PVID to VLAN 200, and the EUV is automatically set to VLAN 200. A frame that is tagged with VLAN 200 would have its tag stripped as it egresses. In contrast a frame with a VLAN tag of 300 will egress with its tag intact.

However, if you set the EUV to 300, the PVID remains at 200. Now, the frame tagged with VLAN 200 retains its tag on egress, and the frame with a VLAN tag of 300 has its tag removed.

Behavior Summary

The following tables summarize packet behavior.

Table 4-1: Ingress Behavior

Ingress Frame	AFT	PVID	Ingress Filter	Behavior
Tagged	Tagged-only	N/A	Disabled	The frame is forwarded if the VLAN exists on the device.
Tagged	Tagged-only	N/A	Enabled	The frame is forwarded if the ingress port is a member of the ingressing frame's VLAN.
Tagged	All	N/A	Disabled	The frame is forwarded if the VLAN exists on the device.
Tagged	All	N/A	Enabled	The frame is forwarded if the ingress port is a member of the ingressing frame's VLAN.
Untagged	Tagged-only	N/A	N/A	The frame is dropped.
Untagged	All	Any	Disabled	The frame is forwarded to all ports that are members of the ingressing port's PVID.
Untagged	All	Any	Enabled	The frame is forwarded to PVID members only if the ingress port is a member of the PVID.

Table 4-2: Egress Behavior

Frame State	EUV State	Egress Behavior
Tagged	VLAN ID = EUV	Frame sent untagged.
Tagged	VLAN ID ≠ EUV	Frame sent tagged.

VLAN/Port Configuration

All of the frame forwarding behaviors discussed in this chapter are port-based features, but require VLANs to tie them together. The VLAN can be thought of as an imaginary wire that connects the ingress port to the egress port(s). VLANs must be created using the CLI, MIB, or the Device Manager, prior to configuring other features on the device. A VLAN is identified by 2 basic parameters:

- **VLAN ID:** value used to identify the VLAN
- **VLAN Name:** (optional) defined by the network operator. VLAN names may not begin with a number



NOTE: A maximum of 500 VLANs are supported without an Advanced Ethernet (AE) license, and up to 4094 VLANs with an AE license.

All commands in the following sections (except “show” commands) require the user to have super user or admin access level. Refer to the **Access Levels** section in Appendix 26, on page 377 for information on CLI access privileges.

To create a VLAN and add port members to it:

Step #	Description	Command
Step 1	Create the VLAN. The VLAN ID (VID) must be specified, but the name is optional. If a VLAN name is not specified, a default name will be assigned in the format of VLAN#<VLAN-id>. For example if the VID entered is 1000 the VLAN name will be VLAN#1000. VLAN names may not begin with a number.	<code>vlan create vlan <VlanIdList> [name <String[31]>]</code>
Step 2	Add ports to the VLAN. Ports can be added to the VLAN either by specifying the VLAN name or VID and a port name.	<code>vlan add vlan <VlanList> port <PortNameList></code>
Step 3	(Optional) Verify the creation of the VLAN. <code>vlan show</code> lists all configured VLANs. <code>vlan show port <PortNameList></code> displays the VLANs to which the specified ports belong. <code>vlan show vlan <VlanList></code> displays information for a specific VLAN.	<code>vlan show [port <PortNameList> vlan <VlanList>]</code>

Example:

1. > vlan create vlan 300
2. > vlan add vlan 300 port 5

3. > vlan show vlan 300

VLAN INFO		
Parameter		Value
VLAN ID		300
Name		VLAN#300
Features		
VLAN Members		
Port	VTag	VS-Sub
5	300	False

Port Configuration

The following examples show how to configure a VLAN/port pair to receive traffic in one state and egress it in a particular state (e.g., receive untagged traffic and egress tagged traffic).

Ingress Tagged Traffic, Egressing Tagged

This scenario is basically the default behavior for the device. The only requirement is to add the ingress and egress ports to the same VLAN. Since the EUV and the PVID are set to VLAN 1 by default, tagged frames will enter the switch and egress the switch with their original tag intact for the VLAN configured.



NOTE: By default, all ports are members of VLAN 1. Frames tagged with VLAN 1 will also be forwarded since the PVID is set to VLAN 1 by default and is not changed in this example.

To configure a port pair that will receive frames tagged with VLAN 300 and egress them with the original tag intact, the following steps are used:

Step #	Description	Command
Step 1	Create the VLAN.	<code>vlan create vlan <VlanList> [name <VlanList>]</code>
Step 2	Add the ingress and egress ports to the VLAN.	<code>vlan add vlan <VlanList> port <PortNameList> [tag {<value> none}]</code>
Step 3	(Optional) Verify the creation of the VLAN.	<code>vlan show [port <PortNameList> vlan <VlanList>]</code>

Example:

1. > vlan create vlan 300
2. > vlan add vlan 300 port 1,5

3. > vlan show vlan 300

VLAN INFO		
Parameter	Value	
VLAN ID	300	
Name	VLAN#300	
Features		
VLAN Members		
Port	VTag	VS-Sub
1	300	False
5	300	False

Ingress Untagged Traffic, Egressing Untagged

This scenario configures a port pair on VLAN 300 that will receive untagged frames and egress them untagged:

Step #	Description	Command
Step 1	Create the VLAN.	<code>vlan create vlan <VlanList> [name <VlanList>]</code>
Step 2	Add the ingress and egress ports to the VLAN.	<code>vlan add vlan <VlanList> port <PortNameList> [tag {<value> none}]</code>
Step 3	Set the AFT on all ports to All. On ports 1-8, this value is the default setting.	<code>port set port <PortNameList> [acceptable-frame-type '<all>' '<tagged-only>']</code>
Step 4	Set the PVID on all ports to the VLAN used in Step 2.	<code>port set port <PortNameList> [pvid <VlanList>]</code>
Step 5	(Optional) Verify the ingress port settings. Note that the egress untagged VLAN automatically changes to the same value as the PVID.	<code>port show port <PortNameList></code>
Step 6	(Optional) Verify the egress port settings. Note that the egress untagged VLAN automatically changes to the same value as the PVID.	<code>port show port <PortNameList></code>

Example:

1. > vlan create vlan 300
2. > vlan add vlan 300 port 1,5
3. > port set port 1,5 acceptable-frame-type all
4. > port set port 1,5 pvid 300

5. > port show port 1

PORT INFO		
Field	Admin	Oper
Type	10/100/G	
Description		
Spanning Tree State	Forwarding	
MAC Address	00:02:a1:07:86:e2	
Phy Loopback	Off	
Link State	Enabled	Enabled
State Group Link State		
Mode	rj45	unknown
Speed	1 Gbps	100 Mbps
Duplex	full	full
Flow Control	off	
Auto Negotiation	Enabled	
Flow Control Advertised	off	
PVID	300	300
Untag Ingress Vtag	1	1
Untag Ingress Data Vid	0	0
Fixed Resolved CoS	0	0
Ingress VLAN Filter	Enabled	Enabled
Ingress VS Filter	Off	Off
Acceptable Frame Type	all	all
Egress Untag VLAN	300	300
Max Frame Size	1526	1526
Untagged Data VS		
Untagged Ctrl VS		
Resolved CoS Policy	dot1d-tag1-cos	dot1d-tag1-cos
Service Port Type	Subscriber	Subscriber
Eth VC EtherType	8100	8100
Eth VC EtherType Policy	all	all
Mirror-port	Off	Off
Ingress-mirror		
Egress-mirror		
Ingress to Egress QMap	Default-RCOS	Default-RCOS
XCVR caps mismatch	<NONE>	
VLAN Membership	300	

6. > port show port 5

Changing Tag Status

In this port pair scenario, traffic for the specified VLAN enters one port untagged and egresses its partner port tagged with a specified VLAN ID. When traffic flows in the opposite direction, frames tagged with the specified VLAN will egress untagged.

In our example, untagged frames ingressing on port 1 will egress port 5 tagged with a VLAN ID of 300. Frames that ingress on port 5 with a VLAN tag of 300 will egress port 1 untagged.

Assume now that port 1 is connected to the subscriber while port 5 connects to the provider network, the frame will pass between the subscriber and the provider networks, but the VLAN tag of 300, which may only have meaning in the provider network, will never be seen in the customer's network.

Step #	Description	Command
Step 1	Create a VLAN.	<code>vlan create vlan <VlanList> [name <VlanList>]</code>
Step 2	Add the ingress and egress ports to the VLAN.	<code>vlan add vlan <VlanList> port <PortNameList></code>
Step 3	Set the PVID on the ingress ports to the VLAN used in Step 2.	<code>port set port <PortNameList> [pvid <VlanList>]</code>
Step 4	Set the AFT on all ports to All. On ports 1-8, this value is the default setting.	<code>port set port <PortNameList> [acceptable-frame-type <'all' 'tagged-only'>]</code>
Step 5	(Optional) Verify the ingress port settings.	<code>port show port <PortNameList></code>
Step 6	Set the EUV on the egress port (provider port) to a VLAN that is different than the VLAN used in Step 2. Note that the value used does not have to correspond to an existing VLAN.	<code>port set port <PortNameList> [egress-untag-vlan <VlanList>]</code>
Step 7	(Optional) Verify the egress port settings.	<code>port show port <PortNameList></code>

Example:

1. `> vlan create vlan 300`
2. `> vlan add vlan 300 port 1,5`
3. `> port set port 1,5 acceptable-frame-type all`
4. `> port set port 1 pvid 300`
5. `> port show port 1`
6. `> port set port 5 egress-untag-vlan 4094`

7. > port show port 5

PORT INFO		
Field	Admin	Oper
Type	10/100/G	
Description		
Spanning Tree State	Forwarding	
MAC Address	00:02:a1:07:86:e2	
Phy Loopback	Off	
Link State	Enabled	Enabled
State Group Link State		
Mode	rj45	unknown
Speed	1 Gbps	100 Mbps
Duplex	full	full
Flow Control	off	
Auto Negotiation	Enabled	
Flow Control Advertised	off	
PVID	300	300
Untag Ingress Vtag	1	1
Untag Ingress Data Vid	0	0
Fixed Resolved CoS	0	0
Ingress VLAN Filter	Enabled	Enabled
Ingress VS Filter	Off	Off
Acceptable Frame Type	all	all
Egress Untag VLAN	4094	4094
Max Frame Size	1526	1526
Untagged Data VS		
Untagged Ctrl VS		
Resolved CoS Policy	dot1d-tag1-cos	dot1d-tag1-cos
Service Port Type	Subscriber	Subscriber
Eth VC EtherType	8100	8100
Eth VC EtherType Policy	all	all
Mirror-port	Off	Off
Ingress-mirror		
Egress-mirror		
Ingress to Egress QMap	Default-RCOS	Default-RCOS
XCVR caps mismatch	<NONE>	
VLAN Membership	300	

Pushing a VID Tag on Untagged Data Frames

When you have the port set to accept all frame types, untagged data frames are allowed to ingress. You can configure the ingress port to add (push) a tag on the frame containing the specified Customer VLAN ID (CVID) and the ingress fixed .1d priority for untagged data frames on ingress. After processing, the header is removed leaving the CVID intact. The CVID tag is automatically removed (popped) on egress.

Step #	Description	Command
Step 1	Create a VLAN.	vlan create vlan <VlanList> [name <VlanList>]
Step 2	Add the ingress and egress ports to the VLAN.	vlan add vlan <VlanList> port <PortNameList> [tag {<value> none}]

Step #	Description	Command
Step 3	Set the ingress untagged data VID on the ingress port. Note that the value used does not have to correspond to an existing VLAN.	port set port <PortNameList> untagged- data-vid <VlanId>
Step 4	Set the AFT on all ports to All. On ports 1-8, this value is the default setting.	port set port <PortNameList> [acceptable-frame-type <'all' 'tagged-only'>]
Step 5	(Optional) Set the ingress fixed .1d priority on the ingress port.	port set port <PortNameList> ingress- fixed-dot1dpri <NUMBER: 0- 7>
Step 6	(Optional) Verify the port settings.	port show port <PortNameList>

Example:

1. > vlan create vlan 4000
2. > vlan add vlan 4000 port 1,5
3. > port set port 1 untagged-data-vid 100
4. > port set port 1,5 acceptable-frame-type all
5. > port set port 1 ingress-fixed-dot1dpri 4
6. > port show port 1

Hybrid Traffic

This scenario configures a port pair that will receive either tagged or untagged frames. Tagged frames will egress with their original tag intact and untagged frames will egress untagged.

In this example, any traffic tagged with VLAN 300 will enter the switch tagged and leave the switch still tagged with VLAN 300, while untagged traffic will enter untagged and leave untagged. The follow commands are used for this scenario:

Step #	Description	Command
Step 1	Create a VLAN.	vlan create vlan <VlanList> [name <VlanList>]
Step 2	Add the ingress and egress ports to the VLAN.	vlan add vlan <VlanList> port <PortNameList> [tag {<value> none}]
Step 3	Set the AFT on the ingress ports to All. On ports 1-8, this value is the default.	port set port <PortNameList> [acceptable-frame-type <'all' 'tagged-only'>]
Step 4	Set the PVID on the ingress ports to VLAN 1 (this is the default setting).	port set port <PortNameList> [pvid <VlanList>]

Step #	Description	Command
Step 5	Set the EUV on the egress ports to VLAN 1 (this is the default setting).	port set port <PortNameList> [egress- untag-vlan <VlanList>]
Step 6	(Optional) Verify the ingress port settings.	port show port <PortNameList>
Step 7	(Optional) Verify the egress port settings.	port show port <PortNameList>

Example:

1. > vlan create vlan 300
2. > vlan add vlan 300 port 1,5
3. > port set port 1,5 acceptable-frame-type all
4. > port set port 1 pvid 1
5. > port set port 5 egress-untag-vlan 1
6. > port show port 1
7. > port show port 5

Tagged Ethernet Port Emulation

In this example, the standard behavior of a tagged Ethernet port is emulated. Standard tagged Ethernet ports will accept tagged frames and drop all untagged frames.

In the following example, VLAN filtering is disabled, allowing all tagged frames to ingress if the VLAN they are tagged with has been configured on the device. Frames that are tagged with a VLAN ID of 300 will egress untagged. To drop frames that are tagged with a VLAN to which the ingress port does not belong, do not disable VLAN Ingress Filtering.

Step #	Description	Command
Step 1	Create a VLAN.	vlan create vlan <VlanList> [name <VlanList>]
Step 2	Add the ingress and egress ports to the VLAN.	vlan add vlan <VlanList> port <PortNameList> [tag {<value> none}]
Step 3	Set the AFT on the ports to Tagged-Only (Tagged-Only is the default setting for ports 9 and 10).	port set port <PortNameList> [acceptable-frame-type <'all' 'tagged-only'>]
Step 4	Disable Ingress VLAN Filtering on the ports. VLAN Ingress Filtering should only be disabled if the ingress port is not a member of the tagged frame's VLAN.	port set <PortNameList> [vlan-ingress-filter <'on' 'off'>]
Step 5	Set the EUV on the ports to the VLAN used in Step 2.	port set port <PortNameList> [egress- untag-vlan <VlanList>]
Step 6	(Optional) Verify the ingress port settings.	port show port <PortNameList>

Step #	Description	Command
Step 7	(Optional) Verify the egress port settings.	port show port <PortNameList>

CLI Example:

1. > vlan create vlan 300
2. > vlan add vlan 300 port 1,5
3. > port set port 1,5 acceptable-frame-type tagged-only
4. > port set port 1,5 vlan-ingress-filter off
5. > port set port 1,5 egress-untag-vlan 300
6. > port show port 1
7. > port show port 5

Port Mirroring

To monitor ingress and egress traffic, you can configure another port to “mirror” the traffic of a specified port, or define up to 5 port state mirror groups (PSMGs). By attaching a protocol analyzer to the port, you can monitor and analyze traffic. Port mirroring actions can only be configured on physical ports.

Monitoring traffic on a port is a two-step process. First, port mirroring must be enabled on the port that is to be the mirror port. Next, direct the input traffic, output traffic, or both to the mirror port (the port to which the analyzer is attached).

Any port can be designated as a mirror port, but only one mirror port can be assigned at a time. However, the ingress/egress traffic from multiple ports can be mapped to a single mirror port. Port mirroring configuration persists after a reboot if the device configuration has been saved.

Each PSMG has a source port group and a list of destination ports. A port can be added to a PSMG in either the source group or destination port list. A port can only be a member of one PSMG at a time.

It should be noted that a port defined as a mirror port will continue to transmit/receive normally based on its configuration, such as its VLAN membership. It may be beneficial to manually remove all configuration on the mirror port and place it in a designated mirror VLAN to isolate the desired traffic.

The following example configures a mirror port to analyze the ingress and egress traffic from port 6 using port 3 as the mirror port.

To configure port mirroring, the following steps are used:

Step #	Description	Command
Step 1	Enable port mirroring on port 3.	port set port <PortNameList> mirror- port on
Step 2	Configure port 6 to mirror its Ingress and Egress traffic to port 3.	port set port <PortNameList> ingress- mirror <PortName> egress- mirror <PortName>

Step #	Description	Command
Step 3	Display the configuration for port 3 (optional).	port show port <PortNameList> [capabilities] [statistics]
Step 4	Display the configuration for port 6 (optional).	port show port <PortNameList>

CLI Example:

1. > port set port 3 mirror-port on
2. > port set port 6 ingress-mirror 3 egress-mirror 3
3. > port show port 3
4. > port show port 6

Port Loopback

External loopback is supported where data that is received on a port in loopback mode will egress the same port, and the loopback occurs in the PHY.

Loopback can be enabled on any physical port independently, regardless of VLAN membership. Setting the loopback attribute automatically sets the port's learn limit to 0, with an action of 'forward'. When the loopback setting is 'off', the configured learn limit is then re-applied.



NOTE: If more than two ports within the same VLAN are configured to participate in a loopback test, there is a danger of creating a broadcast storm.

CLI Example:

The following example starts a loopback on port 5.

1. Enable loopback on port 5.

```
port set port 5 loopback on
```

2. Stop the loopback test.

```
port set port 5 loopback off
```

Port Statistics

The system software tracks statistics per port including:

- **RxBytes** - Number of bytes received in good and bad packets including Frame Check Sequence (FCS) bytes and excluding framing bits.
- **RxPkts** - Number of packets received, including good and bad.
- **RxCrcErrorPkts** - Number of packets received with CRC errors.
- **RxMcastPkts** - Number of good multicast packets received.
- **RxBcastPkts** - Number of good broadcast packets received.

- **UndersizePkts** - Number of packets received that were less than 64 bytes long (excluding framing bits, but including Frame Check Sequence (FCS) bytes) and were otherwise well formed.
- **OversizePkts** - Number of packets received that were longer than 1518 bytes (excluding framing bits, but including FCS bytes) and were otherwise well formed.
- **FragmentsPkts** - Number of packets received that were less than 64 bytes in length (excluding framing bits but including FCS bytes) and had either a bad FCS with an integral number of bytes (FCS Error) or a bad FCS with a non-integral number of bytes (Alignment Error).
- **JabbersPkts** - Number of packets received that were longer than 1518 bytes (excluding framing bits, but including FCS bytes), and had either a bad FCS with an integral number of bytes (FCS Error) or a bad FCS with a non-integral number of bytes (Alignment Error).
- **RxPausePkts** - Number of received pause packets.
- **64OctsPkts** - Number of packets (including bad packets) received that were 64 bytes in length (excluding framing bits but including FCS bytes).
- **65To127OctsPkts** - Number of packets (including bad packets) received that were between 65 and 127 bytes in length inclusive (excluding framing bits but including FCS bytes).
- **128To255OctsPkts** - Number of packets (including bad packets) received that were between 128 and 255 bytes in length inclusive (excluding framing bits but including FCS bytes).
- **256To511OctsPkts** - Number of packets (including bad packets) received that were between 256 and 511 bytes in length inclusive (excluding framing bits but including FCS bytes).
- **512To1023OctsPkts** - Number of packets (including bad packets) received that were between 512 and 1023 bytes in length inclusive (excluding framing bits but including FCS bytes).
- **1024To1518OctsPkts** - Number of packets (including bad packets) received that were between 1024 and 1518 bytes in length inclusive (excluding framing bits but including FCS bytes).
- **TxBytes** - Number of transmitted bytes in good and bad packets including FCS bytes and excluding frame bits.
- **TxPkts** - Number of packets transmitted including good and bad.
- **TxExDeferPkts** - Number of transmitted excessive defer packets.
- **TxGiantPkts** - Number of well formed packets longer than 1518 bytes including FCS bytes and excluding framing bits.
- **TxUnderRunPkts** - Number of transmitted underrun packets.
- **TxCrcErrorPkts** - Number of transmitted packets with CRC errors.
- **TxLCheckErrorPkts** - Number of transmitted length check packets.
- **TxLOutOfRangePkts** - Number of transmitted length out of range packets.
- **TxLateCollPkts** - Number of transmitted late collision packets.
- **TxExCollPkts** - Number of transmitted excessive collision packets.
- **TxSingleCollPkts** - Number of transmitted single collision packets.
- **TxCollPkts** - Number of transmitted collision packets.
- **TxPausePkts** - Number of transmitted pause packets.
- **TxMcastPkts** - Number of good multicast packets transmitted.
- **TxBcastPkts** - Number of good broadcast packets transmitted.

Displaying Port Statistics

Two sets of statistics are stored: the Total statistics, the values since the last boot up, and the Current statistics, the values since the last statistics clear. The system also calculates throughput values to show current statistics in terms of rate.

You can display a summary of current, total, and current throughput statistics for all or specific ports. Optionally, you can control the output to display:

- **Active** - only non-zero values.
- **Delay** - to specify a length of time in seconds to display the statistics.
- **Count** - number of times to repeat the display.
- **Scale** - specifies the units (Giga, Mega, Kilo, or None) in which to display the values. For throughput statistics, the default scale is Mega.
- **Type** - Filters type of statistics: basic (only received and transmitted packets and bytes), tx-only (transmitted only), rx-only (received only), errors or all.

To display a summary of port statistics for all ports:

```
port show statistics|total-statistics|throughput [active] [delay <NUMBER: 1-86400>] [count <NUMBER: 0-4294967295>] [scale <tera|giga|mega|kilo|none>]
```

Examples of all active port statistics summary:

```
> port show statistics active
```

PORT STATISTICS SUMMARY					
Port	Byte		Pkt		
	Tx	Rx	Tx	Rx	
1	8326248088	0	67147162	0	
2	8326247964	0	67147161	0	
12	0	28879569152	0	225621634	

Example of all active port total statistics summary:

```
> port show total-statistics active
```

PORT TOTAL STATISTICS SUMMARY					
Port	Byte		Pkt		
	Tx	Rx	Tx	Rx	
1	169713065596	1053155263708	325536280	1372943892	
2	21452132866	19878912	77950273	310608	
12	885114437038	193572376072	1147664620	490131140	

Example of all active port throughput statistics:

```
CN3920-07> port show throughput active
```

PORT THROUGHPUT SUMMARY			5 SECOND SAMPLE		
Port	Bit Rate (Mbps)		Pkt Rate (Mpps)		
	Tx	Rx	Tx	Rx	
1	0.867		0.001		
2	0.867		0.001		
12		2.008		0.003	

To display statistics for specific ports:

```
port show port <PortList> statistics|total-statistics|throughput [active] [delay <NUMBER: 1-86400>] [count <NUMBER: 0-4294967295>] [scale <tera|giga|mega|kilo|none>][type <all|basic|errors|tx|rx>]
```

Example of port 1 statistics:

```
> port show port 1 statistics active
```

PORT 1 STATISTICS	
Statistic	Value
TxBytes	8383361868
TxPkts	67607757
TxBcastPkts	67607757

Example of port 1 total statistics:

```
> port show port 1 total-statistics active
```

PORT 1 STATISTICS		
Statistic	Total Value	Value
RxBytes	1053155263708	0
RxPkts	1372943892	0
RxMcastPkts	8678509	0
RxBcastPkts	8678545	0
128To2550ctsPkts	8678525	0
512To10230ctsPkts	1355586868	0
1024To15180ctsPkts	8678499	0
TxBytes	169749142776	8393012044
TxPkts	325827225	67685581
TxLOutOfRangePkts	939	0
TxMcastPkts	11277954	0
TxBcastPkts	136721539	67685581

Example of port 1 throughput statistics:

```
> port show port 1 throughput active
```

PORT 1 THROUGHPUT			
Statistic	Current Value	Delta Value	Rate Mpps & Mbps
Time	0:21:45:20	0:00:03:43.4	
TxBytes	8,399.264	23.951	0.107
TxPkts	67.736	0.193	0.001
TxBcastPkts	67.736	0.193	0.001

Monitoring Port Statistics

In addition, you can continuously monitor port statistics. The system will display the statistics and automatically clear the screen before displaying the updated values. To stop monitoring, press Ctrl+C.

To monitor statistics for all ports:

```
port monitor statistics|total-statistics|throughput [active] [delay <NUMBER: 1-86400>] [count <NUMBER: 0-4294967295>] [scale <tera|giga|mega|kilo|none>]
```

Example of monitoring total statistics for all active ports:

```
> port monitor total-statistics active delay 10
<Screen clears>
```

PORT TOTAL STATISTICS SUMMARY				
Port	Byte		Pkt	
	Tx	Rx	Tx	Rx
1	170475797780	1053155263708	331687346	1372943892
2	22214864802	19878912	84101337	310608
12	885114437038	196217923208	1147664620	510799477

Example of monitoring statistics for a specific port:

```
> port monitor port 1 statistics active delay 10
<Screen clears>
```

PORT STATISTICS SUMMARY				
Port	Byte		Pkt	
	Tx	Rx	Tx	Rx
1	9124523384	0	73584866	0
2	9124523756	0	73584869	0
12	0	31648384384	0	247253003

Example of monitoring throughput statistics for a specific port:

```
> port monitor port 1 throughput active
<Screen clears>
```

Info: This CLI output may take a while to display press CTRL-C to abort

<Screen clears>

PORT THROUGHPUT SUMMARY 20 SECOND SAMPLE				
Port	Bit Rate (Mbps)		Pkt Rate (Mpps)	
	Tx	Rx	Tx	Rx
1	0.860		0.001	
2	0.860		0.001	
12		2.984		0.003

To monitor the statistics for specific ports:

```
port monitor port <PortList> statistics statistics|total-statistics|throughput [active]
[delay <NUMBER: 1-86400>] [count <NUMBER: 0-4294967295>] [scale <tera|giga|mega|kilo|none>]
[type <all|basic|errors|tx|rx>]
```

Example of monitoring total statistics for a specific port:

```
> port monitor port 1 total-statistics active delay 10
<Screen clears>
```

INFO: Waiting 10 seconds for display. Abort with CTRL-c

PORT 1 STATISTICS		
Statistic	Total Value	Value
RxBytes	1053155263708	0
RxPkts	1372943892	0
RxMcastPkts	8678509	0
RxBcastPkts	8678545	0
128To2550ctsPkts	8678525	0
512To10230ctsPkts	1355586868	0
1024To15180ctsPkts	8678499	0
TxBytes	170169369228	8813238496
TxPkts	329216148	71074504
TxLOutOfRangePkts	939	0
TxMcastPkts	11277954	0
TxBcastPkts	140110462	71074504

Example of monitoring statistics for a specific port:

```
> port monitor port 1 statistics active delay 10
<Screen clears>
```

INFO: Waiting 10 seconds for display. Abort with CTRL-c

PORT 1 STATISTICS	
Statistic	Value
TxBytes	8800415160
TxPkts	70971090
TxBcastPkts	70971090

Example of monitoring throughput statistics for a specific port:

```
> port monitor port 1 throughput active
<Screen clears>
```

INFO: Waiting 5 seconds for display. Abort with CTRL-c

PORT 1 THROUGHPUT			
Statistic	Current Value	Delta Value	Rate Mpps & Mbps
Time	0:21:52:05	0:00:00:05.2	
TxBytes	8,442.673	0.549	0.110
TxPkts	68.086	0.004	0.001
TxBcastPkts	68.086	0.004	0.001

Clearing Port Statistics

To clear current statistics for all ports:

```
port clear statistics
```

To clear current statistics for specific ports:

```
port clear port <PortList> statistics
```


Chapter Configuring CPU Rate Limiting

5

At a Glance:

- Overview
- Benefits
- Configuration
- Troubleshooting

This chapter explains the purpose and configuration of Central Processing Unit (CPU) rate limiting.

Overview

Network protocol control frames require examination and processing from the CPU. When the CPU must process a large volume of control frames per second, all CPU resources are consumed. This overload causes the CLI and SNMP to become unresponsive.

Benefits

With CPU rate limiting, you can control the number of frames that the CPU must process to help protect the CPU from resource overload, system lockup, and port link loss.

Configuration

By default, CPU rate limiting is globally disabled for the device, and enabled for all individual ports. Before any CPU rate limiting is enforced for the individual ports, you must enable CPU rate limiting globally.

You can configure CPU rate limits in Packets Per Second (PPS) per physical port for the following packet classes:

- Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP) control frames. The default rate limit is 5 PPS.
- Connectivity Fault Management (CFM) control frames. The default rate limit is 50 PPS.
- Tunneled control frames. The default rate limit is 250 PPS.
- 802.1x port-based network access control frames. The default rate limit is 5 PPS.
- Operation, Administration, and Maintenance (EOAM) control frames. The default rate limit is 5 PPS.
- Egress Port Restriction (EPR) Address Resolution Protocol (ARP) control frames. The default rate limit is 5 PPS.

- Internet Group Management Protocol (IGMP) control frames. The default rate limit is 5 PPS.
- Generic Internet Protocol control frames. The default rate limit is 700 PPS.
- Link Aggregation Control Protocol (LACP) control frames. The default rate limit is 5 PPS.
- Link Layer Discovery Protocol (LLDP) control frames. The default rate limit is 5 PPS.
- Multi-Protocol Label Switching (MPLS) control frames. The default rate limit is 5 PPS.
- Provider Edge (PE) ARP control frames. The default rate limit is 5 PPS.
- Per VLAN Spanning Tree (PVST) control frames. The default rate limit is 5 PPS.
- Rapid Spanning Tree Protocol (RSTP) control frames. The default rate limit is 5 PPS.
- Loopback (used for debug). The default rate limit is 5 PPS.
- Remote loopback (used for debug). The default rate limit is 5 PPS.
- Two-Way Active Measurement Protocol (TWAMP) test frames. The default rate limit is 100 PPS.
- Two-Way Active Measurement Protocol (TWAMP) response frames. The default rate limit is 250 PPS.
- Unknown control frames (do not match other packet classes). The default rate limit is 500 PPS.

Setting CPU Rate Limits

When you set CPU rate limits, it can affect services that use control frames within the specified packet class. In a one second interval, the CPU will pass the specified number of packets and drop all following packets of that packet class on the specified port for the remainder of the second.

To set CPU rate limits:

```
flow cpu-rate-limit set
```

Example:

```
> flow cpu-rate-limit set port 15 twamp 300
```

Resetting CPU Rate Limits to Default

You can easily reset the CPU rate limits to default values for specified ports and packet classes. If you do not specify the packet class, then all packet class rate limits will be set to the default values for the specified ports.

To reset CPU rate limits to default:

```
flow cpu-rate-limit unset
```

Example:

```
> flow cpu-rate-limit unset port 15 twamp
```

Enabling CPU Rate Limiting

You can enable CPU rate limiting at the global (system) level and per port. By default, CPU rate limiting is disabled at the global level and administratively enabled per port. When CPU rate limiting is disabled globally, then it is disabled for all ports regardless of the per port state. When you enable CPU rate limiting at the global level, all ports that are administratively enabled per port become operationally enabled and enforce their configured CPU rate limits.

To enable globally:

```
flow cpu-rate-limit enable
```

Example:

```
> flow cpu-rate-limit enable
```

To enable per port:

```
flow cpu-rate-limit enable [port <PhyPortNameList>]
```

Example:

```
> flow cpu-rate-limit enable port 15
```

Disabling CPU Rate Limiting

You can disable CPU rate limiting at the global (system) system level or per port.

To disable globally:

```
flow cpu-rate-limit disable
```

Example:

```
> flow cpu-rate-limit disable
```

To disable per port:

```
flow cpu-rate-limit disable[port <PhyPortNameList>]
```

Example:

```
> flow cpu-rate-limit disable port 15
```

Configuring CPU Rate Limiting

This section provides a typical example of CPU rate limiting for UNI (subscriber) ports and NNI (provider) ports. For the UNI ports, rate limits are increased for DHCP packet classes, and decreased for CFT, CFM, generic IP, and unknown control frames. For the NNI ports, CPU rate limits are set to protect against RSTP, LACP, and LLDP packet storms and minimized for CFT. All other packet classes are left at default.

To configure CPU Rate Limits:

Step #	Description	Command
Step 1	Set the BOOTP/DHCP rate limit for UNI ports.	<code>flow cpu-rate-limit set {port <PhyPortNameList>}</code>
Step 2	Set the CFT rate limit for UNI ports.	<code>flow cpu-rate-limit set {port <PhyPortNameList>}</code>
Step 3	Set the RSTP, LACP, and LLDP rate limit for NNI ports.	<code>flow cpu-rate-limit set {port <PhyPortNameList>}</code>
Step 4	Set the CFT rate limit for NNI ports.	<code>flow cpu-rate-limit set {port <PhyPortNameList>}</code>
Step 5	Enable CPU rate limiting globally.	<code>flow cpu-rate-limit enable</code>

Example:

1. > flow cpu-rate-limit set port 1-5 bootp 50
2. > flow cpu-rate-limit set port 1-5 cft 50 cfm 0 inet 5 dflt 10
3. > flow cpu-rate-limit set port 25-28 rstp 50 lacp 10 lldp 25
4. > flow cpu-rate-limit set port 25-28 cft 10
5. > flow cpu-rate-limit enable

Troubleshooting

Displaying CPU Rate Limiting Status

You can display the global status of CPU rate limiting, including an indication of frames dropped. When the CPU is dropping frames from a given port to enforce configured rate limits, the “Drops” column will show “Yes”, otherwise, it will be empty. If “Yes” is displayed in the “Drops” column, it is recommended that you display the port’s statistics (as shown in **the Displaying CPU Rate Limiting Statistics for a Specific Port section on page 69**) to determine what type of control frames are being dropped.

To display the global status of CPU rate limiting:

flow cpu-rate-limit show

Example:

> flow cpu show

CPU RATE LIMITING			
Parameter		Value	
Device Admin State		Disabled	
Per Port CPU Rate Limiting			
Port	Admin	Operational	Drops
1	Enabled	Disabled	
2	Enabled	Disabled	
3	Enabled	Disabled	
4	Enabled	Disabled	
5	Enabled	Disabled	
6	Enabled	Disabled	
7	Enabled	Disabled	
8	Enabled	Disabled	
9	Enabled	Disabled	
10	Enabled	Disabled	

Displaying CPU Rate Limits for a Specific Port

To display CPU rate limits for a specific port:

```
flow cpu-rate-limit show port <PortName>
```

Example:

```
> flow cpu-rate-limit show port 15
```

Packets Per Second Rate Limits		
Port	Packet Class	PPS Rate
15	Bootp/DHCP	5
15	CFM	50
15	CFT	250
15	Dot 1X	5
15	EOAM	5
15	EPR ARP	5
15	IGMP	5
15	INET/IP	700
15	LACP	5
15	LLDP	5
15	MPLS	5
15	PE ARP	5
15	PVST	5
15	RSTP	5
15	Loopback	5
15	Remote Loopback	5
15	TWAMP TST	100
15	TWAMP RSP	250
15	Default	500

Displaying CPU Rate Limiting Statistics for a Specific Port

To display CPU rate limiting statistics for a specific port:

```
flow cpu-rate-limit show port <PortName> statistics
```

Example:

```
> flow cpu-rate-limit show port 15 statistics
+-----+ Rate Limit Packet Statistics +-----+
| Port | Packet Class | Dropped | Passed |
+-----+-----+-----+-----+
| 15 | Bootp/DHCP | 0 | 13900 |
| 15 | CFM | 0 | 0 |
| 15 | CFT | 0 | 0 |
| 15 | Dot 1X | 0 | 0 |
| 15 | EOAM | 0 | 0 |
| 15 | EPR ARP | 0 | 0 |
| 15 | IGMP | 0 | 0 |
| 15 | INET/IP | 0 | 8511 |
| 15 | LACP | 0 | 4671 |
| 15 | LLDP | 0 | 4590 |
| 15 | MPLS | 0 | 0 |
| 15 | PE ARP | 0 | 0 |
| 15 | PVST | 0 | 0 |
| 15 | RSTP | 8 | 68853 |
| 15 | Loopback | 0 | 0 |
| 15 | Remote Loopback | 0 | 0 |
| 15 | TWAMP TST | 0 | 0 |
| 15 | TWAMP RSP | 0 | 0 |
| 15 | Default | 0 | 0 |
| 15 | Default | 0 | 0 |
| 15 | Drop | 0 | 0 |
+-----+-----+-----+-----+
```

Clearing CPU Rate Limiting Statistics for a Specific Port

To clear CPU rate limiting statistics for a specific port:

```
flow cpu-rate-limit clear port <PortName> statistics
```

Example:

```
> flow cpu-rate-limit clear port 15 statistics
```

Displaying CPU Rate Limiting Configuration in the Configuration File

CPU Rate Limiting configuration is saved to the configuration file in the FLOW/QOS CONFIG: section.

To display CPU rate limiting configuration in the configuration file:

```
> configuration show
! Device Configuration File
! Chassis MAC: 00:02:a1:30:7d:60
! Created: Sat Feb 23 12:17:02 2008
! Created by: su
! SW Package: Slot 1 - xxxx-xx-xx-xx-xxx
! Build Number: 2323
! MIB Number: 02-05-00-9924
!
!...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! FLOW/QOS CONFIG:
!
flow cpu-rate-limit enable
!
!...
!...
```

Chapter Configuring IEEE 802.1x Security

6

At a glance:

- 802.1x Overview
- Deployment Example
- Using 802.1x with LACP
- Configuring 802.1x
- Using 802.1x to Authenticate a PC
- Troubleshooting 802.1x Operation

This chapter discusses IEEE 802.1x security.



NOTE: This version of system software supports the IEEE 802.1X-2001 Standard.

802.1x Overview

The IEEE 802.1x standard defines an authentication protocol that uses a centralized authentication server (typically a RADIUS server) to provide port-based and user-based network access control. This provides a method for authenticating customer premise equipment (CPE) and the Portals, Service Delivery Switches, and/or Service Concentration Switches used to provide the CPE network connection.

When a device configured for 802.1x authentication is connected to the network, it passes an authentication request to the device providing its uplink. That device then passes the request through the network to the authentication server, which compares the device's user name and password to a pre-entered subscriber database entry and decides whether to allow the device full access to the network.

NOTE: If you upgrade from a software release prior to 4.7.2 without first installing the Advanced-Security feature license, will be disabled and its configuration will not be supported.

The use of 802.1x with RADIUS authentication differs from standard RADIUS management authentication. 802.1x uses port-based authentication, whereas RADIUS by itself is used to authenticate *users* who are attempting to access a device in order to change or monitor its configuration. However, the same RADIUS server could be used for authentication in both instances. **Figure 6-1** shows an example of 802.1x authentication.

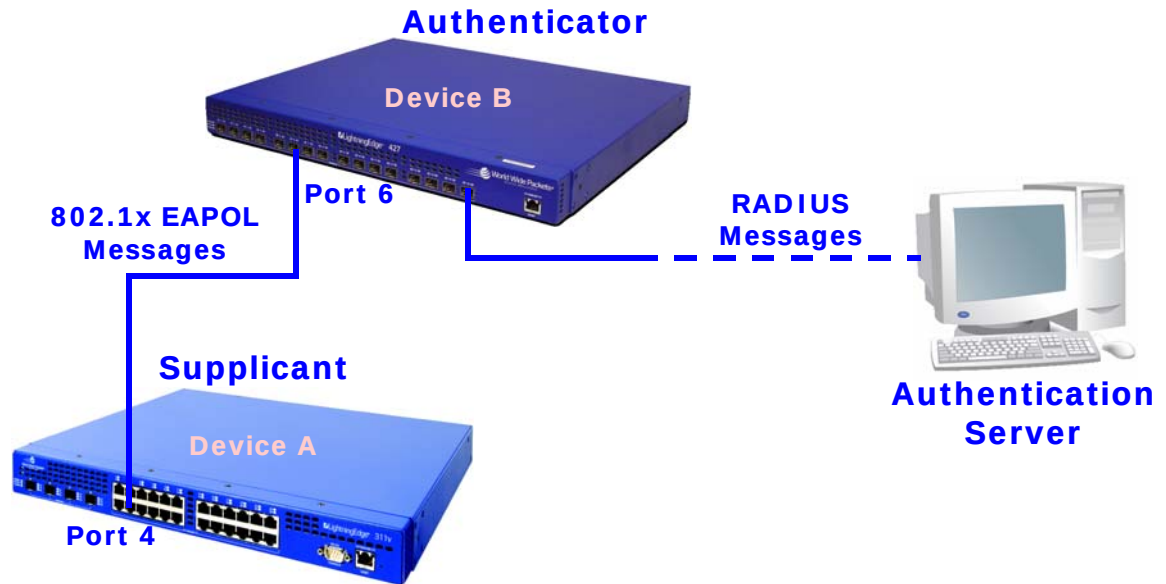


Figure 6-1: IEEE 802.1x Authentication Example

The 802.1x standard specifies the following roles in the authentication process:

- **Suppliant** - is the device requesting access to the network. This could be a subscriber device, such as a PC, or a port on a Portal, Service Delivery Switch, or Service Concentration Switch that is connected to another device providing its uplink. In the case of a PC, the PC's network interface card (NIC) is configured for 802.1x authentication using EAP-MD5. When the NIC is enabled, it issues an 802.1x authentication request to a port on the device providing its uplink that is configured as an 802.1x Authenticator. Until the Suppliant is successfully authenticated, only extensible application protocol over LAN (EAPOL) messages from the Suppliant are accepted by the Authenticator port on the uplink device, while other data packets are dropped.



NOTE: If the Suppliant is configured to use DHCP to obtain an IP address, the DHCP request is not passed to the DHCP server until after the Suppliant has successfully authenticated. If the Suppliant does not authenticate, it does not receive an IP address - preventing it from being reached via an uplink or a subscriber connection. A direct serial port connection to the Suppliant device is then required to correct the problem.

- **Authenticator** - acts as an intermediary between the 802.1x Suppliant and the RADIUS Authentication Server. It receives the EAPOL formatted authentication request from the Suppliant, encapsulates the authentication request into a RADIUS message, and passes the authentication request to the Authentication (RADIUS) Server. The response from the Authentication Server is sent back to the Authenticator, which forwards the response to the Suppliant. The Authenticator also uses the RADIUS response to determine whether to begin passing regular data traffic to/from the Suppliant.

The port acting as the Authenticator can be configured to respond to 802.1x frames in one of the following three ways:

- **Auto** - provides 802.1x operation on a port, allowing only EAPOL frames to be sent and received until the client successfully authenticates. Once authenticated, regular traffic is allowed.
- **Force Authorized** - In this mode, 802.1X is disabled and the port is in an authorized state. The port transmits and receives normal traffic without 802.1X-based authentication of the client.
- **Force Unauthorized** - causes all communications from an 802.1x client to be blocked, preventing the client from authenticating through this port.
- **Authentication Server** - receives the RADIUS authentication requests sent from the Authenticator, looks to see if the Supplicant's user name and password (and additional information if configured) are in its subscriber data base, and responds with a message to allow or deny network access to the Supplicant. For the authentication to succeed, the Authentication Server must be configured to use the same encryption type as the Supplicant (currently only EAP-MD5 is supported).

Deployment Example

Figure 6-2 illustrates a possible network topology where 802.1x is used. Device A has a connection to an Authentication server that is configured with a list of user names and passwords. Device A port 16 is configured as an Authenticator, and is connected to Device B port 25, which is configured as a Supplicant. When Device B is connected to Device A and is powered on, it sends out EAPOL messages to Device A to begin the authentication process. Device A forms the EAPOL messages into a RADIUS message and forwards the request to the Authentication Server. Once authenticated, Device A port 16 allows regular traffic to ingress from Device B port 25. If Device B port 25 fails to authenticate, regular traffic from that port is blocked, preventing traffic from any devices downstream from reaching the network.

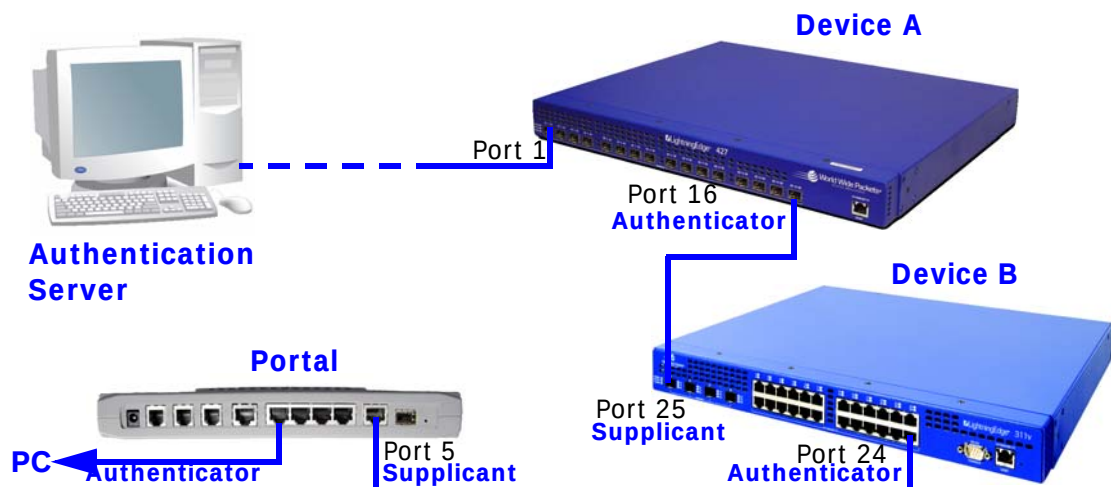


Figure 6-2: 802.1x Deployment Example

After Device B port 25 has successfully authenticated, it can pass data from downstream devices that receive their uplink from that port, such as the Portal connected to port 24. When the Portal connected to Device B is powered on, it sends EAPOL messages out port 5 to Device B port 24, which in turn forms the message into a RADIUS message and

forwards it upstream to the Authentication Server. Once the Portal has successfully authenticated, Device B port 24 will allow regular traffic from the Portal to ingress that port.

If a PC is connected to a subscriber port on the Portal, the same 802.1x process can be used to authenticate the PC and unblock the port on the Portal to provide network access.

Using 802.1x with LACP

802.1X operation controls the state of physical ports, allowing or denying a port access based on its authentication state. Ports that are configured as 802.1x Supplicants that are members of a link aggregation group must be authenticated in order to pass traffic as part of that LACP group.

If a port that is a member of an LACP group becomes unauthenticated during operation, it is removed from the distribution list.

Configuring 802.1x

For all of the following examples refer to **Figure 6-2**. However, these examples configure only Device A and Device B in **Figure 6-2**. Port 16 on Device A is configured as an Authenticator and port 25 on Device B as a Supplicant. These examples also assume that the proper entries have already been entered on the Authentication (RADIUS) server.

As previously described, 802.1x operation consists of three entities: Supplicant, Authenticator, and Authentication Server. The Supplicant and Authenticator are configured on individual physical ports on the devices.

The Authentication Server is a third party device that is separately controlled by the network administrator, but must be accessible by the Authenticator in order to authenticate the Supplicant. The user name(s) and password(s) used by Supplicants must be configured on the server. The server must also be configured to use MD5 encryption. Most Authentication servers can be configured to allow multiple Supplicants to use the same user name and password to authenticate, but may also require each Supplicant to have a unique user name and/or password.



NOTE: The following Authenticator and Supplicant configuration examples assume that all 802.1x controls are in their default state. Only the required controls are changed in order to successfully authenticate the Supplicant device. Additional configuration changes may be required, depending on the actual network topology.

Configuring the Supplicant



CAUTION: Enabling 802.1x operation blocks further access to the Supplicant port until it has been authenticated. Make sure to configure all Supplicant-specific settings *before* enabling 802.1x operation on the device, otherwise, the remaining configuration must be performed using a console port connection or through another port on the device that is also part of the device's management VLAN but is not configured as a Supplicant.

Step #	Description	Command
Step 1	Establish a connection with the Supplicant device (Device B).	Telnet
Step 2	On the Supplicant device (Device B), enter the port number of the Supplicant (Port 25 in this example), the username, and the password for the Supplicant. Be sure to enter the username and password exactly as they are configured on the remote authentication server. Text strings are case sensitive.	dot1x supp set port <PhyPortNameList>
Step 3	Enable Supplicant operation on port 25 of Device B.	dot1x supp enable port <PhyPortNameList>
Step 4	Enable 802.1x operation on Device B.	dot1x enable

CLI Example:

1. dot1x supp set port 25 username Joan password nomoresecrets
2. dot1x supp enable port 25
3. dot1x enable

The Supplicant is now sending EAPOL Start messages, and is looking for an Authenticator.

Configuring the Authenticator

Step #	Description	Command
Step 1	Establish a connection with the Authenticator device (Device A).	Telnet
Step 2	Specifying the RADIUS server that will be used as the Authentication Server. Specify the IP address, UDP port if needed (default 1812), and specify whether the server will be used as a dedicated 802.1x authenticating server (dot1x) or if it will be used for both user authentication AND 802.1x authentication (All).	radius add server <IpHost>
Step 3	Set the RADIUS server key.	radius set
Step 4	Enable the RADIUS server for the Authenticator device.	radius enable [server <IpHostRadius>]

Step #	Description	Command
Step 5	Globally enable RADIUS on the Authenticator device.	radius enable [server <IpHostRadius>]
Step 6	Configure Authenticator settings on port 16 of Device A, setting the PAE mode to auto (default). In auto mode, the port state depends on the result of the authentication process.	dot1x auth set port <PhyPortNameList>
Step 7	Enable Authenticator operation on port 16 of Device A.	dot1x auth set port <PhyPortNameList>
Step 8	Enable 802.1x operation on the Authenticator device.	dot1x enable

CLI Example:

1. > radius add server 10.10.10.10 use-for dot1x
2. > radius set key radiuskey
3. > radius enable server 10.10.10.10
4. > radius enable
5. > dot1x auth set port 16 mode auto
6. > dot1x auth enable port 16
7. > dot1x enable

802.1x operation has now been enabled on the device and port 16 has been configured as an Authenticator.

Verifying Authentication

The Port Access Entity (PAE) state for the Supplicant and the Authenticator monitor the current state of authentication. When the Supplicant has authenticated, both devices should indicate that state.

```
> dot1x show
```

```

+---Global Dot1x Status---+
|           Enable         +
+-----+-----+
+-----+-----+-----+-----+
| Port   | Admin | Operational | Port Role |
|        | State | State       | (Auth/Supp) |
+-----+-----+-----+-----+
| 1      | Disabled | Unknown    | None       |
| 2      | Disabled | Unknown    | None       |
| 3      | Disabled | Unknown    | None       |
| 4      | Disabled | Unknown    | None       |
| 5      | Disabled | Unknown    | None       |
| 6      | Disabled | Unknown    | None       |
| 7      | Disabled | Unknown    | None       |
| 8      | Disabled | Unknown    | None       |
| 9      | Disabled | Unknown    | None       |
| 10     | Disabled | Unknown    | None       |
| 11     | Disabled | Unknown    | None       |
| 12     | Disabled | Unknown    | None       |
| 13     | Disabled | Unknown    | None       |
| 14     | Disabled | Unknown    | None       |
| 15     | Disabled | Unknown    | None       |
| 16     | Enabled  | Authorized  | Authenticator |
| 17     | Disabled | Unknown    | None       |

```

18	Disabled	Unknown	None	
19	Disabled	Unknown	None	
20	Disabled	Unknown	None	
21	Disabled	Unknown	None	
22	Disabled	Unknown	None	
23	Disabled	Unknown	None	
24	Disabled	Unknown	None	
25	Disabled	Unknown	None	
26	Disabled	Unknown	None	
27	Disabled	Unknown	None	
28	Disabled	Unknown	None	
+-----+				

> dot1x auth show port 16

```

+--- Dot1x Authenticator Pae State ----+
+   Authenticated                       |
+-----+

```

+----- Dot1x Authenticator Port Configuration -----+									
Port	Eap	Auth	Quiet	Tx	Supp	Server	Max	Reauth	Reauth
	Result	Mode	Period	Period	Tmo	Tmo	Req	State	Period
+-----+									
16	Succ	Auto	60	30	30	30	2	Ena	3600
+-----+									

+----- Dot1x Authenticator Port Statistics -----+						
Port	Eapol	Eapol	Id Req	Id Resp	Request	Response
	Frames Tx	Frames Rx	Frames Tx	Frames Rx	Frames Tx	Frames Rx
+-----+						
16	32183	70	21421	34	34	34
+-----+						

+----- Dot1x Authenticator Session Statistics -----+	
Parameter	Value
+-----+	
Frames Tx	2794
Frames Rx	1866
Sess Id	2-1
Session Time (seconds)	214
Session Auth Method	Remote Authentication Server
Session Terminate Cause	Not Terminated Yet
Session Username	joan
+-----+	

Using 802.1x to Authenticate a PC

A personal computer (PC) with an 802.1x-capable network interface card (NIC) can be configured as a Supplicant. Using an Access Portal or other device configured as an Authenticator, the PC can be authenticated in order to access the network.

Both the NIC and the PC's operating system must support 802.1x operation. For example, Windows™ 2000 requires Service Pack 4 to enable 802.1x operation. Some NICs provide 802.1x operation while others do not. If an "Authentication" tab is not displayed in the NIC's configuration settings, 802.1x is probably not supported. Consult the NIC's documentation for its capabilities and operating system requirements.

Configuring the NIC

The following steps outline the general procedure to configure the PC's settings. Note that the NIC must be enabled to perform these steps.

1. Access the NIC's properties. In Windows™, select Start > Settings > Network Connections (or access the Network Connections on the Control Panel). Right-click on the entry for the NIC being used and select **Properties**.
2. Select the Authentication tab.

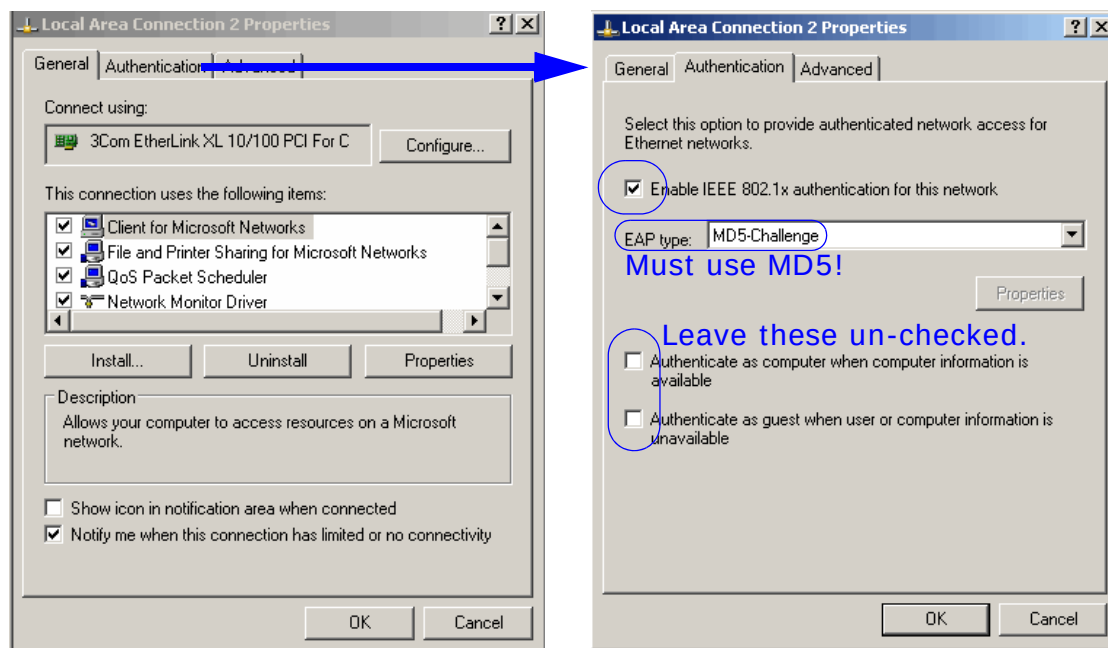


Figure 6-3: Local Area Connection Properties

3. Check the box next to "Enable IEEE 802.1x authentication for this network."
4. Select **MD5-Challenge** for the EAP Type.
5. Un-check any other boxes that may be checked.
6. Select **OK**.
7. Close the NIC properties window.

Logging Into the Network

1. Connect the PC to the port configured as the Authenticator on the Portal or other device connected to the network.
2. After several seconds, the PC displays an alert regarding entering user credentials. Click on the alert to display the entry window.

3. Enter the user name and password exactly as it is entered on the authentication server and select **OK**.

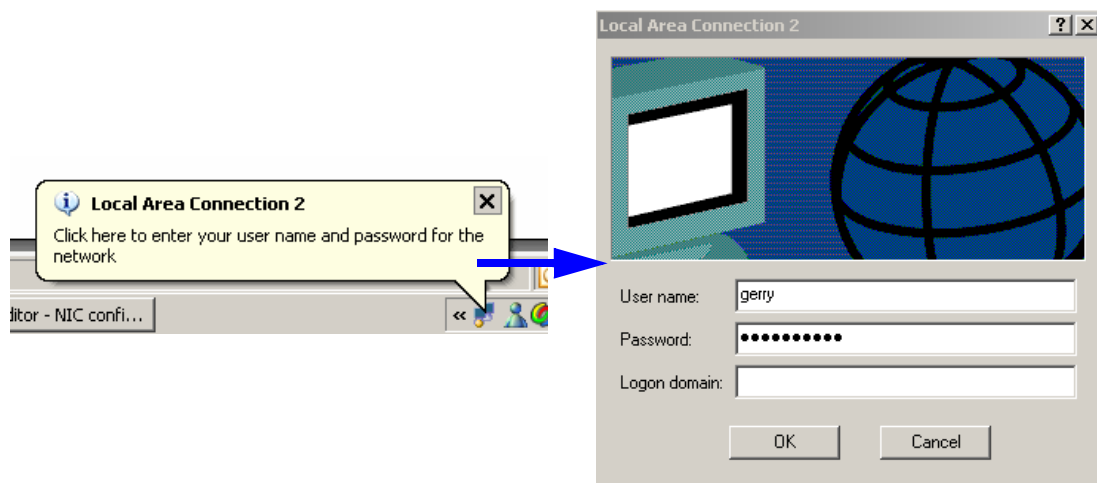


Figure 6-4: Authenticating the PC



NOTE: Even after the PC has successfully authenticated, it will not have network connectivity unless the NIC has either been configured with a static IP address that is within the network's subnet or it has been configured to use DHCP to obtain an IP address and a DHCP server is reachable on the network.

Troubleshooting 802.1x Operation

If a Supplicant fails to authenticate when put into service, or the Supplicant cannot be contacted after it successfully authenticates, verify that the following conditions are met:

- The physical ports on the devices that are configured as the Supplicant and the Authenticator have a direct physical connection to each other. The only exception to this is if control frame tunneling is configured to tunnel 802.1x EAPOL frames through any intermediate device(s) connecting the Supplicant to the Authenticator.
- If the Supplicant is configured to obtain its IP address from a DHCP server, that server must be accessible once the Supplicant has been authenticated.
- Make sure that global 802.1x operation is enabled on the Supplicant and on the Authenticator.
- Verify that MD5 encryption is being used by the authentication server. Other types of encryption, such as Protected EAP (PEAP), are not supported.
- The Supplicant, Authenticator, and Authentication Server must all be on the same VLAN in order to communicate (unless a router exists between the switch and the server). The EAPOL messages sent by the Supplicant are not 802.1q tagged, therefore the Supplicant can successfully authenticate without being on the same VLAN as the Authenticator or the Authentication Server. However, once authentication is successful, the Supplicant will not be able to communicate with the Authenticator if it is on a different VLAN.
- Use the Ping command to verify that the Authenticator can communicate with the Authentication Server.

- Verify that the Authentication Server's authentication port number is the same number specified in the Supplicant's settings.
- Verify that the RADIUS key specified matches the key configured on the Authentication Server.
- Verify that the user name and password specified for the Supplicant are *exactly* the same as they are entered in the Authentication Server's user list (including the use of lower and upper case characters)

Chapter

Link Aggregation and LACP

7

At a Glance:

- Overview
- Link Aggregation Group
- Manual Link Aggregation
- LACP
- Configuring Link Aggregation

This chapter discusses the differences between Link Aggregation and LACP. It also explains how to configure them.

Overview

Link Aggregation is defined in IEEE 802.3ad. This standard defines how two or more full-duplex Ethernet ports of the same speed can be combined into a single logical port to carry traffic between two devices connected in parallel. This logical grouping of ports enables load sharing and load balancing among these ports and thus an aggregation of bandwidth as well. Traffic destined to egress on an aggregated port is distributed among all the links in the group.

Link Aggregation also provides inherent, automatic redundancy for high-traffic network connections. This is achieved by dynamically redirecting traffic from a failed port to the remaining good port in the aggregation group. Link Aggregation can therefore be used to expand bandwidth and add link redundancy.



NOTE: The IEEE 802.3ad standard does not support aggregation of bandwidth between links taking different paths and connecting to different upstream units. Only ports connected in parallel between two units can be aggregated.

Link Aggregation Group

Link Aggregation is configured using the concept of physical ports vs. logical ports. Physical ports are actual ports on the switch, while logical ports or Link Aggregation Groups (LAG) are the collective group the physical ports belong to. Grouped physical ports appear to the system as one logical port. For example, with spanning tree, a physical port assigned to a LAG appears to be operationally down. This excludes the physical port from being considered in the spanning tree topology.

Instead, within the LAG group there is always a 'lead port', which is responsible for sending control frames for protocols such as RSTP. The lowest port number in the LAG is always elected as the lead port. If the lead port should go down, the port with the next lowest port number will assume the role of lead port. If a link failure should occur, it is

almost transparent. The only traffic losses will be the frames either in the egress queue or those already on the wire at the time of failure. Up to 8 LAGs are supported with up to 8 physical ports per unit.

In addition, aggregated ports operate as if they were a single entity with respect to L2 address learning, regardless of which port of the LAG traffic ingresses.

Two types of Link Aggregation are supported, manual Link Aggregation and Link Aggregation Control Protocol (LACP). However, regardless of the type of Link Aggregation, the user is only required to create a LAG, add ports to it, and then specify the mode of aggregation (manual or LACP). The unit will take care of the rest of the configuration itself.



NOTE: EOAM loopback set on the LEAD port of an aggregation will cause the RECEIVE-side aggregation (if it is the lead port in loopback) to NOT forward traffic. EOAM loopback done on ANY other physical port in the aggregation should pass traffic correctly.

Manual Link Aggregation

LACP allows the unit to negotiate link aggregation by sending LACP PDUs to its peer. Manually configured Link Aggregation ports are considered “blind” as they are set up completely by the administrator and never send LACP PDUs. A manual Link Aggregation forms only when a LAG has been specifically configured on two devices following which, their ports are physically connected.

Although Link Aggregation has been a standard since 1998 every vendor has a slightly different implementation (e.g., Cisco Ether Channel, Sun Trunking, etc.). Manual Link Aggregation is most useful when connecting a Ciena device to another vendor’s device that supports manual Link Aggregation.

LACP

IEEE 802.3ad LACP allows for standards-based link aggregation between devices over full duplex, same-speed links. LACP utilizes control packets in order to establish aggregation of links, maintain that aggregation, and distribute or redistribute bandwidth for load balancing and link failure. The LACP protocol is very intricate and prone to configuration errors. Ciena has therefore simplified the configuration of Link Aggregation.

Traditionally, network administrators had to worry about configuring such parameters as Actor Admin Keys, Operational keys, collector max delay, and other such complications. In the Ciena implementation, all of these parameters are handled behind the scenes. After a LAG has been created on one device and ports are added, it will look for eligible ports on its peer to aggregate with. It doesn’t matter if the two LAGs have the same configurations as their peer, as long as the groups are valid they will find each other and negotiate an aggregation.

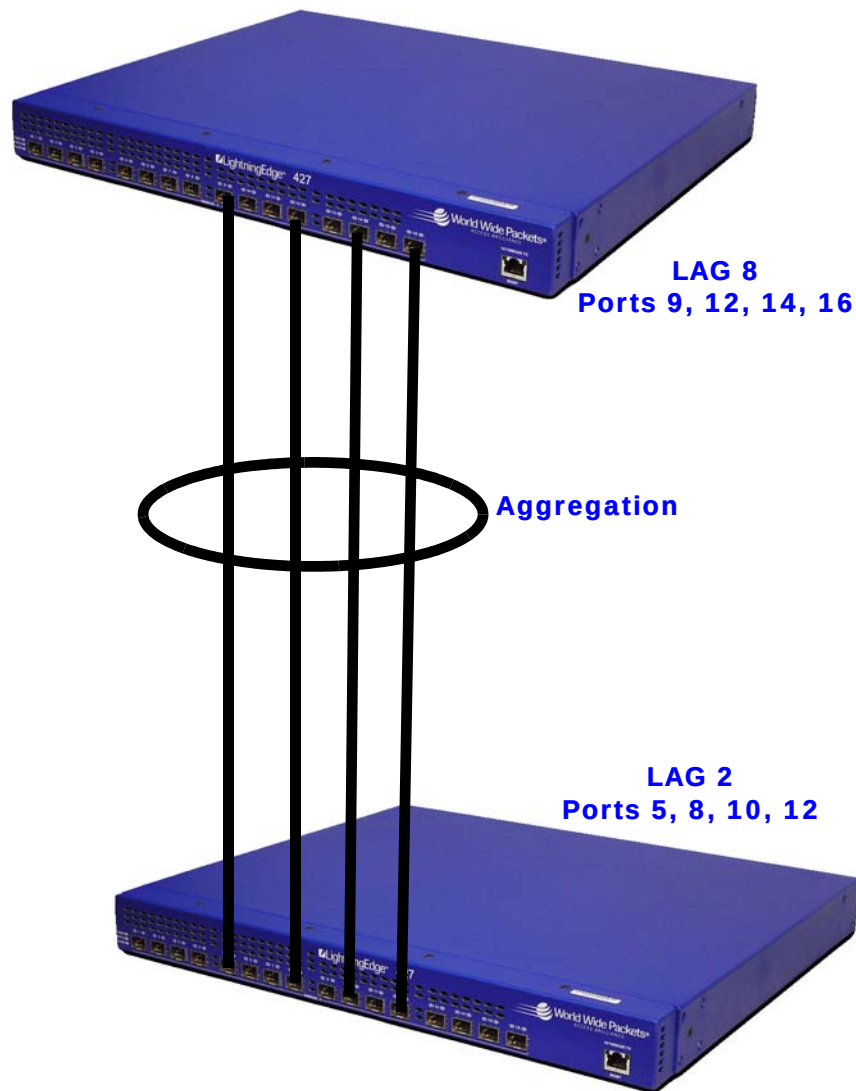


Figure 7-1: Link Aggregation



NOTE: Advanced users may still directly configure parameters and keys for both LAGs and physical ports.

LACP uses two types of control frames; LACP PDUs and Marker Frames. Both messages use a globally unique destination address of 01-80-C2-00-00-02 and a corresponding Ethernet type. LACP PDUs are used for negotiation between links. Marker frames are used to maintain frame sequence order.

As bandwidth is distributed across aggregated ports and a port is made ready to forward frames on the LAG, Marker Frames and Marker Response Frames are exchanged. When an event that requires flow redistribution occurs, the flows that need to be redistributed are first blocked. Once blocked, a Marker Frame that has a response timer tied to it, is sent out each port in the aggregation group to the link partner (i.e. another Service Delivery

Switch/Service Concentration Switch) for each flow. When the Marker Response Frames are received or the response timers expire, the flow is moved in the forwarding database of the newly selected port and forwarding is once again enabled.

Protection Link Aggregation

Additional ports can be added (up to 16 per Aggregation Group, with up to 8 ports active at any given time) to a Link Aggregation Group (LAG) as either Protection (backup) ports, or as regular Distribution ports. By default, all ports are distribution ports. Protection ports collect the same traffic as the Distribution ports, but do not transmit data (if LACP is enabled) until an active port in the LAG becomes disabled, either administratively or operationally.

Designating ports as Protection ports enables port redundancy in the event of a Distribution port failure, and thus smooths out potential traffic bottlenecks.

For example, suppose that 3 ports are designated as Distribution ports, and 2 ports are designated as Protection ports. All 5 ports are grouped together in the same LAG. The Distribution ports handle all the traffic, and the Protection ports are essentially on standby. If a Distribution ports fails, then the Protection port with the lowest port number immediately takes its place.

By default, when a failed Distribution port returns to operational status, it becomes a Protection (backup) port. However, this behavior can be overridden by enabling the `revert-protection` parameter. In this case, the original Distribution port becomes active again (and one of the Protection ports then reverts back to being a backup port) only *after* the `revert-delay` timer expires, or an additional Distribution port fails. The timer delay protects the LAG from a port that may be rapidly flapping between enabled and disabled.

When using the `aggregation show agg member` command, the state of each port in the aggregation group is displayed in the Type field. This field can help determine if a port is participating in the aggregation group or in the case of a Protection port, whether a port is distributing traffic or just collecting traffic. Protection ports are indicated by a "P" next to the port number. The following states are listed:

- Added- the physical port has been administratively added to the logical aggregation port (for example, `aggregation add agg port` command)
- Selec- the physical port has been selected for this aggregation port by the protocol.
- Agged - the physical port has been aggregated to this aggregation port by the protocol. This physical port now belongs the logical aggregation port.
- Dist- The port is forwarding traffic over the logical aggregation port.

Configuring Link Aggregation

The example configures LACP between two devices. When configuring LACP all links in the Aggregation should either be up or down.

For manual Link Aggregation, it is recommended that both devices be configured first, before the physical connections are made. Ciena does not recommend manual configuration of LACP parameters and keys unless the user has a firm understanding of the LACP standard.



NOTE: When naming Link Aggregation Groups, do not use a dash (-) symbol. The CLI will misinterpret the dash as denoting a port range.



CAUTION: When changing the mode of a link aggregation from manual to LACP or from LACP to manual for a single link, a service disruption will occur on the LACP side until the modes match again. If connecting to the device using the management interface, the desired aggregation state must be modified on the “far end” device first or connectivity will be lost unless a backup link exists.

For example, remote connections between Juniper devices are lost after disabling link aggregation. Juniper devices should be set to manual mode with the interfaces <agg group> aggregated-ether-options lacp command.

To minimize service disruption, Ciena recommends provisioning backup links before modifying the link aggregation mode.

To configure Link Aggregation:

Step #	Description	Command
Step 1	Create a Link Aggregation Group (virtual port) on Service Delivery Switch/Service Concentration Switch 1.	aggregation create agg <LagPortName[7]>
Step 2	Add ports to the Aggregation Group.	aggregation add agg <LagPortName[7]> {[port <PhyPortNameList>] [protection-port <PhyPortNameList>]}
Step 3	(optional) Verify the configuration of the LAG.	aggregation show agg <LagPortName[7]> [info] [mode]
Step 4	Create a VLAN for the LAG	vlan create vlan <VlanIdList> [name <String[31]>]
Step 5	Add the aggregation to the VLAN	vlan add vlan <VlanList> port <PortNameList>

Step #	Description	Command
Step 6	(optional) Verify VLAN creation and membership.	vlan show [port <PortNameList> vlan <VlanList>] statistics
Step 7	Repeat the configuration for Service Delivery Switch/Service Concentration Switch 2.	

Since the steps in configuration of both Service Delivery Switches/Service Concentration Switches is the same for both link partners, only device 1 is shown in the following example:

CLI Example:

The following example creates an aggregation group with ports 5,8,11, and 15 named group_1 in VLAN 10.

1. > aggregation create agg group_1
2. > aggregation add agg group_1 port 5,8,11,15
3. > aggregation show agg group_1 info

Agg Port 2049 Info	
Parameter	Value
LAG Port Name & ID	group_1 0x0801(2049)
Added Total Ports	5 8 11 15
Primary Ports	5 8 11 15
Protection Ports	0 -
Selected Ports	5 8 11 15
Admin & Oper State	Up Up
Lacp Mode	LACP
Marker Delay	0
Marker Resp_All_Rcvd Count	0
Time_Out Count	0
Ready Waiting	None
Port Entry	
Aggregator Index	0x0801
ACTOR Port MAC	00:02:A1:07:18:A0
Sys Prio & ID	0x8000 00:02:A1:07:18:A0
Admin & Oper Key	0x0801 0x2801
Agg/Individual	Aggregate
Coll Max. Delay	0
PARTNER Sys Prio & ID	0x8000 00:02:A1:15:57:40
Oper Key	0x2801
Coll Max Delay	0
Revert Time out	5000 (ms)
Revert Protection	Off

4. > vlan create vlan 10
5. > vlan add vlan 10 port group_1
6. > vlan show vlan 10

Configuring Protection Ports

To configure Link Aggregation Protection:

Step #	Description	Command
Step 1	Create a Link Aggregation Group (virtual port) on the Service Delivery Switch/Service Concentration Switch 1.	aggregation create agg <LagPortName[7]>
Step 2	Add ports to the Aggregation Group as regular Distribution ports.	aggregation add agg <LagPortName[7]> {[port <PhyPortNameList>] [protection-port <PhyPortNameList>]}
Step 3	Add additional ports to the Aggregation Group as Protection ports.	aggregation add agg <LagPortName[7]> {[port <PhyPortNameList>] [protection-port <PhyPortNameList>]}
Step 4	Enable/disable revert protection (default = off)	aggregation set agg <LagPortName[7]> revert- protection <on off>
Step 5	Set revert delay timer from 0–60,000 ms (default = 5000 ms)	aggregation set agg <LagPortName[7]> revert- delay <NUMBER: 0-60000>

Since the steps in configuration of both Service Delivery Switches/Service Concentration Switches is the same for both link partners, only device 1 is shown in the following example:

CLI Example:

1. > aggregation create agg 111
2. > aggregation add agg 111 port 1,2,3
3. > aggregation add agg 111 protection-port 4,5,6
4. > aggregation set agg 111 revert-protection on
5. > aggregation set agg 111 revert-delay 10000

Chapter

Monitoring System Status

8

At a Glance:

- Environmental Overview
- Monitoring Temperature and Status
- Monitoring Power Supply Status
- Monitoring Power On Self Tests
- Managing Device Archives
- Displaying Device Identification Attributes
- Displaying Platform Capabilities
- Displaying the Chassis MAC address

This chapter discusses how to monitor the chassis environment, including temperature, power supplies, Power On Self Test (POST), device archive, and device identification information. System resources are also monitored and available for display. System resource items include CPU and memory usage, as well as aggregations, meter profiles, PBT entries, virtual switches, and MAC tables.

Environmental Overview

Environmental monitoring of chassis components can provide early warning indications of possible component failure. Monitoring these components via the CLI ensures safe and reliable system operation and avoids network interruptions.

Monitoring Temperature and Status

Temperature sensors report the device's current operating temperature. Two fixed temperature thresholds are set on each device, a low temperature threshold and a high temperature threshold. The fixed low temperature threshold is set at 0°C and the high temperature threshold at 40°C. Exceeding these temperature thresholds can cause damage to the device and may void the warranty.

The device stores the highest and lowest temperatures. Also, when a high/low temperature violation is detected (e.g., device temperature exceeds 40°C), a counter is incremented. Separate counters are kept for high and low temperature violations.

Setting Temperature Thresholds

You can change the high and low temperature thresholds.

To set the temperature thresholds:

```
chassis set {[high-temp-threshold <NUMBER: 0-60>],[low-temp-threshold <NUMBER: 0-60>]}
```

Example:

```
chassis fan-tray set sensor-id 1 high-temp-threshold 40 low-temp-threshold 5
```

Checking Chassis Temperature

To check chassis temperature:

```
> chassis show temperature

+- TEMPERATURE THRESHOLD -+
| Low           | High          |
+-----+-----+
| 0 C           | 60 C          |
+-----+-----+

+--- TEMPERATURE STATUS ---+
| Current | Low   | High   |
+-----+-----+
| 41 C    | 41 C | 41 C   |
+-----+-----+
```

The temperature threshold and status displays the following:

Field	Description
Low Threshold	The lowest temperature at which the device can be safely operated.
High Threshold	The highest temperature at which the device can be safely operated.
Current	Current device temperature.
Low	Lowest device temperature recorded.
High	Highest device temperature recorded.

Monitoring Power Supply Status

The chassis supports a variety of power configurations with or without UPS, including meter based and power conversion. You can display the status of the power supply.

Checking Power Supply Status

To check the power supply status:

```
>chassis show power
+----- Power Supply Status -----+
| Id      | Type      | State    |
+-----+-----+-----+
| 1       | AC        | Online   |
+-----+-----+-----+
```


The power supply status displays the following:

Field	Description
ID	- ID 1— Main power supply - ID 2— backup battery
Type	Indicates whether the power supply is AC or DC, or not installed (Unequipped).
State	- Online— Power supply is operational. - Offline— Power supply is installed but not turned on. - Faulted— Power supply is not functioning.

Monitoring Power On Self Tests

Power-on Self-tests (POST) run automatically when the chassis is powered up. These tests provide troubleshooting information about the switch, showing failures, port-connectivity problems, or other information. If no problems are found with the device, the POST results will indicate that no errors were detected.

Errors are reported using a 32 bit hex value called a POST Code. The CLI also displays a brief text message with the POST Code that describes the error. If POST errors are found, note the POST Code(s) and any associated messages, then contact Customer Support.



NOTE: On the CN 3940 platform with 2 installed power supplies, if one is not powered up, POST will fail as if the power supply is faulted. Software does not distinguish between a power supply without power and a power supply that is faulted.

Checking POST State and Results

To check POST state and results for all or specific modules:

```
chassis post show
```

Examples of possible POST results using the CLI:

```
>chassis post show
POST is enabled.
POST Results: No errors detected.
```

```
>chassis post show
POST is disabled.
```

```
>chassis post show
POST is enabled.
POST Results:
SWITCH: 14818B180 CXE data line test failed: Wrote 0x01000000 Read 0x00000000
SWITCH: 00103918 CXE address line test failed (address 0x40000000)
CORE: 01020304 Can't write to temp sensor #1
```

Managing Device Archives

Device archives store information related to the environmental status of the device. You can save this information to a file on the flash or export it to a TFTP server.

Displaying Device Archives

You can display all device archives or specify only to show fan, platform, or slot device archives.

To display device archives:

```
device-archive show
```

Example:

```
> device-archive show
```

----- DEVICE ARCHIVE -----	
Parameter	Value
Cumulative system uptime (seconds)	1779
Cumulative system uptime (days:hh:mm:ss)	000:00:29:39
Highest Temperature (degrees Celsius)	0 (60 MAX)
Number of High Temperature Violations	0
Lowest Temperature (degrees Celsius)	50 (0 MIN)
Number of Low Temperature Violations	0
Number of Soft Resets	0
Total Number of Resets	0
Last Reset Reason	Unknown

Saving Device Archives to Flash

You can save all device archives to /mnt/sysfs/archive.

To save device archives to flash:

```
device-archive save
```

Example:

```
> device-archive save
> file cd /mnt/sysfs/archive
> file ls
```

```
-rw-r--r--  1 root    root      167 Jan  1 00:10 default.arc
```

Displaying Device Identification Attributes

Device identification attributes includes:

- Device Type
- Hardware Version
- Serial Number
- MAC Address
- Manufactured Date
- E-PROM (Param) Version

To display device identification attributes:

```
chassis show attributes
```

Example:

```
> chassis show attributes
```

CHASSIS DEVICE ID	
Parameter	
Chassis Device Type	007
Chassis Hardware Version	0
Chassis Serial Number	0
Chassis MAC Address	00:02:a1:07:a4:a0
Manufactured Date	25-10-2007
Param Version	005

Displaying Platform Capabilities

Platform capabilities describe a variety of physical and software resources supported by the chassis.

To display platform capabilities:

```
chassis show capabilities
```

Example:

```
> chassis show capabilities
```

PLATFORM CAPABILITIES	
Parameter	Value
Capabilities Class	0
Platform Type	007
Platform Name	CN 3911
Platform Description	CN 3911 Service Delivery Switch
No. Slots	1
Primary Ctrl Blade	1
DC Power	No
Redundant Power	No
Max Physical Ports	10
Max LAG Ports	0
Max VLANs	256
VLAN Translation	Not Supported
Max IGMP Snoop VLANs	0
Max Mcast Groups	0
Max RSTP Domains	0
Protocol Filters	Not Supported
Max Tunnels	0
Max Ingress Tunnels	0
Max Egress Tunnels	0
Max VCs	0
Max VSS	0
Max VS Subs	0
Multi Subs Per Port	False
VPLS FPGA Support	False
PBT FPGA Support	False
Max Learned Entries	4000
Max FSMT Entries	0
Max FSMT COS Entries	0
Max L4 Prot/P Entries	0
Max SLT Entries	0
Max SACT Entries	0
Max SMT Entries	1024
Max EPR Snids	0
Max SLT wildcards	0

Displaying the Chassis MAC address

The chassis MAC address is assigned at manufacturing.

To display the chassis MAC address:

```
chassis show mac
```

Example:

```
> chassis show mac
```

```
Chassis MAC 00:02:a1:07:a4:a0
```

At a Glance:

- Overview
- Principles of Operation
- Feature Benefits
- Configuring OAM

This chapter provides an overview of the IEEE 802.3ah Operations, Administration, and Maintenance (OAM) and how to configure OAM on devices running this version of SAOS.

Overview

IEEE 802.3ah OAM defines a standard for data link layer Operations, Administration and Maintenance (OAM) sublayer within Layer 2 of the OSI model. It provides mechanisms for monitoring link operation such as remote fault indication and remote loopback control. It is important to note that this OAM functionality only applies to point-to-point Ethernet links. It is the responsibility of higher layer protocols to implement end-to-end OAM functions (over multiple links) in a network.

One of the key functions that can be implemented using OAM is remote loopback mode which is a mechanism by which a Data Terminating Equipment (DTE) requests a remote DTE to go into loopback mode. In this mode all frames sent to the remote DTE are simply looped back unchanged. The return frames can then be analyzed by the sender to determine link quality. Note that in addition to EOAM loopback, a loopback test can also be performed using two physical ports within the same VLAN or broadcast domain using the `port set port loopback` command.

Principles of Operation

OAM remote loopback is the ability to test link quality/performance and isolate link faults by sending frames from one DTE and looping them back at the other DTE. As such, loopback is an intrusive procedure and all normal port operations such as forwarding and learning are disrupted. Any services supported by the ports involved also cease to function. SAOS therefore provides the ability to configure a port to ignore loopback requests.

OAM loopback can only be initiated by DTEs that are configured for OAM Active mode. Active mode DTEs can be switched to loopback mode. In rare cases when two Active mode DTEs simultaneously issue loopback commands for the other DTE, one of the DTEs drops its request and accepts the remote DTE's command.

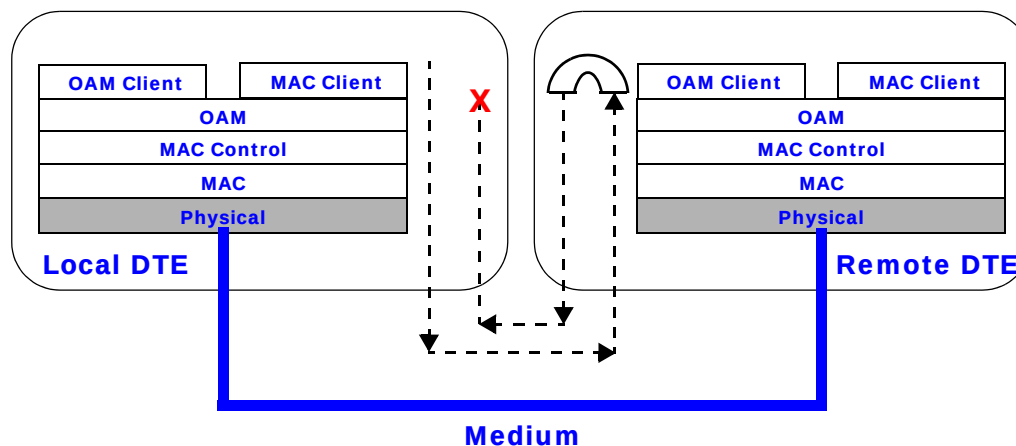


Figure 9-1: Operation of OAM Remote Loopback

Link Events

802.3ah OAM uses 2 types of link events, critical link events and non-critical link events. Critical link events (link fault, dying gasp, etc.) are signaled to the remote DTE by setting the appropriate flag in the OAMPDU frame header. Non-critical events are conveyed using Event Notification PDUs. The data field in an event OAMPDU consists of event TLVs.

Critical Events

Critical events are generated for the following events:

- Dying Gasp- generated when a reboot command is issued administratively, when power is lost, or there is a fatal software error.
- Critical Link Event- generated when the unit temperature crosses above the configured threshold (default = 40°C), unit temperature crosses below the configured threshold (default = 0°C), or fan speed drops below 800 RPM.

Non-Critical Events

Non-critical event notifications are sent under the following conditions:

- Errored Frame Event- generated if the errored frame count is equal to or greater than the specified threshold for that period. Jabber, oversize, undersize, fragment and CRC errors are all monitored.
- Errored Frame Period Event- generated if the errored frame count is greater than or equal to the specified threshold for a period (number of received frames). Jabber, oversize, undersize, fragment and CRC errors are all monitored.
- Errored Frame Seconds Summary Event- generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a 1 second interval wherein at least one frame error is detected. Jabber, oversize, undersize, fragment and CRC errors are all monitored.

Feature Benefits

The primary benefit of 802.3ah OAM is to provide the ability to monitor a link for critical events and then put the remote device into loopback mode to test on the link. OAM functions can be implemented once two directly connected DTEs become aware of each others' OAM capabilities. This is made possible through an OAM discovery process.

OAM information is conveyed in Slow Protocol frames called OAMPDUs. OAMPDUs must be standard length frames (64-1518 octets) and must be untagged. As per the standard, a maximum of 10 OAMPDUs may be sent per second.

Discovery is the process by which the OAM capabilities of peer OAM-enabled entities are discovered. Information OAM Protocols Data Units (OAMPDUs) are used to exchange OAM capability information. In addition, the flags field in the OAMPDU header is used to indicate the current state of OAM discovery. Once discovery is successful other OAM messages/commands can be exchanged between peer OAM entities. The discovery process re-starts automatically if an OAM entity does not receive an Information OAMPDU from the peer OAM entity within 5 seconds.

Support of Standard Tools

OAM is a standards-based protocol. Using OAM rather than a proprietary topology discovery protocol allows the network provider to interoperate with non-devices that support OAM. SNMP MIBs (Management information Database) are supported.

Through the Command Line Interface (CLI), a user can access the SAOS device and manage OAM information. General information, such as loopback configuration for all ports can be displayed and users with proper privileges can configure OAM options. The SAOS software can then detect and manipulate OAM information transmitted.

Configuring OAM

OAM is disabled by default on all ports, but can be enabled or disabled on a per-port basis.



NOTE: To enable EOAM commands, the Advanced OAM feature license must be installed with the software `license install` command.

Enabling OAM

In the following configuration example, the user displays the state of port 5 on a device, then enables OAM on this port. The same configuration is applied to another device on port 11.



NOTE: In this example, configuration settings are verified by using `show` commands. Although these steps are listed as optional, it is good practice to verify command settings using these commands.

Configuration steps:

Step #	Description	Location/Command
Step 1	Enable Global EOAM on both devices.	eoam enable [port <PhyPortNameList>]
Step 2	Display the current state of port 5 on device A.	eoam show [port <PhyPortNameList>] [link-events] [errd-events-statistics] [event-log]
Step 3	Set port 5 to enable mode active on device A and port 11 to enable mode passive on device B.	eoam enable [port <PhyPortNameList>]
Step 4	(Optional) Verify the configuration of the port.	eoam show [port <PhyPortNameList>] [link-events] [errd-events-statistics] [event-log]

CLI Example:

1. > eoam show port 5

```

+--Global Oam Status --+
|      Disable      |
+-----+
+----- Oam Port Statistics -----+
|Port|Admin| Oper State |Mode|OAM Func Support|  Info  |  Info  | Unkn |
|  |State|           |    |UniD|Lb |Ev |Var|  PduTx  |  PduRx  | CodeRx|
+---+---+---+---+---+---+---+---+---+---+---+---+
|5  |Dis  |Disable    |Act |0   |0   |0   |0   |0        |0        |0      |
+---+---+---+---+---+---+---+---+---+---+---+---+

+----- Oam Peer Port Info -----+
| Oper State |Mode|OAM Func Support|Max OamPdu |  Peer Mac Address  |
|           |    |UniD|Lb |Ev |Var|  size  |              |
+---+---+---+---+---+---+---+---+---+
|In-Active  |Un  |0   |0   |0   |0   |0        |00:00:00:00:00:00 |
+---+---+---+---+---+---+---+---+---+

```

2. > eoam enable

3. > eoam enable port 5

4. > eoam show port 5

```

+---Global Oam Status ---+
|           Enable           |
+-----+
+----- Oam Port Statistics -----+
|Port|Admin| Oper State |Mode|OAM Func Support|  Info  |  Info  | Unkn |
|   |State|           |    |UniD|Lb |Ev |Var|  PduTx  |  PduRx  |CodeRx|
+---+---+---+---+---+---+---+---+---+---+---+---+
|5  |En  |Disable  |Act |0   |1   |1   |0   |0        |0        |0      |
+---+---+---+---+---+---+---+---+---+---+---+---+

+----- Oam Peer Port Info -----+
| Oper State |Mode|OAM Func Support|Max OamPdu |  Peer Mac Address  |
|           |    |UniD|Lb |Ev |Var|  size  |              |
+---+---+---+---+---+---+---+---+---+
|In-Active  |Un  |0   |0   |0   |0   |0       |00:00:00:00:00:00 |
+---+---+---+---+---+---+---+---+---+

```

Enabling Loopback

In the following configuration example, the user displays the state of port 5, then enables the loopback on this port. This example assumes that the peer device/port has been enabled to participate in OAM loopback.



NOTE: In this example, configuration settings are verified by using show commands. Although these steps are listed as optional, it is good practice to verify command settings using these commands.

Configuration steps:

Step #	Description	Location/Command
Step 1	Display the current state of port 5 on device A.	eoam show [port <PhyPortNameList>] [link-events] [errd-events-statistics] [event-log]
Step 2	Start loopback on designated port.	eoam loopback start port <PhyPortNameList>
Step 3	(Optional) Verify the configuration of the port.	eoam show [port <PhyPortNameList>] [link-events] [errd-events-statistics] [event-log]
Step 4	View loopback statistics.	eoam loopback show
Step 5	Once troubleshooting has been accomplished, OAM loopback is stopped.	eoam loopback stop port <PhyPortNameList>

CLI Example:

1. > eoam show port 5

```

+--Global Oam Status --+
|           Enable           |
+-----+
+----- Oam Port Statistics -----+
|Port|Admin| Oper State |Mode|OAM Func Support|  Info  |  Info  | Unkn |
|  |State|           |    |UniD|Lb |Ev |Var|  PduTx  |  PduRx  |CodeRx|
+---+---+---+---+---+---+---+---+---+---+---+---+
|5  |En  |SendAny  |Act |0  |1  |1  |0  |192      |38      |0     |
+---+---+---+---+---+---+---+---+---+---+---+---+

```

```

+----- Oam Peer Port Info -----+
| Oper State |Mode|OAM Func Support|Max OamPdu |  Peer Mac Address  |
|           |    |UniD|Lb |Ev |Var|  size  |              |
+---+---+---+---+---+---+---+---+---+
|Active      |Act |0  |1  |1  |0  |1518    |00:02:a1:a1:d1:f0 |
+---+---+---+---+---+---+---+---+---+

```

2. > eoam loopback start port 5

3. > eoam show port 5

```

+--Global Oam Status --+
|           Enable           |
+-----+
+----- Oam Port Statistics -----+
|Port|Admin| Oper State |Mode|OAM Func Support|  Info  |  Info  | Unkn |
|  |State|           |    |UniD|Lb |Ev |Var|  PduTx  |  PduRx  |CodeRx|
+---+---+---+---+---+---+---+---+---+---+---+---+
|5  |En  |SendAny  |Act |0  |1  |1  |0  |257      |102     |0     |
+---+---+---+---+---+---+---+---+---+---+---+---+

```

```

+----- Oam Peer Port Info -----+
| Oper State |Mode|OAM Func Support|Max OamPdu |  Peer Mac Address  |
|           |    |UniD|Lb |Ev |Var|  size  |              |
+---+---+---+---+---+---+---+---+---+
|Active      |Act |0  |1  |1  |0  |1518    |00:02:a1:a1:d1:f0 |
+---+---+---+---+---+---+---+---+---+

```

4. > eoam loopback show port 5

-----Oam Loopback Port Statistics -----							
Port	Lb	Lb Ignore	PeerLb	LbPduTx	LbPduRx	Lb Ctrl	Lb Ctrl
	Status	State	Support			Tx	Rx

5	Dis	Ignore	Yes	0	0	1	0

5. > eoam loopback stop port 5

Chapter

Configuring and Identifying Transceivers

10

At a Glance:

- Overview
- Compliance
- Identification
- Diagnostics
- Displaying Transceiver Information
- Determining Transceiver Speed
- Disabling and Enabling Transceivers
- Setting the Port Connector Mode

This chapter explains transceiver technology and describes the various management options available.

Overview

The Small Form-factor Pluggable (SFP) device used with a device is a hot-swappable compact optical transceiver and is supported by most fiber optic component vendors. SFPs offer high speed (5 Gbps and higher) and physical compactness. Port transceiver information, including status and type, is available via CLI or SNMP.

Compliance

The system software supports SFP transceivers that are compliant with the following documents:

- Small Form Factor Pluggable (SFP) Transceiver Multi Source Agreement, September 14, 2000
- Digital Diagnostic Monitoring Interface for Optical transceivers SFF-8473, Draft Revision 9.0, April 4, 2002.

For a list of supported optics refer to the Hardware Installation and User's Guide for the platform you are working with.

Identification

Ciena devices support transceivers that contain a standard serial erasable programmable read-only memory (EPROM) that provides information on the type of SFP used. The following information is read from the EPROM:

- Identifier Type (GBIC, SFP...)
- Extended Identifier Type

- Connector Type (SC, LC, MU, SG...)
- Vendor Name
- Vendor Organizational Unique Identifier (OUI)
- Vendor Part Number
- Vendor Serial Number
- Vendor Revision Number
- Encoding Algorithm (NRZ, Manchester...)
- Manufacturing Date Code
- Transceiver Code
- Transceiver SFF-8472 Compliance Version

Diagnostics

Ciena devices support advanced transceivers that have an additional diagnostic serial EPROM. The system software determines if the transceiver has the diagnostic EPROM and will provide the following information to the user:

- Wavelength
- Temperature
- Rx Power
- Tx Power
- Tx Disable State
- Tx Fault State
- Rx Rate Select State

The information is stored in a table on a per port basis. The standard EPROM information is updated during initialization or when a new transceiver has been inserted. The diagnostic information is updated at a rate of 1 port per 5 seconds. However, this process has a low priority, and in times of a heavy CPU load, the information may be refreshed slowly or not at all.

Transceivers that support diagnostics can trigger events and SNMP traps, including:

- **SFPs:** BiasHigh, BiasLow, RxPowerHigh, RxPowerLow, TempHigh, TempLow, TxPowerHigh, TxPowerLow, VccHigh, VccLow
- **XFPs:** BiasHigh, BiasLow, RxPowerHigh, RxPowerLow, TempHigh, TempLow, TxPowerHigh, TxPowerLow

Each of these events and traps include a warning and alarm version of each, for example, BiasHighAlarm and BiasHighWarning). Thresholds are set by the SFP vendors, and are not programmable. Both event classes (alarm, warning) are logged under the xcvr-mgr. The warnings are logged using category of debug and the severity of warning. The alarms are logged using category of debug and the severity of minor.

These alarms and warnings are based on flags that are set or cleared inside the SFP. These flags are polled at a low priority and slow rate, so flags may be set and then cleared without generating a trap or event. For example, if the TempHigh alarm threshold is

exceeded for a few seconds, and then cleared before the flag is polled, it will not trigger a TempHigh alarm. You can forcibly clear alarms and warnings by removing and then reinserting the transceiver or disabling g and then enabling the port.

Displaying Transceiver Information

To display diagnostic information for a specified port:



NOTE: The option “diagnostics” is supported for SFPs that actually support diagnostics. If the SFP does not have internal diagnostics capabilities then an error will be returned.

```
port show port <PhyPortNameList> diagnostics
```

Example of SFP that does not support diagnostics:

```
> port xcvr show port 12 diagnostics
No diagnostic data present for port 12
```

Example of SFP that supports diagnostics:

```
> port xcvr show port 1 diagnostics
```

XCVR DIAGNOSTICS - Port 1								
Output	Value	Alarm			Warning			
		Threshold	Flag		Threshold	Flag		
Temp (degC)	31.124	HIGH 90.000	0		HIGH 80.000	0		
		LOW -5.000	0		LOW 0.000	0		
Vcc (volts)	3.295	HIGH 3.630	0		HIGH 3.500	0		
		LOW 2.970	0		LOW 3.100	0		
Bias (mA)	21.520	HIGH 60.000	0		HIGH 50.000	0		
		LOW 3.000	0		LOW 4.000	0		
Tx Power (mW)	1.488	HIGH 3.162	0		HIGH 2.511	0		
		LOW 0.794	0		LOW 1.000	0		
Rx Power (mW)	0.0000	HIGH 0.1590	0		HIGH 0.1262	0		
		LOW 0.0005	0		LOW 0.0010	0		

To display a summary of transceiver status:

```
> port xcvr show
```

Transceiver-Status						
Port	Admin State	Oper State	Vendor Name & Part Number		Ether Medium & Connector Type	Diag Data
9	Empty					
10	Empty					
11	Empty					
12	Ena	Ena	WORLDWIDEPACKETS XCVR-010Y31 Rev10		1000BASE-LX/LC	

To display a summary of transceiver status for a specific port:

```
port xcvr show port <PhyPortNameList> state
```

Example:

```
> port xcvr show port 12
```

Transceiver-Status-----						
	Admin	Oper			Ether Medium &	Diag
Port	State	State	Vendor Name & Part Number		Connector Type	Data
-----	-----	-----	-----		-----	-----
12	Ena	Ena	WORLDWIDEPACKETS XCVR-010Y31 Rev10		1000BASE-LX/LC	
-----	-----	-----	-----		-----	-----

To display vendor EPROM data for a specific port:

```
port show port <PhyPortNameList> vendor
```

Example:

```
> port xcvr show port 9 vendor
```

----- XCVR VENDOR DATA - Port 9 -----			
Parameter	Value	Decoded String Equivalent	
-----	-----	-----	-----
Identifier	0x0	unknown	
Ext. Identifier	0x0	unknown	
Connector	0x0	unknown	
-----	-----	-----	-----
Transceiver Codes	0x0000000000000000		
- SONET Compliance	0x0000		
- Ethernet Compliance	0x00	unknown	
- Link Length	0x00	unknown	
- Transmitter Technology	0x0000	unknown	
- Transmission Media	0x00	unknown	
- Channel speed	0x00	unknown	
Encoding	0x00	unknown	
BR, Nominal	0		
-----	-----	-----	-----
Length(9um fiber) 1km	0	0km	
Length(9um fiber) 100m	0	0m	
Length(50um) 10m	0	0m	
Length(62.5um) 10m	0	0m	
Length(copper) 1m	0	0m	
-----	-----	-----	-----
Vendor Name			
Vendor OUI	0x000000		
Vendor PN			
Vendor Revision			
Wavelength	0		
-----	-----	-----	-----
Options	0x0		
- RATE_SELECT	Bit 5	No	
- TX_DISABLE	Bit 4	No	
- TX_FAULT	Bit 3	No	
- Loss of Signal Invert	Bit 2	No	
- Loss of Signal	Bit 1	No	
-----	-----	-----	-----

BR, max	0	
BR, min	0	
Vender Serial Number		
Date (mm/dd/yy)		
Diag Monitor Type	0x0	
- Legacy diagnostics	Bit 7	No
- Diagnostics monitoring	Bit 6	No
- Internally calibrated	Bit 5	No
- Externally calibrated	Bit 4	No
- Rx power measurement	Bit 3	OAM
Enhanced Options	0x0	
- Alarm/Warning Flags	Bit 7	No
- Soft TX_DISABLE	Bit 6	No
- Soft TX_FAULT	Bit 5	No
- Soft RX_LOS	Bit 4	No
- Soft RATE_SELECT	Bit 3	No
SFF-8472 Compliance	0x0	None

Determining Transceiver Speed

When a transceiver is plugged in, the port speed is blank until a link is established, and then it is set to match the transceiver speed.

To display the optic speed:

> port show

Port Table			Operational Status					Admin Config			
Port Name	Port Type	Link	Link State	Duration	XCVR	STP	Mode	Auto Neg	Link	Mode	Auto Neg
1	10/100/G	Up	0d 5h 4m27s			FWD	100/FD	On	Ena	1000/FD	On
2	10/100/G	Up	0d 5h 4m27s			FWD	100/FD	On	Ena	1000/FD	On
3	10/100/G	Down	0d 0h 0m 0s			Dis		On	Ena	1000/FD	On
4	10/100/G	Down	0d 0h 0m 0s			Dis		On	Ena	1000/FD	On
5	10/100/G	Down	0d 0h 0m 0s			Dis		On	Ena	1000/FD	On
6	10/100/G	Down	0d 0h 0m 0s			Dis		On	Ena	1000/FD	On
7	10/100/G	Down	0d 0h 0m 0s			Dis		On	Ena	1000/FD	On
8	10/100/G	Down	0d 0h 0m 0s			Dis		On	Ena	1000/FD	On
9	10/100/G	Down	0d 0h 0m 0s			Dis		On	Ena	Auto/FD	On
10	10/100/G	Down	0d 0h 0m 0s			Dis		On	Ena	Auto/FD	On
11	10/100/G	Down	0d 0h 0m 0s			Dis		On	Ena	Auto/FD	On
12	Gig	Up	4d 2h48m52s		Ena	FWD	1000/FD	On	Ena	Auto/FD	On

The optic speed can also be determined using the port `xcvr show port <PortNameList> vendor` command. The Encoding “Value” column displays the actual value read from the optic, while the “Decoded String Equivalent” column indicates the port speed supported.

Example:

```
> port xcvr show port 1 vendor
+-----+-----+-----+
| Parameter | Value | Decoded String Equivalent |
+-----+-----+-----+
| Identifier | 0x3 | SFP transceiver |
| Ext. Identifier | 0x4 | SFP/GBIC |
| Connector | 0x7 | LC |
+-----+-----+-----+
| Transceiver Codes | 0x0000000002000000 |
| - SONET Compliance | 0x0000 |
| - Ethernet Compliance | 0x02 | 1000BASE-LX |
| - Link Length | 0x00 | unknown |
| - Transmitter Technology | 0x0000 | unknown |
| - Transmission Media | 0x00 | unknown |
| - Channel speed | 0x00 | unknown |
+-----+-----+-----+
| Encoding | 0x01 | 8B10B |
| BR, Nominal | 13 | Gigabit |
+-----+-----+-----+
...
+-----+-----+-----+
```

Disabling and Enabling Transceivers

When you disable or enable a port directly, the transceiver is disabled or enabled.

To disable transceiver status for a specific port:

```
port disable port <PhyPortNameList>
```

Example:

```
> port disable port 9
```

To enable transceiver status for a specific port:

```
port enable port <PhyPortNameList>
```

Example:

```
> port enable port 9
```

Setting the Port Connector Mode

Some ports support both RJ45 and SFP connectors. Only one of these connectors can be active at a given time. Connectors are enabled by setting the mode for the port. Default modes for ports vary depending on the platform:

- CN 3911 and CN 3920, the default mode is SFP for all dual-mode ports.
- CN 3940, the default mode is RJ45 for ports 1-20, and SFP for ports 21-24.
- CN 5140, the default mode is SFP for all ports.
- CN 3960, the default mode is RJ45 on all of the dual-mode ports.

In addition, speed is set to “Auto” with auto-negotiation enabled. So, you can install 1G or 100M transceivers, and the system will automatically set the speed accordingly. If these settings or other port attributes are set explicitly and do not match the capabilities of the active connector, a mismatch warning will be generated. The warning will be cleared when the attributes match the capabilities of the active connector.



NOTE: If you upgrade a CN 3911 device using an RJ-45 connector from 6.1.0.92 to 6.2.0.91, IP connectivity to the device will be lost. After the upgrade, the remote interface port (9 or 10) defaults to “SFP mode” after the upgrade. At that point, you need to access the device's serial console port to set the port back to RJ-45 mode.



NOTE: If you attempt to set the mode to a connector that is not supported for the specified port, the system generates a “Capability not supported” error message.

To set the mode for a specific port:

```
port set port <PortName> mode <default|rj45|sfp>
```

Example:

```
> port set port 9 mode rj45
```


Chapter Port State Mirroring



At a Glance:

- Overview
- Principles of Operation
- Feature Benefits
- Bi-directional Port State Mirroring
- Configuring Port State Mirroring

This chapter provides an overview of Port State Mirroring and how to configure it on Ciena devices running SAOS software.

Overview

Port State Mirroring (sometimes referred to as link loss forwarding or link state tracking) provides link redundancy by associating the link state of one or more source (uplink) ports with one or more downstream (destination) ports on the switch. If the link is lost on a source port, all of the other destination ports associated with it are automatically placed in a disabled state as well. When used in conjunction with OSPF or RSTP, port state mirroring can be leveraged to force the use of a secondary link.

If port state mirroring is not configured and a link is lost (a cable is disconnected, the connected switch or router goes down, etc.) the link state of the associated interfaces is not affected and a failover to a secondary interface is not initiated.

Principles of Operation

Port state mirroring allows ports to be bundled together in a related group referred to as a port state mirror group (PSMG). Within the group, the link state of the destination ports is dependent upon the link state of the source port(s) in the PSMG. With a single source port, if the source port becomes disabled, all of the destination ports in the group will be forced into a disabled state as well. Likewise, when the source port becomes available again, the destination ports transition back to an enabled state (dependant upon their own availability).

In a PSMG that has more than one source port, all source ports must be disabled in order for the destination ports to be forced into a disabled state. For example, if a PSMG has ports 1 and 2 configured as source ports, both ports must be down to force the destination ports into a disabled state. This also means that only one source port is required to be up in order to transition all destination ports back to the enabled state.

Feature Benefits

Allowing the port state of source ports to directly control the port state of destination ports provides an easy way to shape traffic patterns. Port state mirroring also provides another way to detect link health that otherwise might not be detected.

Bi-directional Port State Mirroring

With bi-directional port state mirroring, ports can mirror their state in both the upstream and downstream directions. This allows the service provider's router port to be automatically disabled if the customer's router port becomes unavailable. Likewise, the converse is true, the customer's router port can be disabled if the service provider's router port should become unavailable.

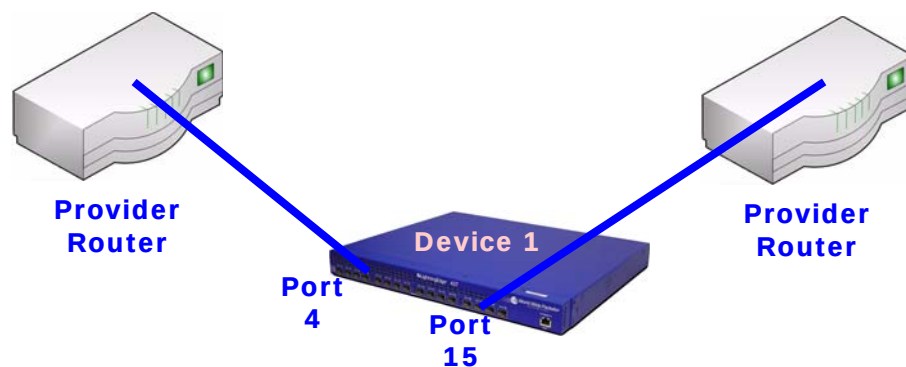


Figure 11-1: Bi-directional Port State Mirroring

In **Figure 11-1**, assume that port 4 and port 15 have been configured in a bi-directional PSMG. If port 15 cannot establish link with the customer router, then port 4 will become disabled as well.



CAUTION: This feature should be configured with care in the event that other customers are serviced by the router connected to Device 1, as they will lose connection to the service provider router as well.

Bi-directional PSMGs are configured the same as a standard PSMG, however, the type must be specified as bi-directional instead of uni-directional.

Configuring Port State Mirroring

In the following configuration example, represented in **Figure 11-2**, a PSMG is configured on Device 1 and another PSMG on Device 2. On Device 1, the downstream (destination) ports 1, 2, 5, and 6 are defined in PSMG 1 with uplink ports 3 and 4 acting as the source ports. For Device 2, downstream ports 7, 8, 11, and 12 are defined in PSMG 2 with uplink ports 9 and 10 acting as the source ports.

Ports 1 and 2 on Device 1 serve as the primary connections for Server 1 and Server 2, whereas port 7 and 8 on Device 2 are the secondary links for Server 1 and Server 2. Likewise, the primary links for Server 3 and Server 4 are through port 11 and 12 on Device 2 with secondary links to Device 1 through ports 5 and 6.

This example forces the servers to switch over to their secondary links when the uplinks become unavailable. In addition, it disables the secondary links when the uplinks are unavailable. Primary links are represented as solid lines, whereas secondary links are represented as dashed lines.

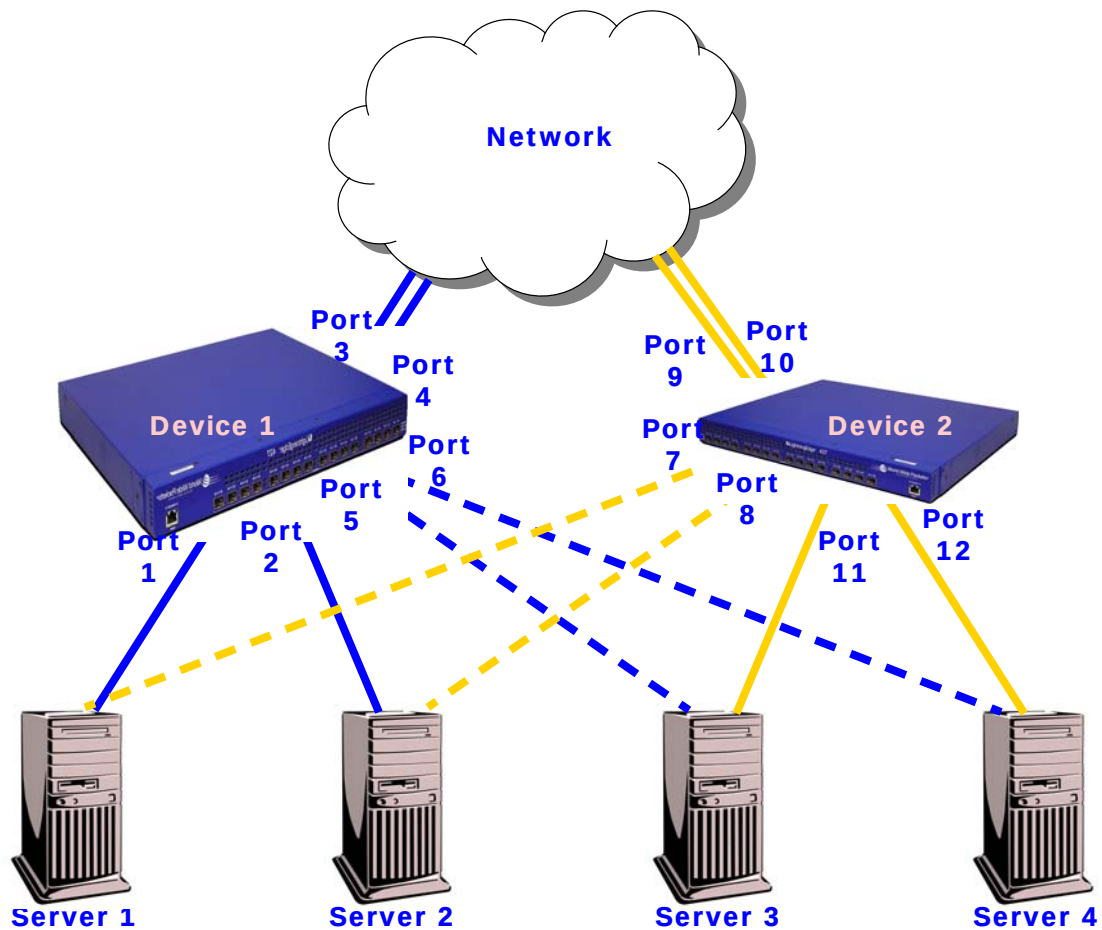


Figure 11-2: Configuring Port State Mirroring

Configuration steps:

This configuration example assumes the proper VLAN/port assignments have already been configured.

Step #	Description	Location/Command
Step 1	Create Port State Mirror Group PSMG1 on Device 1.	port state-mirror-group create <psmg-object (15)>
Step 2	Add source ports 3 and 4 and destination ports 1, 2, 5, and 6 to PSMG1.	port state-mirror-group add {[<psmg-src-group-attr>] [<psmg-dst-list-attr>]}

Step #	Description	Location/Command
Step 3	(optional) Verify that the ports have been assigned to the PSMG and that their operational status displays as Link Up.	port state-mirror-group show [<psmg-object>]
Step 4	Create Port State Mirror Group PSMG2 on Device 2.	port state-mirror-group create <psmg-object (15)>
Step 5	Add source ports 9 and 10 and destination ports 7, 8, 11, and 12 to PSMG2.	port state-mirror-group add {[<psmg-src-group-attr>] [<psmg-dst-list-attr>]}
Step 6	(optional) Verify that the ports have been assigned to the PSMG and that their operational status displays as Link Up.	port state-mirror-group show [<psmg-object>]

CLI Example:

Device 1

1. > port state-mirror-group create group PSMG1
2. > port state-mirror-group add group PSMG1 src-port 3,4 dst-port 1,2,5,6
3. > port state-mirror-group show

```
+----- PORT STATE MIRROR GROUPS -----+
| Name          | Collective | Member Counts |
| Name          | Oper State | Source        | Destination   |
+-----+-----+-----+-----+
| PSMG1         | Enabled   | 2             | 4             |
+-----+-----+-----+-----+
```

```
+----- PORT STATE MIRROR GROUPS MEMBERS -----+
| Port State Mirror Group | Port | Type | Oper State |
+-----+-----+-----+-----+
| PSMG1                   | 1    | Dst  | Link up   |
| PSMG1                   | 2    | Dst  | Link up   |
| PSMG1                   | 3    | Src  | Link up   |
| PSMG1                   | 4    | Src  | Link up   |
| PSMG1                   | 5    | Dst  | Link up   |
| PSMG1                   | 6    | Dst  | Link up   |
+-----+-----+-----+-----+
```

Device 2

1. > port state-mirror-group create group PSMG2
2. > port state-mirror-group add group PSMG2 src-port 9,10 dst-port 7,8,11,12

3. > port state-mirror-group show

PORT STATE MIRROR GROUPS			
		Collective	Member Counts
Name	Oper State	Source	Destination
PSMG2	Enabled	2	4

PORT STATE MIRROR GROUPS MEMBERS			
		Member	
Port State Mirror Group	Port	Type	Oper State
PSMG1	7	Dst	Link up
PSMG1	8	Dst	Link up
PSMG1	9	Src	Link up
PSMG1	10	Src	Link up
PSMG1	11	Dst	Link up
PSMG1	12	Dst	Link up

At a Glance:

- Overview
- Service Access Control
- User Management
- Service Access Control
- RADIUS
- TACACS+
- IP Access Control Lists

This chapter explains how to configure various security features of devices running SAOS. Security features are employed to prevent unauthorized access to network resources and to deployed services.

Overview

SAOS employs several methods to prevent unauthorized access to devices and to control the way that services are distributed through the network. Some features restrict certain types of protocols or packets, while others restrict port access. The following security features can be combined to provide an increased security level:

- Service Access Control- controls device access to the network.
- RADIUS- grants conditional access to configured users using Remote Authentication Dial In User Service (RADIUS).
- TACACS- performs authentication, authorization and accounting (AAA) functions using Terminal Access Controller Access Control System (TACACS).

Service Access Control

Service Access Control (SAC) provides a way to control packet forwarding based on MAC addresses. If a service provider knew the MAC address of every device connected to the network, packet forwarding could be strictly controlled. However, subscribers can connect a myriad of devices to the network. Keeping track of the changing list of these MAC addresses would be extremely difficult. Therefore, SAOS devices employ SAC to:

- Allow static MAC addresses.
- Control the number of dynamically learned MAC addresses on a per-port basis.

By configuring static MAC entries, security is provided to allow only those frames to be forwarded that have a source MAC address that is recognized by the device.

When an SAC entry is created, a maximum number of dynamic MAC addresses is entered for a specific port. Setting this limit specifies the number of dynamic MAC addressees without having to know their actual value. Once the limit is reached, additional MAC addresses will not be learned and frames from subsequent devices can be configured to either be forwarded or dropped. The learn limit does not apply to static MAC addresses. For example, if the learn limit is set to four, the device will learn the MAC addresses of the first four subscriber devices connected to the network and allow them to send frames, and can drop frames that come from a fifth device (assuming that all devices are connected to the network at the same time). Frames containing source addresses that match static addresses in the device will be forwarded, and are unaffected by the MAC limit set on the port.

A MAC aging timer can also be set for dynamically learned MACs, which clears entries from the MAC table when they have been inactive for the period of time specified. Static MAC addresses are never aged out. In the previous example, although only four devices may be connected to the network at one time, devices may be unplugged from the network and new devices (i.e., new MAC addresses) will be allowed once the old MAC address ages out.

It should be noted that limiting MAC addresses does not provide absolute security as a MAC address can still be spoofed (made to look like an authorized MAC address).

Benefits

SAC protects the Provider network from unauthorized access and can help prevent denial of service attacks. In addition, Service providers could use SAC to offer different subscriber access packages without having to know any specifics about the subscriber devices. For example, a SAC could be created for “Gold” level subscribers that allows them to connect up to 5 devices (i.e. 5 MAC addresses) to the network, while “Bronze” level subscribers are only allowed to connect 1 device to the network at a time.

Configuration

This section provides configuration examples for configuring SAC.



NOTE: The device is capable of learning a maximum of 16,000 dynamic MACs (32,000 on the CN 3960), which requires installation of the Advanced Ethernet (AE) license key. Without the AE license, the device is restricted to learning a maximum of 4,000 dynamic MACs. License keys can be purchased by contacting Ciena customer support.

Configuring Service Access Control with MAC Aging

In this first configuration example, an SAC entry is created on port 5 that limits the number of learned MAC addresses to 4. The MAC address of a set top box is also entered as a static MAC, and will not interfere with the maximum number of dynamic MACs set for the port. In addition, MAC address aging is enabled in order to allow dynamic MACs to age out. MAC address aging is an optional step.



NOTE: The MAC aging timer is configured for the entire device, it cannot be set on a VLAN or port basis. Depending on the location of this device in the network, changing the MAC aging timer may cause connectivity issues with critical devices. When changing the MAC aging timer, be certain that desirable devices will not be inadvertently aged out.



NOTE: In the following example, configuration settings are verified by using show commands. Although these steps are listed as optional, it is good practice to verify command settings using these commands.

Configuration steps:

Step #	Description	Location/Command
Step 1	Create the SAC entry for the port.	flow access-control create port <PortNo> {max-dynamic-macs <max-macs-value>} [forward-unlearned <on off>]
Step 2	Enable MAC aging. MAC aging is enabled by default.	flow aging {disable enable}
Step 3	Set MAC aging to 120 seconds. The default MAC aging timer is 300 seconds.	flow aging set time <10 - 1000000>}
Step 4	Enter the static MAC address. Note that in order to add a static MAC on port 5, the VLAN used must already be created and port 5 must be a member of the VLAN	flow static-mac add vlan <VlanID> mac <xx:xx:xx:xx:xx:xx> port <PortNo>}
Step 5	(Optional) Verify the SAC entry.	flow access-control show
Step 6	(Optional) Verify the MAC aging settings.	flow aging show
Step 7	(Optional) Verify the static MAC entry.	flow show static-mac

CLI Example:

1. > flow access-control create port 5 max-dynamic-macs 4
2. > flow aging enable
3. > flow aging set time 120
4. > flow static-mac add vlan 300 port 5 mac aa:bb:cc:dd:ee:ff
5. > flow access-control show

FLOW ACCESS-CONTROL TABLE					
Instance Type	Value	Dynamic Addresses		Threshold	Oper Status
		Maximum	Learned		
Port	5	4	0	Not Reached	Enabled

6. > flow aging show

FLOW AGING-INFO	
Parameter	Value
Status	Enabled
Time (Seconds)	120

7. > flow show static-mac

FLOW MAC-LEARN TABLE			
VLAN	Address (SA)	Port	Type
1	00:BB:CC:DD:EE:FF	1	Dyna
127	00:AA:CC:DD:EE:FF	1	Dyna
300	AA:BB:CC:DD:EE:FF	5	Stat

Configuring Static MACs and SAC on the Same Device

By using static or dynamic MAC entries, access to a service can be restricted. For instance, on port 5, to limit access to video services for a specific set top box, a static MAC address could be created for the STB, along with disabling MAC learning on the port by creating a SAC entry with a learn limit of 0. In this scenario, only the set top box would have access to the video services, and no other MACs would be serviced on the port.

On a different port, for example port 6, a SAC entry with a learn limit of 1 could be created for the port so that only one device, with a dynamic address, can be learned and serviced by the port

Note that disabling MAC aging will keep the learned MAC address in the MAC table until it is flushed by one of the following events:

- Using the `flow mac-addr flush` CLI command
- Spanning Tree topology change
- Link state change
- Reboot of device

In the following example, access to a port is limited to one device, such as a set top box, for ports 5 and 6.

On port 5, the device's MAC address is entered manually, no dynamic learning will take place on that port and no other devices will be accepted on this port. On port 6, the MAC address is learned dynamically, but MAC address aging is disabled for the device.

On port 6, if the Ethernet device is removed, its source MAC address will remain in the MAC Learning table until the MAC table is flushed. Until such time, the SAOS device will not forward packets from a different device on if it is attached to port 6.



NOTE: In the following example, configuration settings are verified by using show commands. Although these steps are listed as optional, it is good practice to verify command settings using these commands.

Configuration steps:

Step #	Description	Command
Step 1	Create the SAC entry. Set the maximum number of allowed MAC addresses to 0.	<code>flow access-control create port <PortNo> {max-dynamic-macs <max-macs-value>}</code>
Step 2	Enter the static MAC address. In order to add a static MAC on port 5, the VLAN used must already be created and port 5 must be a member of the VLAN	<code>flow static-mac add vlan <VlanID> mac <xx:xx:xx:xx:xx:xx> port <PortNo></code>

Step #	Description	Command
Step 3	(Optional) Verify the SAC entry.	flow access-control show
Step 4	(Optional) Verify the static MAC entry.	flow show static-mac
Step 5	Create a SAC entry and set the maximum number of allowed MAC addresses to 1.	flow access-control create port <PortNo> {max-dynamic-macs <max-macs-value>}
Step 6	Disable MAC aging. MAC aging is disabled by default.	flow aging disable
Step 7	(Optional) Verify the SAC entry.	flow access-control show

CLI Example:

1. > flow access-control create port 5 max-dynamic-macs 0
2. > flow static-mac add vlan 300 mac aa:bb:cc:dd:ee:ff port 5
3. > flow access-control show

FLOW ACCESS-CONTROL TABLE					
Instance	Dynamic Addresses		Oper		
Type	Value	Maximum	Learned	Threshold	Status
Port	5	0	0	Reached	Enabled

4. > flow mac-addr show

FLOW MAC-LEARN TABLE			
VLAN	Address (SA)	Port	Type
1	00:BB:CC:DD:EE:FF	1	Dyna
127	00:AA:CC:DD:EE:FF	1	Dyna
300	AA:BB:CC:DD:EE:FF	5	Stat

5. > flow access-control create port 6 max-dynamic-macs 1
6. > flow aging disable
7. > flow access-control show

FLOW ACCESS-CONTROL TABLE					
Instance	Dynamic Addresses		Oper		
Type	Value	Maximum	Learned	Threshold	Status
Port	6	1	0	Not Reached	Enabled

Configuring the Device to Forward or Drop Unknown Addresses

The Forward-Unlearned option allows for the Forwarding or Dropping of Unknown DA MACs, when the SAC limit has been reached on a port.

When the Forward-Unlearned option is turned **on**, and the maximum number of dynamic MACs have been learned on the port, additional MACs sent to the port, that are unknown to the device, will be flooded to all ports in the same broadcast domain (VLAN or Virtual Switch). When the Forward-Unlearned option is turned **off**, unknown DA MACs will be dropped instead of flooded.

The following CLI commands are used to turn the Forward-Unlearned option on or off:

```
> flow access-control create port 1 max-dynamic-macs 25 forward-unlearned on
> flow access-control create port 1 max-dynamic-macs 25 forward-unlearned off
```

Note that packets will be forwarded if an SA is unlearned and the table is full. Because the device learns at line rate, the `flow show mac-addr` command will lag behind the hardware when learning at a high rate.

User Management

Telnet access to the CLI through user accounts can be limited. When logging in, users are asked to supply a user name and a password. If they do not supply the correct password, or the user account does not exist, they will be denied access. The user account password can be specified as a secret (encrypted) or as clear text in order to ensure that the password cannot be easily viewed.

When a user account is created, it is assigned a privilege level. The privilege level determines the access rights for that user. The CLI provides the following user privilege levels:

- **Limited User** - can only execute commands that show system configuration information but cannot change the configuration of the device.
- **Super User** - includes all the privileges of the limited user, can make system configuration changes, and perform execute commands.

At least one of each type of user must be configured on the device. To delete a default user, the network operator must first create a user of the same type and then delete the default account. This ensures that the network operator controls access rights to the device.

Two user names/passwords are provided by default:

User Name	Privilege Level	Password	Access Rights
su	Super User	wwp	Read/Write
user	Limited User	<empty>	Read-Only

If a user password is forgotten, it cannot be retrieved. However, a super user can assign the user a new password or the user can be deleted and added again with a different password.

NOTE: When you create users and save the configuration, the `user create user` command is saved in the `SECURITY CONFIG:` section of the configuration file. The plain text password is encrypted and saved with the attribute of `secret`. For example:
`user create user superuser1 access-level super secret`
`abcd1234467890e`

You can copy this line from the configuration file of one device to the configuration file of another device to ensure the user is configured the same on both devices. The user will be able to log on to both devices with the same plain text password.



Feature Benefit

Controlling device access through user accounts enables the network operator to expressly define those users that can view configuration information and those that can view and modify configuration information.

Configuring Users

If your user ID has super access level, you can create users with limited (read-only) or super (read/write) access level. User names and passwords are case sensitive and are limited to a length of 16 characters. Also, you can delete users. Before deleting a default user, create a user of the same type and then delete the default account. If a user forgets their password, it cannot be retrieved. However, you can assign the user a new password or delete the user and create it again with a different password. When you create users and save the configuration, the user create user command is saved in the SECURITY CONFIG: section of the configuration file. The plain text password is encrypted and saved with the attribute of secret. For example:

```
user create user superuser1 access-level super secret
abcd1234467890e
```

You can copy this line from the configuration file of one device to the configuration file of another device to ensure the user is configured the same on both devices. The user will be able to log on to both devices with the same plain text password. Optionally, you can create or update users to use the secret attribute to use a pre-encrypted password.

To configure a user account:

Step #	Description	Command
Step 1	Create the user account, specifying a name, access level, and password.	<code>user create user <String[16]></code>
Step 2	(Optional) Verify the account creation.	<code>user show</code>

The following example creates 2 users, one with super user privilege and the other with limited user access level.

CLI Example:

```
> user create user MIS access-level super password 2manysecrets
> user create user data access-level limited password blue32
> user show
+-----+ USER ACCOUNT TABLE +-----+
| Username | Privilege | Flags |
+-----+-----+-----+
| MIS      | super    | P     |
| data     | limited  | P     |
| su       | super    | DP    |
| user     | limited  | D     |
+-----+-----+-----+
```



NOTE: The DP and D shown in the Flags column above indicates that an account is a default account. These accounts may be deleted if desired, however one active user account of each privilege level must always exist.

Displaying Users

If your user ID has super or limited user access, you can display created users, users who are currently logged on, and your own user name and access level.

To display all created users:

```
> user show
+-----+ USER ACCOUNT TABLE +-----+
| Username | Privilege | Default |
+-----+-----+-----+
| su       | super    | *       |
| user     | limited  | *       |
+-----+-----+-----+
```

To display all users currently logged on to the device:

```
> user who
+-----+-----+-----+-----+
| Username | Idle Time | Pid | Terminal |
+-----+-----+-----+-----+
| su       | 0m       | 131204 | /telnet_192.168.3.153:1287 |
| su       | 0m       | 196735 | /telnet_192.168.3.153:1116 |
+-----+-----+-----+-----+
```

To display your user name and access level:

```
> user whoami
username: su access-level: super
```

Configuring Authorization Providers

Three methods of user authorization are supported: local, RADIUS, and TACACS+, and separate authorization methods can be set for the serial port and remote access (Telnet). By default, the local user database only is used for authorization.

You can configure the device to use a backup authorization method and priority. The backup authentication method will only be used if the primary authentication method does not complete because a server is not available (not configured, not enabled, or failed to contact as in a communication error). If the server is contacted and the authentication is denied (not allowed), the secondary method will not be called.

For a given authentication method, the scope defines the method called dependent upon the source of the login attempt. For a scope policy equal to "remote", the authentication method will only be called for login attempts originating from either the local or remote management interfaces. For a scope policy equal to "serial", the authentication method will only be called for login attempts originating from the serial port. For a scope policy of "all", the authentication method will be called for all management interfaces, remote, local and serial. In all cases, the priority backup authentication rules described above apply.

CLI Example:

To set the authorization scope, priority, and method:

```
user auth set [scope <all|serial|remote>] [priority <NUMBER: 1...3> ]
[method <none|local|radius|tacacs>]
```

To display authorization providers and statistics:

```
> user auth show
+-----+-----+-----+-----+-----+-----+
| Priority | Method | Called | Success | Failure | Skipped | Scope |
+-----+-----+-----+-----+-----+-----+
| 1       | local  | 6      | 5       | 1       | 0       | all   |
+-----+-----+-----+-----+-----+-----+
```

To specify separate TACACS and serial authentication methods. There will be no backup for TACACS, and the TACACS server will only be used for local and remote login attempts. The local DB will be used only for serial port login attempts:

```
> user auth set priority 1 method tacacs scope remote
> user auth set priority 2 method local scope serial
```

To specify TACACS server used only for local and remote interface login attempts and use the local DB for serial port and primary backup login attempts:

```
> user auth set priority 1 method tacacs scope remote
> user auth set priority 2 method local scope serial
```

To clear authorization statistics:

```
> user auth clear [priority <NUMBER 1-3>]
```

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a client/server system used to secure networks against unauthorized remote access such as with Telnet. When authenticating a telnet user, the device sends authentication requests to a RADIUS server or servers. The RADIUS servers keep track of all user authentication and service access information. The RADIUS server returns authentication results to the device and the user is either allowed or denied access based on this information.

RADIUS servers are also used as the preferred server for 802.1x authentication. The 802.1x framework uses RADIUS messages for communication between the authenticator and the authentication server. For this purpose, RADIUS configuration includes a parameter that allows the RADIUS server to be designated strictly as a user authentication server, an 802.1x authentication server, or both.

Feature Benefit

RADIUS servers allow the network operator to configure and control user accounts in one central location instead of having to configure accounts on every device on the network. RADIUS enables access and authentication control to be very flexible in the way it regulates access.

Configuring RADIUS

RADIUS can be enabled/disabled either on a global basis or on a server by server basis. By default RADIUS is globally enabled. When a RADIUS server is configured on the device, that server is enabled by default. The destination UDP port number for the server can also be specified. If it is not specified, the default port number of 1812 will be used. A specific priority that controls the order in which servers are contacted can be set for each server, if desired. The server priority continues sequentially and increases or decreases automatically so there are no gaps in server priority. If a new server is added without specifying a priority, it is assigned a priority based on the last server present in the list.

In addition, the servers can be searched by their priority or cached value (last accessed). Also, the authentication key can be specified in MD5 encrypted format rather than clear text.

Various attributes can be set that determine how the device interacts with configured RADIUS servers:

Field	Description
Timeout	Length of time, in seconds, that the device will wait for a response from the RADIUS server.
Retries	Number of times the client should attempt to contact the RADIUS server before declaring it unreachable.
Key	The authentication string used to verify that the device is authorized to access the RADIUS server. The key must be between 8 and 128 characters in length and must be the same for all RADIUS servers specified.

The following example enters a RADIUS server, and then sets the global parameters for using RADIUS authentication.



NOTE: In the following example, configuration settings are verified by using show commands. Although these steps are listed as optional, it is good practice to verify command settings using these commands.

To configure a RADIUS server and client:

Step #	Description	Command
Step 1	Enable RADIUS globally.	<code>radius enable [server <IpHostRadius>]</code>
Step 2	Add a RADIUS server.	<code>radius add server <IpHost></code>
Step 3	(Optional) set the RADIUS server's attributes.	<code>radius set</code>
Step 4	(Optional) Verify RADIUS configurations.	<code>radius show [stats]</code>
Step 5	(Optional) Check the RADIUS server statistics.	<code>radius show [stats]</code>

CLI Example:

```
> radius enable
> radius add server 10.10.10.100
> radius set server 10.10.10.100 use-for user-login
> radius set key 2manysecrets retries 2 timeout 2
> radius set search-method cached
> radius show
```

```
+-- RADIUS ATTRIBUTES --+
| Parameter | Value |
+-----+-----+
| Admin State | Enabled |
| Oper State | Enabled |
| Retries | 3 |
| Timeout | 1 |
| Key | ***** |
| Search type | Cached |
+-----+-----+
```

```
+----- RADIUS SERVER TABLE -----+
| IP Address | HostName | Pri | UDP | State | App |
| | | | Port | | |
+-----+-----+-----+-----+-----+
| 10.10.10.100 | | 1 | 1812 | Ena | User-login |
+-----+-----+-----+-----+-----+
```

```
> radius show stats
+----- Radius Server Statistics -----+
+-----+
| IP Address : 10.10.10.100 |
| Access Requests : 971 |
| Access Rejects : 0 |
| Access Accepts : 971 |
| Access Challenges : 0 |
| Access Retransmission : 0 |
| Bad Authenticators : 0 |
| Pending Requests : 0 |
| Packets Dropped : 0 |
| Malformed Responses : 0 |
+-----+
```



NOTE: If the RADIUS server does not respond to requests or is not accessible, the only way to access the device is through SNMP/EMS unless you have configured the authorization provider to use the local database as a second priority authorization method.

TACACS+

TACACS+ is a security protocol that performs the following AAA functions between a Network Access Server (NAS) and an authentication server:

- Authentication—Grants users access when they first log in to a device or request a service.
- Authorization—Determines which actions users are allowed to perform when they do have access to a device. Authorization will be performed only if authentication was done by TACACS+.
- Accounting—Records user actions in order to perform security audits or for billing purposes. Accounting will be performed only if authentication was done by TACACS+.

The TACACS+ protocol client is supported where the device operates as a NAS. The TACACS+ client can be configured to support up to 8 authentication, authorization and accounting servers via the CLI or SNMP. If a TACACS+ server is not configured, a locally configured password file is used for authentication. Local authentication is used only if the user authentication provider order is configured properly to allow for it.

NOTE: TACACS+ is not compatible with previous TACACS and XTACACS protocols.

Feature Benefit

TACACS+ provides an industry standard means of controlling AAA functions. It also provides security by using a shared key to encrypt information between the NAS and the authentication server.

Configuring TACACS+

TACACS+ can be enabled/disabled on a global basis, and can also be enabled on specific Authentication, Authorization or Accounting servers. (Note that authentication must be enabled for Authorization or Accounting to be operational.)



NOTE: To configure TACACS+, you need to install the Advanced Security license key. To obtain the Advanced Ethernet license key, contact Ciena Sales.

By default TACACS+ is globally enabled, only Authentication is enabled, and no default TACACS+ servers are configured. Up to 8 servers can be configured for each of the individual AAA functions and the global lists. If the authentication, authorization, or accounting server list cannot be used or has no specified servers, the global list will be used by default. The global list will also be used if no TACACS+ authentication, authorization or accounting servers are specified. In addition, the servers can be searched by their priority or cached value (last accessed).

Each TACACS+ server has a unique priority number within the specific AAA/or global list between 1 and 8, where 1 is the highest priority. The server priority continues sequentially and increases or decreases automatically so there are no gaps in server priority. If a new server is added without specifying a priority, it is assigned a priority based on the last server present in the list. In addition to priority, the TCP port number can be specified for each server. If it is not specified, the default port number of 49 is used.

When performing authentication, the login password allows all ASCII values from 32 to 126 except ASCII 34 ("). This is because passwords that contain a space (ASCII 32) must be enclosed in quotes, and the quotes are removed prior to encryption. Also, spaces at the beginning or end of the password are discarded, and should not be used. In addition, the password can be specified as a secret (encrypted) as well as clear text.

Authentication will fail under the following circumstances:

- The TACACS server operational state is DISABLED
- The number of authentication retries has been met

If all servers have been tried without success, or if a server rejects the user credentials, then the authentication is considered to have failed. The user login/authentication attempt is denied.

Authenticated users can execute commands and their associated arguments, and these are passed as fully expanded CLI commands to the TACACS+ server. Attribute-Value types other than "cmd" and "cmd-arg" are not supported.

When session and command accounting are enabled, start and stop messages are sent for each login session and command that is executed. TACACS+ statistics can be viewed and cleared.

The following example creates 3 TACACS+ servers to be used for authentication, sets the global parameters for using TACACS+ authentication, and then enables AAA.



NOTE: In the following example, configuration settings are verified by using show commands. Although these steps are listed as optional, it is good practice to verify command settings using these commands.

To configure TACACS+:

Step #	Description	Command
Step 1	Configure the list of TACACS+ servers.	<code>tacacs add server <IP address or host name></code>
Step 2	Enable TACACS+ globally.	<code>tacacs enable [server <IP address or host name>]</code>
Step 3	Set the global TACACS+ attributes.	<code>tacacs set</code>
Step 4	Enable authentication.	<code>tacacs authentication <disable enable></code>
Step 5	Enable authorization.	<code>tacacs authorization <disable enable></code>
Step 6	Enable accounting.	<code>tacacs accounting <disable enable></code>
Step 7	Enable or disable Syslog.	<code>tacacs syslog <disable enable></code>
Step 8	(Optional) Verify TACACS+ configurations.	<code>tacacs show [statistics]</code>

CLI Example:

```
> tacacs add server 10.10.10.100
> tacacs add server 10.10.10.200
> tacacs enable
> tacacs set key 543432
> tacacs set retries 2
> tacacs set timeout 24
> tacacs set privilegelvlrw 3
> tacacs set server 10.10.10.200 priority 1
> tacacs authentication enable
> tacacs authorization enable
> tacacs accounting enable
```

IP Access Control Lists

An IP Access Control List (IP-ACL) provides basic security for IP Protocols that terminate within the device. When IP-ACLs are enabled, the IP source address and (optionally) the ingress physical port number of incoming IP frames are compared to an ACL that defines combinations that are allowed to communicate with the device. Frames containing items that do not match a configured ACL entry are discarded.

NOTE: Be careful to not enable the IP-ACL feature without ensuring that the IP addresses/subnets are configured correctly or you have local or serial access to the device, as you might not be able to reach the device once IP-ACLs are enabled. This can affect all communications to the remote management interface which includes TWAMP, SNMP, MPLS signalling, etc.

Feature Benefit

IP-ACLs control inbound access to the device, preventing unauthorized IP addresses from communicating with the device.

Configuring IP-ACL

The IP-ACL feature is controlled via a global enable setting. When the feature is disabled, incoming frames are not examined. When enabled, a default drop entry is enabled, with individual IP-ACL entries specifying exceptions to the drop entry. Incoming frames are then tested against a table of configured IP-ACL entries to determine their eligibility for further processing.

IP-ACL entries can be added to the table and must contain, at a minimum, an IP source address (IP-SA) and IP mask (IP-MASK). A list of allowed ingress ports can optionally be specified when an IP-ACL entry is added. This list defines which specific hardware ports of the device the frame can be accepted from. A port list can be specified as a single port number, a comma separated list of port numbers, a port range, or some combination of these. If not specified, frames can ingress from any valid port.

The IP address and IP mask information for interfaces that are configured on the device can be imported into the IP-ACL access list table. This way, the IP-ACL table can be pre-loaded to avoid being locked out of the device when the IP-ACL feature is enabled.

Existing IP-ACL entries can be modified to alter their optional parameters, but not their IP-SA or IP-MASK. Existing IP-ACL entries can be removed by specifying their IP-SA and IP-MASK.

To configure IP-ACL:

Step #	Description	Command
Step 1	Configure an ACL.	<code>interface ip-acl add</code>
Step 2	Enable IP-ACL globally.	<code>interface ip-acl enable</code>
Step 3	(Optional) View the IP-ACL configuration.	<code>interface ip-acl show</code>
Step 4	(Optional) Import the IP addresses and IP mask of configured interfaces.	<code>interface ip-acl import</code>
Step 5	(Optional) Clear IP-ACL statistics.	<code>interface ip-acl clear statistics</code>

CLI Example:

In this example, there is only 1 host IP address that can match this ACL:

```
> interface ip-acl add ip 10.10.10.100 netmask 255.255.255.255
> interface ip-acl enable
> interface ip-acl show
> interface ip-acl clear statistics
```

In this example, the valid hosts range from 10.10.10.1 through 10.10.10.255 and source from either port 27 or port 28:

```
> interface ip-acl add ip 10.10.10.0 netmask 255.255.255.0 port 27,28
> interface ip-acl enable
```

In this example, the IP addresses and IP mask of configured interfaces are imported into the IP ACL list:

```
> interface ip-acl import
> interface ip-acl enable
```


Chapter Configuring Broadcast Containment

13

At a Glance:

- Overview
- Benefits
- Configuring Broadcast Containment
- Troubleshooting

This chapter how to configure broadcast containment.

Overview

Broadcast containment prevents services from being disrupted by broadcast storms on specified ports. A broadcast storm occurs when broadcast packets flood the network, creating excessive traffic and degrading performance. When a broadcast filter is created and one or more ports are added to it, the device monitors incoming broadcast packets for a specified period of time. Broadcast packets exceeding the configured threshold are dropped. SNMP traps are sent when the configured broadcast threshold is exceeded and when broadcast traffic goes below the configured threshold.

The system software supports containment rates for the following flood traffic types:

- Unknown unicast traffic
- Layer 2 Broadcast traffic
- Layer 2 Unknown Multicast traffic

Benefits

Broadcast containment prevents services from being disrupted by Layer 2 broadcast storms and Denial of Service (DoS) attack.

Configuring Broadcast Containment

The system software supports one broadcast containment filter for each port.



NOTE: To enable broadcast containment commands, the Advanced Ethernet feature license must be installed with the `software license install` command.

Enabling and Disabling Broadcast Containment

By default, broadcast containment is disabled.

To enable broadcast containment:

```
broadcast-containment enable
```

Example:

```
> broadcast-containment enable
```

To disable broadcast containment:

```
broadcast-containment disable
```

Example:

```
> broadcast-containment disable
```

Creating a Broadcast Containment Filter

When creating a broadcast containment filter, you specify a filter name and set the containment rate. These attributes are as follows:

- **filter** - Unique name for the broadcast containment filter.
- **kbps** - Rate from 0-10000000 in kilobits per second.
- **port** - List of ports to apply the filter to.
- **containment-classification** - Specifies one or more flood traffic types to filter, Unknown unicast traffic (unknown-ucast), Layer 2 Broadcast traffic (bcast), or Layer 2 Unknown Multicast traffic (l2-mcast). By default, the filtered traffic types are Layer 2 Broadcast traffic (bcast) and Layer 2 Unknown Multicast traffic (l2-mcast).



NOTE: If you downgrade to a software release prior to 6.5, any containment classification settings you configure will be lost, and filtered traffic types will revert to Layer 2 Broadcast traffic (bcast) and Layer 2 Unknown Multicast traffic (l2-mcast).

The maximum number of filters that can be created per platform is as follows:

- CN 3911 - 15
- CN 3920 - 18
- CN 3940 and CN 5140 - 36
- CN 3960 - 18

To create a broadcast containment filter:

```
broadcast-containment create {filter <String [15]>} [kbps <NUMBER: 0-10000000>]
[port <PortNameList>] [containment-classification <[bcast],[l2-mcast],[unknown-
ucast]>]
```

Example:

```
> broadcast-containment create filter denial kbps 2000 port 1
```

Setting Broadcast Containment Filter Attributes

After creating a filter, you can update the containment rate and rename it.

To set broadcast containment profile attributes:

```
broadcast-containment set {filter <FilterName>} kbps <NUMBER: 0-10000000> name
<String [15]> <[bcast],[l2-mcast],[unknown-ucast]>]
```

Example:

```
> broadcast-containment set filter denial kbps 1000 containment-classification
bcast,l2-mcast,unknown-ucast
```

Deleting a Broadcast Containment Filter

You can delete a broadcast containment filter.

To delete a broadcast containment filter:

```
broadcast-containment delete {filter <String>}
```

Example:

```
> broadcast-containment delete filter denial
```

Adding Ports to a Broadcast Containment Filter

After creating a broadcast containment filter, you can add additional ports to it.



NOTE: Multiple ports can be added to a filter, but only one filter may be applied to a specific port at a time. Also, when multiple ports are added to a filter, the bandwidth for the filter is shared among the ports.

To add a port to a broadcast containment filter:

```
broadcast-containment add filter <String> port <PortNameList>
```

Example:

```
> broadcast-containment add filter denial port 5
```

Removing Ports from a Broadcast Containment Filter

You can remove ports from a broadcast containment filter.

To add a port to a broadcast containment filter:

```
broadcast-containment remove filter <String> port <PortNameList>
```

Example:

```
> broadcast-containment add filter denial port 5
```

Sample Configuration

The following example creates a Broadcast Containment filter that limits the number of broadcast packets received on port 10 to 2000 kbps.

To configure broadcast containment:

Step #	Description	Command
Step 1	Enable broadcast containment.	broadcast-containment enable
Step 2	Create the broadcast containment filter. Step 2, 3, and 4 may be combined into a single step.	broadcast-containment create
Step 3	Set the containment rate and classification for the filter.	broadcast-containment set
Step 4	Add port 10 to the filter.	broadcast-containment add

CLI Example:

1. > broadcast-containment enable
2. > broadcast-containment create filter denial
3. > broadcast-containment set filter denial kbps 2000 containment-classification l2-mcast
4. > broadcast-containment add filter denial port 10

Troubleshooting

Displaying Broadcast Containment Filters

To display broadcast containment status and a summary of broadcast containment filters:

```
broadcast-containment show
```

Example:

```
> broadcast-containment show
+----- Broadcast Containment Globals -----+
|           Parameter           |           Value           |
+-----+-----+-----+-----+
| Admin Status                   | Enabled                    |
+-----+-----+-----+-----+

+----- Broadcast Containment Filters -----+
|           Filter           |           ID           | Kbps | Dropping |
+-----+-----+-----+-----+
| Denial                        | 1                       | 2000 | No       |
+-----+-----+-----+-----+
```

To display details about a specific broadcast containment filter:

```
broadcast-containment show [filter <FilterName>]
```

Example:

```
> broadcast-containment show filter denial
+----- Broadcast Containment Filter -----+
| Parameter                     | Value                     |
+-----+-----+-----+-----+
| Filter Name                   | denial                    |
| Index                         | 1                         |
| Kilobits Per Second (Kbps)   | 2000                     |
| Broadcast                     | Off                      |
| L2 Multicast                  | On                       |
| Unknown Unicast               | Off                      |
+-----+-----+-----+-----+

+----- Associated Members -----+
|                               |                           |
| Port 10                      |                           |
+-----+-----+-----+-----+
```

To display filter membership for specified ports:

```
broadcast-containment show [port <PortNameList>]
```

Example:

```
> broadcast-containment show port 1
+-----+-----+-----+-----+
|          Port          |          Filter          |
| Name      | Description      | Name      | ID      |
+-----+-----+-----+-----+
| 1          | test             | denial    | 1       |
+-----+-----+-----+-----+
```

Displaying Broadcast Containment Configuration in the Configuration File

Broadcast containment configuration is saved to the configuration file in the BCAST FILTER CONFIG: section.

To display broadcast containment configuration in the configuration file:

```
> configuration show
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! NETWORK CONFIG:  vlans!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! BCAST FILTER CONFIG:
!
broadcast-containment create filter denial kbps 2000
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```


Chapter Quality of Service

14

At a Glance:

- Overview
- Ingress Resolved CoS Mapping
- Traffic Profiling
- Ingress R-CoS to Egress CoS Queue Mapping
- Congestion Avoidance
- Egress Scheduling
- Egress Shaping
- Configuring Frame Bandwidth Calculation

This chapter details Quality of Service (QoS) features of the system software. QoS refers to the management of bandwidth to ensure that network traffic is allocated the desired amount of network resources.

Overview

This chapter describes the mechanisms for managing bandwidth, including:

- Ingress Resolved Class of Service Mapping - applies a Resolved CoS Policy.
- Traffic Profiling - provide ingress traffic classification and metering.



NOTE: To configure traffic profiling, you need to install the Advanced Ethernet license key. To obtain the Advanced Ethernet license key, contact Ciena Sales.

- Ingress R-CoS to Egress CoS queue mapping — assigns traffic to CoS queues based upon R-CoS values.
- Congestion avoidance processing — method for managing CoS queue traffic when congestion occurs on egress.



NOTE: To enable configurable congestion avoidance, you need to install the Advanced Ethernet license key. To obtain the Advanced Ethernet license key, contact Ciena Sales.

- Egress Scheduling — determines the order in which the physical queues are processed.
- Egress Shaping - controls bandwidth for taking frames out of queues at egress.
- Configurable frame bandwidth calculation — configure whether to use the inter-frame-gap (IFG) in the calculations for ingress metering and egress shaping.

Ingress Resolved CoS Mapping

The system software associates an internal Resolved CoS (R-CoS) value and Resolved Color (R-COLOR) with every ingress frame that classifies to a port. The R-CoS and R-COLOR values provide the baseline for CoS treatment of a frame as it switches through the device. The R-CoS value ranges from 0-7, where 7 has the highest priority and 0 has the lowest priority. R-COLOR values are green, yellow or red. The initial R-CoS and R-Color values depend upon the configuration of the Resolved CoS Policy.



NOTE: The Resolved CoS policy on a port is ignored when it is involved in one or more virtual switch (subscriber) memberships. With that configuration, the R-CoS is determined by the encap CoS policy (and priority) that is configured at the virtual switch. However, when the encap CoS policy configured on a Virtual Switch Member is port-inherit, the Resolved CoS Policy is not ignored.

Configuring Resolved CoS Policies

The Resolved CoS Policy defines how the internal R-CoS value is determined and is applied per port as follows:

- Fixed (fixed-cos)- CoS values in the frame are ignored and fixed R-CoS and R-COLOR are applied to the frame from the Fixed Resolved CoS value for the port. When this policy is applied, CoS mapping is in untrusted mode. The default Fixed Resolved CoS value is 0.
- Outer .1D mapped (dot1d-tag1-cos)- The PCP/L2 CoS value from the outer-tag is mapped to an R-CoS value derived from the Resolved CoS Mapping table. When this policy is applied, CoS mapping is in trusted mode.
- Layer 3 DSCP CoS (l3-dscp-cos) - The Differentiated Services Code Point CoS value from the Layer 3 Type Of Service (TOS) byte is mapped to an R-CoS value from the Resolved CoS Mapping table. When this policy is applied, CoS mapping is in trusted mode.
- The default Resolved CoS Policy for all ports is Outer .1D mapped. The default Resolved CoS Map is shown in **Table 14-1**, in this chapter.

Table 14-1: Default Resolved Cos Map

PCP/L2 CoS Type	Frame CoS	R-CoS	R-Color
0	0	0	Green
1	1	1	Green
2	2	2	Green
3	3	3	Green
4	4	4	Green
5	5	5	Green
6	6	6	Green
7	7	7	Green
Untagged	Untagged	Ingress port fixed .1D value	Green

To set the Resolved CoS Policy:

```
port set port <PortNameList> [resolved-cos-policy <dot1d-tag1-cos|fixed-cos|l3-dscp-cos>]
```

Example:

```
> port set port 1 resolved-cos-policy dot1d-tag1-cos
```

To set the Fixed Resolved CoS:

```
port set port <PortNameList> [fixed-rcos <NUMBER: 0-7>]
```

Example:

```
> port set port 1 resolved-cos-policy dot1d-tag1-cos
```

To display the Resolved CoS Policy and Fixed Resolved CoS settings of a port:

```
port show port <PortName>
```

Example:

```
> port show port 1
```

PORT INFO		
Field	Admin	Oper
Type	10/100/G	
Description		
Spanning Tree State	Disabled	
MAC Address	00:03:18:43:de:b2	
Phy Loopback	Off	
Link State	Enabled	Disabled
State Group Link State		
Mode	rj45	unknown
Speed	1 Gbps	0 Gbps
Duplex	full	
Flow Control	off	
Auto Negotiation	Enabled	
Flow Control Advertised	off	
PVID	1	1
Untag Ingress Vtag	1	1
Untag Ingress Data Vid	0	0
Fixed Resolved CoS	0	0
Ingress VLAN Filter	Enabled	Enabled
Ingress VS Filter	Off	Off
Acceptable Frame Type	all	all
Egress Untag VLAN	1	1
Max Frame Size	1526	1526
Untagged Data VS		
Untagged Ctrl VS		
Resolved CoS Policy	dot1d-tag1-cos	dot1d-tag1-cos
Service Port Type	Subscriber	Subscriber
Eth VC EtherType	8100	8100
Eth VC EtherType Policy	all	all
Mirror-port	Off	Off
Ingress-mirror		
Egress-mirror		
Ingress to Egress QMap	Default-RCOS	Default-RCOS
XCVR caps mismatch	<NONE>	

Traffic Profiling

Traffic profiling classifies ingress traffic based upon each frame's CoS value and compares the traffic flow to a configured Committed Information Rate (CIR) and Peak Information Rate (PIR) defined in kilobits per second (kbps). Depending upon how the traffic flow compares to these rates, the R-COLOR of each frame is set to a specific value upon ingress. Traffic ingressing at a rate:

- Up to CIR will be marked Green and allowed through.
- Above CIR and less than PIR will be marked Yellow and allowed through.
- Above PIR will be marked Red and dropped.



NOTE: On a 100 Mbps port the CIR cannot be set to the full amount of physical bandwidth of the port (100 Mbps). This is because 1 Mb of bandwidth is reserved for the ingress and egress of BPDUs and other high priority traffic. To commit all of the physical bandwidth to a CIR could create a serious condition in which the device does not receive critical frames. To avoid this issue, the CIR should only be configured to a maximum of 99 Mbps.

Enabling and Disabling Traffic Profiling

Traffic profiling can be enabled per port and globally. By default, traffic profiling is disabled both globally and per port.

To enable traffic profiling:

```
traffic-profiling enable [port <PortNameList>]
```

To display the global and per port status of traffic profiling:

```
traffic-profiling show
```

Example:

```
> traffic-profiling show
```

```
+-----+-----+
| Profiling Status | Disabled |
+-----+-----+

+-----+-----+
| Port | Status | Mode |
| Admin | Oper  |      |
+-----+-----+
| 1 | Disabled | Disabled | standard-dot1dpri |
| 2 | Disabled | Disabled | standard-dot1dpri |
| 3 | Disabled | Disabled | standard-dot1dpri |
| 4 | Disabled | Disabled | standard-dot1dpri |
| 5 | Disabled | Disabled | standard-dot1dpri |
| 6 | Disabled | Disabled | standard-dot1dpri |
| 7 | Disabled | Disabled | standard-dot1dpri |
| 8 | Disabled | Disabled | standard-dot1dpri |
| 9 | Disabled | Disabled | standard-dot1dpri |
| 10 | Disabled | Disabled | standard-dot1dpri |
+-----+-----+
```

Configuring Per Port Attributes

Traffic profiling can be configured per port with the following attributes:

- **arp-standard-profile** - Sets whether non-conforming ARP frames are associated with an existing standard profile or bypass traffic profiling. ARP frames are treated specially because they are required for IP networks to function. Dropping ARP frames would result in breaking an IP network. The default setting is bypass.
- **meter-pool** - A meter pool provides the meter resources for traffic profiles. The system provides 8 meter pools with each containing 64 meters. A single traffic profile consumes 1 meter. You can change the meter pool for a given port as long as there are enough resources in the newly assigned meter pool. A given port can only be assigned to one meter pool.
- **mode** - The mode sets the inspection point for the remarking:
 - **standard-dot1dpri** - Finds a matching traffic profile using 802.1D priority. This mode is the default.
 - **standard-ip-prec** - Finds a matching profiling using the upper 3 bits of the TOS byte that make up the IP precedence.
 - **standard-dscp** - Finds a matching profiling using the DSCP value.
 - **standard-vlan** - Finds a matching profiling based upon the VLAN ID.
 - **standard-vlan-dot1dpri** - Finds a matching profiling based upon the VLAN ID and outer .1D priority value in the frame.
 - **standard-vlan-ipp** - Finds a matching profiling based upon the VLAN ID and ip-precedence value in the frame.
 - **standard-vlan-dscp** - Finds a matching profiling based upon the VLAN ID and the DSCP value in the frame.
- **nonconform-standard-profile** - Sets whether non-conforming frames (that are not ARP) are associated with a standard profile or dropped. Non-conforming frames are those ingressing frames that do not match one of the configured per-port traffic profiles. For example, non-conforming 802.1D priority frames are those frames that do not have a matching 802.1D priority configured in one of the traffic profiles. The same applies to DSCP (no matching 6 bit code point), and IP-Precedence (no matching 3 bit IP Precedence value). Note that certain frames, such as ARPs and non-IP frames, will always be non-conforming because these frames do not contain the DSCP field. The default setting is drop.

To set the per port attributes:

```
traffic-profiling set port <PortName> {[arp-standard-profile <bypass|<Traffic
ProfilingStandardName>], [meter-pool <TrafficProfilingMeterPoolName>], [mode <standard-
dot1dpri|standard-ip-prec|standard-dscp|standard-vlan|standard-vlan-dot1dpri|standard-vlan-
ipp|standard-vlan-dscp], [nonconform-standard-profile
<drop|<TrafficProfilingStandardName>>]}
```

Example:

```
> traffic-profiling set port 1 arp-standard-profile bypass meter-pool TP-POOL1 mode standard-
vlan nonconform-standard-profile drop
```

To display per port attributes:

```
traffic-profiling show
```

Example:

```
> traffic-profiling show port 1
```

+----- TRAFFIC PROFILING TABLE -----+		
Port	1	
Profiling Admin State	Disabled	
Profiling Oper State	Disabled	
Profiling Mode	standard-dot1dpri	
Meter Pool	TP-P00L3	
Non-Conform Standard Profile	drop	
ARP Standard Profile	bypass	
+-----+		

To display meter pool assignments for all ports:

```
traffic-profiling show meter-pool
```

Example on CN 3920:

```
> traffic-profiling show meter-pool
```

+----- TRAFFIC-PROFILING METER-POOL MAP -----+				
Meter-Pool	Ports	Total	Used	
+-----+				
TP-P00L1		64	0	
+-----+				
TP-P00L2		64	0	
+-----+				
TP-P00L3	1 2	64	0	
+-----+				
TP-P00L4	3 4	64	0	
+-----+				
TP-P00L5	5 6	64	0	
+-----+				
TP-P00L6	7 8	64	0	
+-----+				
TP-P00L7	9 10	64	0	
+-----+				
TP-P00L8	11 12	64	0	
+-----+				

Configuring Standard Profiles

Standard profiles define the CoS values for classification and metering rates. You can configure up to 64 standard profiles per port with a maximum of 512 standard profiles per system and a maximum of 64 profiles per metering pool:

- **profile** - If a name is specified and Profile ID is not, a Profile ID will be automatically picked for the traffic profile.
- **dot1dpri** - Classifies to the traffic profile based on 802.1d priority value ranging 0-7. Up to 8 classifiers are supported per port. (Optional)
- **ip-prec** - Classifies to the traffic profile based on IP precedence value ranging 0-7. Up to 8 classifiers are supported per port.(Optional)
- **dscp** - Classifies to the traffic profile based on DSCP. Up to 60 classifiers are supported per port.(Optional)
- **dscp-remark-policy** - IPv4 frames that classify to the traffic profile will have the DSCP value marked with a fixed value, or leave as is.
- **fixed-dscp** - Fixed DSCP value to use when remarking an IPv4 frame for a traffic profile with a dscp-remark-policy of fixed.
- **cir** - Committed information rate. (Mandatory, if PIR is not specified)
- **pir** - Peak information rate. (Mandatory, if CIR is not specified)

- **cbr** - Committed burst size.
- **ebs** - Excess burst size.
- **name** - Traffic profile name with up to 15 characters. If you do not specify a name, one is automatically created for the profile number (STD#1 through STD#64).
- **vlan** - Classifies to the traffic profile based on VLAN ID. One VLAN classifier is supported per port per profile. (Optional)



NOTE: The configured CIR and PIR will always normalize to the rate equal to or greater than the configured value in 64 kilobit increments in order to be processed by the hardware.

To create a standard profile:

```
traffic-profiling standard-profile create {port <PortNameList>} [profile <ProfileNumber>]
[dot1dpri <NUMBER LIST: 0-7>] [ip-prec <NUMBER LIST: 0-7>] [dscp <NUMBER LIST: 0-63>] [fixed-
dscp <0-63>] [{cir <kbps>}, [pir <kbps>], [cbs <kbytes>], [ebs <kbytes>}] [name
<TrafficProfilingStandardName[15]>] [vlan <VLAN>]
```

Example:

```
> traffic-profiling standard-profile create port 1 profile 1 cir 128 pir 128 ip-prec 1 dscp 1
```

To delete a standard profile:

```
traffic-profiling standard-profile delete {port <PortNameList>} {profile <NUMBER: 1-8>}
```

To set attributes for a standard profile:

```
traffic-profiling standard-profile set {port <PortName>} {profile <ProfileNumber>} [{dot1dpri
<NUMBER LIST: 0-7>] [ip-prec <NUMBER LIST: 0-7>] [dscp <NUMBER LIST: 0-63>] [dscp-remark-
policy <leave | fixed'>] [fixed-dscp <0-63>] [{cir <NUMBER>}, [pir <NUMBER>}] [cbs <kbytes>],
[ebs <kbytes>}] [name <TrafficProfilingStandardName[15]>] [vlan <VLAN>] [vlan <VLAN>]
```

Example:

```
> traffic-profiling standard-profile set port 1 profile 1 dot1dpri 1
```

To remove classification attributes for a standard profile:

```
traffic-profiling standard-profile unset {port <PortNameList>} {profile
<TrafficProfilingStandardName[15]>} [dot1dpri <NUMBER LIST: 0-7>] [ip-prec <NUMBER LIST: 0-
7>] [dscp <NUMBER LIST: 0-63>] [vlan]
```

Example:

```
> traffic-profiling standard-profile unset port 1 profile 1 dot1dpri 1
```

To display a summary of standard traffic profiles:

```
traffic-profiling standard-profile show
```

Example:

```
> traffic-profiling standard-profile show
```

STANDARD PROFILE TABLE						
Port	Profile ID	Name	BW (Kbps)		CLASSIFIERS	
			CIR	PIR		
1	1	STD#1	128	128	IPP 1 DSC 1	
1	2	STD#2	0	256		
2	3	STD#3	1024	1024	IPP 1	
2	4	STD#4	0	256		

To display standard profiles associated with a specified port:

```
traffic-profiling standard-profile show [port <PortName>]>
```

Example:

```
> traffic-profiling standard-profile show port 1
```

STANDARD PROFILE TABLE						
Port	Profile ID	Name	BW (Kbps)		CLASSIFIERS	
			CIR	PIR		
1	1	STD#1	128	128	IPP 1 DSC 1	
1	2	STD#2	0	256		

To clear statistics for all standard profiles:

```
traffic-profiling standard-profile clear statistics
```

Example:

```
> traffic-profiling standard-profile clear statistics
```

To display statistics for all standard profiles:

```
traffic-profiling standard-profile show [statistics]
```

Example:

```
> traffic-profiling standard-profile show statistics
```

STANDARD PROFILE TABLE				
Port	Profile ID	Name	Statistics	
			Type	Bytes
1	1	STD#1	Accepted	0
			Dropped	0
1	2	STD#2	Accepted	0
			Dropped	0

Configuring Per-Port Traffic Profiling

The configuration example in this section shows how to configure per-port traffic profiling to meter ingress traffic based upon 802.1D priority.

Configuration steps:

Step #	Description	Command
Step 1	Enable traffic profiling globally.	traffic-profiling enable
Step 2	Enable traffic profiling on port 1.	traffic-profiling enable port <PortName>
Step 3	Confirm the global configuration (optional).	traffic-profiling show
Step 4	Set traffic profiling mode on port 1 to standard-dot1dpri (default).	traffic-profiling set port <PortName>
Step 5	Confirm the per port configuration for port 1.	traffic-profiling show port <PortName>
Step 6	Create Traffic profile 1 on port 1 with CIR 3,000Kbps and PIR 3,200Kbps, dot1dpri 0,1,2.	traffic-profiling standard-profile create
Step 7	Create Traffic profile 2 on port 1 with CIR 3,000Kbps and PIR 3,200Kbps, dot1dpri 3,4,5.	traffic-profiling standard-profile create
Step 8	Create Traffic profile 3 on port 1 with CIR 2,000Kbps and PIR 2,432Kbps, dot1dpri 6,7.	traffic-profiling standard-profile create
Step 9	Display the traffic profiles associated with port 1 (Optional).	traffic-profiling standard-profile show port <PortName>

Example:

1. > traffic-profiling enable
2. > traffic-profiling enable port 1
3. > traffic-profiling show

```

+-----+ TRAFFIC PROFILING GLOBAL TABLE +-----+
| Profiling Status | Enabled |
+-----+

+-----+ PORT TRAFFIC PROFILE TABLE +-----+
| Port | Status | Mode |
| Admin | Oper  |      |
+-----+
| 1 | Enabled | Enabled | standard-dot1dpri |
| 2 | Disabled | Disabled | standard-dot1dpri |
| 3 | Disabled | Disabled | standard-dot1dpri |
| 4 | Disabled | Disabled | standard-dot1dpri |
| 5 | Disabled | Disabled | standard-dot1dpri |
| 6 | Disabled | Disabled | standard-dot1dpri |
| 7 | Disabled | Disabled | standard-dot1dpri |
| 8 | Disabled | Disabled | standard-dot1dpri |
| 9 | Disabled | Disabled | standard-dot1dpri |
| 10 | Disabled | Disabled | standard-dot1dpri |
+-----+

```

4. > traffic-profiling set port 1 mode standard-dot1dpri
5. > traffic-profiling show port 1

TRAFFIC PROFILING TABLE	
Port	1
Profiling Admin State	Enabled
Profiling Oper State	Enabled
Profiling Mode	standard-dot1dpri
Non-Conform Standard Profile	drop
ARP Standard Profile	bypass
Meter Pool	TP-P00L1

6. > traffic-profiling standard-profile create port 1 profile 1 cir 3000 pir 3200 dot1dpri 0,1,2
7. > traffic-profiling standard-profile create port 1 profile 2 cir 3000 pir 3200 dot1dpri 3,4,5
8. > traffic-profiling standard-profile create port 1 profile 3 cir 2000 pir 2432 dot1dpri 6,7
9. > traffic-profiling standard-profile show port 1

STANDARD PROFILE TABLE						
Port	Profile		BW (Kbps)		CLASSIFIERS	
	ID	Name	CIR	PIR		
1	1	STD#1	3008	3200	.1D	0 1 2
1	2	STD#2	3008	3200	.1D	3 4 5
1	3	STD#3	2048	2432	.1D	6 7

Configuring Per-Port and Per-VLAN Traffic Profiling

The configuration example in this section shows how to configure per-port and per-VLAN traffic profiling to meter ingress traffic based upon VLAN tag. Port 1 is the UNI port and port 9 is the NNI port.

Configuration steps:

Step #	Description	Command
Step 1	Enable traffic profiling globally.	traffic-profiling enable
Step 2	Enable traffic profiling on UNI port 1.	traffic-profiling enable port <PortName>
Step 3	Set traffic profiling mode on port 1 to standard-vlan.	traffic-profiling set port <PortName>
Step 4	Confirm the global configuration (optional).	traffic-profiling show
Step 5	Confirm the per port configuration for port 1.	traffic-profiling show port <PortName>
Step 6	Create VLAN 1001, 1002, 1003.	vlan create
Step 7	Add port 1 and 9 to VLAN1001, 1002, 1003.	vlan add vlan <VlanList> port <PortNameList>
Step 8	Confirm the VLAN configuration (optional).	vlan show
Step 9	Create Traffic profile 1 on port 1 with CIR 100 kbps and PIR 1024 Kbps, and classifier VLAN 1001.	traffic-profiling standard-profile create
Step 10	Create Traffic profile 2 on port 1 with CIR 100 kbps and PIR 1024 Kbps, and classifier VLAN 1002.	traffic-profiling standard-profile create
Step 11	Create Traffic profile 3 on port 1 with CIR 100 kbps and PIR 1024 Kbps, and classifier VLAN 1003.	traffic-profiling standard-profile create
Step 12	Display the traffic profiles associated with port 1 (Optional).	traffic-profiling standard-profile show port <PortName>

1. > traffic-profiling enable
2. > traffic-profiling enable port 1

3. > traffic-profiling show

----- TRAFFIC PROFILING GLOBAL TABLE -----				
Profiling Status		Enabled		

----- PORT TRAFFIC PROFILE TABLE -----				
Port	Status		Mode	
	Admin	Oper		
1	Enabled	Enabled	standard-dot1dpri	
2	Disabled	Disabled	standard-dot1dpri	
3	Disabled	Disabled	standard-dot1dpri	
4	Disabled	Disabled	standard-dot1dpri	
5	Disabled	Disabled	standard-dot1dpri	
6	Disabled	Disabled	standard-dot1dpri	
7	Disabled	Disabled	standard-dot1dpri	
8	Disabled	Disabled	standard-dot1dpri	
9	Disabled	Disabled	standard-dot1dpri	
10	Disabled	Disabled	standard-dot1dpri	

4. > traffic-profiling set port 1 mode standard-vlan

5. > traffic-profiling show port 1

----- TRAFFIC PROFILING TABLE -----		
Port	1	
Profiling Admin State	Enabled	
Profiling Oper State	Enabled	
Profiling Mode	standard-vlan	
Non-Conform Standard Profile	drop	
ARP Standard Profile	bypass	
Meter Pool	TP-P00L1	

6. > vlan create vlan 1001-1003

...This may take a while depending upon the VLAN range...

7. > vlan add vlan 1001-1003 port 1,9

...This may take a while depending upon the VLAN range...

8. > vlan show

VLAN	Ports	
ID VLAN Name	1234567890	
1 Default	xxxxxxxxxx	
127 VLAN#127	xx	
270 Mgmt	x	
1001 VLAN#1001	x	x
1002 VLAN#1002	x	x
1003 VLAN#1003	x	x

9. > traffic-profiling standard-profile create port 1 profile 1 cir 100 pir 1024 vlan 1001

10.> traffic-profiling standard-profile create port 1 profile 2 cir 100 pir 1024 vlan 1002

```
11.> traffic-profiling standard-profile create port 1 profile 3 cir
    100 pir 1024 vlan 1003
12.> traffic-profiling standard-profile show port 1
```

STANDARD PROFILE TABLE						
Port	Profile		BW (Kbps)		CLASSIFIERS	
	ID	Name	CIR	PIR		
1	1	STD#1	128	1024	VLN	1001
1	2	STD#2	128	1024	VLN	1002
1	3	STD#3	128	1024	VLN	1003

Ingress R-CoS to Egress CoS Queue Mapping

Each physical port supports 8 CoS queues. Depending upon the policies applied to the port, the R-CoS and R-COLOR values may change during processing. The final internal R-CoS value is used to map the frame to one of the 8 physical port CoS queues as shown in **Table 14-2**, in this chapter.

Table 14-2: Default Internal R-CoS Mapping

R-CoS	Physical Port CoS Queue
0	0
1	0
2	1
3	2
4	3
5	4
6	5
7	6
Reserved for outbound CPU frames	7

In addition to the default queue mapping, up to 7 custom Queue Map Profiles can be created to configure R-CoS to CoS queue mapping. The mapping-mode of custom queue map profiles is always R-CoS mapped. Any port can use a custom queue map profile by configuring the *ingress-to-egress-qmap* attribute on the port. R-CoS values (0 - 7) can be mapped to CoS Queues (0 - 7), or any combination thereof (for example, all 7 R-CoS values mapped to the same CoS queue, etc.).

To create/modify a custom R-CoS to CoSQ table and assign it to an egress port:

```
> traffic-services queuing queue-map create rcos-map custom-map-1
> traffic-services queuing queue-map set rcos-map custom-map-1 rcos 0 queue 3
> traffic-services queuing queue-map show rcos-map custom-map-1
> port set port 9 ingress-to-egress-qmap custom-map-1
```

To delete a custom R-CoS map from the system:



NOTE: A custom R-CoS queue map profile cannot be deleted if it is assigned to a port, as it must first be removed from the port before it can be deleted.

```
> port set port 9 egress-queue-map Default-RCOS
```



NOTE: You cannot unset a port's egress-queue-map profile, as this is a required parameter. To remove a custom R-CoS profile from a port you must replace it with another R-CoS profile (for example, the Default-RCOS profile).

```
> traffic-services queuing queue-map delete rcos-map custom-map-1
> traffic-services queuing queue-map show
```

Example of the default R-CoS map:

-----RCOS TO QUEUE MAPPING -----									
Name					Default-RCOS				
Id					1				
Type					RCOS To Queue Mapping				
RCOS:	0	1	2	3	4	5	6	7	
+-----+									
Queue:	0	0	1	2	3	4	5	6	

Congestion Avoidance

Congestion avoidance processing determines whether a frame should be enqueued or dropped. Congestion avoidance is configured per queue based on a congestion avoidance profile associated with each CoS queue. This profile contains the drop parameters for traffic. Drop parameters are defined by the following general attributes:

- **Drop Threshold**—defines the percentage of the queue capacity that is reached before packets are eligible to be dropped.
- **Drop Probability**—define the percentage of packets that are dropped once the threshold is exceeded.

By dropping packets before the queue fills up, congestion avoidance controls the average buffer queue size by indicating to the end hosts when they should temporarily slow down transmission of TCP packets. Randomly dropping packets *prior* to periods of high congestion tells the packet source to decrease its transmission rate. Assuming the packet source is using TCP, it will decrease its transmission rate until all the packets reach their destination, indicating that the congestion is cleared. TCP not only pauses, but it also restarts quickly and adapts its transmission rate to the rate that the network can support.

Depending upon the hardware platform, the system software supports Simple Random Early Detection (sRED) profiles or simple Weighted Random Early Discard (sWRED) profiles for congestion avoidance that are enabled by default. You can configure custom congestion avoidance profiles for your platform and configure the egress port queues to use them.

Creating and modifying sRED profiles

The CN 3911, CN 3920, CN 3940, and CN 5140 platforms support sRED profiles. By default there is one congestion avoidance profile (Default-SRED) in the system that all queues reference, and each port supports two default sRED curves per queue, one for TCP yellow traffic and one for TCP green traffic. Each sRED curve supports a lower drop threshold and drop probability. The upper threshold is not configurable, and supports 128 packets per port.

When the number of packets are below the lower threshold, no packets are dropped. When they exceed the lower threshold, and are below the upper threshold, they are dropped according to the drop probability value. When the number of packets reaches the upper threshold, all packets are dropped (100 percent drop probability) until the number of packets is below the upper threshold.

For yellow packets, the default drop threshold is 50 percent. For green packets, the default drop threshold is 75 percent. This means that the queue capacity can be filled with 75 percent green packets, and 50 percent yellow packets before the packets are eligible to be dropped. Additionally, both sRED curves assign a drop probability percentage for green (0.09765625 percent or 1/1024) and yellow (6.25 percent or 1/16) packets per CoS queue that is applied via a congestion avoidance profile. You can create up to 7 custom congestion avoidance profiles and modify their configuration.

Lower drop threshold values for green or yellow traffic range from 1-100 percent. Drop probability values for green or yellow traffic include:

- 100pct - 100 percent
- 6.25pct - 6.25 percent or 1/16.
- 3.125pct - 3.125 percent or 1/32.
- 1.5625pct - 1.5625 percent or 1/64.
- 0.78125pct - 0.78125 percent or 1/128.
- 0.390625pct - 0.390625 percent or 1/256.
- 0.1953125pct - 0.1953125 percent or 1/512.
- 0.09765625pct - 0.09765625 percent or 1/1024.

If you create a custom sRED profile without specifying the thresholds or drop probability values, the profile will be the same as the Default-SRED profile.

To create an sRED profile:

```
traffic-services queuing congestion-avoidance-profile create profile <String[15]>
[green-threshold <NUMBER: 1-100>] [green-drop-probability <100pct|6.25pct|3.125pct|
1.5625pct|0.78125pct|0.390625pct|0.1953125pct|0.09765625pct>]
[yellow-threshold <NUMBER: 1-100>][yellow-drop-probability <100pct|6.25pct|3.125pct|
1.5625pct|0.78125pct|0.390625pct|0.1953125pct|0.09765625pct>]]
```

Example:

```
traffic-services queuing congestion-avoidance-profile create profile green-yellow-1 green-
threshold 100 yellow-threshold 1 yellow-drop-probability 100pct
```

To modify an sRED profile:

```
traffic-services queuing congestion-avoidance-profile set profile  
<CongestionAvoidanceProfile> {[green-threshold <NUMBER: 1-100>], [green-drop-probability  
<100pct|6.25pct|3.125pct|1.5625pct|0.78125pct|0.390625pct|0.1953125pct|0.09765625pct>],  
[yellow-threshold <NUMBER: 1-100>], [yellow-drop-probability <100pct|6.25pct|3.125pct|  
1.5625pct|0.78125pct|0.390625pct|0.1953125pct|0.09765625pct>]}
```

Example:

```
traffic-services queuing congestion-avoidance-profile set profile green-yellow-1 green-  
threshold 90 green-drop-probability 0.1953125pct yellow-threshold 25
```

Creating and modifying sWRED profiles

The CN 3960 platform supports simple Weighted Random Early Discard (sWRED) profiles to handle three types of traffic:

- TCP green traffic
- TCP yellow traffic (has been metered to yellow from traffic profiling)
- Non-TCP traffic

For each traffic type, an sWRED profile supports an sWRED curve with a configurable start threshold (1-100 percent), upper threshold (1-100 percent), and a maximum drop probability. Maximum drop probability values include:

- 100pct - 100 percent
- 75pct - 75 percent
- 50pct - 50 percent
- 25pct - 25 percent
- 10pct - 10 percent
- 9pct - 9 percent
- 8pct - 8 percent
- 7pct - 7 percent
- 6pct - 6 percent
- 5pct - 5 percent
- 4pct - 4 percent
- 3pct - 3 percent
- 2pct - 2 percent
- 1pct - 1 percent
- 0pct - 0 percent

When the number of packets are below the start threshold, no packets are dropped. When they exceed the start threshold, and are below the upper threshold, they are dropped according to the maximum drop probability value. When the number of packets reaches the upper threshold, all packets are dropped according to the maximum drop probability until the number of packets is below the upper threshold.

The default sWRED profile (Default-S-WRED) is configured as follows:

- TCP green start threshold - 75 percent
- TCP green maximum upper threshold - 100 percent
- TCP green maximum drop probability - 0 percent
- TCP yellow start threshold - 50 percent
- TCP yellow maximum upper threshold - 100 percent

- TCP yellow maximum drop probability - 100 percent
- Non-TCP start threshold - 50 percent
- Non-TCP maximum upper threshold - 100 percent
- Non-TCP maximum drop probability - 100 percent

If you create a custom sWRED profile without specifying the thresholds or drop probability values, the profile will be the same as the Default-S-WRED profile.

To create an sWRED profile:

```
traffic-services queuing congestion-avoidance-profile create profile <String[15]>
[tcp-green-threshold <NUMBER: 1-100>] [tcp-green-upper-threshold <NUMBER: 1-100>]
[tcp-green-drop-probability <100pct|75pct|50pct|25pct|10pct|9pct|8pct|7pct|6pct|5pct|4pct|
3pct|2pct|1pct|0pct>] [tcp-yellow-threshold <NUMBER: 1-100>] [tcp-yellow-upper-threshold
<NUMBER: 1-100>] [tcp-yellow-drop-probability <100pct|75pct|50pct|25pct|10pct|9pct|
8pct|7pct|6pct|5pct|4pct|3pct|2pct|1pct|0pct>] [non-tcp-threshold <NUMBER: 1-100>] [non-tcp-
upper-threshold <NUMBER: 1-100>] [non-tcp-drop-probability <100pct|75pct|50pct|25pct|10pct|
9pct|8pct|7pct|6pct|5pct|4pct|3pct|2pct|1pct|0pct>]
```

Example:

```
traffic-services queuing congestion-avoidance-profile create profile green-yellow-1 tcp-
green-upper-threshold 100 tcp-yellow-upper-threshold 1 tcp-yellow-drop-probability 100pct
```

To modify an sWRED profile:

```
traffic-services queuing congestion-avoidance-profile set profile
<CongestionAvoidanceProfile> [tcp-green-threshold <NUMBER: 1-100>] [tcp-green-upper-
threshold <NUMBER: 1-100>] [tcp-green-drop-probability <100pct|75pct|50pct|25pct|10pct|
9pct|8pct|7pct|6pct|5pct|4pct|3pct|2pct|1pct|0pct>] [tcp-yellow-threshold <NUMBER: 1-100>]
[tcp-yellow-upper-threshold <NUMBER: 1-100>] [tcp-yellow-drop-probability <100pct|
75pct|50pct|25pct|10pct|9pct|8pct|7pct|6pct|5pct|4pct|3pct|2pct|1pct|0pct>] [non-tcp-
threshold <NUMBER: 1-100>] [non-tcp-upper-threshold <NUMBER: 1-100>] [non-tcp-drop-
probability <100pct|75pct|50pct|25pct|10pct|9pct|8pct|7pct|6pct|5pct|4pct|3pct|2pct|
1pct|0pct>]
```

Example:

```
traffic-services queuing congestion-avoidance-profile set profile green-yellow-1 non-tcp-
upper-threshold 1 non-tcp-drop-probability 100pct
```

Displaying custom congestion avoidance profiles

You can display configuration of all or specific congestion avoidance profiles, including: name, ID, type, thresholds, and drop probability.

To display all congestion avoidance profiles:

```
traffic-services queuing congestion-avoidance-profile show
```

To display a specific congestion avoidance profile:

```
traffic-services queuing congestion-avoidance-profile show profile
<CongestionAvoidanceProfile>
```

Example of the default sRED congestion avoidance profile:

```
traffic-services queuing congestion-avoidance-profile show profile Default-SRED
```

----- CONGESTION AVOIDANCE PROFILE DATA -----									
Name					Default-SRED				
Id					1				
Type					SRED				
Green					Yellow				
Threshold		Drop Probability			Threshold		Drop Probability		
75	%	0.09765625pct.(1/1024)			50	%	6.25pct.....(1/16)		

Example of the default sWRED congestion avoidance profile:

```
traffic-services queuing congestion-avoidance-profile show profile Default-S-WRED
```

----- CONGESTION AVOIDANCE PROFILE DATA -----																
Name				Default-S-WRED												
Id				1												
Type				WRED-Simple												
Lower Threshold			Tcp-Green Upper Threshold		Drop Prob	Lower Threshold			Tcp-Yellow Upper Threshold		Drop Prob	Non-Tcp Lower Threshold		Upper Threshold		Drop Prob
75			100		0pct	50			100		100pct	75		100		0pct

Configuring the congestion avoidance profile for egress port queues

The default congestion avoidance profile for egress port queues is to use Default-SRED or Default-S-WRED, depending upon the platform. After creating custom congestion avoidance profiles, you can set the egress port queues to use them. The queue is identified by queue number and egress port queue group (PortQueueGroup), which is the egress port name.

To update the congestion avoidance profile for an egress port queue:

```
traffic-services queuing egress-port-queue-group set queue <NUMBER: 0-7> port
<PortQueueGroup> congestion-avoidance-profile <CongestionAvoidanceProfileName>
```

Example:

```
traffic-services queuing egress-port-queue-group set queue 2 port 1 congestion-avoidance-
profile green-yellow-1
```

To clear the congestion avoidance profile to the default for an egress port queue:

```
traffic-services queuing egress-port-queue-group unset queue <NUMBER: 0-7> port
<PortQueueGroup> congestion-avoidance-profile
```

Example:

```
traffic-services queuing egress-port-queue-group unset queue 2 port 1 congestion-avoidance-
profile
```

To display the congestion avoidance profile for an egress port queue:

```
traffic-services queuing egress-port-queue-group show queue <NUMBER: 0-7> port
<PortQueueGroup>
```

Example of sRED:

```
> traffic-services queuing egress-port-queue-group show queue 0 port 1
```

QUEUE DATA						
Queue Id				0		
Queue Group Name [Port]				1		
Congestion Avoidance Profile				Default-SRED		
Scheduler		Size	CIR	CBS	EIR	EBS
Pri Idx	Weight	(Pckts)	(Kbps)	(Kbytes)	(Kbps)	(Kbytes)
10000	20	100	0	0	1000000	256

Example of sWRED:

```
> traffic-services queuing egress-port-queue-group show queue 0 port 1
```

QUEUE DATA						
Queue Id			0			
Queue Group Name [Port]			1			
Congestion Avoidance Profile			Default-S-WRED			
Scheduler		Size	CIR	CBS	EIR	EBS
Pri Idx	Weight	(Pckts)	(Kbps)	(Kbytes)	(Kbps)	(Kbytes)
10000	20	100	0	0	1000000	256

Deleting a custom congestion avoidance profile

You can delete custom congestion avoidance profiles that are not in use.

To delete a congestion avoidance profile:

```
traffic-services queuing congestion-avoidance-profile delete profile
<CongestionAvoidanceProfile>
```

Renaming custom congestion avoidance profile

You can change the name of a custom congestion avoidance profile.

To rename a congestion avoidance profile:

```
traffic-services queuing congestion-avoidance-profile rename profile
<CongestionAvoidanceProfile> name <String[15]>
```

Egress Scheduling

Scheduling determines the order in which the physical queues are processed. Currently, the system software follows strict priority scheduling by default. CoS queue 7 has the highest priority while CoS queue 0 has the lowest priority. When contention (or congestion) for bandwidth occurs in the system, the higher priority CoS queues will be serviced before the lower priority CoS queues. By default, the 802.1p priority (VLAN priority in the frame) is used to map to an internal priority (resolved CoS) which is then mapped to a physical CoS queue. The result is that frames with a higher priority will transmit before those with a lower priority. Strict priority queuing reduces resources for low priority packets, but ensures low-latency servicing of high-priority packets.

In addition to strict priority, three other scheduling methods can be configured. When configured for any of these scheduler modes, if the scheduling weight of a queue in the egress port queue group is set to 0, the scheduler will treat that queue as if it is in strict priority mode.

- Weighted Round Robin (WRR)—queues in the queuing group are scheduled in a weighted fashion according to the per-queue scheduler-weight.
- Round-Robin (RR)—queues in the queuing group are scheduled as if all queues in the queuing group have equal weighting.
- Weighted Deficit Round Robin (WDRR)—queues in the queuing group are scheduled in a weighted fashion according to the per-queue scheduler-weight and frame size.

To change an egress port's scheduler algorithm for the egress queue group:

```
traffic-services queuing egress-port-queue-group set port <PortQueueGroup> scheduler-  
algorithm <strict|round-robin|weighted-deficit-round-robin|weighted-round-robin>
```

Example:

```
> traffic-services queuing egress-port-queue-group set port 9 scheduler-algorithm weighted-  
round-robin
```

To change a queue's weight for use with the port's scheduler algorithm:

```
traffic-services queuing egress-port-queue-group set queue <NUMBER: 0-7> port  
<PortQueueGroup> scheduler-weight <NUMBER: 0-1000>
```



NOTE: The default weight for CoS Queue 7 is 0, which is serviced in a strict-priority fashion being the highest priority over all other CoS queues in the Egress Queue group. Queue 7 is typically reserved for CPU-Sourced traffic and should not be changed.

Example:

```
traffic-services queuing egress-port-queue-group set queue 0 port 9 scheduler-weight 100
```

To display queue weight and scheduler algorithms for all or a specific egress port:

```
traffic-services queuing egress-port-queue-group show [port <PortQueueGroup>]
```

Example:

```
> traffic-services queuing egress-port-queue-group show port 9
```

QUEUE GROUP DATA									
Name [Port]					9				
Id					9				
Queue Count					8				
Scheduling Algorithm					weighted-round-robin				
Shaper Bandwidth (Kbps)					1000000				
Q	Pri	Schedul Idx	Weight	Size (Pckts)	CIR (Kbps)	CBS (Kbytes)	EIR (Kbps)	EBS (Kbytes)	
0	10000	100	100	100	0	0	1000000	256	
1	20000	30	100	100	0	0	1000000	256	
2	30000	40	100	100	0	0	1000000	256	
3	40000	50	100	100	0	0	1000000	256	
4	50000	60	100	100	0	0	1000000	256	
5	60000	70	100	100	0	0	1000000	256	
6	70000	80	100	100	0	0	1000000	256	
7	80000	0	100	100	1024	256	1000000	256	

Egress Shaping

A shaper-rate and burst size can be configured on the egress port queue group that limits the amount of egress bandwidth a port uses and controls the amount of traffic that can burst. Each queue can also be individually shaped according to the following parameters:

- **CIR** in Kbps—this is rate of traffic that can egress from a queue and be considered guaranteed traffic.
- **CBS** in Kbytes—this is the amount of CIR traffic that can burst from a queue (the CIR bucket size).
- **EIR** in Kbps—this is the rate of traffic that can egress from a queue above CIR and is considered non-guaranteed traffic.
- **EBS** in Kbytes—this is the amount of EIR traffic that can egress from a queue (the EIR bucket size).

In order to guarantee CIR, the individually set CIR on queues must not be oversubscribed for the egress port that the frames are egressing. That is, the sum of all CIRs for the physical queues and the virtual queues in a queue group on a port should not exceed the administrative (and operational) speed of the port. When the shaper rate of the egress port queue group is set, it sets a single Information Rate (IR) regardless of the CIR and EIR of the individual queues. To guarantee CIR, the sum of the CIRs on each queue cannot exceed the IR of the egress port queue group.

When a queue or an attribute of the egress queue group of an aggregated port is modified, that value is updated at each queue or physical port of the aggregation, with the exception of the shaper rate bandwidth. The shaper rate bandwidth is divided equally amongst the number of distributing ports. This means that the shaper rate can be used to control the total bandwidth that the ports share, otherwise the ports would each have an amount of bandwidth that would add up to a cumulative amount of bandwidth for the aggregation member ports.

When you set the burst size, the value is rounded to the nearest larger 4Kbyte block. The burst size is not divided among ports in an aggregation group.

To set the egress port shaper-rate bandwidth:

```
traffic-services queuing egress-port-queue-group set port <PortQueueGroup> shaper-rate  
<NUMBER: 0-100000000>
```

Example:

```
> traffic-services queuing egress-port-queue-group set port 3 shaper-rate 1200
```

To set the egress port shaper-rate burst-size:

```
traffic-services queuing egress-port-queue-group set port <PortQueueGroup> burst-size  
<NUMBER: 4-10240>
```

Example:

```
> traffic-services queuing egress-port-queue-group set port 3 burst-size 1024
```

To set the egress shaping parameters per queue:

```
traffic-services queuing egress-port-queue-group set queue <NUMBER: 0-7> port  
<PortQueueGroup> cir <NUMBER: 0-100000000> cbs <NUMBER: 0-256> eir <NUMBER: 0-100000000> ebs  
<NUMBER: 0-256>
```

Example:

```
> traffic-services queuing egress-port-queue-group set queue 0 port 9 cir 5000 cbs 5000 eir  
4000 ebs 3000
```

Configuring Frame Bandwidth Calculation

The system supports 20 bytes of IFG that can be considered when calculating bandwidth for traffic profiling according to CIR and PIR settings in a traffic profile for ingress metering and egress shaping.

To set the Bandwidth calculation mode:

```
> flow bw-calculation-mode set mode <payload | transport>
```

To NOT use IFG in bandwidth calculations:

```
> flow bw-calculation set mode payload
```

To use IFG in bandwidth calculations:

```
> flow bw-calculation set mode transport
```

Note that when the system is in payload calculation mode, the 20-byte IFG is not considered in the bandwidth equations. However, the physical port must still operate according to Ethernet standards and take into account the IFG when transmitting packets. Therefore, the operator could possibly configure a CIR sum at a port that would exceed the physical bandwidth of the port due to the required IFG on the wire. The software does not attempt to adjust bandwidth or issue user-events when in payload mode. The software assumes bandwidth to be configured and consumed according to transport mode.

Chapter Configuring Multicast Services

15

At a Glance:

- Overview
- IGMP Snooping
- Unknown Multicast Filtering
- Configuring Multicast

This chapter details how to configure multicast services in some typical situations.

Overview

Typical Internet Group Management Protocol (IGMP) was designed for environments that have a low volume of multicast packets and no real-time traffic requirements for processing IGMP messages. IGMP was designed for networks where multicast services are critical, such as networks delivering IP broadcast video. Devices employ enhanced IGMP snooping and various filters to limit multicast streams and assure their timely delivery.

IGMP Snooping

While traditional IGMP snooping works well in most enterprise networks, service providers delivering converged services need to deliver high-bandwidth multicast services to many subscribers without disruptions. These types of networks must handle near-real-time join/leave processing for all subscribers.

In order to support these requirements, several enhancements to traditional IGMP are provided, including Proxy Query Delay, IGMP message shaping, an IGMP query engine, IGMP message filtering, configurable IGMP leave modes, rapid topology response, and fast join/leave processing. It should be noted that multicast services (IGMP) is globally enabled for the entire device by default, however, it can be enabled or disabled for each multicast VLAN individually.

IGMP Message Shaping

Traditional IGMP snooping sends a proxy query to all devices at once. In response all ports in a device tend to reply a nearly the same time. This causes bursts or spikes of IGMP join messages that all reach the router at the same time. To alleviate this problem, a type of proxy reporting called IGMP message shaping is used. When an IGMP query is received, IGMP membership reports are sent at a constant rate to the router, based on the list of active multicast groups. This eases the burden on the multicast querier.

Proxy Query Delay

Another problem with traditional IGMP snooping occurs on the downstream devices. When a general query is received, it is forwarded to all ports on the device at the same time. This request requires it to update its multicast tables, which prompts the hosts on all ports in the VLAN to reply almost simultaneously, which demands a great amount of CPU processing. It is far more desirable, from a CPU load perspective, to spread query responses out over time.

This normalization of query responses is accomplished by internally forwarding query messages to just one port at a time. This delay smooths out the load on the CPU and helps to reduce channel-change latency. This delay between ports is configured as the query delay. In addition, since the device employs IGMP Message Shaping, the router is unaware of any delay in the report (refer to the **IGMP Message Shaping** section).

Proxy Query also helps to detect the path between the device and the router. If a link failure occurs that affects the path between the router and the service delivery switch, it is able to find the new path to the router even if the router does not send a query message. Instead of waiting for a query from the router, which could take minutes or even hours. The maximum time required to locate the new router path is only as long as the Proxy Query delay interval.

IGMP Query Engine

In a traditional multicast environment, all requests and queries are processed through a multicast router. Typically, these routers are overburdened with processing requirements and thus cannot respond as quickly as is needed in converged service network. To eliminate the need for a separate IGMP router and speed up multicast response times, you can configure service delivery switches to use a built-in IGMP query engine.

The query engine can be configured to generate query packets at regular intervals performing the function of a multicast router. However, only one device on the network can act as an IGMP query agent at a time and all multicast servers must interface directly with this device. Queriers negotiate with each other to determine which device should be the active querier. However, if multiple queriers are seen by the service delivery switch, it acts only on the queries from the device with the lowest IP address and ignores any other active queriers. Therefore a unique, non-zero source IP address must be set for the query engine when it is enabled.

Figure 15-1 is an example of an active Query Engine in a network. The multicast server interfaces directly with the “top-level” device (device 1), which is also acting as the IGMP querier for the network. The other devices forward IGMP messages to the “top-level” device only. Multicast streams flow from device 1 to device 2 and from device 1 to device 3.

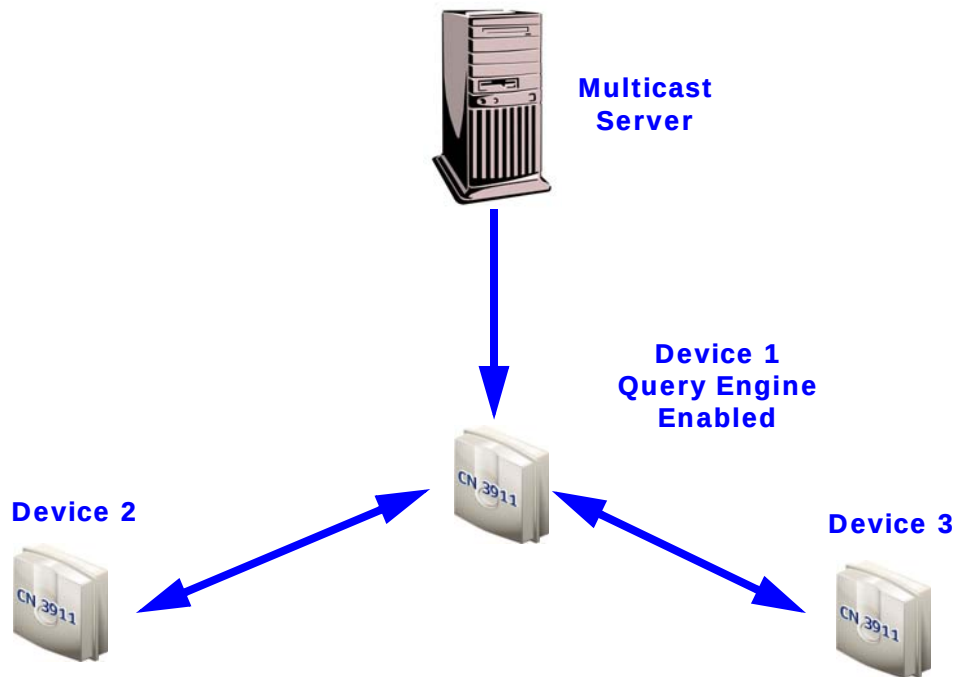


Figure 15-1: Query Engine Deployment

If the query engine was enabled on device 2 instead of device 1, no membership reports would forward from device 2 to device 1, and no multicast streams would flow from device 1 to device 2.

When using the Query Engine, the device must not have a learned or configured router port for the VLAN. Additionally, you need to set the Source IP address to a value other than the default value of 0.0.0.0.



NOTE: Do not enable this feature if using a traditional IGMP router on the network.

IGMP Message Filtering

Traditional IGMP join message processing involves forwarding each IGMP join message received from a host to the server ports. Forwarding each IGMP join message to the server ports is a scaling issue for those devices higher in the network and ultimately the IGMP router. Enabling IGMP Message Filtering is a scaling feature that causes the system

software to intelligently forward IGMP join messages to server ports only if that IGMP join message is required to cause a multicast stream to flow to the host. IGMP join messages that are redundant are filtered.

NOTE: If two IGMP join messages are received on two ports, and the last 3 octets of the destination IP address are the same, the second port cannot be part of the multicast group. For example, Port 1 receives a JOIN with destination IP 224.1.2.3, and it becomes part of the multicast group. If Port 2 receives a JOIN message with destination IP 225.1.2.3, then Port 2 cannot become part of the multicast group.

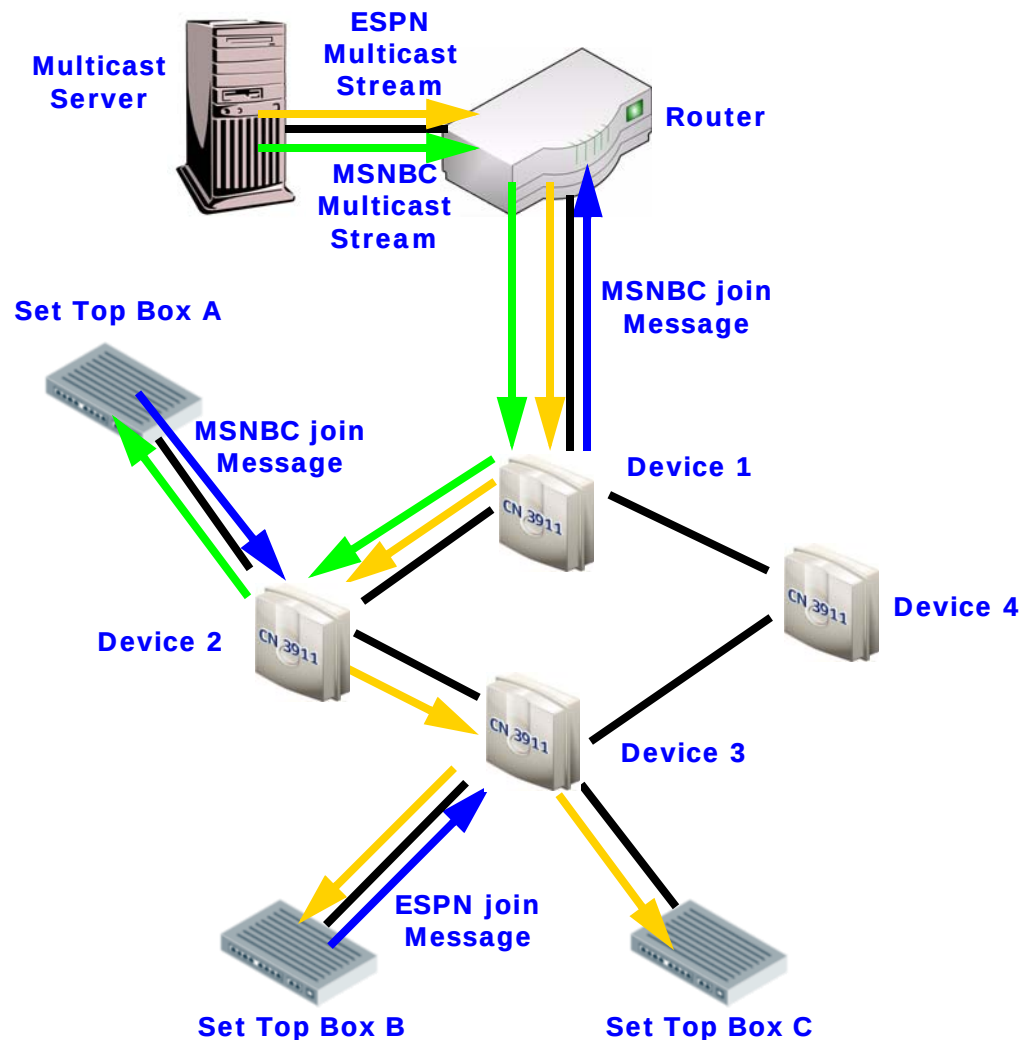


Figure 15-2: IGMP Message Filtering

For example, if a subscriber on Set Top Box A is watching a video channel such as ESPN, when the subscriber on Set Top Box B changes the channel to ESPN (subscribes to the ESPN multicast group) Set Top Box B sends an IGMP join message to device number 3. However, device 3 does not forward the join message upstream since the multicast stream is already present. In contrast, if Set Top Box A joins the MSNBC multicast group, a join message would be sent all the way upstream back to the multicast router since the router does not have any active members in the MSNBC group.

StreamCast

Typical multicast video deployments support a centralized server topology where a single video source provides all multicast content for a VLAN. While backup servers may exist, only one server delivers content.

A distributed solution allows a number of multicast servers to deliver content on a VLAN. **Figure 15-3** shows such an architecture where two multicast routers each actively provide video content on the same VLAN. StreamCast is the solution that supports distributed video architecture, which allows service offerings that provide customers the ability to set up video conferences between many remote offices or other multicast streaming applications.

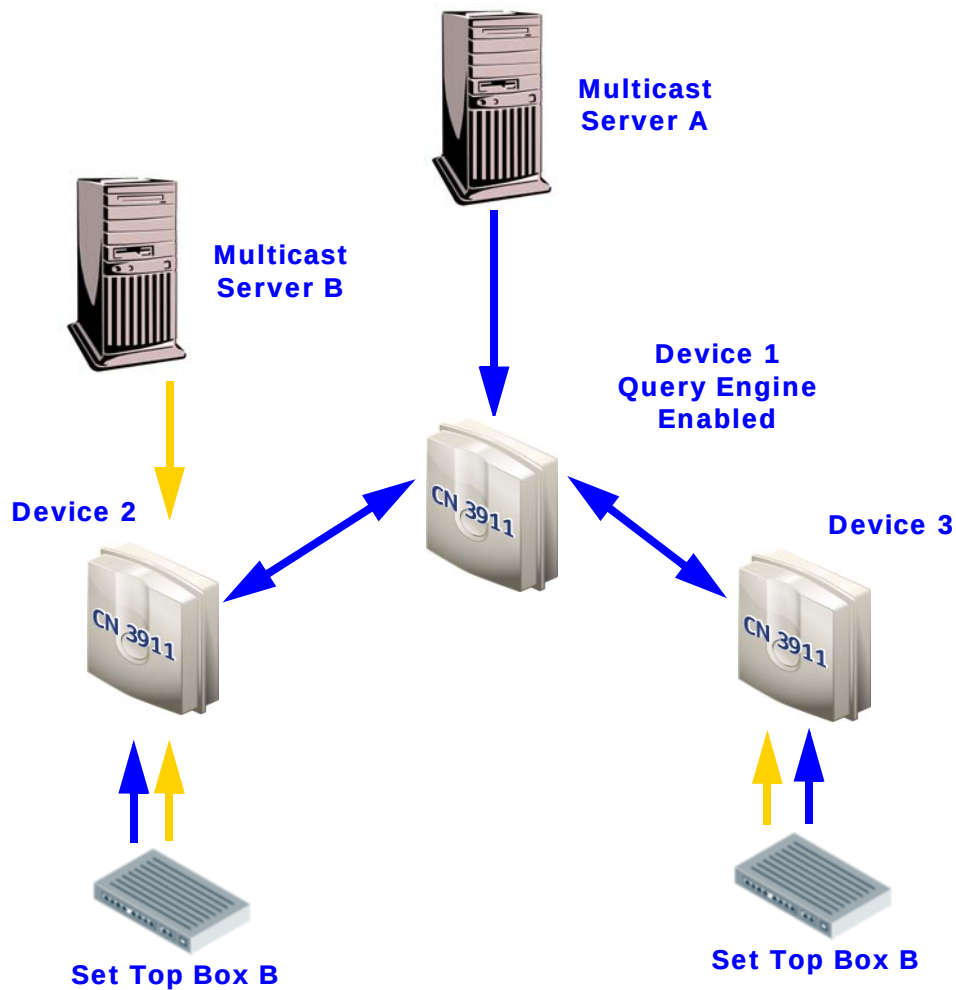


Figure 15-3: StreamCast

IGMP Leave Modes

Two methods for handling IGMP leaves are supported, Fast Leave and Inquisitive Leave. In Fast Leave mode, a port is removed from the multicast group immediately after a leave report is received for the port. The multicast stream no longer flows to the port.

In Inquisitive Leave mode, a timer is used to determine when ports are removed from a multicast group. Instead of immediately removing a port, when the device receives the leave report, it starts a timer and also sends out a group-specific membership query. If a

membership report is received for the group on that port before the timer expires, the timer is cancelled. However, if the port does not receive a membership report, the port will be removed as soon as the timer expires.

This delay, reduces channel-change latency, which can be especially useful in situations such a last channel recall. It also resolves problems introduced when a subscriber connects a hub or non-IGMP switch to their customer premises equipment (CPE).

Inquisitive leave should only be enabled on devices that have a CPE (e.g., a set top box) attached to them.

IGMP Parameters

The following table is a summary of IGMP parameters. In cases where these parameters have different names between the Device Manager and the CLI, the Device Manager name is listed in parentheses.

Field	Description
IGMP Snooping (Active State)	Displays whether IGMP is active for the entry selected.
Default Router Port	The port on the device used to communicate with the router. This port sends and receives the IGMP query and join/leave messages. If a router port is not assigned, the value will be 0. Used if the actual router port is not known.
IGMP Leave Mode (Inq. Leave State)	Enables inquisitive leave. When enabled, the Active Linger Timeout is used to remove ports from the multicast group membership table. When a leave report is received by the device, the Last Member Query Interval timer is started and a group-specific query will egress the port. The timer is canceled if a membership report is received on the port. The port is removed from the group when the timer expires.
Last Member Query Interval (Last Mem. Query Int.)	Max response time inserted into group-specific queries sent in response to leave messages. Also determines the amount of time between group-specific queries. Ignored when inquisitive-leave is disabled.
L2 Packet Priority (Priority)	802.1p priority value assigned to IGMP packets for this VLAN. Default priority is 7.
Snooping State	Enables or disables IGMP snooping for the VLAN.
Robustness	Number of IGMP join or IGMP leave messages to send for each multicast group.
Linger Timeout	The time, in seconds, that a filter will remain in the IGMP table after all hosts have left the group. This is done to give sufficient time for the upstream IGMP router to receive and process the leave message. The filter is removed when the Linger Timeout expires.
Active Linger Timeout	Used for inquisitive leaves. If no join message are received before the timer expires, the port is removed from the group.

Field	Description
Router Query Interval (Router Query Int.)	Determines the time (in seconds) to wait for the router to send a General Query message.
Minimum Query Response Time	Time, in deciseconds (1/10 of a second), that hosts have to respond to an IGMP query.
Group Address Range (Start) (Rtr. Range Start IP)	Configures the starting IP address in the multicast range for the IGMP router that corresponds to this multicast entry. Each router should be configured to use a separate range of multicast addresses to avoid conflict.
Group Address Range (End) (Rtr. Range End IP)	Configures the ending IP address in the multicast range for the IGMP router that corresponds to this multicast entry.
Proxy Query Source Address (Source IP Address)	When the query engine is enabled, this address is used as the source for all query packets. This IP address must be unique for the VLAN.
IGMP Query Engine (Query Engine State)	Enables/Disables the IGMP query engine.
Proxy Query Interval (Query Interval)	Determines the interval, in seconds when the query engine will send IGMP general queries.
Proxy Query Response Interval	Determines the rate at which devices respond to IGMP queries from the router.
Proxy Query Delay	Query messages are sent to one port at a time. This setting determines the delay between forwarding messages to each port.

Unknown Multicast Filtering

Various filters are used to limit multicast traffic. Normally when a Layer-2 switch receives a multicast packet with an unknown destination address, it floods the packet to all ports in the VLAN. Unknown multicast filtering (UMF) is used to filter (drop) these unknown packets. A destination address is considered unknown if it is not found in the list of active multicast groups.

UMF is useful when a multicast server is connected directly to the Layer-2 network, bypassing the Layer-3 router. In this case, the multicast server continuously floods the device with multicast traffic. With UMF enabled, the switch will simply drop all multicast streams that have not been joined until a join message is received. UMF is enabled by setting this feature to Filter (drop). UMF should be enabled before reaching host devices otherwise, they will be flooded with multiple multicast streams.

Configuring Multicast

The following examples show various IGMP configurations in ring topologies. The default settings for the IGMP timers should work well for most applications.

In addition, there are two important configuration settings on the multicast router that can affect IGMP performance.

- **Query-Response-Interval** -determines how fast the device must respond to a general query. A short interval results in a burst of responses within a very short time, causing the CPU load to spike. A larger value helps avoid this peak thereby easing CPU load. Where possible, this value should be set as close to (but not exceeding) the query-interval.
- **Query-Interval** -on the router, this value determines how often the router sends a general-query message. Each time the device receives a general query, it must use system resources to respond to the router. If the interval is too short it could cause the device to become sluggish. The minimum value should be about one minute for every 100 multicast groups on the network. The value chosen for query-interval on the router should be less than or equal to the value chosen for router-query-interval on the device.



NOTE: To configure Multicast, you need to install the Advanced Ethernet license key. To obtain the Advanced Ethernet license key, contact Ciena Sales.

Multicast Router Topology

This example demonstrates how to configure devices in a network where a multicast server is delivering services over the network via a multicast router. This router is also the querier and controls the delivery of multicast streams.

In this example, multicast services are delivered on VLAN 300.

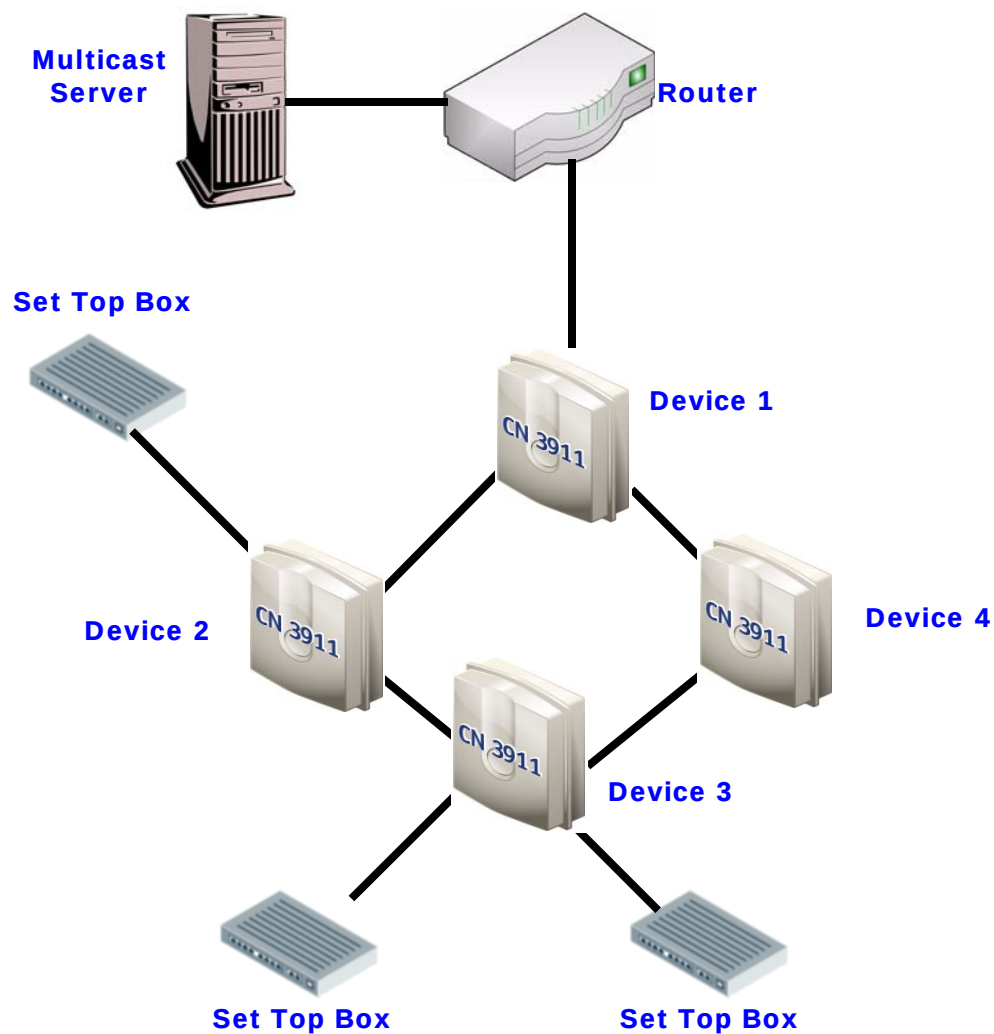


Figure 15-4: Multicast Services with a Multicast Router

To configure multicast services:

Step #	Description	Command
Step 1	Create a multicast entry for the VLAN on all four devices. This enables multicast services for the specified VLAN.	<code>multicast-services create vlan <VlanList></code>
Step 2	Set the query timers to the same values as on the multicast router. The default value for the query-ip-source-address is 0.0.0.0. This value is used as the source address for all query messages as well as for proxy-reply messages sent to the router. The default value should work in most cases. However, if this address must be changed because of a router on the network, make sure to use the correct address for the router interface you are using, otherwise, the router may discard all proxy-reply messages from the device.	<code>multicast-services igmp- snooping set</code>
Step 3	Enable IGMP snooping on all four devices.	<code>multicast-services igmp- snooping enable</code>
Step 4	(Optional) Enable UMF on the specified VLAN for the devices that have subscriber equipment connected to them (in our example, device 2 and 3). In this scenario, UMF blocks multicast streams originating from subscriber equipment or other locations in the network. It also ensures the subscriber devices receive only the multicast streams they have joined.	<code>multicast-services umf drop</code>
Step 5	(Optional) Verify the IGMP settings.	<code>multicast-services show configuration</code>

Since the configuration of each box is very similar, the following example will configure device 2 from **Figure 15-4**.

CLI Example:

1. `> multicast-services create vlan 300`
2. `> multicast-services igmp-snooping set query-response-interval
100`
3. `> multicast-services igmp-snooping enable`
4. `> multicast-services umf drop vlan 300`

5. > multicast-services show configuration vlan 300

MULTICAST CONFIGURATION VLAN 300 VLAN#300		
Global Multicast Services		enable
Multicast Services		enable
UMF		drop
WKM Forwarding		disabled
IGMP CONFIGURATION (general)		
IGMP Snooping		enable
IGMP Server Topology		centralized
IGMP Query Engine		off
IGMP Leave Mode		fast
L2 Packet Priority		7
Robustness		1
IGMP CONFIGURATION (proxy query)		
Proxy Query Interval (s)		125
Proxy Query Response Interval (ds)		100
Proxy Query Delay (ds)		10
Proxy Query Source Address		0.0.0.0
Last Member Query Interval (ds)		10
IGMP CONFIGURATION (router)		
Router Query Interval (s)		250
Linger Timeout (s)		120
Active Linger Timeout (s)		30
Minimum Query Response Interval (ds)		50
Group Address Range (start)		0.0.0.0
Group Address Range (end)		0.0.0.0
Default Router Port		0

Multicast Server Topology

This example shows how to configure devices in a network that does not employ a multicast router. The multicast server floods a set of multicast streams on the network. The device connected to the multicast server is configured to contain the multicast streams and to act as the querier (Query Engine enabled) for downstream devices.

For this example, multicast services are delivered on VLAN 300. In the topology represented in **Figure 15-5**, UMF is required on device 1 to contain the streams being flooded by the multicast server. On all other devices, UMF is optional.

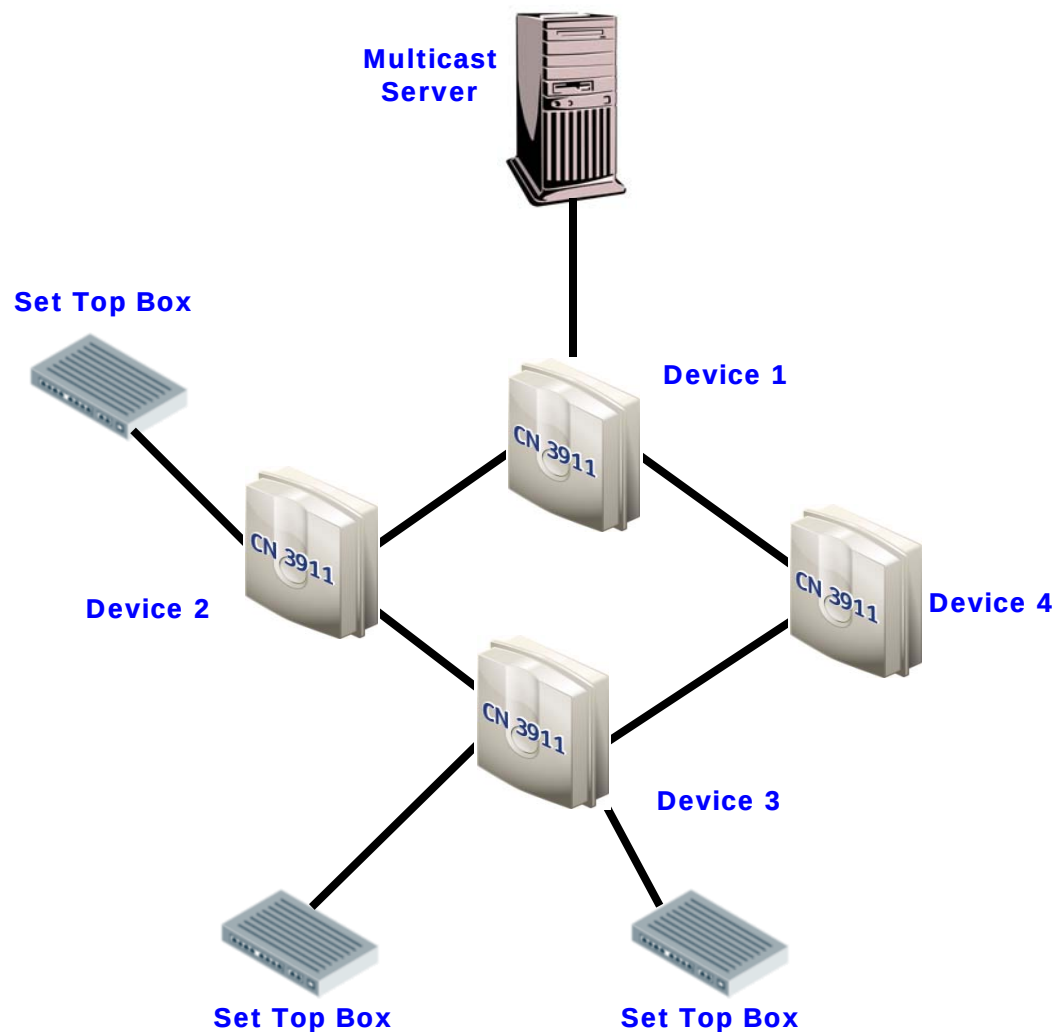


Figure 15-5: Delivering Multicast Services using the Query Engine

To configure multicast services:

Step #	Description	Command
Step 1	Create a multicast entry for the VLAN on all four devices. This enables multicast services for the specified VLAN.	<code>multicast-services create vlan <VlanList></code>
Step 2	Configure the Query Engine on the same device. When using this command, the source IP address must be set before the Query Engine is enabled. In addition, the router port must be set to 0 (unlearned).	<code>multicast-services igmp- snooping set</code>

Step #	Description	Command
Step 3	Enable IGMP snooping on all four devices.	<code>multicast-services igmp-snooping enable</code>
Step 4	Enable UMF on device 1. (Optional) Enable UMF on the specified VLAN for the devices that have subscriber equipment connected to them (in our example, device 2 and 3).	<code>multicast-services umf drop</code>
Step 5	(Optional) Verify the IGMP settings.	<code>multicast-services show configuration</code>

The following examples configure device 1 from **Figure 15-5**.

CLI Example:

1. `> multicast-services create vlan 300`
2. `> multicast-services igmp-snooping set query-ip-source-addr 10.10.10.10 query-engine on`
3. `> multicast-services igmp-snooping enable`
4. `> multicast-services umf drop vlan 300`
5. `> multicast-services show configuration vlan 300`

MULTICAST CONFIGURAITON VLAN 300 VLAN#300		
Global Multicast Services	enable	
Multicast Services	enable	
UMF	drop	
WKM Forwarding	disabled	
IGMP CONFIGURAITON (general)		
IGMP Snooping	enable	
IGMP Query Engine	on	
IGMP Leave Mode	fast	
L2 Packet Priority	7	
Robustness	1	
IGMP CONFIGURAITON (proxy query)		
Proxy Query Interval (s)	125	
Proxy Query Response Interval (ds)	100	
Proxy Query Delay (ds)	10	
Proxy Query Source Address	10.10.10.10	
Last Member Query Interval (ds)	10	
IGMP CONFIGURAITON (router)		
Router Query Interval (s)	250	
Linger Timeout (s)	120	
Active Linger Timeout (s)	30	
Minimum Query Response Interval (ds)	50	
Group Address Range (start)	0.0.0.0	
Group Address Range (end)	0.0.0.0	
Default Router Port	0	

Multicast with Redundant Routers

This example demonstrates how to configure devices in a network that has two (or more) redundant multicast servers. Both multicast servers are connected to the network via a multicast router.

In this scenario, only one router with its associated multicast server, is active at a time. The second router and server in a standby mode. The active server is determined by identifying the router that has the lowest IP address. This router will handle general queries and “authorize” the delivery of various streams through the network.

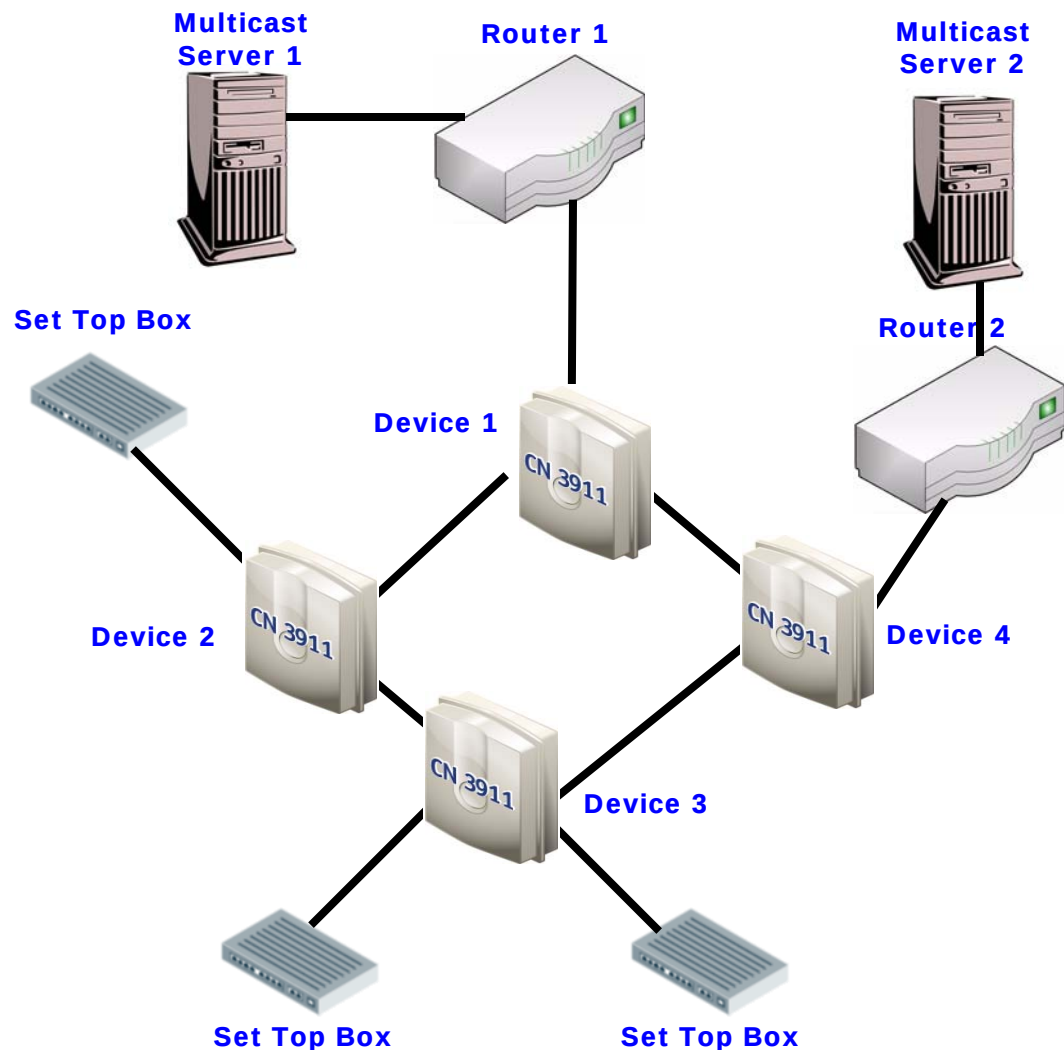


Figure 15-6: Delivering Multicast Services Using Redundant Multicast Routers

In response to a topology change, for example, if the link that has the router port for the device goes down, device will advertise a router address of 0.0.0.0 to indicate that it has lost the router. For example, assuming that router 1 has a lower IP address than Router 2, if the link between device 1 and Router 1 goes down, devices 1, 2, 3 and 4 will send out general queries advertising a router address of 0.0.0.0. Device 4 will become the interface for multicast services and all joins/leaves will then be sent to it. However, when Router 1 is restored, it will again become the primary router and Router 2 will again go into standby mode.

This allows the network to continue delivery of multicast services while ensuring the least delay in service possible. This also allows order to be maintained between the two multicast routers, so that there is no competition or confusion.

In this example, multicast services are assumed to be delivered on VLAN 300. For the network represented in **Figure 15-6**, UMF is required on device 1, and device 2. On all other devices, it is optional.

To configure multicast services:

Step #	Description	Command
Step 1	Create a multicast entry for the VLAN on all four devices. This enables multicast services for the specified VLAN.	<code>multicast-services create vlan <VlanList></code>
Step 2	Enable UMF on device 1 and device 4. (Optional) Enable UMF on the specified VLAN for the devices that have subscriber equipment connected to them (in our example, device 2 and 3).	<code>multicast-services umf drop</code>
Step 3	Set the query timers to the same values as on the multicast router. The default value for the query-ip-source-address is 0.0.0.0. This value is used as the source address for all query messages as well as for proxy-reply messages sent to the router. The default value should work in most cases. However, if this address must be changed because of a router on the network, make sure to use the correct address for the router interface you are using, otherwise, the router may discard all proxy-reply messages from the device.	<code>multicast-services igmp- snooping set</code>
Step 4	Enable IGMP snooping on all four devices.	<code>multicast-services igmp- snooping enable</code>
Step 5	(Optional) Verify the IGMP settings.	<code>multicast-services show configuration</code>

Since the configuration of each box is very similar, the following example will configure device 1 from **Figure 15-6**. Note that device 1 and device 4 should be configured exactly the same.

CLI Example:

1. `> multicast-services create vlan 300`
2. `> multicast-services umf drop vlan 300`
3. `> multicast-services igmp-snooping set query-response-interval
100`
4. `> multicast-services igmp-snooping enable`

5. > multicast-services show configuration vlan 300

+-----+-----+		
	MULTICAST CONFIGURATION VLAN 300 VLAN#300	
	+-----+-----+	
	Global Multicast Services	enable
	Multicast Services	enable
	UMF	drop
	WKM Forwarding	disabled
	+-----+-----+	
	IGMP CONFIGURATION (general)	
	+-----+-----+	
	IGMP Snooping	enable
	IGMP Server Topology	centralized
	IGMP Query Engine	off
	IGMP Leave Mode	fast
	L2 Packet Priority	7
	Robustness	1
	+-----+-----+	
	IGMP CONFIGURATION (proxy query)	
	+-----+-----+	
	Proxy Query Interval (s)	125
	Proxy Query Response Interval (ds)	100
	Proxy Query Delay (ds)	10
	Proxy Query Source Address	0.0.0.0
	Last Member Query Interval (ds)	10
	+-----+-----+	
	IGMP CONFIGURATION (router)	
	+-----+-----+	
	Router Query Interval (s)	250
	Linger Timeout (s)	120
	Active Linger Timeout (s)	30
	Minimum Query Response Interval (ds)	50
	Group Address Range (start)	0.0.0.0
	Group Address Range (end)	0.0.0.0
	Default Router Port	0
	+-----+-----+	

Redundant Query Engines

This example demonstrates how to configure devices in a network that has redundant links between the multicast server and the rest of the network.

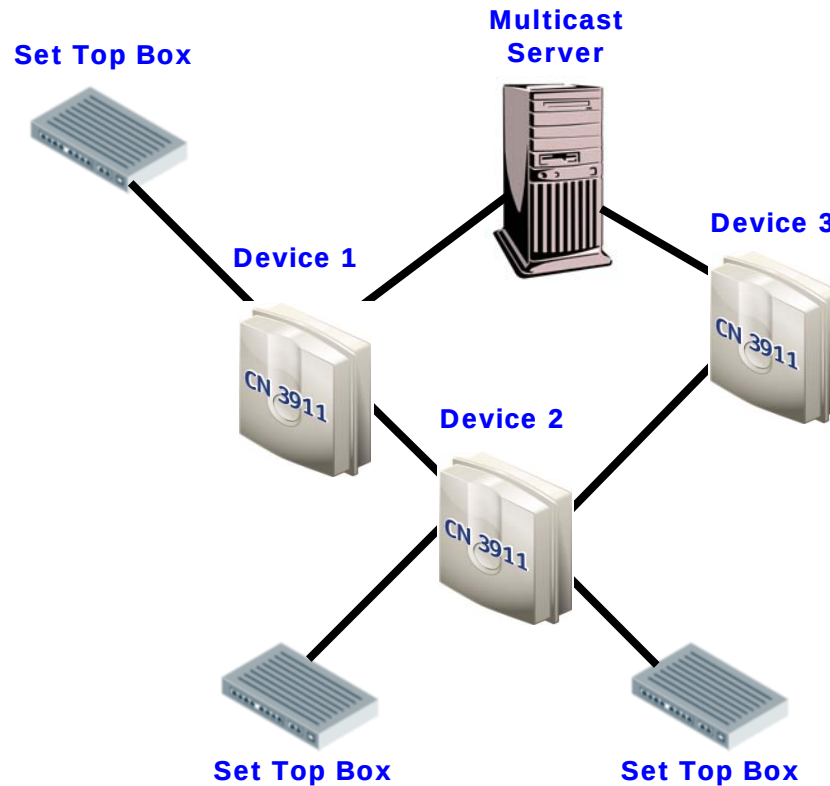


Figure 15-7: IGMP Snooping

In this scenario, the Query Engine must be enabled on device 1 and device 3, but only one Query Engine will be active at a time. The second Query Engine will effectively be in standby mode. The active Query Engine is determined by identifying the engine with the lowest source IP address. This Query Engine then handles general queries and “authorizes” the delivery of various streams through the network.

In response to a topology change, for example, if the link that has the router port for a device goes down, the device will advertise a router address of 0.0.0.0 to indicate that it has lost the router.

For example, assuming that device 1 has a lower source IP address than device 3, if the link between device 1 and the Multicast Server goes down, devices 1, 2, and 3 will send out general queries advertising a router address of 0.0.0.0. Device 3 will then become the interface for multicast services and all joins/leaves will then be sent to it. However, when the link between device 1 and the Multicast Server is restored, it will again become the primary Query Engine, and device 3 will return to standby mode.

This allows the network to continue delivery of multicast services while ensuring the least delay in service possible. This also allows order to be maintained between the two Query Engines, so that there is no competition or confusion.

In this example, multicast services are assumed to be delivered on VLAN 300. The network should also be using RSTP. For the network represented in **Figure 15-7**, UMF is required on device 1, and device 3. On all other devices, it is optional.

To configure multicast services:

Step #	Description	Command
Step 1	Create a multicast entry for the VLAN on devices 1, 2, and 3. This enables multicast services for the specified VLAN.	<code>multicast-services create vlan <VlanList></code>
Step 2	Configure the Query Engine on devices 1 and 3. When using this command, the source IP address must come before the Query Engine is enabled, in order to function properly. In addition, the router port must be set to 0 (unlearned). Make sure that the source IP address for the two devices is different and that the device that should become the primary Query Engine has a lower IP address.	<code>multicast-services igmp-snooping set [query-ip-source-addr <IpAddress>] [query-engine <on off>]</code>
Step 3	Enable IGMP snooping on devices 1, 2, and 3.	<code>multicast-services igmp-snooping set</code>
Step 4	Enable UMF on devices 1 and 3. (Optional) Enable UMF on devices that have subscriber equipment connected to them (in our example, device 2).	<code>multicast-services umf drop</code>
Step 5	(Optional) Verify the IGMP settings.	<code>multicast-services show configuration</code>

Since the configuration of each box is very similar, the following example will configure device 1 from **Figure 15-5**. Note that with the exception of the Query Engine source IP address, the configuration for device 1 and device 3 should be exactly the same.

CLI Example:

1. `> multicast-services create vlan 300`
2. `> multicast-services igmp-snooping set query-ip-source-addr 10.10.10.10 query-engine on`
3. `> multicast-services igmp-snooping enable`
4. `> multicast-services umf drop vlan 300`

5. > multicast-services show configuration vlan 300

MULTICAST CONFIGURAITON VLAN 300 VLAN#300	
Global Multicast Services	enable
Multicast Services	enable
UMF	drop
WKM Forwarding	disabled
IGMP CONFIGURAITON (general)	
IGMP Snooping	enable
IGMP Query Engine	on
IGMP Leave Mode	fast
L2 Packet Priority	7
Robustness	1
IGMP CONFIGURAITON (proxy query)	
Proxy Query Interval (s)	125
Proxy Query Response Interval (ds)	100
Proxy Query Delay (ds)	10
Proxy Query Source Address	10.10.10.10
Last Member Query Interval (ds)	10
IGMP CONFIGURAITON (router)	
Router Query Interval (s)	250
Linger Timeout (s)	120
Active Linger Timeout (s)	30
Minimum Query Response Interval (ds)	50
Group Address Range (start)	0.0.0.0
Group Address Range (end)	0.0.0.0
Default Router Port	0

Chapter Layer 2 VPNs

16

At a Glance:

- Overview
- Principles of Operation
- Q-in-Q Encapsulation
- Ethernet Virtual Private Line
- Ethernet Private Line/LAN
- EVPL Bundling

This chapter details the configuration of Layer 2 VPNs on devices running SAOS software, providing support for 802.1ad Provider Bridging.

Overview

Virtual Private Networks (VPNs), generally based on traditional Frame Relay and ATM services, have been broadly used with carriers and customers, providing point to point and WAN solutions. These technologies were historically expensive to install and complicated to operate. However, new end-user services have been implemented using Ethernet LAN services as a broadcast technology.

This solution supports the deployment of L2 VPNs or Transparent LAN Services that enable a service provider to provide Ethernet Private Line/LAN (EPL) or Ethernet Virtual Private Line (EVPL) to their encap customers. The customer perspective is that their connection to the service provider is a direct connection to a private line or LAN between their sites. Up to 64 provider bridges can be supported.

L2 VPNs transport Ethernet/802.3 and VLAN tagged traffic between multiple sites that belong to the same L2 broadcast domain or VPLS service. These services are deployed over Ethernet using an extension of 802.1Q, called Q-in-Q.

Principles of Operation

Q-in-Q is implemented via the attachment of a Virtual Circuit (defining the Provider VLAN) to a Virtual Switch (defining the Subscriber VLANs), as shown in **Figure 16-3**. The customer perspective is that their connection to the service provider is a direct connection using a private LAN between geographically separated sites.

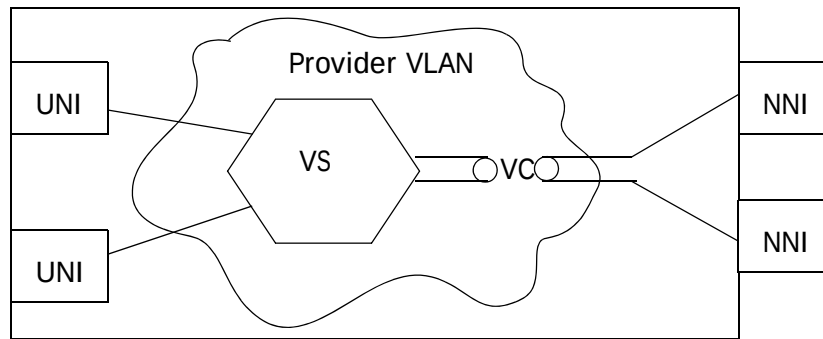


Figure 16-1: Provider VLAN Overview Using Q-in-Q



NOTE: In order to use the 802.1ad provider bridging feature, you need to install the Advanced Ethernet (AE) license key. License keys can be purchased by contacting Ciena customer support.

Virtual Switch

A virtual switch (VS) is a Layer 2 forwarding domain between a customer bundle (multiple per-port per-VLAN entries) or per-port entries and the network transport interfaces (VCs). Ethernet switches have long been governed by the use of VLANs. Traffic tagged with a specific VLAN is forwarded to other VLAN member ports. However, in geographically separated networks, the same VLAN ID may be used by more than one subscriber group, but for security and administrative purposes, the VLAN must remain separated.

A virtual switch essentially separates the forwarding plane from the data plane, thus the virtual switch is customer-centric, while the virtual circuit is service-centric.

A virtual switch should be configured whenever there is a need for a Point-to-Point, Ethernet Virtual Private LAN solution.

Reserved VLAN

A reserved VLAN is used internally to link a virtual switch with an internal switching domain, and acts to connect both subscriber and provider facing interfaces. A reserved VLAN must be created for each virtual switch before the virtual switch is configured. The reserved VLAN pool is part of the same 1-4094 range as the system VLAN pool. The system assigns the reserved VLAN from this pool when the VS is created.

Subscriber/UNI traffic can also be switched without connecting to the provider/transport network.

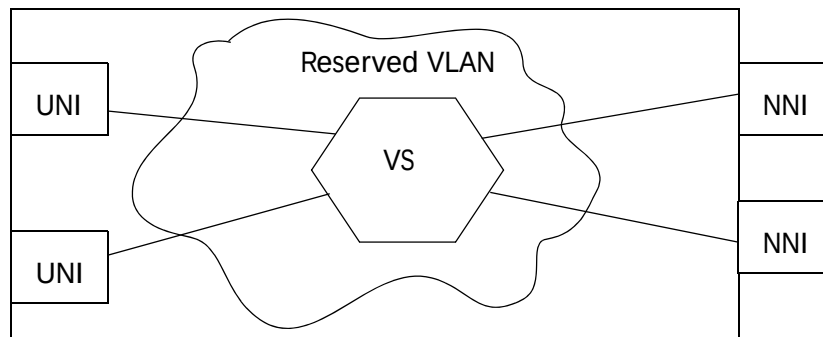


Figure 16-2: Reserved VLAN

Reserved VLANs are configured using the `virtual-switch add reserved-vlan` CLI command. Reserved VLANs cannot be deleted using the `vlan delete` CLI command, instead they must be removed using the `virtual-switch remove reserved-vlan` command. In addition, the default name for a reserved VLAN cannot be changed, so reserved VLANs will always appear in the format of `VLAN#XXX`.

The `virtual-switch show` command can be used to see which reserved VLAN is associated with a virtual switch:

```
> virtual-switch show
```

Virtual Circuits

A virtual circuit (VC) defines a secure logical connection between one or more customer endpoints. It is a service trunk, where transport services start and end (encap and decap). This association is based on an extension to IEEE 802.1ad VLAN standard referred to as double tagging (Q-in-Q). Virtual circuits encapsulate and decapsulate L2 tags over the service provider's network to allow data to be easily switched without the need for in-depth individual packet analysis or routing decisions at each network device. They can be thought of as the provider VLAN.

Provider VLAN

The provider VLAN is defined by the VLAN assigned to the virtual circuit when it is created. When a VC with a provider VLAN is attached to a VS, the provider VLAN itself becomes the double-tagged (encapsulated) VLAN. The virtual circuit references the provider VLAN, and the VC VLAN has a service port associated with it.

Q-in-Q Encapsulation

Encapsulating an 802.1Q VLAN tagged frame within another 802.1Q tag enables the service provider to encapsulate the customer VLAN tagging information while using VLANs within the provider network. SAOS allows Ethernet virtual circuits to be statically created. An Ethernet-VC uses an additional 802.1Q VLAN tag and includes the following:

- Service Etype (default 0x8100)
- Service VLAN ID (range)
- Service .1d (range)

An Ethernet-VC has the following properties which can be configured statically:

- Name
- Provider VLAN ID and port
- Encapsulation (encap) Priority Policy (802.1D)

The following configurations are supported:

- Per-port (PP) Q-in-Q
- Per-port-per-VLAN (PPV) Q-in-Q

Q-in-Q Ethertype

The Ethertype of the outer VLAN tag can be customized. This allows compatibility with standard 802.1Q encapsulation methods like Extreme's vMAN that uses the 9100, and 802.1ad for Provider Bridging. Using the `virtual-circuit ethernet set port` command, the Ethertype value to use can be configured as described in **Table 16-1**, in this chapter.

Table 16-1: Ethertype Setting (Per-Port)

Name	Description
8100	This indicates to use normal 802.1Q Ethertype for all frames egressing the port.
9100	This indicates to use the 0x9100 Ethertype on frames using the user configured policy described in Table 16-2 , in this chapter.
88a8	This indicates to use the 802.1ad Ethertype on frames using the user configured policy described in Table 16-2 , in this chapter.

The `virtual-circuit ethernet set port` command includes a setting that allows the operator to specify the policy or rules for applying that configured Ethertype on a per-port basis as described in **Table 16-2**, in this chapter.

Table 16-2: Ethertype Policy (Per-Port)

Name	Description
all	When this policy is set then only Q-in-Q encapsulated frames going out the port will use the configured Ethertype (see Table 16-1 , in this chapter).
encap-only	When this policy is set then only encapsulated frames going out a port will use the configured Ethertype (see Table 16-1 , in this chapter). This will affect both single and double tagged frames that have had a provider VLAN tag added to them.

NOTE: The only policy available on current platforms is All. This means that all VLAN tagged frames that egress the port will be affected by the configured Ethertype as the outer tag e-type.

CVLAN to S-PRI COS Policy Override

You can override the `encap-cos-policy` of the VS by setting the `encap-cos-policy` of the VS member to `fixed`. The fixed COS value is then obtained from the `encap-fixed-dot1dpri` parameter of the VS member.

CLI Example:

```
> virtual-switch ethernet add vs vsName port 1 vlan 300 encap-cos-policy fixed  
encap-fixed-dot1dpri 5
```

Ethernet Virtual Private Line

Figure 16-3 illustrates a point to point Ethernet Virtual Private Line (EVPL) that supports multiple Ethernet-VCs per UNI. Frames from port-VLAN-based classified UNI ingress are forwarded to the NNI egress by adding a specified SVID.

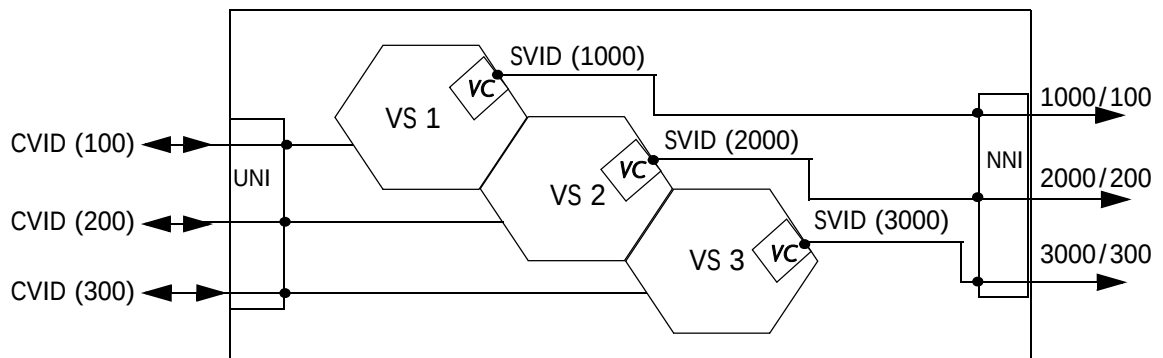


Figure 16-3: EVPL Provider Bridging

To create an EVPL provider bridge:

1. Create a provider VLAN and add the NNI port to the VLAN.
2. Create an Ethernet virtual circuit for the provider VLAN.
3. Create a virtual switch and add UNI port(s) to the subscriber VLAN.
4. Attach the Ethernet VC to the VS.

CLI Example:

```
> vlan create vlan 100  
> vlan create vlan 200  
> vlan create vlan 300  
> vlan add vlan 100,200,300 port 7,8  
> virtual-circuit ethernet create vc vc0 vlan 100  
> virtual-circuit ethernet create vc vc1 vlan 200  
> virtual-circuit ethernet create vc vc3 vlan 300  
> virtual-switch add reserved-vlan 1000-1002  
> virtual-switch ethernet create vs vs1 vc vc0 encap-fixed-dot1dpri 0  
> virtual-switch ethernet create vs vs2 vc vc1 encap-fixed-dot1dpri 1  
> virtual-switch ethernet create vs vs3 vc vc2 encap-fixed-dot1dpri 2  
> virtual-switch ethernet add vs vs1 port 1 vlan 100  
> virtual-switch ethernet add vs vs2 port 1 vlan 200  
> virtual-switch ethernet add vs vs3 port 1 vlan 300
```


Ethernet Private Line/LAN

SAOS supports point to point Ethernet Private Line (EPL) with one EVC per UNI. Frames from port-based and port-vlan-based classified UNI ingress are forwarded to an NNI egress by adding a specified SVID, and are forwarded to a UNI egress by removing the SVID. The UNI port will only accept an untagged-data-vs configuration that matches the VS of the Per Port (EPL) member. This can be used in conjunction with the ingress-vs-filter.

As an example, **Figure 16-4** shows an example of an EPL provider bridge.

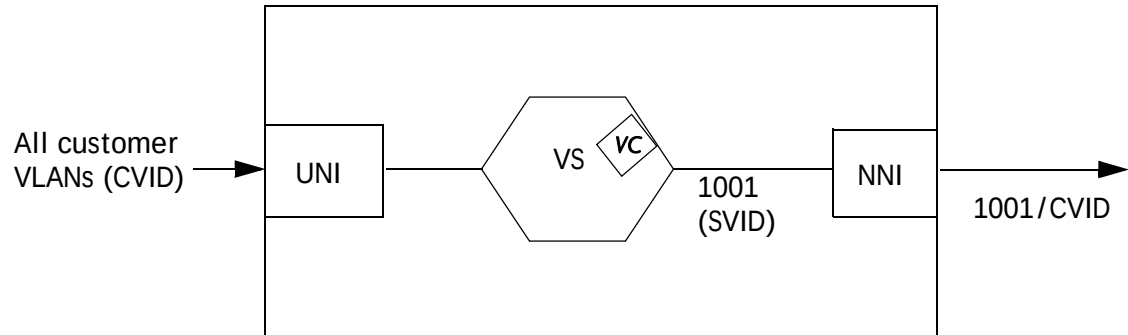


Figure 16-4: Ethernet Private Line

CLI Example:

```

> vlan create vlan 101
> vlan add vlan 101 port 10
> virtual-switch add reserved-vlan 1001

> virtual-circuit ethernet create vc EVC101 vlan 101
> virtual-switch ethernet create vs EVS100 vc EVC101 encap-fixed-dot1dpri 3
> virtual-switch ethernet add vs EVS100 port 1 vlan 100
  
```

SAOS also supports point to multipoint Ethernet Virtual Private LAN (EVP-LAN) with multiple EVCs per UNI and fixed policy priority bit re-marking on ingress.

EVPL Bundling

SAOS supports Ethernet Virtual Private Line (EVPL) bundling. EVPL bundling allows multiple customer VLAN IDs (C-VIDs) to be mapped to one or more virtual switches. Up to 4094 unique VLANs can be configured on one port. It should be noted that EVPL bundling will only function where traffic is being encapsulated.

As an example, **Figure 16-5** shows multiple C-VIDS ingressing on port 28. VLANs 10-20 have been mapped to virtual switch 2, and VLANs 100-110 and 250 are mapped to Ethernet-VS 1. This allows multiple C-VIDs to be mapped to two separate virtual switches.

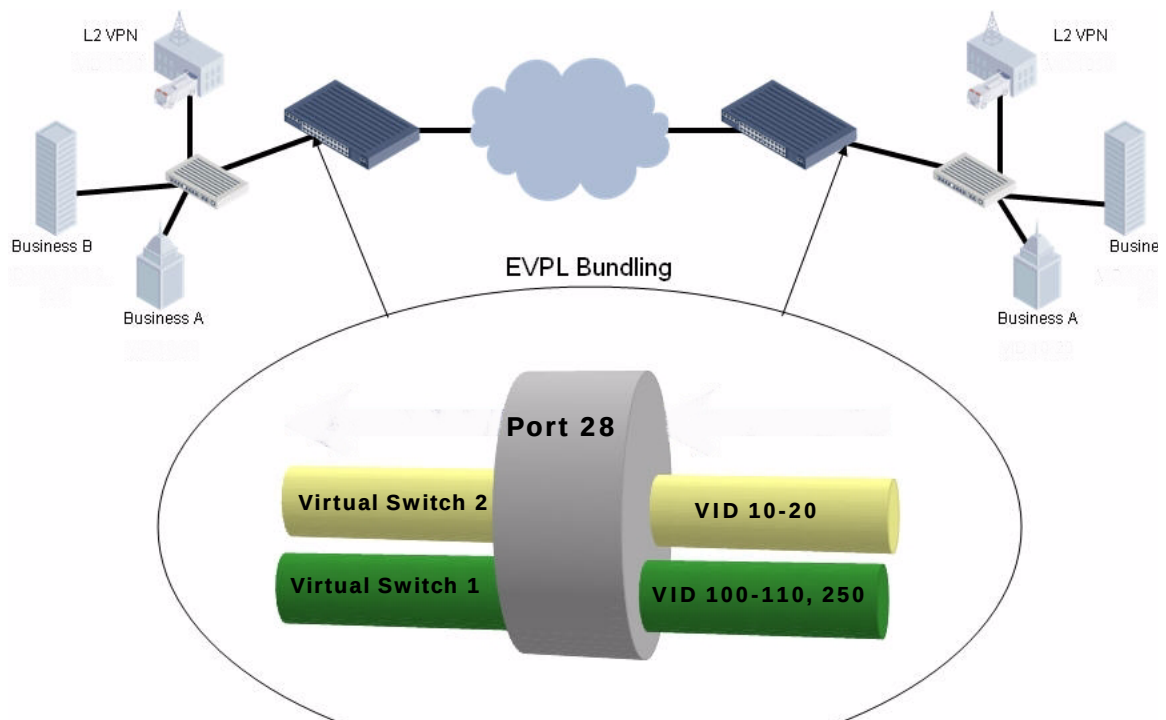


Figure 16-5: Multiple C-VIDS to Multiple VS

CLI Example:

```
> virtual-switch ethernet add vs vs1 port 28 vlan 100-110,250  
> virtual-switch ethernet add vs vs2 port 28 vlan 10-20
```



NOTE: If the port vlan-ingress-filter parameter is set to on, only frames that match a configured VLAN tag will be forwarded.

Chapter 17

Configuring Connectivity Fault Management

At a glance:

- Overview
- Benefits
- Configuring CFM Globally
- Configuring CFM Services
- Configuring MEPs
- Configuring Remote MEPs
- Configuring MIPs
- Configuring CFM Services for a VLAN Service
- Configuring CFM Services for a Virtual Switch
- CFM Over Q-in-Q
- Troubleshooting

This chapter discusses the Ciena implementation of the IEEE P802.1ag/D8 Connectivity Fault Management (CFM) protocol that is used to detect and isolate network service connectivity problems.

Overview

Connectivity Fault Management (CFM) provides a method to continuously monitor the end-to-end network connectivity of a network service, such as a Virtual Switch (VS) or a VLAN. Services can be monitored over a single hop, a point-to-point link, or over multiple hops, using equipment managed by one or more service providers and operations entities. Services are identified by a collection of Service Access Points (SAPs) called a Service Instance. There are two types of SAPs:

- Maintenance End Points - Maintenance End Points (MEPs) are created at the edge (entry/exit) points of the service being monitored.
- Maintenance Intermediate Points - Maintenance Intermediate Points (MIPs) are created between MEPs to track faults at intermediate points.

MEPs send periodic multicast messages (called Continuity Check Messages or CCMs) to each other through the VS or VLAN service to determine the status of the service connection. These can be thought of as heartbeat messages. Devices not configured for CFM forward CCMs as they would any other multicast message. If an expected CCM is not received by a MEP on a participating network device within the specified period, a fault alarm regarding the service is issued in the form of an SNMP trap and system log message.

In **Figure 17-1**, the service being monitored is VLAN 5. The MA consists of three MEPs (one on each edge of the service) and several MIPs. One of the MEPs monitors VLAN 5 at its source, which is the connection to the service provider. The other two MEPs monitor VLAN 5 at the devices that connect directly to the customer premise equipment (CPE). The MIPs represent one or more CFM-configured network devices (switches/Service Delivery Switches/Service Concentration Switches) used to connect VLAN 5 to multiple subscribers.

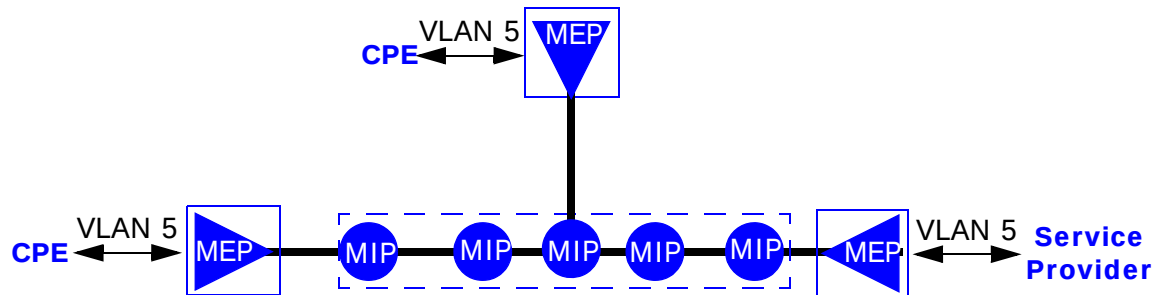


Figure 17-1: Example Maintenance Association (MA)

Maintenance Domains

Unless a dedicated end-to-end physical connection is used (such as a fiber optic cable), delivering Ethernet services between remote sites typically requires connections through equipment installed and controlled by a separate administrative entity. Each of these entities needs to monitor the status of the services that they are providing in order to be aware of any loss of service and at what point the service has been disrupted.

In order to monitor the same service through the equipment used by various carrier entities, portions of the network under the control of a common administrative entity are identified by a Maintenance Domain (MD). CFM provides up to eight MDs each numbered from 0-7 to identify its position relative to adjacent CFM domains. The values assigned must be carefully chosen, with the lowest numeric value used for the “inner most” domain levels and higher numbered domain levels assigned in sequence as they are configured outward toward the ends of the service. CFM domains must be fully nested, that is, an inner domain must be fully contained within a surrounding domain.

The default MD level is 3. The MD level does not necessarily have to be changed to configure CFM. The level would only have to be changed when the Operator’s CFM needs are different from what a level 3 MD can provide.



NOTE: If a Maintenance Domain name is changed, it must be changed on *all* other units. The name must be the same on each end point.

The three general types of domains are: Customer, Provider, and Operator. These names are guidelines to indicate the type of entity typically associated with a particular maintenance domain.

- **Customer** domains contain the devices connected to the customer and to the source of the service being monitored. For example, if two physically separate business entities are connecting to each other, customer equipment is configured for CFM operation at both ends to monitor the connection, specifying the same domain at both ends. The Customer domain is assigned a level in the range of 5 to 7.

- **Provider** domains represent the connection used to join each end of the Customer domain. For example, this could be the Internet service provider used by the business. The Provider domain is assigned a level in the range of 3 to 4.
- **Operator** domains are the central physical infrastructure provider. This could be the owner of a fiber optic network that spans the distance between the cities where the two business units are located. The Operator domain is assigned a level in the range of 0 to 2.

Figure 17-2 shows three Maintenance Domains associated with a Service Instance used to monitor connectivity across a Provider network between two CE devices. Devices CE1 and CE2 reside in the outer-most MD at MD Level 5. The CE devices may be administered by either the Customer or the Provider. The Provider administers devices MTU1 and MTU2 in a second MD at MD Level 4, which is surrounded by the Customer MD. The CE devices connect to the service at Domain Service Access Points (DSAPs) on the boundary between the Customer and Provider MDs. DSAPs are members of the MD that offer the ability to connect to external systems and lie on the edge of the MD. These DSAPs correspond to the same physical ports as those associated with the SAPs in **Figure 17-2**. The example includes a third MD at MD Level 2, contained within the Provider MD. This illustrates that the Provider has contracted with an Operator to transport the service between its MTU devices. The Provider connects its devices to the Operator's network at a second set of DSAPs, which lie on the boundary between the Provider and Operator Maintenance Domains. The Provider has no knowledge of the internal topology or configuration of the network contained within the Operator MD.

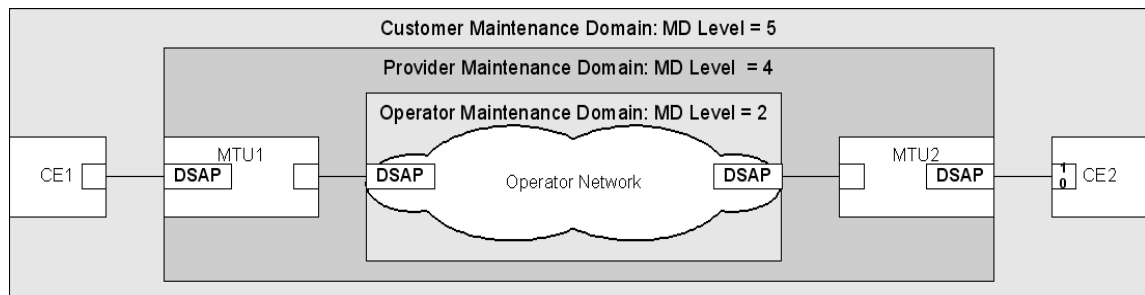


Figure 17-2: Nested Maintenance Domains

MEPs pass CCMs of higher relative domain levels without acting on them. For example, when one of the MEPs in the Customer domain sends a CCM, the MEPs in the Provider and Operator domain pass the CCMs on to the MEP at the other end of the Customer domain. This is what allows Connection Fault Management to work across multiple domains. However, CCMs with equal or lower relative domain levels are not passed on by MEPs in order to contain those messages within their respective domains.

Maintenance Associations

A Maintenance Association (MA) relates a Service Instance with a Maintenance domain and includes the group of SAPs belonging to the Service Instance. CFM frames carry a Maintenance Association Identifier (MAID) that identifies the connection between SAPs. The MAID includes the Maintenance Domain name along with a Short MA Name.

MEPs

As previously mentioned, MEPs send and receive continuity check messages (CCMs) over the service on a periodic basis to determine if that service is still available. Each MEP is assigned a unique numeric identifier (MEPID) and maintains a table of other MEPs (referred to as remote MEPs) that belong to its MA. This table, called the MEP-CCM-Database, is used to determine if one or more remote MEPs are no longer sending CCMs. MEPs are directional: *Up* or *Down*. A Down MEP sends CCMs towards and receives them from the physical medium. Down MEPs monitor service connectivity from one device to another carrying the same service. This could be a direct connection or a connection through several other devices and MIPs. An Up MEP sends CCMs towards and receives them from the MAC Relay Entity.

MIPs

Like MEPs, MIPs respond to and forward link-trace messages that are used to identify the point in an MA where the service is lost. MEPs and MIPs also respond to loopback messages that are also used to isolate faults at intermediate service nodes. Unlike MEPs, MIPs do not exchange CCMs, but they do act on CCMs and forward them. A MIP is not affiliated with a single MA, and processes CFM protocol frames for all MAs traversing an SI at or above its specified MD Level. Another function of a MIP is to record all CCMs received by a logical interface that are at or above its MD Level, in order to construct the MIP-CCM Database. This database serves as a record of the CFM monitored services that are using a service instance, and provides a learn table of the MAC addresses used by MEPs. In the event that entries have aged-out of the normal MAC learn table due to a service failure, the MIP-CCM database can be alternatively queried to resolve forwarding information for Linktrace requests during the troubleshooting process.

Continuity Check Messages

CCMs have the following characteristics:

- Transmitted at a configurable interval (see **Table 17-2**, in this chapter); the same value is used for all MEPs in the MA.
- Catalogued by MIPs at the same MD level.
- Terminated by remote MEPs at the same MD level.
- Carry information that drives several internal state machines, but do not solicit a response.

Loopback Messages

Loopback messages are unicast frames that a MEP transmits, at the request of an administrator, to verify connectivity to a particular MEP or MIP. Upon reception, the MEP or MIP transmits a Loopback Reply (LBR) to the initiator. A loopback message can also be configured to contain arbitrary data, which can be used to diagnose faults that are sensitive to frame size, or a specific data pattern.

Linktrace Messages

Linktrace messages are multicast frames that a MEP transmits, at the request of an administrator, to either isolate a service fault to a specific MEP, or to trace the path through the network to a particular MEP or Target MAC address. When the fdb-only parameter is specified, only the normal forwarding database is used to look up the target MAC, and not the MEP CCM and MIP CCM databases that would also be used otherwise. When processing a received linktrace message, the UseFDBOnly flag in the message is honored when looking up the target MAC.

For each visible MIP, linktrace messages indicate ingress action, relay action, and egress action. Linktrace messages also contain a TTL value (configurable), which is decremented each time the Linktrace messages are forwarded by the MEP or MIP. Linktrace messages are multicast, reply messages are unicast.

ITU-T Y.1731 Performance Measurements

Y.1731, introduced by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) complements the IEEE 802.1ag standard, adding the following:

- Frame delay- the Delay Measurement Message (DMM) and the Delay Measurement Reply (DMR) include time stamps that are used to calculate two-way frame delay. These measurements are configured per CFM service. Each MEP can be enabled to perform frame delay and frame delay variation measurements to peer MEPs in the same ME.
- Jitter- frame delay variation is calculated by tracking the round-trip DMMs. Note that all DMMs expected must be returned in order to make the jitter calculation.
- Frame loss- frame loss is calculated by sending counters within Loss Measurement Messages (LMMs) and Loss Measurement Replies (LMRs). The far-end counters are then compared with the local counters to calculate frame loss for two-way delay measure, port-to-port measurements as a ratio. A bidirectional service is determined unavailable if either of the two directions is declared unavailable, therefore, each MEP must be able to perform near-end and far-end frame loss measurements.

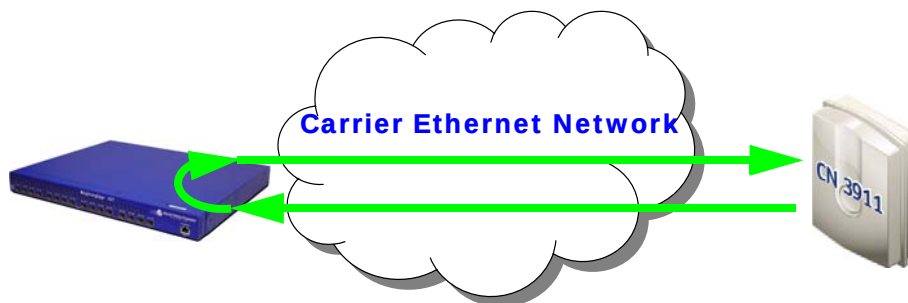


Figure 17-3: Y.1731 Messages Are Initiated Between Two MEPs

Y.1731 tests are initiated by the network administrator and are sent between specific MEPs in the same ME. This then triggers the unicast DMMs or LMMs to be sent to the desired remote MEP with a specified packet count at a configurable interval (default is 100 ms). MIPs do not participate in delay/jitter or frame loss measurements.

As an example, in *Figure 17-4*, MEP 12 could initiate a delay/jitter or frame loss measurement test to MEP 10 or 11. When the test is completed, the delay and jitter measurements from the test will be available and will remain in the system until it is rebooted or another test is run for the same service.

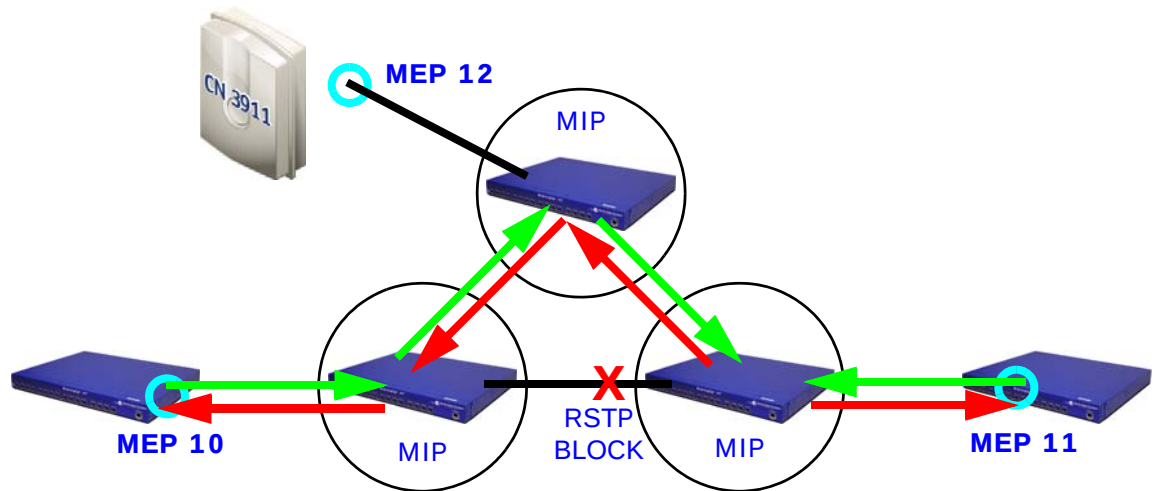


Figure 17-4: Illustration of Path Taken by Y.1731 Messages

Figure 17-4 displays the path that DMMs and LMMs would take (green lines) and the return path for DMRs and LMRs (red lines) for a test of delay/jitter or frame loss initiated on MEP 10 to MEP 11.

Benefits

CFM provides utilities to maintain network connectivity including:

- **Path discovery** - Linktrace messages are used to determine the path taken to a target MAC address.
- **Fault detection** - CCMs are used to detect both connectivity failures and unintended connectivity between Service Instances.
- **Fault verification and isolation** - Loopback messages are used to perform fault verification, or to confirm successful initiation or restoration of connectivity. Linktrace messages and loopback messages are used to isolate faults.
- **Fault notification** - Fault notification is provided by the MEP that detected a connectivity fault either because expected CCMs were not received, unexpected or invalid CCM were received, or the CCM carried a notification of the failure of its associated MEP.
- **Fault recovery** - Fault notifications help network operators correct configuration errors or replace failed components.

Maintenance Association Examples

Provider Example

In this example, a Provider has created a Maintenance Association (MA) to monitor a Service Instance on VLAN 10, associated with a data service sold to the Subscriber. This MA allows the Provider to determine whether or not the fault lies within its own network if a Subscriber reports that the service is down.

For simplicity, this example depicts only the relationship between two MEPs on two Service Delivery Switches in Multi-tenant Units (MTU1 and MTU2). **Figure 17-5** depicts the MEP on MTU1, port 2, and MTU2 port 9. The Provider creates Maintenance Association PROVIDER1 at Maintenance Domain Level 4 on each MTU device. MEPs 1 and 2 on port 2 and port 9 respectively are then added to this Maintenance Association.

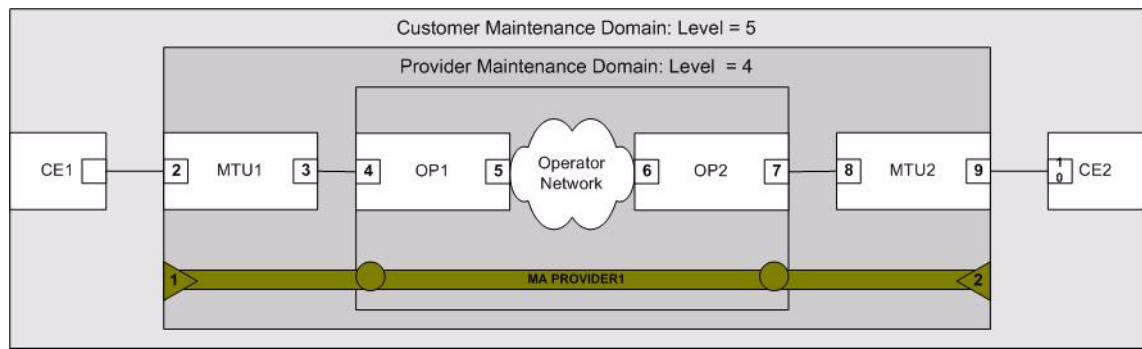


Figure 17-5: Provider Maintenance Association

In order for the Provider to monitor and troubleshoot service connectivity to the edge of the Operator network, the Operator must expose MIPs at the ports where the service connects to its network. Although the Provider is unable to administratively manage these MIPs, they allow the Provider to use CFM Loopback and Linktrace mechanisms to determine whether or not a service fault lies within the Operator network.

The Operator creates MIPs for VLAN 10 at MD Level 4 in ports 4 and 7. These MIPs are not associated with a specific Maintenance association, and are accessible by any Maintenance Association associated with its VLAN and MD Level. Thus, the Operator is able to provide MIPs to the Provider without specific knowledge of the Provider's Maintenance Association configuration.

Operator Example

In this example, the Operator (OPERATOR1) and the Provider wish to use CFM to simultaneously monitor the service on VLAN 10. To this end, the Operator creates its own Maintenance Association for the service at Maintenance Domain Level 2. This MA allows the Operator to monitor and troubleshoot connectivity for the service within its own network without interfering with the operation of the Provider's Maintenance Association on the same VLAN, but at a higher MD Level.

As shown in **Figure 17-6**, configuration of this MA requires the creation of the OPERATOR1 Maintenance Association on devices OP1 and OP2, and MEPs on ports 4 and 7. Although not depicted in the diagram, the Operator could also create MIPs on any intermediate devices that transport the service.

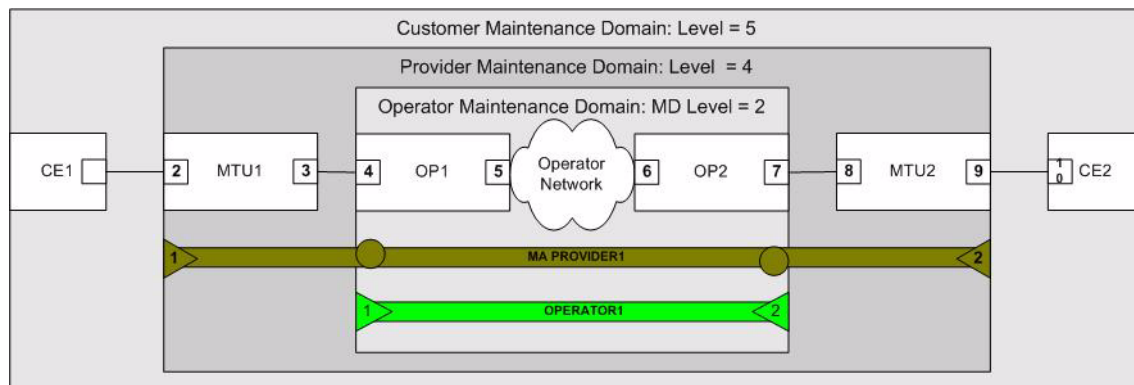


Figure 17-6: Operator Maintenance Association

Customer Example

CFM can also monitor the VLAN 10 service between Subscriber devices in the Customer Maintenance Domain, independent of the Maintenance Associations in the Provider and Operator Maintenance Domains. Although a Customer MA will verify end-to-end service connectivity, the Customer is only able to isolate a fault to a specific link if the fault lies within the Customer Maintenance Domain. A fault can be isolated to the interior of the Provider network, but the Provider must be contacted to further troubleshoot the service disruption.

Figure 17-7 shows a Customer configured MA between the two CE devices. This configuration coexists with the previously defined PROVIDER1 and OPERATOR1 Maintenance Associations. The CUSTOMER1 MA is created on devices CE1 and CE2. MEPs are configured on CE1, port 1 and CE2, port 10. The MIPs shown on the Provider devices MTU1 and MTU2 must be created by the Provider.

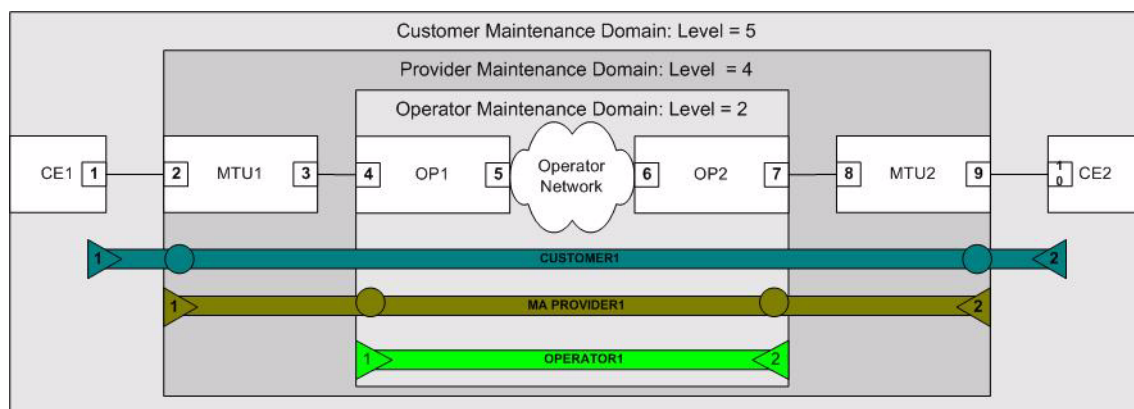


Figure 17-7: Customer Maintenance Association

Physical Link Example

The Maintenance Domain Level 0 is typically reserved for Maintenance Associations that directly monitor physical links. A physical link MA may be associated with a link contained within a single Maintenance Domain, or a link that spans two MDs. Physical Link Maintenance Associations include a MEP on each port at both ends of the link.

In **Figure 17-8**, two physical link Maintenance Associations have been added to the configuration, OPPHY1 and P1. MA OPPHY1 monitors the link between OP1 port 5 and OP2 port 6. The Operator creates this MA at MD Level 0, so that it will not interfere with the operation of the higher-level Maintenance Associations. MEPs are then added to OPHY1 for the ports at each end of the link.

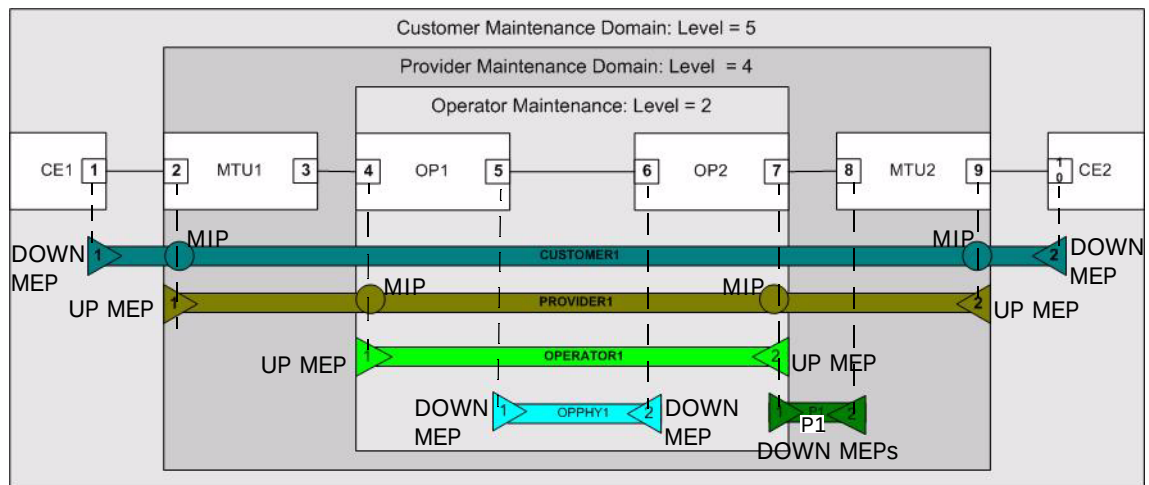


Figure 17-8: Physical Link Maintenance Association

Maintenance Association P1 is configured for the physical link connecting the Provider and Operator networks. Therefore, this requires that the Operator and Provider agree on a Maintenance Domain Level and a Maintenance Association name. The Operator and Provider must each create MA P1 on their respective devices. The Operator creates the MEP for OP2 port 7, while the Provider creates the MEP for MTU2 port 8. Once configured, MA P1 can be used by both Operator and Provider to monitor VLAN 10 connectivity across the link connecting their networks.

Configuring CFM Globally

Global CFM configuration includes:

- Enabling and disabling CFM
- Setting CFM attributes
- Setting and displaying Maintenance Domains



NOTE: In order to configure CFM, you need to install the Advanced OAM (AOAM) license key. License keys can be purchased by contacting Ciena customer support.

Enabling and Disabling CFM

By default CFM is globally disabled.

To enable CFM:

```
cfm enable
```

To disable CFM:

```
cfm disable
```

Setting CFM Attributes

CFM global attributes include:

- **Strict Compliance for 802.1ad (dot1ad-strict)** -When enabled, only CFM frames that contain a single VLAN tag or are untagged are recognized as CFM frames. A double-tagged CFM frame will be forwarded as a normal data frame on interfaces containing MEPs and/or MIPs, and CFM processing is bypassed.
- **Ethertype (ethertype)** - The Ethertype value sent in CFM frames entered in decimal or hexadecimal format. The default is 35074 (0x8902 hexadecimal).
- **MIP Level Enforcement (mip-level-enforcement)** - the level configured on the MIP is ignored when mip-level-enforcement is off.
- **Remote MEP Hold Time (rmep-hold-time)** -When a remote MEP is first detected, it is not declared active and the RMEP fault is not cleared for the time period equal to the remote MEP hold time.
- **Y1731 Ethertype (y1731ethertype)** - The Y1731 Ethertype value sent in CFM frames entered in decimal or hexadecimal format. The default is 35074 (0x8902 hexadecimal).

To set CFM global attributes:

```
cfm set {[dot1ad-strict <enable|disable>], [ethertype <NUMBER: 1-65535>], [mip-level-enforcement <on|off>], [rmep-hold-time <NUMBER: 10-300000>], [y1731ethertype <NUMBER: 2048...65535>]}
```

Example:

```
> cfm set ethertype 35272 mep-hold-time 300000 dot1ad-strict enable mip-level-enforcement on
```

Displaying Global CFM Configuration

To display global CFM configuration:

```
cfm show [statistics]
```

Example:

```
> cfm show
+----- CFM GLOBAL CONFIGURATION -----+
| Parameter                               | Value                               |
+-----+-----+
| Admin State                             | Enabled                             |
| Ethertype                               | 0x8902                             |
| Y1731 Ethertype                         | 0x8902                             |
| Remote MEP Hold Time (ms)              | 10000                              |
| 802.1ad Strict Mode                     | Off                                 |
| MIP Level Enforcement                   | Off                                 |
| MIP CCM Database Learning               | Enabled                             |
| Frames/sec Avail                        | 1998                               |
| Source MAC For PBT CFM Frames           | 00:02:A1:31:23:C0                 |
| Total Rx Frames                         | 360999                             |
| Total Tx Frames                         | 585314                             |
+-----+-----+
```

Setting and Displaying Maintenance Domains

SAOS provides eight pre-configured Maintenance Domains. The name for each maintenance domain defaults to “md” followed by the level: md0, md1, md2, and so on. If desired, you can change the name of the maintenance domain.



NOTE: If a Maintenance Domain name is changed, it must be changed on *all* other units. The name must be the same on each end point.

To change the name of a maintenance domain:

```
cfm md set level <NUMBER: 0-7> name <String[31]>
```

Example:

```
> cfm md set level 7 CustomerMD7
```

To display a list of maintenance domains:

```
cfm md show
```

Example:

```
> cfm md show
+---- CFM MAINTENANCE DOMAINS ----+
|Level|Name          |Services|
+-----+-----+-----+
|0     |md0            |0       |
|1     |md1            |0       |
|2     |md2            |0       |
|3     |md3            |2       |
|4     |md4            |0       |
|5     |md5            |0       |
|6     |md6            |0       |
|7     |md7            |0       |
+-----+-----+-----+
```

To display details about a specific maintenance domain:

```
cfm md show level <NUMBER: 0-7>
```

Example:

```
> cfm md show level 3
+----- CFM MAINTENANCE DOMAIN INFO -----+
| Parameter          | Value          |
+-----+-----+
| Level              | 3              |
| Name                | md3            |
| Index              | 4              |
| Number of Services | 2              |
| MD Name             | md3            |
| MD Name Length     | 3              |
| MD Name Format      | String         |
+-----+-----+
```

To display services for a specific maintenance domain:

```
cfm md show level <NUMBER: 0-7> services
```

Example:

```
> cfm md show level 3 services
+----- CFM SERVICES: MD LEVEL 3 -----+
|Name          |Type|Service Network|Vid|Lvl|Adm|Loc|Rem|XC|CC|RM|PS|RD|IS|
+-----+-----+-----+---+---+---+---+---+---+---+---+---+---+
|VLAN#1001     |VLAN|VLAN#1001     |1001|3  |dis|0  |0  |||||
+-----+-----+-----+---+---+---+---+---+---+---+---+---+---
```

Configuring CFM Services

You can configure CFM services for static primary and backup PBT tunnels, virtual switches, and VLANs. Multiple CFM services can be created at the same MD level in a common VS or VLAN. Only a single MEP or MIP is allowed per interface MD level, but MEPs at the same MD level can belong to different CFM services.



NOTE: For examples of configuring CFM services for PBT tunnels, refer to the **Configuring PBT** section in Chapter 23, on page 351.

Creating a CFM Service

When creating a service, the following attributes apply:

- **Level**—Maintenance Domain Level for the service. The default is 3.
- **Name**—Name for the service. By default, the name matches the virtual switch or VLAN associated with the service. This identifier will be used as the Short MA Name of its associated MA. The link partner associated with the same service on the far end must be configured with the same identifier for CFM to function correctly.
- **Next MEPID**—CFM has a configurable nextMepid value, with the range 1-8191, which is used to determine default MEPIDs. When a MEP is created without a specified MEPID, the current value of nextMepid will be used as the MEPID of the new MEP, and then incremented by one. If the resulting value of nextMepid is already used by an existing MEP, nextMepid will be continually incremented until a unique value is found. The purpose of nextMepid is to provide a mechanism for generating MEPIDs that are unique in the MA across all devices in the Service network. Be sure to assign each device a nextMepid value that will guarantee MEPID uniqueness across all MEPs.



NOTE: A total of up to 256 combined CFM services are supported on the CN 3911 and CN 3920, and up to 530 on the CN 3940, CN 3960, and CN 5140. This includes VS, VLAN, and PBT tunnel services (on platforms that support the service).

To create a CFM service for a virtual switch:

```
cfm service create vs <VirtualSwitchName> [level <NUMBER: 0-7>] [name <String[31]>] [next-mepid <NUMBER:1 - 8191>]
```

Example:

```
> cfm service create vs VS-1 name CFM-SRV-VS-1 next-mepid 300
```

To create a CFM service for a VLAN:

```
cfm service create vlan <VlanID> [level <NUMBER: 0-7>] [name <String[31]>] [next-mepid <NUMBER:1 - 8191>]
```

Example:

```
> cfm service create vlan 1001
```

Setting Service Attributes

CFM services have the following configurable attributes:

Alarm Priority—Determines what priority level will be used to trigger an alarm. For each fault event, CFM reports a defect type that corresponds to a priority level. If a detected fault's priority level is lower than the alarm priority setting, it will not be reported. The range is 1-5, and the default is 3. Priority levels and corresponding defect types are shown in **Table 17-1**, in this chapter.

Table 17-1: Alarm Priority

Priority Level	Defect Type	Service Fault

Table 17-1: Alarm Priority

1	RDI - Remote Defect Indicator shows that the remote MEP is not receiving CCMs from some other MEP in the service. In CFM-PBT services, an RDI fault indicates that only one of the tunnels in the pair has faulted, and that traffic is only flowing in one direction.	RD
2	MAC Status Defect indicates the remote MEP transmitted CCM for a non-forwarding interface (Not applicable for PBT CFM services).	MS
3	Remote MEP CCM Defect indicates that the local MEP is not receiving CCMs from Remote MEP(s).	RM
4	Error CCM Defect indicates misconfiguration of MEPID or ccm-interval.	CC
5	CCM Cross Connect Defect indicates misconfiguration of MAID or MD Level. When a CCM has an incorrectly configured MAID or MD level, it triggers a Cross Connect Defect (XC) fault. However, this CCM is still counted as a valid CCM, and will increment the valid received (Rx) statistics counter.	XC
6	A new service initially has the Instability (IN) service fault until a stable remote MEP is detected. The service should not have any faults after the remote MEP is detected and determined to be stable. This fault cannot be suppressed by the alarm priority setting, and will always be reported.	IN

- **Alarm Time**—Time (in milliseconds) that defects must be present before issuing a Fault Alarm. The Alarm Time starts whenever a fault greater than the Alarm Priority is detected. The range is 0 - 36000 milliseconds. Default = 1000 ms (1 second). The lower the value, the faster a fault alarm is issued.

- **CCM Interval**—The CCM Interval refers to the frequency at which CCM messages are transmitted. The default value is 1 second. Valid CCM intervals are defined in **Table 17-2**, in this chapter.

Table 17-2: CCM Intervals

Interval	Period
0 or off	Disables CCM transmission from all MEPs in a given Maintenance Association.
1 or 4ms	4 milliseconds
2 or 10ms	10 milliseconds
3 or 100ms	100 milliseconds
1 or 4ms	4 milliseconds
2 or 10ms	10 milliseconds
3 or 100ms	100 milliseconds
4 or 1sec	1 second (Default)
5 or 10sec	10 seconds
6 or 1min	60 seconds
7 or 10min	10 minutes



NOTE: Setting the CCM Interval to 4 milliseconds is not recommended for a production environment, although it can be used for testing. Also, note that faster CCM rates are more CPU intensive.

- **DMM Interval**—The DMM Interval refers to the frequency at which DMM messages are transmitted. The default value is 1 second. Valid DMM intervals are defined in **Table 17-3**, in this chapter.

Table 17-3: DMM Intervals

Interval	Period
0 or off	Disables DMM transmission from all MEPs in a given Maintenance Association.
1 or 4ms	4 milliseconds
2 or 10ms	10 milliseconds
3 or 100ms	100 milliseconds
4 or 1sec	1 second (Default)
5 or 10sec	10 seconds
6 or 1min	60 seconds
7 or 10min	10 minutes



NOTE: Setting the DMM Interval to 4 milliseconds is not recommended for a production environment, although it can be used for testing.

- **LMM Interval**—The LMM Interval refers to the frequency at which LMM messages are transmitted. The default value is 1 second. Valid LMM intervals are defined in **Table 17-4**, in this chapter.

Table 17-4: LMM Intervals

Interval	Period
0 or off	Disables DMM transmission from all MEPs in a given Maintenance Association.
1 or 4ms	4 milliseconds
2 or 10ms	10 milliseconds
3 or 100ms	100 milliseconds
4 or 1sec	1 second (Default)
5 or 10sec	10 seconds
6 or 1min	60 seconds
7 or 10min	10 minutes



NOTE: Setting the LMM Interval to 4 milliseconds is not recommended for a production environment, although it can be used for testing.

- **CCM Loss Bucket Size**—CCM loss bucket size for CCM loss statistics ranging from 1-60 minutes. The default bucket duration is 15 minutes, which provides a default history of 24 hours.
- **CCM Loss Num**—CCM loss number ranging from 1-255.

- **CCM Loss Stats**—Enables or disables CCM loss statistics collection. When enabled, the history of CCM frame sequence errors for a remote MEP are saved. Each sequence error is used to compute the number of CCM frames that have been lost. This number is then added to the current history bucket. SAOS has a total of 96 history buckets. Changes to the enable/disable state or bucket duration flush the history.
- **Level**—Maintenance Domain Level for the service. The default is 3.
- **Name**—Name for the service. By default, the name matches the virtual switch or VLAN associated with the service. This identifier will be used as the Short MA Name of its associated MA. The link partner associated with the same service on the far end must be configured with the same identifier for CFM to function correctly.
- **Next MEPID**—CFM has a configurable nextMepid value, with the range 1-8191, which is used to determine default MEPIDs. When a MEP is created without a specified MEPID, the current value of nextMepid will be used as the MEPID of the new MEP, and then incremented by one. If the resulting value of nextMepid is already used by an existing MEP, nextMepid will be continually incremented until a unique value is found. The purpose of nextMepid is to provide a mechanism for generating MEPIDs that are unique in the MA across all devices in the Service network. Be sure to assign each device a nextMepid value that will guarantee MEPID uniqueness across all MEPs.
- **Remote MEP aging time**—Time period in milliseconds that a Remote MEP in the service can stay in an RMEP fault state before it is deleted. For example, if it is set to 60000, a Remote MEP will be deleted one minute after CCMs are no longer received from it. The default value is 0, which disables remote MEP aging.
- **Remote Mep Discovery** - Enables or disables Remote MEP Discovery for the service. When disabled, Remote MEPs must be explicitly configured and will not be discovered through CCM reception.
- **Reset Time**—Time period for which there should be no fault identified before clearing previous faults.
- **Sender ID Type (sender-id-type)** -Sender ID TLV type.

To set CFM service attributes:

```
cfm service set service <CFMServiceName> {[alarm-priority <NUMBER: 0-7>], [alarm-time <NUMBER: 0-36000>], [ccm-interval <NUMBER: 0-7|off|4ms|10ms|100ms|1sec|10sec|1min|10min>], [ccm-loss-bucket-size <NUMBER: 1-60>], [ccm-loss-num <NUMBER: 1-255>], [ccm-loss-stats <enable|disable>], [encapsulation <dot1q|dot1ad>], [level <NUMBER: 0-7>], [name <String[31]>], [next-mepid <NUMBER: 1 - 8191>], [remote-mep-aging-time <NUMBER: 0...3600000>], [reset-time <NUMBER: 10-36000>], [sender-id-type <none|chassis|manage|chassis-manage>]}
```

Example:

```
> cfm service set service CFM-SRV-VS-1 name VS-CFM-1
```

Deleting a CFM Service

Deleting CFM on a tunnel will result in the deletion of its dedicated MA and associated MEPs. Also, if any fault states exist on the associated Virtual Switch or VLAN, they will be cleared.

To delete a CFM service:

```
cfm service delete service <CFMServiceName>
```

Example:

```
> cfm service delete service VS-CFM-1
```

Enabling a CFM Service

When you create a CFM service, it is disabled by default.

To enable a CFM service:

```
cfm service enable service <CFMServiceName>
```

Example:

```
> cfm service enable service VS-CFM-1
```

Disabling a CFM Service

After a CFM service is disabled, any fault states will be cleared.

To disable a CFM service:

```
cfm service disable service <CFMServiceName>
```

Example:

```
> cfm service disable service VS-CFM-1
```

Displaying CFM Services

You can display a list of all CFM service along with the status, or detailed information for:

- A specific CFM service.
- MEPs for a specific CFM service.
- Remote MEP for the specified CFM service.

The list of all CFM services indicates existence of a fault with an "X" for the following service faults:

- **XC (Cross-connect)** - Indicates that a CCM was received with an incorrect MAID (MEGID), or was for an MD Level different than the service MD Level.
- **CC (Error CCM)** - Indicates that a CCM was received with an incorrect ccm-interval, or that the Remote MEP's MEPID equals the MEPID of a local MEP in the service.
- **RM (RMEP Error)** - Indicates that a CCM not been received from a Remote MEP within $3.5 * \text{ccm-interval}$.
- **PS (Port Status)** - Indicates that one or more Remote MEPs reside in a ports that are not forwarding.
- **RDI (RDI)** - Indicates that one or more Remote MEPs have detected service faults.
- **IS (Instability)** - Indicates that the service is yet to discover a stable Remote MEP.

Faults indicated here may not have been reported through a service fault event, as that requires a fault to have a priority greater than the service alarm-priority and be present for a period of time longer than the service alarm-time. A CFM service that is completely healthy will not have any Service Fault indicators. Some service fault conditions may be expected. For example, if a service has a Remote MEP in a port that is disabled, then the PS fault will always be present.

To display all CFM services:

```
cfm service show
```

Example:

```
> cfm service show
```

CFM SERVICES													
Name	Type	Service Network	Vid	Lvl	Adm	Loc	Rem	XC	CC	RM	PS	RD	IS
VLAN#1001	VLAN	VLAN#1001	1001	3	dis	0	0						

To display a specific CFM service:

```
cfm service show service <CFMServiceName>
```

Example of a service without faults:

```
> cfm service show service VLAN#1001
```

CFM SERVICE INFO	
Parameter	Value
CFM Service Name	VLAN#1001
Index	1
Service Type	VLAN
Vs or VLAN Name	VLAN#1001
Service Network	1001
Encapsulation	IEEE 802.1Q
Maint. Domain Level	3
Maint. Domain Name	md3
Short MA Name	VLAN#1001
MAID	md3VLAN#1001
Admin State	disabled
Oper State	disabled
CCM Interval	4 or 1sec
CCM Loss Number	3
Alarm Priority	3
Alarm Time	3000
Reset Time	3000
Remote MEP Aging Time	0
Next MEPID	1
Total MEPS	0
Active Meps	0
Total Remote MEPS	0
Service Faults	
Last Fault CCM	<none>
CCM Loss Statistics	Disabled
CCM Loss Bucket Size	15
DMM Interval	3 or 100ms
LMM Interval	3 or 100ms

Example of a service with a fault:

If an "XC" or "CC" fault condition is present, a raw hex dump of the last CCM frame that triggered the fault is shown in the detailed display for the CFM service.

```
> cfm service show service vl100l2
```

CFM SERVICE INFO	
Parameter	Value
CFM Service Name	vl100l2
Index	1
Service Type	VLAN
PBT,Vs or VLAN Name	VLAN#100
Service Network	100
Encapsulation	IEEE 802.1Q
Maint. Domain Level	2
Maint. Domain Name	md2
Short MA Name	vl100l2
MAID	md2vl100l2
Admin State	enabled
Oper State	enabled
CCM Interval	3 or 100ms
CCM Loss Number	3
Alarm Priority	3
Alarm Time	3000
Reset Time	3000
Next MEPID	601
Total MEPs	1
Active Meps	1
Total Remote MEPs	1
Service Faults	XCON
Last Fault CCM	Frame Length: 112 01 80 C2 00 00 31 00 02 A1 31 23 C7 81 00 E0 64 89 02 20 01 03 46 00 00 02 62 00 3A 04 03 6D 64 31 02 07 76 6C 31 30 30 6C 31 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 01 00 08 06 04 00 02 A1 31 23 C7 02 00 01 02 04 00 01 01 00
CCM Loss Statistics	Disabled
CCM Loss Bucket Size	15
DMM Interval	3 or 100ms
LMM Interval	3 or 100ms

To display MEPs for a specific CFM service:

```
cfm service show service <CFMServiceName> mep
```

Example:

```
> cfm service show service VLAN#1001
```

CFM MEPs							
Service	Port	Mepid	Type	Mac Address	Admin State	CCM State	CCM Pri
VLAN#1001	1	1	down	00:02:A1:24:0E:32	en	on	7

To display remote MEPS for a specific CFM service:

```
cfm service show service <CFMServiceName> remote-mep
```

Example:

```
> cfm service show service CFM_VLAN_777 remote-mep
```

CFM REMOTE MEPS									
Service	Mepid	Mac Address	State	Total	Seq	Last	Fault		
			Ad Op	Rx CCM	Error	Seq Num	F M R		
CFM_VLAN_777	101	00:02:A1:07:94:00	en en	1249	0	1249			

Configuring MEPS

In order for CCM messages to be generated and processed, MEPS must be configured for the CFM service.

Creating a MEP

Attributes for a MEP include:

- **vlan** - Customer VLAN ID specified for MEPS on ports that are members of a virtual switch. The default is 0.
- **type** - The type determines whether CFM Messages processed by a MEP ingress and egress through its associated logical interfaces (down), or are logically forwarded to and from its logical interface from other logical interfaces in the service instance (up). The default type is up.
- **mepid** - Numeric identifier unique for every MEP in the Maintenance Association. The default MEPID is the next MEP ID available.



NOTE: A total of up to 256 MEPS are supported on the CN 3911 and CN 3920, and up to 530 MEPS are supported on the CN 3940, CN 3960, and CN 5140.

When you create a CFM service for virtual switches, an up MEP is automatically created for each subscriber port. A separate MEP is created for each customer VLAN (C-VID) on every subscriber port. You can also create MEPS manually. For example, you can create a down MEP on a subscriber port for monitoring within the customer network or a down MEP on a provider port to monitor the provider network. Note that once a VLAN parameter is specified when creating a MEP on a subscriber port, it is not configurable once the MEP is created.

To create a MEP:

```
cfm mep create service <CFMServiceName> port <PortName> [vlan <VlanId>] [type <up|down>] [mepid <NUMBER: 1-8191>]
```

Example:

```
> cfm mep create service CFM_VLAN_777 port 10 type down mepid 2
```

To create a MEP on a subscriber port C-VID:

```
> cfm mep create service CFM_VLAN_777 port 3 vlan 10 mepid 3
```

Specifying MEPs in CLI Commands

MEPs can be specified at the CLI in one of three ways:

- By MEPID using the local-mepid parameter. This form is applicable to both subscriber and provider ports, and is the recommended form:
 > cfm mep set service CFM_VLAN_777 local-mepid 2 ccm-priority 4
- By port only. This is applicable to both subscriber and provider ports, but on a provider port, it is the equivalent of specifying the port with vlan 0:
 > cfm mep set service CFM_VLAN_777 port 10 ccm-priority 4
- By port and VLAN. This form is applicable to subscriber ports only:
 cfm mep set service CFM_VLAN_777 port 3 vlan 10 ccm-priority 4

A MEP is specified using one of these three forms for all commands that pertain to MEPs (for example, enable, disable, delete, show, linktrace, loopback, delay, and frame-loss). In most commands (except set) the MEPID parameter is called mepid instead of local-mepid.

Setting MEP Attributes

You can set the attributes for MEPs, including:

- **ccm-priority** - CCM message priority value 0-7. Default is 3.
- **ccm-state** - Default is on. For troubleshooting purposes, you can set the state to off, and the MEP will process the CCMs that it receives, but will not transmit any.
- **ltm-priority** - Linktrace Message priority value 0-7. Default is 3.
- **mepid** - MEP Identifier. Default is the next MEP ID available in the Maintenance Association.
- **tag-vid** - The VLAN ID of the additional tag for 802.1ad CFM traffic.
- **tag-priority** - The dot1p priority encoded in the additional tag.
- **tag-mode** - Enables CVID support for VLAN CFM services.
- **type** - MEP type. Default is down.

To set MEP attributes:

```
cfm mep set {local-mepid <NUMBER: 1-8191> | port <PortName> [vlan <Vlan>]} [ccm-priority <NUMBER: 1-5>][ccm-state <on|off>][ltm-priority <NUMBER: 1-5>][mepid <NUMBER: 1-8191>][tag-vid <0-4095>][tag-priority <0-7>][tag-mode <on|off>][type <up|down>]
```

Example:

```
> cfm mep set service CFM_VLAN_777 port 10 mepid 201
```

Deleting a MEP

If needed, you can delete MEPs no longer in use for a CFM service.

To delete a MEP:

```
cfm mep delete service <CFMServiceName> {local-mepid <NUMBER: 1-8191> | port <PortName> [vlan <Vlan>]}
```


Example:

```
> cfm mep delete service CFM_VLAN_777 port 10
```

Disabling a MEP

For troubleshooting, you can disable a MEP to prevent processing of CFM messages.

To disable a MEP:

```
cfm mep disable service <CFMServiceName> {local-mepid <NUMBER: 1-8191> | port <PortName> [vlan <Vlan>]}
```

Example:

```
> cfm mep disable service CFM_VLAN_777 port 10
```

Enabling a MEP

Newly created MEPs are automatically enabled. If you disabled a MEP, you can enable it.

To enable a MEP:

```
cfm mep enable service <CFMServiceName> {local-mepid <NUMBER: 1-8191> | port <PortName> [vlan <Vlan>]}
```

Example:

```
> cfm mep enable service CFM_VLAN_777 port 10
```

Displaying MEPs

You can display a summary of all CFM MEPS including the associated CFM services, logical interfaces, MEP ID, type, MAC address, administrative state, CCM state, CCM priority, and Loopback Message priority. Also, you can display additional detailed configuration and statistics for specified MEPs, such as transmitted and received CCMs, loopback messages, and linktrace messages.

To display all MEPs:

```
cfm mep show
```

Example:

```
> cfm mep show
```

CFM MEPS								
Service	Port	Vid	Mepid	Type	Mac Address	Admin State	CCM State	CCM Pri
vl100l4	1	0	58	up	00:02:A1:31:23:C2	en	on	4
vl100l4	1	10	59	up	00:02:A1:31:23:C2	en	on	7
vl100l4	1	20	66	up	00:02:A1:31:23:C2	en	on	7
vl100l5	1	10	59	up	00:02:A1:31:23:C2	en	on	7
vl100l5	1	4094	60	up	00:02:A1:31:23:C2	en	on	7
vl100l5	2	0	67	up	00:02:A1:31:23:C3	en	on	7
vl100l5	2	20	61	up	00:02:A1:31:23:C3	en	on	7
vl100l5	7	10	63	up	00:02:A1:31:23:C8	en	on	7
vl100l5	7	20	64	up	00:02:A1:31:23:C8	en	on	7
vl100	6	100	58	down	00:02:A1:31:23:C7	en	on	7
vl32l7	5	32	59	up	00:02:A1:31:23:C6	en	on	7

To display detailed MEP information for a specific CFM service:

```
cfm mep show [service <CFMServiceName> {mepid <NUMBER: 1-8191> | port <PortName> [vlan <Vlan>]}] [order-by-mepid][exclude-evpl]
```

Example:

```
> cfm mep show service vs102 mepid 2002
```

CFM MEP INFO	
Parameter	Value
Service	vs102
Service Type	VLAN
VLAN Name	VLAN#102
Service Network	102
Port	1
VLAN	1002
MEPID	2002
Mac Address	00:02:A1:31:23:C2
Type	Up
Admin State	enabled
CCM State	on
CCM Priority	7
Tag Mode	off
Tag VID	0
Tag Priority	7
Next Loopback Sequence Number	1
Next Linktrace Sequence Number	1
Rx Total Valid Frames	0
Rx Total Invalid Frames	0
Rx Invalid Message Overflow	0
Rx Invalid Port Status TLV	0
Rx Invalid Interface Status TLV	0
Rx Invalid Sender ID TLV	0
Tx CCM	0
Rx Valid CCM	0
Rx CCM In Sequence	0
Rx CCM Sequence Errors	0
Rx MD Level Xcon CCM	0
Rx MAID Xcon CCM	0
Rx MEPID Error CCM	0
Rx CCM-Interval Error CCM	0
Rx Invalid CCM	0
Tx Loopback Message	0
Tx Loopback Reply	0
Rx In-order Loopback Reply	0
Rx Out-of-order Loopback Reply	0
Rx Content Mismatch Loopback Reply	0
Rx Unexpected Loopback Reply	0
Rx Invalid Loopback Reply	0
Rx Valid Loopback Message	0
Rx Invalid Loopback Message	0
Tx Linktrace Message	0
Rx Valid Linktrace Message	0
Rx Total Invalid Linktrace Message	0
Rx Invalid Linktrace Relay Action	0
Tx Linktrace Reply	0
Delay Measurement Repeats	Disabled
Delay Measurement Delay (min)	0
Tx Delay Measurement Message	0
Rx Delay Measurement Message	0
Tx Delay Measurement Reply	0
Rx Delay Measurement Reply	0
Rx Delay Measurement Reply Timeout	0
Frame Loss Measurement Repeats	Disabled
Frame Loss Measurement Delay (min)	0
Tx Frame Loss Measurement Message	0
Rx Frame Loss Measurement Message	0
Tx Frame Loss Measurement Reply	0
Rx Frame Loss Measurement Reply	0
Rx Frame Loss Measure Reply Timeout	0
Last Loopback Message	
Target Remote MEPID	0
Target Mac Address	00:00:00:00:00:00
Priority:	7

Count:	0									
First Sequence Number	0									
LBMs Sent	1									
LBMs To Send	0									
Rx In-order Loopback Reply	0									
Rx Out-of-order Loopback Reply	0									
Rx Content Mismatch	0									
----- Last Delay Measurement Message -----										
Target Remote MEPID	0									
Target Mac Address	00:00:00:00:00:00									
Priority	0									
Frame Count Tx	0									
Frame Count Rx	0									
Delay in us	0									
Jitter in us	0									
----- Last Frame Loss Measurement Message -----										
Target Remote MEPID	0									
Target Mac Address	00:00:00:00:00:00									
Priority	0									
Frame Count Tx	0									
Frame Count Rx	0									
Frame Loss Near	0									
Frame Loss Far	0									
----- Last Linktrace Message -----										
Target Remote MEPID	0									
Target Mac Address	00:00:00:00:00:00									
Priority	7									
Sequence Number	0									
Initial TTL	0									
Use FDB Only	No									
----- Linktrace Responses -----										
Ttl	Idx	Trans Id	Remote MEP	Relay	Ingress	Egress	Flags			
Ttl	Idx	Trans Id	Mac Address	Actn	Port	Actn	Port	Actn	FY	TM

Configuring Remote MEPs

A Remote MEP monitors connectivity with a service endpoint on another device in the network. Every valid CCM received from a MEP on a remote device that belongs to the same MA as a local service is associated with a Remote MEP in the service.

A Remote MEP can either be manually created or added to a service upon discovery through CCM reception. Once CCMs are consistently received from a Remote MEP for a configurable hold-time, it is automatically activated. Failure to receive a configurable number of consecutive CCMs from an active Remote MEP constitutes loss of connectivity with the remote endpoint, and triggers a service fault. Remote MEP discovery can be enabled or disabled per CFM service.

A Remote MEP also serves as the target for Loopback and Linktrace operations used for monitoring service health and troubleshooting service faults.



NOTE: A total of up to 4609 Remote MEPs are supported on the CN 3911 and CN 3920, and up to 8192 Remote MEPs are supported on the CN 3940, CN 3960, and CN 5140.

Creating a remote MEP

A manually created MEP must be assigned a MEPID that is not equal to the MEPID of any local or remote MEP already associated with the service. Manually created Remote MEPs are administratively disabled by default, and will persist in the system. The MAC address

associated with a Remote MEP can be configured to a fixed value, and the MAC address is uninitialized until it is either explicitly configured or a CCM containing the MEPID associated with that Remote MEP is processed.

To create a remote MEP:

```
cfm remote-mep create [service <CFMServiceName> mepid <NUMBER:1-8191>]
```

Example:

```
> cfm remote-mep create service VLAN#1001 mepid 100 hold-state lock
```

To set remote MEP attributes:

```
cfm remote-mep set [service <CFMServiceName> mepid <NUMBER:1-8191>][hold-state  
<enabled|disabled|lock>][mac <MacAddress>]
```

Example:

```
> cfm remote-mep set service CFM-1 hold-state disabled
```

Deleting a remote MEP

You can delete a remote MEP.

To delete a remote MEP:

```
cfm remote-mep delete [service <CFMServiceName> mepid <NUMBER:1-8191>]
```

Example:

```
> cfm remote-mep delete service CFM-1 mepid 100
```

Remote MEP States

The enable/disable operation and hold-state settings are factors in determining Remote MEP operational state. The following rules apply to Remote MEP states:

- A discovered Remote MEP is initially administratively enabled, while a manually created Remote MEP is initially administratively disabled.
- A Remote MEP can only cause a service fault when it is operationally enabled.
- A Remote MEP that is administratively disabled is always operationally disabled.
- Remote MEP hold-state has three settings: enable, disable, and lock.
- When a Remote MEP is administratively enabled and its hold-state is "disable", it immediately becomes operationally enabled.
- When a Remote MEP is administratively enabled and its hold-state is "enable" it will transition to an operational "hold" state, and remains there until it is free of RMEP faults for a period of time equal to the global rmep-hold-time setting. Once this occurs, the Remote MEP transitions to an operationally enabled state.
- If the hold-state is set to "lock", then the behavior in the previous bullet applies, except the Remote MEP will remain in an operational "hold" state indefinitely. The "lock" hold-state is used to hold the Remote MEP in a diagnostic state that is fully operational other than it cannot trigger a service fault.

Disabling a remote MEP

When you disable a remote MEP, it cannot trigger a service fault. You can disable remote MEPs that have not been discovered by CFM.

To disable a remote MEP:

```
cfm remote-mep disable service <CFMServiceName> mepid <NUMBER:1-8191>
```

Example:

```
> cfm remote-mep disable service VS-CFM-1 mepid 2
```

Enabling a remote MEP

When a new remote MEP is discovered, it is added to MEP CCM Database in a hold state. If valid CCMs are continuously received from the remote MEP for the time specified in the rmep-hold-time and the MEP is administratively enabled, the remote MEP automatically transitions to the enabled operational state. If the MEP has been administratively disabled, it will remain in the hold state indefinitely. You can enable remote MEPs that have not been discovered by CFM.

To enable a remote MEP:

```
cfm remote-mep enable service <CFMServiceName> mepid <NUMBER:1-8191>
```

Example:

```
> cfm remote-mep enable service VS-CFM-1 mepid 2
```

Disabling Remote MEP discovery

When Remote MEP discovery is disabled at the CFM service level, a Remote MEP will not be automatically added to the service if CCMs that are received by one of its MEPs contain an unknown MEPID, and in this case an Error CCM service fault is triggered.

To disable remote MEP discovery:

```
cfm service set remote-mep-discovery
```

Example:

```
> cfm service set service vl100l5 remote-mep-discovery disable
```

Displaying remote MEPs

You can display the remote MEP summary table to verify CCM reception and to display faults as shown in the following fields:

- **Seq Error** - Number of CCM sequence errors. A sequence error occurs when the sequence number of a CCM is not one greater than the sequence number of the last CCM received from the Remote MEP, and indicates that a CCM is lost or received out of order.
- **Fault** - Remote MEP fault indicators. All defects currently in effect for a Remote MEP are designated with an "X":

- **F** - Remote MEP Fault. A CCM has not been received from the Remote MEP within $\text{ccm-interval} \times 3.5$.
- **P** - Port Status. The last CCM received from the Remote MEP indicated a Port Status fault.
- **R** - RDI - The last CCM received from the Remote MEP indicated an RDI fault.

In a healthy service, Remote MEPs will typically not have any fault indicators. A non-zero value for "Seq Error" indicates that one or more CCMs from the Remote MEP were lost in transit. CCMs that are delayed for a period of time $> \text{ccm-interval} \times 3.5$ are not reflected in the "Seq Error" field, although such a condition may trigger and RMEP Fault (F).

Also, you can display details for a specific remote MEP.

To display a summary of all remote MEPs:

```
cfm remote-mep show
```

Example:

```
> cfm remote-mep show
```

CFM REMOTE MEPS									
Service	Mepid	Mac Address	State	Total	Seq	Last	Fault		
			Ad Op	Rx CCM	Error	Seq Num	F M R		
VS-CFM-1	2	00:00:00:00:00:00	en hd	0	0	0	X		

To display details about a specific remote MEPs:

```
cfm remote-mep show [service <CFMServiceName>] [mepid <NUMBER: 1-8191>]
```

Example:

```
> cfm remote-mep show service vl100l5 mepid 3
```

----- CFM REMOTE MEP INFO -----	
Parameter	Value
Service	vl100l5
MEPID	3
Mac Address	00:00:00:00:00:00
Service Network	100
MD Level	5
Admin State	enabled
Operational State	hold (locked)
Hold State	lock
Time since last state change (ms)	8326968
CCM Sequence Errors	0
Total CCM Lost	0
Total Rx CCM	0
CCM Failure Defect	No
Port Status Defect	None
RDI Error Defect	No
DMM Tx Count	0
DMR Rx Count	0
DMM Ave Delay (us)	0
DMM Ave Jitter (us)	0
LMM Tx Count	0
LMR Rx Count	0
LMM Frame Loss Near	0
LMM Frame Loss Far	0
CCM Loss Statistics	Disabled
CCM Loss Statistics Wrapped	No
CCM Current Loss Statistics Index	0
CCM Loss Bucket Size (minutes)	15

Configuring MIPs

A MIP is able to forward and respond to Linktrace messages, and it provides an intermediate target for Loopback messages, making fault isolation possible. Note that you can disable the MIP CCM Database. When the database is disabled, MIPs will not process CCMs to create new entries and any entries currently in the database are removed. In addition, the global mip-level-enforcement setting can be turned off to ignore the level configured on the MIP.

Creating MIPs

When you have intermediate devices (between the devices containing service MEPs) in a VLAN service, you need to create a MIP. Similar to MEPs, MIPs can be created on individual C-VIDs of a VS subscriber port.

To create MIPs:

```
cfm mip create {vlan <VlanId>} {port <PortName>} [level <NUMBER: 0-7>]
```

Example:

```
> cfm mip create vlan 1001 port 1
```

Setting MIP Attributes

To set the MIP maintenance domain level:

```
cfm mip set {vlan <VlanId>} {port <PortName>} {level <NUMBER: 0-7>}
```

Example:

```
> cfm mip set vlan 1001 port 1 level 0
```

Deleting MIPs

To delete a MIP:

```
cfm mip delete {vlan <VlanId>} {port <PortName>}
```

Example:

```
> cfm mip delete vlan 1001 port 1
```

Disabling the MIP Database

To disable the MIP database:

```
cfm mip database {enable|disable}
```

Example:

```
> cfm mip database disable
```

Displaying MIP configuration

To display MIP configuration:

```
cfm mip show [vlan <VlanId> port <PortName>]
```

Example:

```
> cfm mip show
```

```
+----- CFM MIPs -----+
| Service Instance |Vlan Id |Port  |Level |Mac Address |
+-----+-----+-----+-----+-----+
|VLAN#1001         |1001    |1     |3     |00:02:A1:24:0E:32 |
+-----+-----+-----+-----+-----+
```

Displaying the MIP Database

To display the MIP database:

```
cfm mip-ccm-db show
```

Example:

```
> cfm mip-ccm-db show
```

```
+----- MIP CCM Database -----+
|      |      |      |Total |      Last CCM Information      |
|VLAN|  MAC Address  |Port |CCM Rx|Seq Num |Time  |Lv|Mepid| PS |RDI|
+-----+-----+-----+-----+-----+-----+-----+
|777 |00:02:A1:30:A1:78|9     |101   |2784   |0     |3 |200 |Up |X |
+-----+-----+-----+-----+-----+-----+-----+
```

Configuring CFM Services for a VLAN Service

This configuration example shows how to configure CFM to monitor connectivity between the two CE devices by configuring a VLAN CFM service.

To configure CFM on CE1:

Step #	Description	Command
Step 1	Create the VLAN.	<code>vlan create</code>
Step 2	Add the ports to the VLAN.	<code>vlan add</code>
Step 3	Re-name MD level 5 to Customer.	<code>cfm md set</code>
Step 4	Create the CFM service.	<code>cfm service create</code>
Step 5	Create a down MEP for the network facing port.	<code>cfm mep create</code>
Step 6	Enable CFM globally.	<code>cfm enable</code>
Step 7	Enable the CFM service.	<code>cfm service enable</code>

Example:

1. `> vlan create vlan 10`
2. `> vlan add vlan 10 port 1`
3. `> cfm service create vlan 10 name CFM_VLAN_10 level 5`
4. `> cfm md set level 5 name Customer`
5. `> cfm mep create service CFM_VLAN_10 port 1 type down mepid 1`
6. `> cfm enable`
7. `> cfm service enable service CFM_VLAN_10`

To configure CFM on CE2:

Step #	Description	Command
Step 1	Create the VLAN.	<code>vlan create</code>
Step 2	Add the ports to the VLAN.	<code>vlan add</code>
Step 3	Re-name MD level 5 to Customer.	<code>cfm md set</code>
Step 4	Create the CFM service.	<code>cfm service create</code>
Step 5	Create a down MEP for the network facing port.	<code>cfm mep create</code>
Step 6	Enable CFM globally.	<code>cfm enable</code>
Step 7	Enable the CFM service.	<code>cfm service enable</code>

Example:

1. > vlan create vlan 10
2. > vlan add vlan 10 port 10
3. > cfm service create vlan 10 name CFM_VLAN_10 level 5
4. > cfm md set level 5 name Customer
5. > cfm mep create service CFM_VLAN_10 port 10 type down mepid 2
6. > cfm enable
7. > cfm service enable service CFM_VLAN_10

Configuring CFM Services for a Virtual Switch

CFM is supported for Ethernet type Virtual Switches (VS) to provide:

- Service fault monitoring of a provider VLAN associated with an attached virtual circuit.
- Transmission and receipt of Q-in-Q encapsulated CFM frames over a virtual circuit for monitoring of subscriber VLANs.
- Ability to process and forward EVPL bundled CFM frames.

CFM on VS automatically creates an Up MEP on every C-VID on all subscriber ports. This allows connectivity between all service endpoints in the network to be monitored by creating CFM Services for corresponding virtual-switches on other devices in the service. Each device will automatically detect a Remote MEP for all non-local service endpoints. A VS-based CFM service is also dynamic, so if a new subscriber port is added to its associated VS, then a MEP is automatically added to the service for that port. The primary benefit of using a VS-based CFM services is to facilitate connectivity monitoring between all endpoints in a service network. You can also manually create down MEPs on provider ports to monitor provider VLANs.

VS-based CFM services monitor the active VLAN for service faults. If the virtual switch has an attached virtual circuit, the active VLAN is the provider VLAN associated with the virtual circuit. Otherwise, the active VLAN is the VS reserved VLAN. You can configure a CFM service to monitor the active VLAN directly along with a CFM service to monitor the VS as long as the services are at different MD levels.

To configure CFM for a virtual switch:

Step #	Description	Command
Step 1	Create the CFM service.	cfm service create vs <VirtualSwitchName> [level <NUMBER: 0-7>] [name <String[31]>] [next-mepid <NUMBER:1 - 8191>]
Step 2	Enable CFM globally.	cfm enable
Step 3	Enable the CFM service.	cfm service <CfmServiceName> enable

Example:

1. > cfm service create vs VS-1 name CFM_VS_1
2. > cfm enable
3. > cfm service enable service CFM_VS_1

CFM Over Q-in-Q

The partitioning of a VS into CFM interface groups allows CFM to operate over individual Subscriber VLANs by mimicking the frame transformations applied to data frames forwarded by the VS. Specifically, a CFM frame originating from a MEP in a Subscriber interface, is transmitted out Provider interfaces using Q-in-Q encapsulation, with a C-VID equal to the Subscriber interface VID, and the S-VID equal to the Provider interface VID. Similarly when a Q-in-Q encapsulated CFM frame is received on a Provider interface, it is forwarded to the interfaces in the interface group corresponding to the frame's C-VID tag, after removing the frame's outer S-VID tag.

CFM Frame Origination

A MEP's interface type and VID determines how the frames that it originates are initially encapsulated:

- **Down MEP on any interface:** Frame is single-tagged with interface VID
- **Up MEP on Subscriber interface:** Frame is single-tagged with interface VID
- **Up Mep on Provider interface:** Frame is untagged.

A frame transformation is then potentially applied at each egress interface, depending upon the interface type:

- **Subscriber egress interface:** No transform
- **Provider egress interface:** Push interface VID

Table 17-5, in this chapter summarizes these Up MEP frame transformations and the resulting frame encapsulation for each possible combination of MEP and egress interface types.

Table 17-5: Encapsulation of Originated CFM Frames

Up MEP Ifc Type	Up MEP Ifc VID	MEP Frame Encap	Egress Ifc Type	Egress Ifc VID	Egress Ifc Transform	Egress Frame Encap
Subscriber	10	802.1Q VID=10	Provider	300	Push Egress Ifc VID	802.1ad S-VID=300 C-VID=10
Subscriber	20	802.1Q VID=20	Subscriber	20	None	802.1Q VID=20
Subscriber	0	Untagged	Subscriber	0	None	Untagged
Subscriber	0	Untagged	Provider	200	Push Egress Ifc VID	802.1Q VID=200
Provider	N/A	Untagged	Provider	100	Push Egress Ifc VID	802.1Q VID=100
Provider	N/A	Untagged	Subscriber	40	None	802.1Q VID=40

Handling CFM Frames Received on a VS

When a CFM frame is received on a VS interface, it may be consumed by a MEP on that interface. If not, it is forwarded to other VS interfaces, each of which may either consume or forward the frame. A frame that is not consumed by the ingress interface is normalized by applying an frame transformation based on the ingress interface type, before it is forwarded. The result of this normalization determines the interface group used for forwarding the frame.

A CFM frame received on a Subscriber interface is not transformed, while the S-VID (outer) tag is popped off a frame that ingresses a Provider interface. If the transformed frame is tagged, then its VID determines the interface group for forwarding. If the frame is untagged, the interface group for VID=0 is used. **Table 17-6**, in this chapter summarizes this behavior.

Table 17-6: Transformation and Forwarding of CFM Frames Received on a VS

Ingress Ifc Type	Ingress Ifc VID	Ingress Frame Encap	Ingress Transform	Transformed Frame Encap	Action
Subscriber	10	802.1Q VID=10	None	802.1Q VID=10	Forward to all other Subscriber interfaces with VID = 10 and all Provider interfaces.
Subscriber	0	Untagged	None	Untagged	Forward to all other Subscriber interfaces with VID = 0 and all Provider interfaces.
Provider	100	802.1ad S-VID=100 C-VID=20	Pop S-VID	802.1Q VID=20	Forward to all other Provider interfaces and all Subscriber interfaces with VID=20.
Provider	200	802.1Q VID=200	Pop S-VID	Untagged	Forward to all other Provider interfaces and all Subscriber interfaces with VID=0.

Troubleshooting

Sending and Displaying Loopback Messages

Loopback is a unicast CFM frame sent from a MEP to specific MEPs or MIPs. Multiple messages may be sent to the same destination and loopback catalogs the responses by how many were received in order and how many were out of order. You can display the loopback replies, including the following information:

- **Tx** — Number of LBMs transmitted
- **ToTx** — Number of LBMs for transmission remaining
- **Io** — Number of In Order LBRs received
- **Ooo** — Number of Out of Order LBRs received
- **Con** — Number of LBRs received having a Content Mismatch with the corresponding LBM.

Normally, the Tx LBM value is equal to the LBR in Order value to indicate that an LBR was received for each LBM, and that all LBRs were received in the expected order. If LBR Out of Order is greater than 0, then some LBRs were not received in the same order as their associated LBMs were transmitted. If Tx LBM is greater than the LBR In Order value plus the LBR Out of Order value, then an LBR was not received for every LBM transmitted.

To send a loopback message to a MEP:

```
cfm loopback send service <CFMServiceName> {local-mepid <NUMBER: 1-8191> | port <PortName>
[vlan <Vlan>]} {mepid <NUMBER: 1-8191>}
```

To send a loopback message to a MAC address:

```
cfm loopback send service <CFMServiceName> {local-mepid <NUMBER: 1-8191> | port <PortName>
[vlan <Vlan>]} {mac <MacAddress>}
```

To display loopback replies:

```
cfm loopback show [service <CFMServiceName>]
```

Example of sending a loopback message to a MEP specified by MEP ID:

```
> cfm loopback send service vl100l5 local-mepid 59 mepid 1 count 100
> cfm loopback show
```

MEP LOOPBACK MESSAGE INFORMATION									
Service	Local Mepid	Remote Mac Address	Rem Mepid	Next Seq Number	LBM Tx	ToTx	Rx Io	LBR Ooo	Con
vl100l5	59	00:02:A1:30:B1:04	1	51	50	50	50	0	0

Example of sending multiple messages to obtain an order count:

```
> cfm loopback send service cfmvlan port 1 mepid 100 count 10
> cfm loopback show
```

Example of sending messages to a specific MAC address:

```
> cfm loopback send-mac service cfmvlan port 1 mac 00:02:A1:15:56:E0
> cfm loopback show
```

Sending and Displaying Linktrace Messages

Linktrace is a multicast CFM frame originated from a MEP. When received by a MIP, the MIP checks its forwarding table and responds that the request was received on port X and forwarded out of port Y. In the case of a MEP to MEP message, all intermediate MIPs on the path will respond on a per box basis. All linktrace responses are unicast back to the originator.



NOTE: Linktrace requests may also be sent to any arbitrary MAC address, not necessarily a MEP/MIP. This feature can be used to trace paths, even those outside of a given Maintenance Association.

You can display the linktrace replies, including the following information:

- **Ttl** - Time to Live. An LTR is received from each CFM aware node that handles and propagates the LTM. Each node decrements the LTM Ttl by one and encodes the resulting value in the LTR. Normally, the Ttl values in the LTR list start at the initial LTM Ttl - 1, and decrease by one for each row in the table. Non-sequential Ttl values indicate that not all LTRs sent by intermediate nodes were received, or that the LTM Ttl was incorrectly decremented at some point.
- **Ttl Idx** - Time to Live Index. A locally assigned value used to differentiate multiple LTRs received with the same Ttl value. Normally, one LTR is received for each Ttl, and its Ttl index is 1. Multiple LTR entries for the same Ttl indicate an error condition, as it is the result of the LTM being handled on multiple forwarding paths through the network to the target DA.

Linktrace Responses									
Ttl	Idx	Trans Id	Remote MEP Mac Address	Relay Actn	Ingress Port	Actn	Egress Port	Actn	Flags FY TM
63	1	1	00:02:A1:31:23:C7	Hit	6	Ok	5	Ok	
63	2	1	00:02:A1:12:34:56	Hit	9	Ok	5	Ok	

- **Relay Action** - Indicates how the LTM was handled by the MEP or MIP as follows:
 - **Hit** - The LTM reached the target MEP or MIP.
 - **FDB** - The egress port for forwarding to the LTM target MAC was resolved using the MAC learn table.
 - **MFDB** - The egress port for forwarding to the LTM target MAC was resolved using the MEP or MIP CCM Database.
 - **-nodef-** - Undefined. This value should never be present in an LTR Relay Action.
- **Ingress Port** - Name of the port on which the LTM was received. The name is either a port number or aggregation name.
- **Ingress Action** - Reports how a data frame to the LTM target MAC would be handled at the ingress port as follows:
 - **Ok** - The frame would be accepted for forwarding
 - **Down** - The ingress port is not operational.
 - **Blocked** - The ingress port is blocked by topology enforcement.
 - **VID** - The ingress port is not a member of the LTM's VID, and ingress filtering is enabled.
 - **-nodef-** - Undefined. This value should never be returned as an Ingress Action.

- **Egress Port** - Name of the port that is the target of the LTM, or the port that a data frame to the LTM target MAC would be transmitted out when forwarded. The name is either a port number or aggregation name.
- **Egress Action** - Reports how a frame to the LTM target MAC would be handled as it passes through the egress port as follows:
 - **Ok** - The frame would be forwarded.
 - **Down** - The frame would be discarded because the egress port is not operational.
 - **Blocked** - The frame would be discarded because the egress port is blocked by topology enforcement.
 - **VID** - The frame would be discarded because the egress port is not a member of the LTM VID and egress filtering is enabled.
 - **-nodef-** - Undefined. This indicates that the frame would not reach the egress port. For example, in the case where the LTM is targeted at a MEP in the ingress port, the output would look like this:

Linktrace Responses										
Ttl			Remote MEP		Relay	Ingress		Egress		Flags
Ttl	Idx	Trans Id	Mac Address		Actn	Port	Actn	Port	Actn	FY TM
63	1	1	00:02:A1:31:23:C7		Hit	6	Ok	5	nodef	

- **Flags** - Reports two flags in the linktrace responses:
 - **FY** - FwdYes.
 - **TM** - TerminalMEP.

A normal linktrace result is to receive one LTR for each intermediate MIP (if any) along the forwarding path to the target MAC, and a LTR from the target MEP or MIP, or the Remote MEP that handles an LTM targeted at an arbitrary DA. Failure to receive any LTRs indicates one or more of the following conditions:

- The LTM was not handled by any MEP or MIP that could resolve how to forward to the target MAC.
- The LTM did not traverse any MEPs or MIPs as it was multicast through the network.
- All LTRs were lost in transit.
- The LTR Ttl values should be consecutive. A Ttl value that is more than one less than Ttl value of the LTR immediately above it in the output typically indicates that one or more LTRs were lost in transit.

To send a linktrace to another MEP:

```
cfm linktrace send service <CFMServiceName> {local-mepid <NUMBER:1-8191> | port <PortName>
[vlan <Vlan>]} {mepid <NUMBER: 1-8191>}
```

To send a linktrace to a MAC address:

```
cfm linktrace send-mac service <CFMServiceName> {local-mepid <NUMBER:1-8191> | port <PortName>
[vlan <Vlan>]} {mac <MacAddress>}
```

To display linktrace replies:

```
cfm linktrace show [service <CFMServiceName>]
```

Example of sending a linktrace to a Remote MEP with one LTR received:

```
> cfm linktrace send service vl100 port 5 mepid 600
> cfm linktrace show
```

Linktrace Message									
Service	Port	Vlan	Mep	Mac Address	Mepid	Trans Id	Ttl	FDB	
vl100	5		61	00:02:A1:30:B1:02	600	1	64	No	
Linktrace Responses									
Ttl	Idx	Trans Id	Remote MEP Mac Address	Relay Actn	Port	Ingress Actn	Port	Egress Actn	Flags FY TM
63	1	1	00:02:A1:30:B1:02	Hit	1	Ok	1	Ok	

Example of sending a linktrace to a MAC address with no LTRs received:

```
> cfm link-trace send-mac service vl100 port 5 mac 00:11:22:33:44:55
> cfm link-trace show
```

Linktrace Message									
Service	Port	Vlan	Mep	Mac Address	Mepid	Trans Id	Ttl	FDB	
vl100	5		61	00:11:22:33:44:55		2	64	No	
Linktrace Responses									
Ttl	Idx	Trans Id	Remote MEP Mac Address	Relay Actn	Port	Ingress Actn	Port	Egress Actn	Flags FY TM

Sending and Displaying Y.1731 Delay Measurement Messages

When sending DMM transmissions from a CFM Service, you need to specify the following:

- CFM service name (service).
- Local MEP ID (local-mepid).
- Remote MEP ID (remote-mepid) or unicast Mac address of target Remote MEP (mac).
- Priority and drop eligible values to be used in the VLAN tag of the transmitted frame (priority). Default is 7. (Optional)
- Number of DMM frames to transmit per delay measurement test (count). Valid range is 2 - 600 and the default value is 2. (Optional)
- Auto-Repeat Interval (repeat), if the test should be repeated. Valid range 0 - 1440 minutes. By default a test will not be auto-repeated. A value of 0 indicates that the test should run continuously. (Optional)
- Delay threshold to generate an event and trap when test results continuously exceed the value. (Optional)
- Jitter threshold to generate an event and trap when test results continuously exceed the value. (Optional)

To send DMMs to a remote MEP:

```
cfm delay send {service <CFMServiceName>} {local-mepid <NUMBER: 1-8191>} {remote-mepid  
<NUMBER: 1-8191>} [count <NUMBER: 2-600>] [priority <NUMBER: 1-7>] [repeat <NUMBER: 1-  
7>] [delay-threshold <NUMBER>] [jitter-threshold <NUMBER>]}
```

Example:

```
cfm delay send service CFM_VLAN_10 local-mepid 2 remote-mepid 1
```

To send DMMs to a MAC address:

```
cfm delay send-mac {service <CFMServiceName>} {local-mepid <NUMBER: 1-8191>} {mac
<MacAddress>} [count <NUMBER: 2-600>] [priority <NUMBER: 1-7>] [repeat <NUMBER: 1-7>] [delay-
threshold <NUMBER>] [jitter-threshold <NUMBER>]
```

Example:

```
> cfm delay send-mac ervice CFM_VLAN_10 local-mepid 2 mac 01:02:03:04:05:06
```

To display DMM test results:

```
cfm delay show [service <CFMServiceName>]
```

Example:

```
> cfm delay show
```

```
+----- MEP DELAY MEASUREMENT MESSAGE INFORMATION -----+
| | Local | Remote | Remote | | | Delay | Jitter | Rep |
| Service | Mepid | Mac Address | Mepid | DMM's | DMR's | in us | in us | Time |
+-----+-----+-----+-----+-----+-----+-----+-----+
| CFM_VLAN_10 | 2 | 00:02:A1:30:7D:70 | 1 | 10 | 10 | 891 | 31 | |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

To cancel remote MEP DMM transmission:

```
cfm delay cancel {service <CFMServiceName>} {local-mepid <NUMBER: 1-8191>} {remote-mepid
<NUMBER: 1-8191>}
```

Example:

```
> cfm delay cancel service CFM_VLAN_10 local-mepid 2 remote-mepid 1
```

To cancel MAC address DMMs transmission:

```
cfm delay cancel-mac {service <CFMServiceName>} {local-mepid <NUMBER: 1-8191>} {mac
<MacAddress>}
```

Example:

```
> cfm delay cancel-mac service CFM_VLAN_10 local-mepid 1 mac 01:02:03:04:05:06
```

To clear delay measurement statistics for all or a specific service local MEP ID:

```
cfm delay clear [service <CFMServiceName>] [local-mepid <NUMBER: 1-8191>]
```

Example:

```
> cfm delay clear
```

Sending and Displaying Y.1731 Frame Loss Measurement Messages

When sending LMM transmissions from a CFM Service, you need to specify the following:

- CFM service name (service).
- Local MEP ID (local-mepid).
- Remote MEP ID (remote-mepid) or unicast Mac address of target Remote MEP (mac).
- Priority and drop eligible values to be used in the VLAN tag of the transmitted frame (priority). Default is 7. (Optional)
- Number of LMM frames to transmit per loss measurement test (count). Valid range is 2 - 600 and the default value is 2. (Optional)
- Auto-Repeat Interval (repeat), if the test should be repeated. Valid range 0 - 1440 minutes. By default a test will not be auto-repeated. A value of 0 indicates that the test should run continuously. (Optional)
- Near loss threshold to generate an event and trap when test results continuously exceed the value. (Optional)
- Far loss threshold to generate an event and trap when test results continuously exceed the value. (Optional)

To send LMMs to a remote MEP:

```
cfm frame-loss send {service <CFMServiceName>} {local-mepid <NUMBER: 1-8191>} {remote-mepid <NUMBER: 1-8191>} [count <NUMBER: 2-600>] [priority <NUMBER: 1-7>] [repeat <NUMBER: 1-7>] [near-loss-threshold <NUMBER: 0-600>] [far-loss-threshold <0-600>]
```

Example:

```
cfm frame-loss send service CFM_VLAN_10 local-mepid 2 remote-mepid 1
```

To send LMMs to a MAC address:

```
cfm frame-loss send-mac {service <CFMServiceName>} {local-mepid <NUMBER: 1-8191>} {mac <MacAddress>} [count <NUMBER: 2-600>] [priority <NUMBER: 1-7>] [repeat <NUMBER: 1-7>] [near-loss-threshold <NUMBER: 0-600>] [far-loss-threshold <0-600>]
```

Example:

```
> cfm frame-loss send-mac service CFM_VLAN_10 local-mepid 2 mac 01:02:03:04:05:06 repeat 1 count 250 delay-threshold 2000 jitter-threshold 4000
```

To display LMM test results:

```
cfm frame-loss show [service <CFMServiceName>]
```

Example:

```
> cfm frame-loss show
```

MEP FRAME LOSS MEASUREMENT MESSAGE INFORMATION									
	Local	Remote	Remote		Frame	Frame	Rep		
Service	Mepid	Mac Address	Mepid	LMM's	LMR's	LossN	LossF	Time	
CFM_VLAN_10	2	00:02:A1:30:7D:70	1	71	71	0	0		

To cancel remote MEP LMM transmission:

```
cfm frame-loss cancel {service <CFMServiceName>} {local-mepid <NUMBER: 1-8191>} {remote-mepid <NUMBER: 1-8191>}
```

Example:

```
> cfm frame-loss cancel service CFM_VLAN_10 local-mepid 2 remote-mepid 1
```

To cancel MAC address LMMs transmission:

```
cfm frame-loss cancel-mac {service <CFMServiceName>} {local-mepid <NUMBER: 1-8191>} {mac <MacAddress>}
```

Example:

```
> cfm frame-loss send-mac service CFM_VLAN_10 local-mepid 2 mac 01:02:03:04:05:06
```

Displaying and Clearing CFM Statistics

You can display and clear statistics for all CFM services or for specific CFM services.

To display global CFM statistics:

```
cfm show statistics
```

Example:

```
> cfm show statistics
```

```
+----- CFM GLOBAL STATISTICS -----+
| Tx Total Frames                      | 0 |
| Tx Flooded frames                    | 0 |
| Tx Flood ignored - Invalid Level     | 0 |
| Tx Flood ignored - High Level Mep Exist | 0 |
| Tx Flood ignored - STP State         | 0 |
| Rx Total Frames                      | 0 |
| Rx Drop - Invalid Etype              | 0 |
| Rx Drop - Invalid Op-Code            | 0 |
+-----+
| CCM:                                |   |
|   Tx Total CCM                      | 0 |
|   Tx Total CCM Flooded              | 0 |
|   Rx Total CCM                      | 0 |
|   Rx Total CCM Sequence Errors      | 0 |
|   Rx Invalid MAID                   | 0 |
|   Rx Invalid CCM Interval           | 0 |
|   Rx Invalid First Tlv Offset       | 0 |
|   Rx Invalid Port Status Tlv        | 0 |
|   Rx Invalid Interface Status Tlv   | 0 |
|   Rx Invalid Logical Interface      | 0 |
|   Rx Invalid Service Instance       | 0 |
|   Rx Invalid PBT Encap Tunnel       | 0 |
|   Rx Drop - Admin Disable           | 0 |
|   Rx Drop - STP state not Forwarding | 0 |
|   Rx Drop - CCM Blocked by Opp. Mep | 0 |
|   Rx Drop - CCM Leakage             | 0 |
|   Rx Drop - CCM Too Long            | 0 |
|   Rx Drop - CCM Service Disabled    | 0 |
```

+-----+-----+		
	Loopback:	
	Tx Total LBM	0
	Tx Total LBR	0
	Rx Total LBM	0
	Rx Total LBR	0
	Rx LBM Invalid First TLV Offset	0
	Rx LBR Invalid First TLV Offset	0
	Rx Unresolved LBM	0
	Rx Unresolved LBR	0
+-----+-----+		
	LinkTrace:	
	Tx Total LTM	0
	Tx Total LTR	0
	Rx Total LTM	0
	Rx Total LTR	0
	Rx LTM Invalid First TLV Offset	0
	Rx LTR Invalid First TLV Offset	0
	Rx LTR Invalid Relay Action	0
	Rx Unresolved LTM	0
	Rx Unresolved LTR	0
+-----+-----+		

To display CFM statistics for a specific service:

cfm services show service <CFMServiceName> statistics

Example:

> cfm service show service vl100 statistics

+----- CFM SERVICE STATS -----+		
	Parameter	Value
+-----+		
	CFM Service Name	vl100
	Service Index	2
	Service Type	VLAN
+-----+		
	CCM Stats	
	Total Tx	178
	Total Rx	180
+-----+		
	Linktrace Stats	
	Total Tx LTM	0
	Total Tx LTR	0
	Total Rx LTM	0
	Total Rx LTR	0
	Total Rx Spoof LTR	0
+-----+		
	Loopback Stats	
	Total Tx LBM	0
	Total Tx LBR	0
	Total Rx LBM	0
	Total Rx LBR	0
	Total Rx 000 LBR	0
+-----+		
	Delay Stats	
	Total Tx DMM	0
	Total Tx DMR	0
	Total Rx DMM	0
	Total Rx DMR	0

+-----+-----+		
Loss Stats		
Total Tx LMM		0
Total Tx LMR		0
Total Rx LMM		0
Total Rx LMR		0
+-----+-----+		

To clear global CFM statistics:

```
cfm clear statistics
```

Example:

```
> cfm clear statistics
```

To clear CFM statistics for all services:

```
cfm services clear statistics
```

Example:

```
> cfm service clear statistics
```

To clear CFM statistics for a specific service:

```
cfm service clear service <CFMServiceName> statistics
```

Example:

```
> cfm service clear service v1100 statistics
```

To clear CFM statistics for all MEPs:

```
cfm mep clear statistics
```

Example:

```
> cfm mep clear statistics
```

To clear CFM statistics for a specific MEP:

```
cfm mep clear service <CFMServiceName> port <PortName> statistics
```

Example:

```
> cfm mep clear service v1100 port 5 statistics
```

To clear CFM statistics for all remote MEPs:

```
cfm remote-mep clear statistics
```

Example:

```
> cfm remote-mep clear statistics
```

To clear CFM statistics for a specific remote MEP:

```
cfm remote-mep clear service <CFMServiceName> mep-id <NUMBER: 1-8191> statistics
```

Example:

```
> cfm remote-mep clear service v1100 mep-id 600 statistics
```

To clear delay measurement statistics for all or a specific service local MEP ID:

```
cfm delay clear [service <CFMServiceName>] [local-mepid <NUMBER: 1-8191>]
```

Example:

```
> cfm delay clear
```

To clear loss measurement statistics for all or a specific service local MEP ID:

```
cfm frame-loss clear [service <CFMServiceName>] [local-mepid <NUMBER: 1-8191>]
```

Example:

```
> cfm frame-loss clear
```

Displaying CFM Port Stack information

CFM port stack information includes the MEPs and MIPs present in each interface, along with the service associated with each MEP.

To display CFM port stack information:

```
cfm stack show [vlan <VlanId>]
```

Example:

```
> cfm stack show
```

```
+----- CFM Interface Stacks -----+
|Service Inst|Vlan|Port  |Type|L|Mep |Adm|Service           |MAC Address   |
+-----+-----+-----+-----+-----+-----+-----+
|VLAN#1001   |1001|1      |Down|3|1   |en |VLAN#1001         |00:02:A1:24:0E:32|
+-----+-----+-----+-----+-----+-----+-----+-----+
```


Chapter

Configuring L2 Control Frame Tunneling

18

At a Glance:

- Overview
- Benefits
- Configuration
- Troubleshooting

This chapter explains how to configure the treatment of Layer 2 (L2) control frames with L2 control frame tunneling.



NOTE: To configure L2 control frame tunneling, you need to install the Advanced Ethernet license key. To obtain the Advanced Ethernet license key, contact Ciena Sales.

Overview

A device identifies the associated protocol of L2 control frame based upon the Media Access Control Destination Address (MAC DA) and other information within the frame. Depending upon the state of processing, L2 control frames can be in three forms:

- **Untagged** - standards based definition of the protocol's control frame. In this form, the frame does not have a VLAN tag, but does have the protocol specific MAC DA. Depending upon the protocol, it may have a specific EtherType value and other information. Typically, control frames in this format are received from the subscriber facing interface.
- **Transparent (tagged)**- one or more 802.1 VLAN tags have been added to transform the frame, and the protocol specific MAC DA is left intact. This form occurs when a control frame is received from a subscriber facing interface, encapsulated as a data frame, and then forwarded from a network facing interface for transport through the provider network.
- **L2 Protocol Tunneling (L2PT)** - standard MAC DA has been transformed to the L2PT special MAC DA.

In conformance with IEEE standards, the default configuration does not propagate untagged L2 control frames through the network. If the default disposition is “discard”, the frames are dropped without further processing. If the disposition is “peer”, the frames are forwarded to the software process that handles the specific protocol. **Table 18-1, in this chapter** shows the frame format for the three forms for each protocol along with the default disposition for each.

Table 18-1: Control Frame Formats and Disposition

Control Frame Name (with CLI attribute)	Form	Default Disposition	DA MAC Address	Type/Length Encapsulation	LLC or EtherType	Subtype
Rapid Spanning Tree Protocol (rstp)	Untagged	Peer	01-80-C2-00-00-00		DSAP/SSAP=0x42 Ctrl=0x03	
	Tagged	Same as data frame	01-80-C2-00-00-00		DSAP/SSAP=0x42 Ctrl=0x03	
	L2PT	Same as data frame	01-00-0C-CD-CD-D0		DSAP/SSAP=0x42 Ctrl=0x03	
Link Aggregation Control Protocol (lacp)	Untagged	Peer	01-80-C2-00-00-02		88-09	01
	Tagged	Same as data frame	01-80-C2-00-00-02		88-09	01
	L2PT	Same as data frame	01-00-0C-CD-CD-D0		88-09	01
LACP Marker (lacp- marker)	Untagged	Peer	01-80-C2-00-00-02		88-09	02
	Tagged	Same as data frame	01-80-C2-00-00-02		88-09	02
	L2PT	Same as data frame	01-00-0C-CD-CD-D0		88-09	02
802.3ah Operation, Administration, and Maintenance (oam)	Untagged	Discard	01-80-C2-00-00-02		88-09	03
	Tagged	Same as data frame	01-80-C2-00-00-02		88-09	03
	L2PT	Same as data frame	01-00-0C-CD-CD-D0		88-09	03
IEEE Std. 802.1X/EAPOL(802.1x)	Untagged	Discard	01-80-C2-00-00-03		88-8E	
	Tagged	Same as data frame	01-80-C2-00-00-03		88-8E	
	L2PT	Same as data frame	01-00-0C-CD-CD-D0		88-8E	
LLDP 802.1ab(Ildp)	Untagged	Peer	01-80-C2-00-00-0E		88-CC	
	Tagged	Same as data frame	01-80-C2-00-00-0E		88-CC	
	L2PT	Same as data frame	01-00-0C-CD-CD-D0		88-CC	

Table 18-1: Control Frame Formats and Disposition

Generic Attribute Registration Protocol (GARP) Block (garp-block)	Untagged	Discard	01-80-C2-00-00-2X		
	Tagged	Same as data frame	01-80-C2-00-00-2X		
	L2PT	Not supported	Not Supported		
GARP Multicast Registration Protocol (gmrp)	Untagged	Discard	01-80-C2-00-00-20		00-01
	Tagged	Same as data frame	01-80-C2-00-00-20		00-01
	L2PT	Not supported	Not Supported		
GARP VLAN Registration Protocol (gvrp)	Untagged	Discard	01-80-C2-00-00-21		00-01
	Tagged	Same as data frame	01-80-C2-00-00-21		00-01
	L2PT	Not supported	Not Supported		
Cisco-Port Aggregation Protocol (cisco-pagp)	Untagged	Discard	01-00-0C-CC-CC-CC	SNAP	01-04
	Tagged	Same as data frame	01-00-0C-CC-CC-CC	SNAP	01-04
	L2PT	Same as data frame	01-00-0C-CD-CD-D0	SNAP	01-04
Cisco-Unidirectional Link Detection (cisco-udld)	Untagged	Discard	01-00-0C-CC-CC-CC	SNAP	01-11
	Tagged	Same as data frame	01-00-0C-CC-CC-CC	SNAP	01-11
	L2PT	Same as data frame	01-00-0C-CD-CD-D0	SNAP	01-11
Cisco Discovery Protocol (cisco-cdp)	Untagged	Discard	01-00-0C-CC-CC-CC	SNAP	20-00
	Tagged	Same as data frame	01-00-0C-CC-CC-CC	SNAP	20-00
	L2PT	Same as data frame	01-00-0C-CD-CD-D0	SNAP	20-00
Cisco-Dynamic Trunking Protocol (cisco-dtp)	Untagged	Discard	01-00-0C-CC-CC-CC	SNAP	20-04

Table 18-1: Control Frame Formats and Disposition

	Tagged	Same as data frame	01-00-0C-CC-CC-CC	SNAP	20-04
	L2PT	Same as data frame	01-00-0C-CD-CD-D0	SNAP	20-04
Cisco-VLAN Trunking Protocol (cisco-vtp)	Untagged	Discard	01-00-0C-CC-CC-CC	SNAP	20-03
	Tagged	Same as data frame	01-00-0C-CC-CC-CC	SNAP	20-03
	L2PT	Same as data frame	01-00-0C-CD-CD-D0	SNAP	20-03
Cisco-Per VLAN Spanning Tree (cisco-pvst)	Untagged	Discard	01-00-0C-CC-CC-CD	SNAP	01-0B
	Tagged	Same as data frame	01-00-0C-CC-CC-CD	SNAP	01-0B
	L2PT	Same as data frame	01-00-0C-CD-CD-D0	SNAP	01-0B
Cisco-VLAN Bridge (vlan-bridge)	Untagged	Discard	01-00-0C-CD-CD-CE	SNAP	01-0C
	Tagged	Same as data frame	01-00-0C-CD-CD-CE	SNAP	01-0C
	L2PT	Same as data frame	01-00-0C-CD-CD-D0	SNAP	01-0C
Cisco STP Fast Uplink (cisco-stp-uplink-fast)	Untagged	Discard	01-00-0C-CD-CD-CD	SNAP	20-0A
	Tagged	Same as data frame	01-00-0C-CD-CD-CD	SNAP	20-0A
	L2PT	Same as data frame	01-00-0C-CD-CD-D0	SNAP	20-0A
Bridge Block (bridge-block)	Untagged	Discard	01-80-C2-00-00-0X		
	Tagged	Same as data frame	01-80-C2-00-00-0X		
	L2PT	Not supported	Not Supported		
All Bridges Block (all-bridges-block)	Untagged	Discard	01-80-C2-00-00-1X		
	Tagged	Same as data frame	01-80-C2-00-00-1X		
	L2PT	Not supported	Not Supported		

Benefits

With L2 Control Frames Tunneling, you can change the handling of untagged L2 control frames to be processed and forwarded as if they were data frames instead of being discarded or locally processed. Also, you can change the handling of transparent L2 control frames to be transformed to L2PT frame format.

Configuration

L2 control frame tunneling directs untagged L2 control frames into a forwarding domain of a virtual switch. Every virtual switch is associated with an L2 control frame tunneling configuration container. The container storing the configuration information is called an L2 control frame tunneling instance, which includes:

- **Administrative Status** - whether or not L2 control frame tunneling is enabled or disabled for the virtual switch.
- **Fixed .1D priority**- sets the .1D priority value applied to untagged L2 control frames to provide the baseline for Class of Service (CoS) treatment of the frame as it switches through the device. The priority value ranges from 0-7, where 7 has the highest priority and 0 has the lowest priority.
- **Protocol Disposition List** - sets a user-defined list of protocols to be processed by L2 control frame tunneling along with a disposition action of forward or discard.

Adding Untagged L2 Control Frame Classification to a Port

In order for untagged L2 control frames to be directed from a port to a forwarding domain, you need to add the untagged L2 control frame traffic classification (untagged-ctrl-vs) to the port and the port must have some membership in the designated virtual switch (virtual-switch ethernet add vs <VirtualSwitchName> port <PortName> vlan <VlanId>). When the untagged-ctrl-vs attribute has been designated, then the L2 control frame tunneling instance of the specified virtual switch will be used to handle the untagged L2 control frames that ingress the logical-port.

To add L2 control frame traffic classification for port:

```
port set port <PortName> untagged-ctrl-vs <VirtualSwitchName>
```

Removing Untagged L2 Control Frame Classification from a Port

When the untagged-ctrl-vs attribute is removed, an untagged L2 control frame is processed at the port according the default disposition for its protocol.

To remove L2 control frame traffic classification for a port:

```
port unset port <PortName> untagged-ctrl-vs <VirtualSwitchName>
```

Enabling L2 Control Frame Tunneling

You can enable an L2 control frame tunnel on each port of each device simultaneously.

To enable L2 control frame tunneling:

```
virtual-switch l2-cft enable vs <VirtualSwitchName>
```

Disabling L2 Control Frame Tunneling

When you disable L2 control frame tunneling for a specified virtual switch, any configured L2PT transforms will not occur, and untagged L2 control frames will be handled according to their default disposition.

To disable L2 control frame tunneling:

```
virtual-switch l2-cft disable vs <VirtualSwitchName>
```

Adding Control Protocols

When adding a control protocol, you can optionally specify the disposition. If you do not specify the disposition, the default disposition for the control protocol is used.

Possible disposition values are:

- **Discard** - Frame is discarded without further processing.
- **Forward** - frame is directed to the forwarding domain associated with the L2 control frame tunneling instance. Frames with this disposition are subject to all ingress and egress transformations configured on the interface. In addition, these frames are flooded to all logical interfaces attached to the virtual switch associated with the L2 control frame tunneling instance.

To add a control protocol to an L2 control frame tunneling instance:

```
virtual-switch l2-cft protocol add vs <VirtualSwitchName> {ctrl-protocol <802.1x|all-bridges-  
block|bridge-block|cisco-cdp|cisco-dtp|cisco-pagp|cisco-pvst|cisco-stp-uplink-fast|cisco-  
udld|cisco-vtp|garp-block|gmrp|gvrp|lacp|lacp-marker|lldp|oam|rstp|vlan-bridge>}  
[disposition <discard|forward>]
```

Removing Control Protocols

When you remove a control protocol from a L2 control frame tunneling instance, untagged L2 control frames will be processed according to the default disposition for the control protocol.

To remove a control protocol from an L2 control frame tunneling instance:

```
virtual-switch l2-cft protocol remove vs <VirtualSwitchName> {ctrl-protocol <802.1x|all-  
bridges-block|bridge-block|cisco-cdp|cisco-dtp|cisco-pagp|cisco-pvst|cisco-stp-uplink-  
fast|cisco-udld|cisco-vtp|garp-block|gmrp|gvrp|lacp|lacp-marker|lldp|oam|rstp|vlan-bridge>}
```

Setting the Disposition of Control Protocols

After you add a control protocol to an L2 control frame tunneling instance, you can modify its disposition.

To set the disposition of a control protocol in an L2 control frame tunneling instance:

```
virtual-switch l2-cft set vs <VirtualSwitchName> {ctrl-protocol <802.1x|all-bridges-  
block|bridge-block|cisco-cdp|cisco-dtp|cisco-pagp|cisco-pvst|cisco-stp-uplink-fast|cisco-  
udld|cisco-vtp|garp-block|gmrp|gvrp|lacp|lacp-marker|lldp|oam|rstp|vlan-bridge>}  
{disposition <discard|forward>}
```

Setting the Fixed .1D Priority Value

When an untagged frame is forwarded (encapsulated) by the L2 control frame tunneling instance, it is given a Fixed .1D priority value. The default Fixed .1D priority value is 6. You can modify it to a value between 0 and 7.

To set the Fixed .1D Priority value for frames forwarded by an L2 control frame tunneling instance:

```
virtual-switch l2-cft set vs <VirtualSwitchName> priority <NUMBER: 0-7>
```

Setting the Tunnel Method

The tunnel method controls the classification and processing of untagged L2 control frames. You can set the tunnel method for a virtual switch to one of two modes, transparent or L2PT. The default mode is L2PT.

To set the tunnel mode:

```
virtual-switch l2-cft set vs <VirtualSwitchName> tunnel-method <l2pt|transparent>
```

Transparent Mode

When the tunnel method is in transparent mode, the switching chip hardware handles dispositions without sending frames to the CPU for processing, and is referred to as "fast path" operation. With "fast path" operation, untagged L2 control frame dispositions are maintained when the control frame ingresses a customer-facing interface with the untagged-ctrl-vs specified. Protocol dispositions are not maintained when the equivalent tagged L2 control frame ingresses a network-facing interface(s). In transparent mode, the L2 control frame is encapsulated accordingly, and the IEEE or Cisco MAC DA is left intact.

L2PT Mode

When the virtual switch is configured for L2PT mode, L2 control frames are classified and either dropped or forwarded, according to each protocol's disposition and the untagged-ctrl-vs designation at each customer-facing interface. In L2PT mode the L2 control frame is fully decoded based on the proper IEEE or Cisco MAC DA and any relevant Op-Codes in the frame. If there is a specific protocol match on a protocol that supports L2PT stamping, the frame is eligible for conversion to and from L2PT and proper IEEE or Cisco MAC DA. Certain protocols do not support L2PT transformation, since their classification data does not contain enough information to uniquely identify the protocol once the protocol-specific MAC DA has been replaced. Such protocols do not have an L2PT form. In general, when the virtual switch is in L2PT mode, the switching chip hardware sends L2 control frames to the CPU for "slow-path" processing. The frame agent will egress that frame out the customer-facing interfaces as a "proper" IEEE or Cisco L2 control frame, and egress the frame out network-facing interfaces as the same L2PT frame.

L2 control frames that ingress a network-facing interface are processed as follows:

- If the L2 control frame is in the L2PT-equivalent form and is fully decodable, it is converted back to the proper IEEE or Cisco MAC DA.
 - Egressing Customer-Facing Interface(s): The proper IEEE or Cisco MAC DA form of the frame will egress out all customer-facing interfaces of the virtual switch.

- Egressing Network-Facing Interface(s): The L2PT form of the frame will egress out all network-facing interfaces, except for the interface on which the frame ingressed.
- If the L2 control frame has an L2PT MAC DA, but is not decodable, that frame will be switched out all customer-facing and network-facing interfaces with no conversion of MAC DA.
- If the L2 control frame is already in the proper IEEE or Cisco MAC DA form, that frame will be switched out all customer-facing and network-facing interfaces with no conversion of MAC DA to L2PT. This means that if an IEEE L2 control frame enters a network-facing interface, that same frame will egress interfaces regardless of the L2PT mode enabled on the virtual switch.

L2 control frames that ingress a customer-facing Interface are processed as follows:

- If the L2 control frame is in the L2PT-equivalent form, it will be treated as a data frame and switched out all customer-facing and network-facing interfaces with no conversion of MAC DA.
- If the L2 control frame is in the proper IEEE or Cisco MAC DA untagged form, that frame will subject to the disposition set for the protocol at the virtual switch L2 control frame tunneling instance. This untagged L2 control frame has classified to the customer facing port based upon the untagged-ctrl-vs attribute of that port.
 - Egressing Customer-Facing Interface(s): The proper IEEE or Cisco MAC DA form of the frame will egress out all customer-facing interfaces of the virtual switch. From customer-to-customer, the L2PT form will not propagate.
 - Egressing Network-Facing Interface(s): The L2PT form of the frame will egress out all network-facing interfaces, except for the interface on which the frame ingressed.
- If the L2 control frame has an IEEE or Cisco MAC DA, but is not decodable, that frame will be switched out all customer-facing and network-facing interfaces with no conversion of MAC DA.

Configuring L2 Control Frame Tunneling

In general, L2 control frame tunneling includes the following steps:

1. Add a disposition of forward or discard for each protocol to be handled by L2CFT to the L2CFT Instance associated with the virtual switch to be used as a L2CF forwarding-domain.
2. Enable the L2CFT Instance.
3. Specify the untagged-ctrl-vs for each customer-facing virtual switch interface member. Those interface members will handle untagged L2CFs.
4. Enable L2PT mode at the virtual switch if L2PT transforms are to occur for tunneled L2CFs.
5. Configure the L2 control frame fixed .1D priority value - this is the frame PCP that will go onto the frame when encapsulated.

The configuration example in this section shows how you can configure virtual switches and ports to classify untagged L2 control frames and then transform them into the L2PT form. The ingress port classification allows untagged L2 control frames and frames with VLAN tag 100. The L2 control frame tunneling instance is enabled for the virtual switch. Also, RSTP and LACP are added to the protocol disposition list with the disposition of forwarding.

To configure L2 control frame tunneling:

Step #	Description	Command
Step 1	Create the VLAN 100.	<code>vlan create vlan <VlanId></code>
Step 2	Add the ingress and egress ports to VLAN 100.	<code>vlan add vlan <VlanId> port <PortName></code>
Step 3	Confirm the creation of VLAN 100 (Optional).	<code>vlan show</code>
Step 4	Confirm the ports are members of VLAN 100.	<code>vlan show vlan <VlanId></code>
Step 5	Create a virtual circuit and assign it to VLAN 100.	<code>virtual-circuit ethernet create vc <VirtualCircuitName> vlan <VlanId></code>
Step 6	Confirm the creation of the virtual circuit (Optional).	<code>virtual-circuit show</code>
Step 7	Confirm the VLAN 100 is associated with the virtual circuit (Optional).	<code>virtual-circuit show vc <VirtualCircuitName></code>
Step 8	Add reserved VLAN 1000.	<code>virtual-switch add reserved-vlan <VlanId></code>
Step 9	Create the virtual switch.	<code>virtual-switch ethernet create vs <VirtualSwitchName> vc <VirtualCircuitName></code>
Step 10	Add the ingress port to the virtual switch.	<code>virtual-switch ethernet add vs <VirtualSwitchName> port <PortName></code>
Step 11	Enable L2 control frame tunneling for the virtual switch.	<code>virtual-switch l2-cft enable vs <VirtualSwitchName></code>
Step 12	Add the control protocols to the protocol disposition list with the desired disposition for the L2 control frame tunneling instance.	<code>virtual-switch l2-cft protocol add vs <VirtualSwitchName></code>
Step 13	Add the L2 control frame classification to the port for ingress traffic.	<code>port set port <portName> untagged-ctrl-vs <VirtualSwitchName></code>
Step 14	Confirm the L2 control frame tunnel configuration of the virtual switch (Optional).	<code>virtual-switch l2-cft show vs <VirtualSwitchName></code>

Example:

1. `> vlan create vlan 100`
2. `> vlan add vlan 100 port 1`
3. `> vlan show`
4. `> vlan show vlan 100`
5. `> virtual-circuit ethernet create vc cft-vc vlan 100`

6. > virtual-circuit show

+----- ETHERNET VIRTUAL CIRCUIT TABLE -----+		
Name	VLAN	
cft-vc	100	

7. > virtual-circuit show vc cft-vc

+----- ETHERNET VIRTUAL CIRCUIT INFO -----+		
Parameter	Value	
Name	cft-vc	
ID	1	
Provider VLAN	(100)	VLAN#100
Psuedo-Wire Type	untagged	
VS Using		

8. > virtual-switch add reserved-vlan 1000

9. > virtual-switch ethernet create vs cft-vs vc cft-vc

10.> virtual-switch ethernet add vs cft-vs port 1

11.> virtual-switch l2-cft enable vs cft-vs

12.> virtual-switch l2-cft protocol add vs cft-vs ctrl-protocol
rstp disposition forward
> virtual-switch l2-cft protocol add vs cft-vs ctrl-protocol
lacp disposition forward

13.> port set port <portName> untagged-ctrl-vs <VirtualSwitchName>

14.> virtual-switch l2-cft show vs cft-vs

+----- L2 Ctrl Protocol Tunneling - cft-vs -----+		
Parameter	Value	
Admin State	Enabled	
Tunnel Method	l2pt	
Priority	6	
Protocol Name	Disposition	
rstp	forward	
lacp	forward	

Troubleshooting

Displaying Enabled L2 Control Frame Tunneling Instances

You can display a summary of all currently enabled L2 control frame tunneling instances or details about a single L2 control frame tunneling instance specified by virtual switch.

To display a summary of enabled L2 control frame tunneling instances:

```
virtual-switch l2-cft show
```

Example:

```
> virtual-switch l2-cft show
+----- L2 Ctrl Protocol Tunneling -----+
| Virtual Switch | Admin State | Tunnel Method | Priority |
+-----+-----+-----+-----+
| cft_0          | Disabled   | l2pt          | 6        |
| cft_1          | Disabled   | l2pt          | 6        |
| cft_2          | Disabled   | l2pt          | 6        |
| cft_3          | Disabled   | l2pt          | 6        |
| cft_4          | Disabled   | l2pt          | 6        |
| cft_5          | Disabled   | l2pt          | 6        |
| cft_6          | Disabled   | l2pt          | 6        |
| cft_7          | Disabled   | l2pt          | 6        |
| cft_8          | Disabled   | l2pt          | 6        |
| cft-vs         | Disabled   | l2pt          | 6        |
+-----+-----+-----+-----+
```

To display details about a specific enabled L2 control frame tunneling instance:

```
virtual-switch l2-cft show [vs <VirtualSwitchName>]
```

Example:

```
> virtual-switch l2-cft show vs cft-vs
+----- L2 Ctrl Protocol Tunneling - cft-vs -----+
| Parameter      | Value      |
+-----+-----+
| Admin State    | Enabled    |
| Tunnel Method  | l2pt       |
| Priority       | 6          |
+-----+-----+
| Protocol Name  | Disposition|
+-----+-----+
| rstp           | forward    |
| lacp           | forward    |
+-----+-----+
```

Displaying the L2 control frame classification for a port

You can display the status of L2 control frame classification for a specific port.

To display the status of L2 control frame classification for a port:

port show

Example:

> port show port 9

PORT INFO		
Field	Admin	Oper
Type	10/100/G	
Description		
Spanning Tree State	Forwarding	
MAC Address	00:02:a1:07:86:e2	
Phy Loopback	Off	
Link State	Enabled	Enabled
State Group Link State		
Mode	rj45	unknown
Speed	1 Gbps	1 Gbps
Duplex	full	full
Flow Control	off	off
Auto Negotiation	Enabled	Enabled
Flow Control Advertised	off	Enabled
PVID	300	300
Untag Ingress Vtag	1	1
Untag Ingress Data Vid	0	0
Fixed Resolved CoS	0	0
Ingress VLAN Filter	Enabled	Enabled
Ingress VS Filter	Off	Off
Acceptable Frame Type	all	all
Egress Untag VLAN	300	300
Max Frame Size	1526	1526
Untagged Data VS		
Untagged Ctrl VS		
Resolved CoS Policy	dot1d-tag1-cos	dot1d-tag1-cos
Service Port Type	Subscriber	Subscriber
Eth VC EtherType	8100	8100
Eth VC EtherType Policy	all	all
Mirror-port	Off	Off
Ingress-mirror		
Egress-mirror		
Ingress to Egress QMap	Default-RCOS	Default-RCOS
XCVR caps mismatch	<NONE>	

Displaying L2 Control Frame Tunneling Configuration in the Configuration File

L2 control frame tunneling related configuration is saved to the configuration file in various sections, including:

- VIRTUAL-CIRCUIT CONFIG:
- VIRTUAL-SWITCH CONFIG:
- L2 CFT PROTOCOL CONFIG:

Example:

```
> configuration show
...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! VIRTUAL-CIRCUIT CONFIG:  virtual circuits
!
virtual-circuit ethernet create vc cft-vc0 vlan 100
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! VIRTUAL-SWITCH CONFIG:
!
virtual-switch add reserved-vlan 1000
!
virtual-switch ethernet create vs cft-vs vc cft-vc0
!
virtual-switch ethernet add vs cft-vs port 9
!
port set port 9 untagged-ctrl-vs cft-vs
!
!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! L2 CFT CONFIG:
!
virtual-switch l2-cft enable vs cft-vs
!
virtual-switch l2-cft protocol add vs cft-vs ctrl-protocol rstp disposition forward
virtual-switch l2-cft protocol add vs cft-vs ctrl-protocol lacp disposition forward
!
!
...
```


Chapter Configuring TWAMP

19

At a Glance:

- Overview
- Benefits
- Configuring TWAMP
- Troubleshooting

This chapter explains the implementation and configuration of Two-Way Active Measurement Protocol (TWAMP).



NOTE: To configure TWAMP functionality, you need to install the Advanced OAM license key. To obtain the Advanced OAM license key, contact Ciena Sales.

Overview

As defined in RFC4656, One-Way Active Measurement Protocol (OWAMP) measures uni-directional IP performance between two devices. Based upon OWAMP, TWAMP provides bi-directional measurements of IP performance between two devices through an exchange of test messages. The system software supports the following TWAMP modes:

- TWAMP Light Responder
- TWAMP Complete Server
- TWAMP Client

In order to ensure accurate time-stamping of response frames, it is recommended that you configure the NTP client to set the system date and time with a minimum of three configured NTP servers.



NOTE: For additional information regarding NTP, see the **Configuring NTP** section in Chapter 3, on page 27.

To maintain system performance, this implementation of TWAMP does not authenticate with the method described in the standard.

Protocols

In compliance with the Internet Engineering Task Force (IETF) draft document, draft-ietf-ippm-twamp-06.txt, TWAMP Light Responder and Complete TWAMP use the TWAMP-Test protocol to exchange TWAMP test packets between the devices. Complete TWAMP uses a second protocol, TWAMP-Control to initiate, start, and stop a TWAMP test session.

Operational Roles

In a TWAMP-Test session, devices operate in the following roles:

- **Session-Sender** - Endpoint device that sends TWAMP measurement packets.
- **Session-Reflector** - Endpoint device that receives TWAMP measurement packets with the ability to create and send TWAMP measurement packets in response.
- **Server** - Endpoint device that manages one or more TWAMP-Test sessions, including the state of the session endpoint devices.
- **Control-Client** - Endpoint device that initiates requests, triggers the start and stop of a test session.

Relationship Between Protocols and Operational Roles

Figure 19-1 illustrates the relationship between the TWAMP protocols and the operational roles and shows a potential implementation where four separate devices operate in each role.

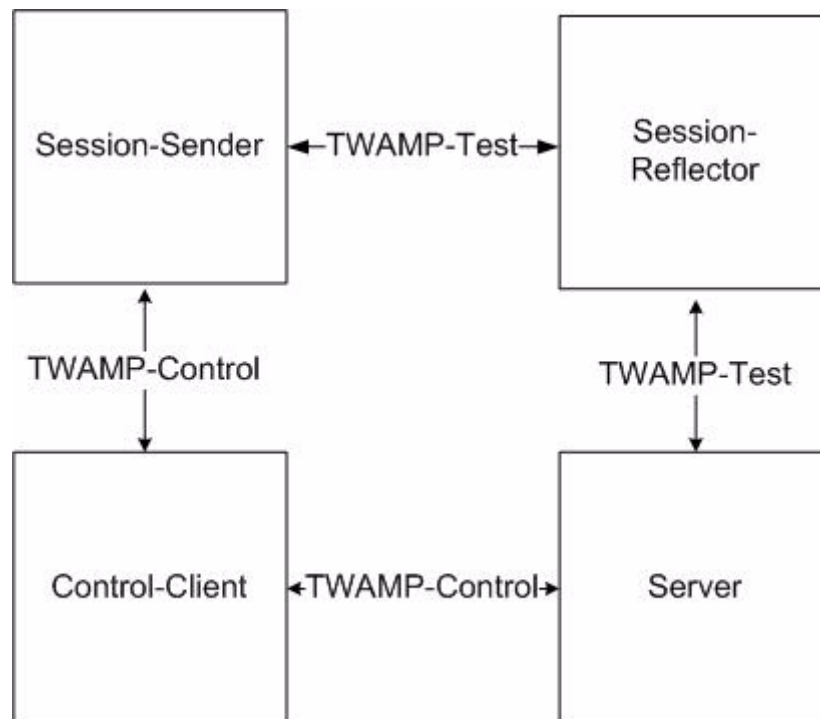


Figure 19-1: TWAMP relationships

TWAMP Light Responder

With TWAMP Light Responder mode, devices operate as Session-Reflectors only, and a performance management system operates in the Session-Sender, Control-Client, and Server roles. **Figure 19-2** shows the relationship between the TWAMP-Test protocol and operational roles in TWAMP Light Responder.

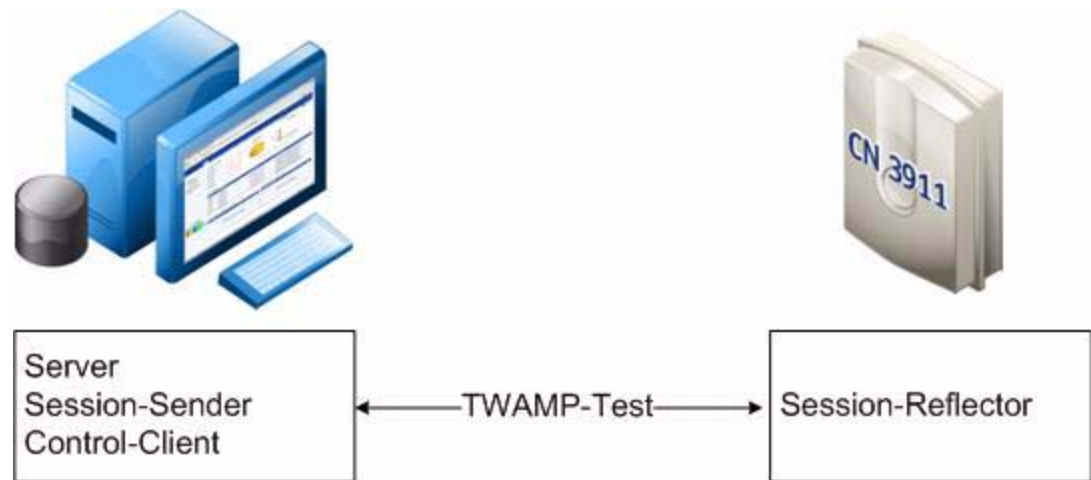


Figure 19-2: TWAMP Light Responder

While the TWAMP-Test session runs, the Session-Sender sends TWAMP-Test packets to the device. When incoming frames contain a UDP packet and the UDP destination port matches the device's configured active TWAMP port, the Session-Reflector processes the packets and returns response packets to the Session-Sender. After the exchange of test packets is complete, the Control-Client ends the session.

TWAMP Complete Server

With TWAMP Complete Server mode, devices operate as Session-Reflectors and Servers for up to 10 sessions, and a performance management system operates in the Session-Sender and Control-Client roles. **Figure 19-3** illustrates the relationship between the TWAMP protocols and the operational roles in TWAMP Complete Server.

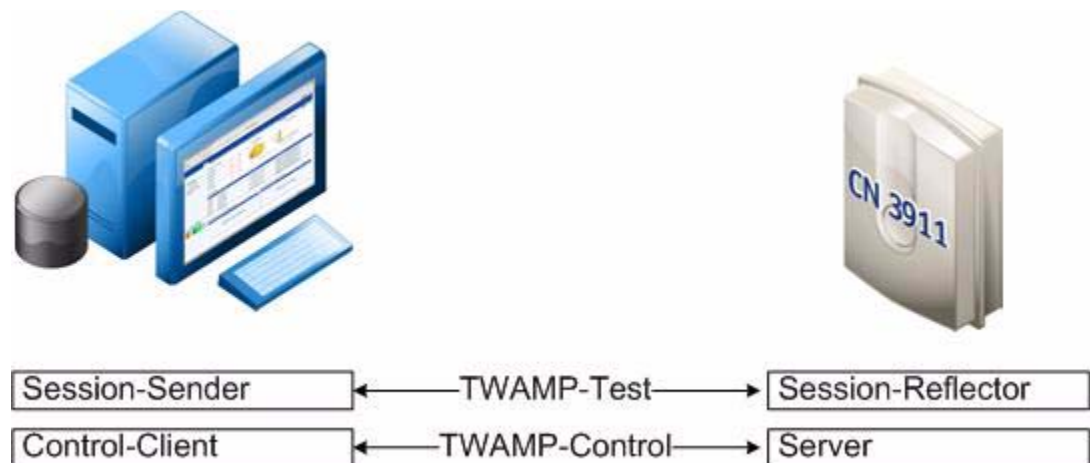


Figure 19-3: TWAMP Complete relationships

During a TWAMP session, the Server component recognizes an incoming TCP-based test session request, and configures itself for this test session. Operating in this mode, only one test session is supported at a time and test responses are returned only to the control device that established the session. Any other incoming UDP test messages are dropped. Formal requests to establish a test session while one exists will be refused.

TWAMP Client

With TWAMP Client mode, devices operate as a Control-Client and a Session-Sender enabling the device to establish test sessions and generate test initiation messages. Devices may be used as test originators and manage multiple test sessions with multiple remote devices. **Figure 19-4** illustrates the relationship between the TWAMP protocols and the operational roles where one device is operating in TWAMP Client mode and the other in TWAMP Complete mode.

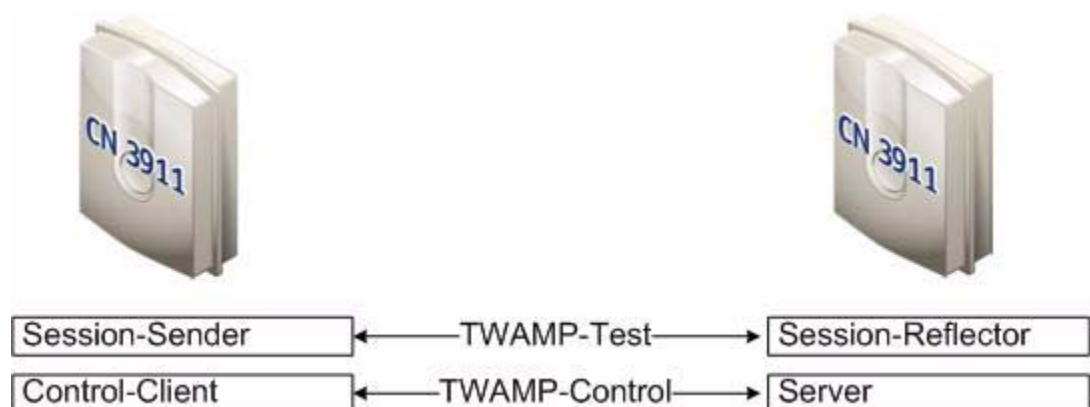


Figure 19-4: TWAMP Client relationships

TWAMP-Test Packets

TWAMP supports variable sizes of TWAMP-Test packets, and can process at a minimum of 1200 packets per minute. Currently, the Session-Sender packet follows the format shown in **Figure 19-5**.

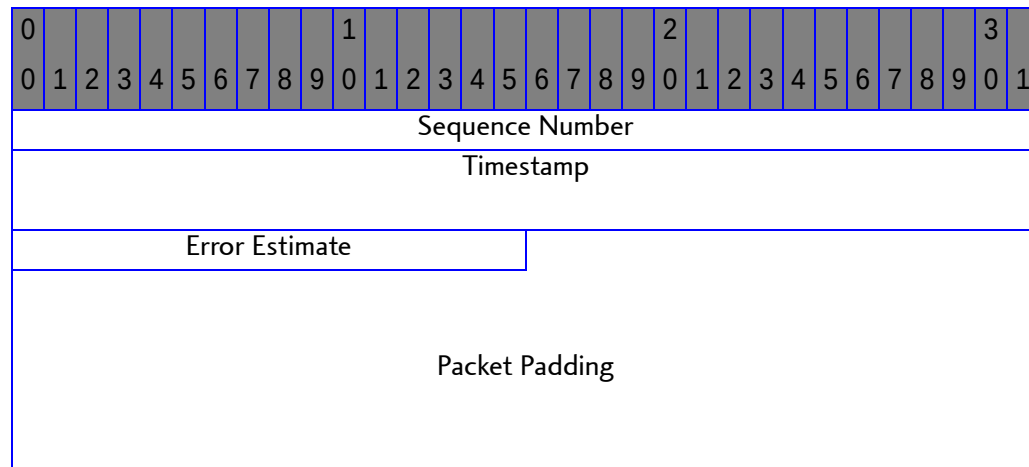


Figure 19-5: TWAMP-Test packet format from Session-Sender

The response packet format is shown in **Figure 19-6**.

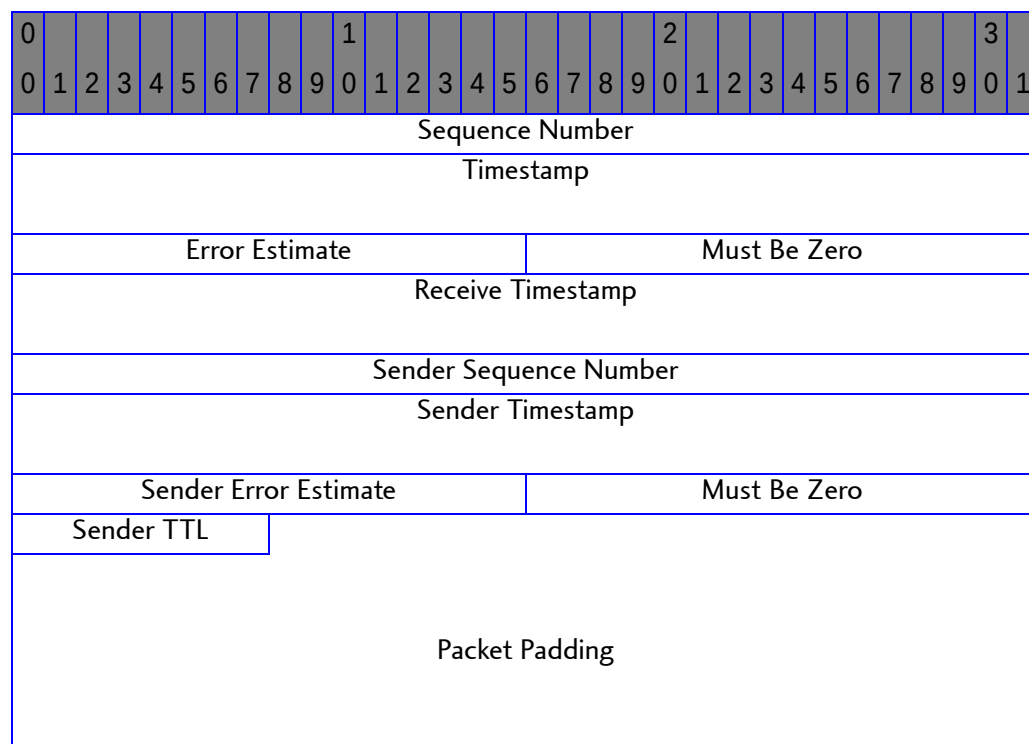


Figure 19-6: TWAMP-Test Response Packet from Session-Reflector

Benefits

TWAMP provides a way for network administrators to quickly measure latency and jitter between two devices with real-time processing.

Configuring TWAMP

TWAMP configuration includes the following:

- Enabling and disabling the TWAMP state globally and per port.
- Configuring the global TWAMP attributes.
- Enabling and disabling the TWAMP Light Responder.
- Enabling and disabling TWAMP Complete Server.
- Configuring TWAMP Client.

Enabling and Disabling TWAMP

By default, TWAMP is disabled at the global level. When you enable TWAMP at the global level, then it is automatically enabled for all ports.

To enable globally:

```
twamp enable
```

Example:

```
> twamp enable
```

To enable per port:

```
twamp enable [port <PhyPortNameList>]
```

Example:

```
> twamp enable port 15
```

To disable globally:

```
twamp disable
```

Example:

```
> twamp disable
```

To disable per port:

```
twamp disable [port <PhyPortNameList>]
```

Example:

```
> twamp disable port 15
```

Configuring Global TWAMP Attributes

The global TWAMP client DSCP and server DSCP entries set the respective DSCP values in TCP messages used for control session communications. By default, the global DSCP values for TWAMP Client and Complete Server are set to 0. You can individually set the DSCP values between 0-63. The default setting for the active TWAMP port is 861. When setting the port, be sure to select the port setting defined in the performance management system for testing devices. In addition, you can set a time out value for abandoned session recovery. By default, the time out value is 90 seconds.

To set the global TWAMP attributes:

```
twamp set {[client-dscp <NUMBER: 0-63>], [server-dscp <NUMBER: 0-63>], [port <NUMBER: 256-65535>], [timeout <NUMBER: 60-86400>]}
```

Example:

```
> twamp set port 5678
```

To reset the port and timeout attributes to their default values:

```
twamp unset {[port], [timeout]}
```

Example:

```
> twamp unset port timeout
```

Enabling and Disabling TWAMP Light Responder

You can disable or enable the TWAMP Light Responder state globally. By default TWAMP Light Responder is disabled.

To disable globally:

```
twamp light disable
```

Example:

```
> twamp light disable
```

To enable globally:

```
twamp light enable
```

Example:

```
> twamp light enable
```

Enabling and Disabling TWAMP Complete Server

You can disable or enable the TWAMP Complete Server state globally. By default, TWAMP Complete Server is disabled. When TWAMP Complete Server is enabled, the device can operate as Session-Reflectors and Servers for up to 10 sessions.

To disable globally:

```
twamp server disable
```

Example:

```
> twamp server disable
```

To enable globally:

```
twamp server enable
```

Example:

```
> twamp server enable
```

Configuring TWAMP Client

Enabling and Disabling TWAMP Client

You can disable or enable the TWAMP Client state globally. By default, TWAMP Client is disabled. Before you can create any sessions, you must enable the TWAMP Client. In order for the session to start with a target, the target must be configured to support TWAMP Complete Server. On devices running this system software, you need to enable TWAMP Complete Server.



NOTE: TWAMP Client cannot be disabled with existing TWAMP sessions, as each session has memory allocated to it for statistics gathering. Before the disable command will be accepted, delete all sessions. To stop a test, run the `twamp client test stop` command.

To disable globally:

```
twamp client disable
```

Example:

```
> twamp client disable
```

To enable globally:

```
twamp client enable
```

Example:

```
> twamp client enable
```

Creating a TWAMP Client Session

You can create up to 20 TWAMP Client sessions choosing a fixed interval test packet stream or a Poisson distribution packet stream. You can specify that the packets are marked with a CoS policy and priority value, IP Precedence (0-7) or Differentiated Services Code Point (DSCP) values (0-63), to measure "Real Time" and "Best Effort" paths across the network. **Table 19-1**, in this chapter shows the attributes of the supported packet streams.

Table 19-1: Packet Stream Attributes

Packet Stream Type	Inter-packet Frequency	Packet Size	CoS Marking	Cycle Time
Fixed Interval	100ms	Variable - 64-1500 byte test messages.	2 shared among test sessions and denoted by IP precedence (0-7) or DSCP (0-63) values.	15
Poisson Distribution	Average 3.3s, 300ms to 12s	Fixed - 238 bytes	4 shared among test sessions and denoted by IP precedence (0-7) or DSCP (0-63) values.	15

To create a TWAMP Client session:

```
twamp client session create name <String [15]> host <IpAddress> [commport <TCP/UDP port to use if different from global>] [cos-policy <dscp|ip-prec>] [dot1dpri <NUMBER:1-7>] [dscp <NUMBER: 0-63>] [ip-prec <NUMBER: 0-7>] [pkt-size <NUMBER: 64-1500>] [repeat <on|off>] [type <fixed|poisson>]
```

Example:

```
> twamp client session create name myTest host 192.168.12.34 cos-policy ip-prec ip-prec 7 repeat off type fixed
```

Displaying TWAMP Client Sessions

You can display a list of configured TWAMP Client sessions.

To display TWAMP Client sessions:

```
twamp client show
```

Example:

```
+-----+
|                                     TWAMP Client Sessions                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Name      | IP Addr   | State | Port | CoS | DSCP | IPP | Size | RPT | Type | Seq# |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| myTest    | 192.168.12.34 | Idle | 861 | I   | 0    | 7   | 142 | N   | Fix  | 0    |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```


Updating a TWAMP Client Session

You can update the attributes of an existing session.

To update a TWAMP Client session:

```
twamp client session set name <SessionName> {[host <IpAddress>], [commport <TCP/UDP port to
use if different from global>], [cos-policy <dscp|ip-prec>], [dscp <NUMBER: 0-63>], [ip-prec
<NUMBER: 0-7>], [pkt-size <NUMBER: 64-1500>], [repeat <on|off>], [type <fixed|poisson>]}
```

Example:

```
> twamp client session set name myTest type poisson
```

Deleting a TWAMP Client Session

To delete a TWAMP Client session:

```
twamp client session delete name <SessionName>
```

Example:

```
> twamp client delete name myTest
```

Establishing and Stopping a Test Session

While TWAMP Client tests are in session, the device still responds to incoming TWAMP test sessions.

To establish or stop a TWAMP Client session:

```
twamp client test name <SessionName> [host <IpAddress>] [stop]
```

Example of establishing a session:

```
> twamp client test name myTest
```

Example of stopping a session:

```
> twamp client test name myTest stop
```

Displaying and Clearing TWAMP Client Statistics

TWAMP Client test statistics are collected and stored daily. Statistics are collected in 15 minute intervals. After a TWAMP Client session is started, statistics are available about 15 minutes later. For a TWAMP session that is set to "repeat," statistics will be stored in 15 minute increments for up to 24 hours. The statistics storage area works in a First In, First Out fashion. Statistics are stored in RAM and are lost upon reboot.

To display TWAMP Client statistics:

```
twamp client show [statistics [name <SessionName>] [mode <long|short>] [period <last|8-hour|24-hour>]]
```

Example:

```
> twamp client show statistics name myTest
```

Name	RT 95th	RT 99.9th	Tx	Rx	RL	OL	Completion Time
myTest	0.312	0.410	272	272	0	0	08/ 5/08 21:29

To clear TWAMP Client statistics:

```
twamp client clear statistics {name <SessionName>|all}
```

Example:

```
> twamp client clear statistics name myTest
```

Displaying Active TWAMP Sessions on the Target Device

You can display active test sessions on target devices running this system software.

To display the test session on the target:

```
twamp server show
```

Example:

```
> twamp server show
```

TWAMP Server Test Sessions						
ID	State	Src Port	Host IP	Pkts	SeqNum	
1	Test	49154	192.168.12.342	9000	0	
2	Listen	0	0.0.0.0	0	0	
3	Listen	0	0.0.0.0	0	0	
4	Listen	0	0.0.0.0	0	0	

Clearing a TWAMP Session on the Target Device

You can force a TWAMP session down from the target devices running this system software.

To clear a session:

```
twamp server clear session <Session ID: 1-4>
```

Example:

```
> twamp server clear session 1
```

Sample Configuration

This configuration example shows the steps for configuring TWAMP components, including the steps for configuring NTP.

To configure TWAMP:

Step #	Description	Command
Step 1	Set the active TWAMP port. The default is 861.	<code>twamp set</code>
Step 2	Enable TWAMP globally.	<code>twamp enable</code>
Step 3	Enable TWAMP Light Responder.	<code>twamp light enable</code>
Step 4	Enable TWAMP Complete.	<code>twamp server enable</code>
Step 5	Enable Mini-WIPM.	<code>twamp client enable</code>
Step 6	Create a TWAMP Client test session.	<code>twamp client create session</code>
Step 7	(Recommended) Add a minimum of three NTP servers to the NTP Client server list.	<code>ntp-client add server <IpHost></code>

Example:

1. `> twamp set port 5678`
2. `> twamp enable`
3. `> twamp light enable`
4. `> twamp server enable`
5. `> twamp client enable`
6. `> twamp client session create name myTest host 192.168.12.34 cos-policy ipprec ipprec 7 type fixed`
7. `> ntp-client add server 192.2.3.4`
`> ntp-client add server 192.6.7.8`
`> ntp-client add server 192.9.10.11`

Troubleshooting

Displaying TWAMP information

You can display the global state, per port state, and active TWAMP port. Optionally, you can display the setting for the active TWAMP port only.

To display TWAMP configuration:

```
twamp show [port]
```

Example:

```
> twamp show
+----- TWAMP State Info -----+
| Parameter | Value |
+-----+-----+
| Device Admin State | Disabled |
| Client | Disabled |
| Server | Disabled |
| Light Reflector | Disabled |
| Client HW Assist | On |
| Server HW Assist | On |
+-----+-----+

+----- Active TWAMP Port -----+
| TCP/UDP Port | 861 |
+-----+-----+

+----TWAMP Server Session Timeout----+
| Timeout | 90 seconds |
+-----+-----+

+----- TWAMP DSCP Settings -----+
| Client TCP DSCP | 0 |
| Server TCP DSCP | 0 |
+-----+-----+

+-----+-----+
| Per Port TWAMP State Info |
+-----+-----+
| Port | Admin | Operational |
+-----+-----+
| 1 | Enabled | Disabled |
| 2 | Enabled | Disabled |
| 3 | Enabled | Disabled |
| 4 | Enabled | Disabled |
| 5 | Enabled | Disabled |
| 6 | Enabled | Disabled |
| 7 | Enabled | Disabled |
| 8 | Enabled | Disabled |
| 9 | Enabled | Disabled |
| 10 | Enabled | Disabled |
| 11 | Enabled | Disabled |
| 12 | Enabled | Disabled |
+-----+-----+
```

Displaying TWAMP Configuration in the Configuration File

TWAMP configuration is saved to the configuration file in the TWAMP CONFIG: section.

To display TWAMP configuration in the configuration file:

```
> configuration show
!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
! NETWORK CONFIG: vlans!  
!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
...  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
! TWAMP CONFIG:  
!  
twamp set port 5678  
twamp enable  
!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Chapter Configuring MSTP

20

At a Glance:

- Overview
- Benefits
- Configuration
- Troubleshooting

This chapter explains the implementation of the Multiple Spanning Tree Protocol (MSTP).

Overview

Multiple Spanning Tree Protocol (MSTP - IEEE 802.1Q-2005) is a standards based version of creating multiple spanning trees where each VLAN has its own Multiple Spanning Tree Instance (MSTI). Each instance has an independent spanning tree topology to provide multiple forwarding paths for data traffic, enable load balancing and reduce the number of spanning tree instances required to support a large number of VLANs. MSTP was developed to replace Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

Like STP, defined in IEEE 802.1D, MSTP provides a loop-free topology in bridged networks and delivers efficient reconfiguration (convergence) of the loop-free topology in the event that a link fails. MSTP inherits its rapid transition mechanism from RSTP, defined in IEEE 802.1W, to achieve fast convergence times.

MST Regions and Spanning Trees

An MST Region is a set of physically connected LANs and MST bridges that support the same MSTP configuration. A region can have one bridge or multiple bridges. Each bridge must be capable of processing RSTP BPDUs. There is no limit to the number of MST regions in a network, and each region supports up to 8 MSTIs. One of these MSTIs is called an Internal Spanning Tree (IST), which connects all MSTP bridges in an MST Region. An IST is a sub tree in the Common Spanning Tree (CST) that spans the network and interconnects MST Regions. The collection of ISTs and the CST make up the Common and Internal Spanning Tree (CIST).

NOTE: This implementation does not yet support MSTI configuration. By default, all VLANs are mapped to the CIST.



Bridges

The bridge with the best priority among all STP, RSTP, and MSTP enabled network bridges is called the CIST Root. The boundary bridge between regions becomes the CIST Regional Root. If there are multiple boundary bridges, the one with the best cost to the CIST Root becomes the CIST Regional Root. If all the bridges within a network are in one MST region, the CIST Root is also the CIST Regional Root.

BPDUs

Like its predecessors, STP and RSTP, MSTP-enabled devices send out bridge protocol data units (BPDUs) to detect topology changes in the network. BPDUs are sent when a device is powered up, when a topology change is detected, and at regular intervals (every few seconds). Thus, if a device fails, its neighbors realize that they have not received BPDUs and initiate a spanning tree recalculation. When a device receives these BPDUs, it does not forward them, but uses them to create its own BPDUs.

MSTP BPDUs carry the following information:

- **Protocol Identifier** - STP, RSTP, or MSTP.
- **Protocol Version Identifier** - STP (0), RSTP (2), or MSTP (3).
- **BPDU Type** - Configuration or topology change MSTP/RSTP BPDUs.
CIST Flags - Identifies the message as a topology change, proposal, port role, learning, forwarding, agreement, or topology change acknowledgement.
- **CIST Root Identifier**- the bridge priority and base MAC address of the device that the transmitting device considers to be the CIST Root.
- **CIST External Root Path Cost** - an additive cost of all the links between the transmitting bridge and the CIST Root bridge. A root path cost of 0 indicates this BPDUs came from the same region as the CIST Root, each device then adds its link cost towards root to 0 and uses that cost when generating the new BPDUs.
- **CIST Regional Root Identifier**- the bridge priority and base MAC address of the device that the transmitting device considers to be the CIST Regional Root.
- **CIST Port Identifier** - The port priority and base MAC address of the port transmitting the BPDUs.
- **Forward Delay (forward-delay)** - Forward delay is the time taken before a root or designated port starts forwarding after being selected and determined not to satisfy the rapid transition condition. The operational value is set to the value distributed by the root bridge via BPDUs and the configured value is not set until this bridge becomes the elected root bridge. The default value is 15.
- **Message Age** - The current age of the BPDUs.
- **Max Age**- The BPDUs life span.
- **Hello Time** - The time between two consecutive periodic BPDUs.
- **Forward Delay** - The time taken before a root or designated port starts forwarding after being selected and determined not to satisfy the rapid transition condition.
- **Version 1 Length** - Indicates whether or not Version 1 (IEEE Standard 802.1Q) information is present. For MSTP, the value is 0 to indicate that no Version 1 information is present.
- **Version 3 Length** - The number of bytes that are to follow in the packet.
- **MST Configuration Identifier** - The “finger print” of the MSTP configuration for the bridge, including the following:
 - **Configuration Id Format Selector**- The format of the MST Configuration Identifier, which is 0, the value defined for MSTP in the 802.1Q-2005 standard.
 - **Configuration Name**- Configurable character string that uniquely identifies the region. The default value is the device's MAC address.

- **Revision Level**- Configurable numeric value that provides an additional parameter to further differentiate MST regions.
- **Configuration Digest**- A 16-octet signature that is calculated with the HMAC_MD5 algorithm from the configured VLAN ID and MSTID mapping table as specified in the standard.
- **CIST Internal Root Path Cost** - specifies how close the device is to the CIST Root bridge.
- **CIST Bridge Identifier** - base MAC and bridge priority of the CIST Bridge.
- **CIST Remaining Hops** - Number of hops remaining before reaching the maximum hop value.
- **MSTI Configuration Messages** - Information used by MSTP to calculate vectors for the specified multiple spanning tree instances (MSTIs), including:
 - **MSTI Flags** - Identifies the message as a topology change, proposal, port role, learning, forwarding, agreement, or master.
 - **MSTI Regional Root Identifier** - base MAC and bridge priority of the MSTI Regional Root.
 - **MSTI Internal Root Path Cost** - an additive cost of all the links between the transmitting bridge and the MSTI Regional Root bridge. An MSTI Regional Root path cost of 0 indicates this BPDU came directly from the MSTI Regional Root, each device then adds its link cost towards MSTI Regional Root to 0 and uses that cost when generating the new BPDU.
 - **MSTI Bridge Priority** - bridge priority value.
 - **MSTI Port Priority** - port priority value.
 - **MSTI Remaining Hops** - hops remaining before the number exceeds the maximum hop count.

Port Roles

Based on the MSTP calculation for load balancing, ports in the CIST are assigned port roles. The port roles are similar to the port roles in STP and RSTP.

Table 20-1: MSTP Port Role and State Summary

MSTP Port Role	Port State	Description
CIST Root Port	Forwarding	Represents the best path (lowest cost) to the Root bridge of the CIST of the bridge.
Alternate Port	Discarding (Blocking)	Secondary port (Root Port being primary) that provides an alternate path to the root bridge of the CIST should the root port fail.
Designated Port	Forwarding	Port that provides the best path to the root bridge of the CIST for the link.
Backup Port	Discarding (Blocking)	Port that provides a backup path to a LAN segment if the Designated Port of the CIST fails.
CIST Regional Root Port	Forwarding	For MSTI only, this port provides connectivity from the Region to a CIST Root that lies outside the Region.



NOTE: This implementation does not support the learning state as defined by the IEEE. When a port is behaving as defined by the IEEE learning state, it will be in the blocking state in this implementation.

Boundary Port

A boundary port connects an MST region to:

- A different MST region
- A single STP box
- A single RSTP box

At the boundary port of the region, MSTP configuration changes so that the control of the STP state is per port. For this reason, MSTP calculated roles do not apply to its boundary ports. Instead, the boundary port state is forced to be the same as the IST port state.

Network Convergence

When a MSTP bridge initializes, it claims itself as both the CIST Root and CIST Regional Root via BPDU. When superior CIST Root information is received, it relinquishes its claim as the CIST Root. When superior IST information is received, it then relinquishes its claim as the CIST Regional Root. Finally, the MST region is converged when all bridges agree on the same CIST Regional Root and all port roles are synchronized.

MSTP limits the scope of topology change. If any MSTI topology change is detected by the non-boundary ports, it only triggers a MAC flush to the MSTI within the region. A topology change detected by the boundary port, however, will trigger MAC flushes more widely.

When the network is converged, each MST region independently allocates any frames to any given VLAN in a stable network. The CIST Root, Designated, and CIST Regional Root ports forward data frames, and Alternate, Backup and Disabled ports do not.

Backward Compatibility

As designed by IEEE, MSTP is fully backward compatible with RSTP and STP. MSTP operates with switches that support STP, RSTP, and traditional 802.1q through the selection of a designated MSTP bridge to function as the representative of that entire region to the CST. This enables MSTP regions composed of many switches and bridges to appear as a single switch to other Ethernet switches and bridges in a network. BPDUs for the STP instances are exchanged only between switches within an MSTP region. Since this information is not propagated outside the MSTP region, switch CPU cycles are reduced. Also, keeping this information within the region prevents network flapping and frequent network reconvergence caused by link and port outages.

The MSTP uses version 3 BPDU which attaches the CIST and MSTI information at the end of legacy STP and RSTP BPDUs. The CST takes care of the connectivity for all MST regions and all the RSTP and STP bridges in the network. The MST region appears as a virtual bridge cluster to adjacent STP or RSTP bridges (as well as to other MST regions.)

When an MST enabled bridge port receives an STP BPDU (version 0 BPDU) or an RSTP BPDU (version 2 BPDU), it knows that it is at the boundary of the region. Based on the version of the BPDU received, an MST enabled bridge will send the corresponding version of BPDU

to communicate with its counterpart. However, when its neighbor bridge switches its force-version to MSTP, it will not force this link to MSTP automatically. A per port protocol migration check will force the port to MSTP for a short period of time.



NOTE: MSTP backward compatibility supports RSTP mode and STP mode. However, it does not support Ciena proprietary RSTP port based domain functionality.

Benefits

The main benefits of MSTP are:

- Scalability on large networks. Both STP and RSTP 802.1W allow the total BPDU traversing of maximum 24 bridges from the root bridge. RSTP 802.1D/D4 (2003) allows the BPDU traversing of maximum 40 bridges. Within an MST region, MSTP limits BPDU traversing of maximum of 30 bridges, with no limit on the number of regions.
In case of ring topology, the number of bridges a BPDU can traverse is limited to the maximum number of bridges configured on the ring, taking the worst case of link failure into consideration. In a meshed topology, however, the maximum number of bridges can be included in the topology is much more than the limit.
- Limited Topology changes. MSTP limits the topology change events as within the region as possible. This makes a lot of sense, especially for large networks.
- Redundant links and load balancing. MSTP supports the assignment of a number of VLANs to a single spanning tree instance, and multiple instances are supported within each spanning tree region. These multiple Spanning Tree instances enable L2 networks to have redundant physical links because VLANs can be assigned to different Virtual bridges (spanning tree instances); this also enables load balancing.

Configuration

Assume a network with two regions, each with three bridges, separated by an RSTP bridge.

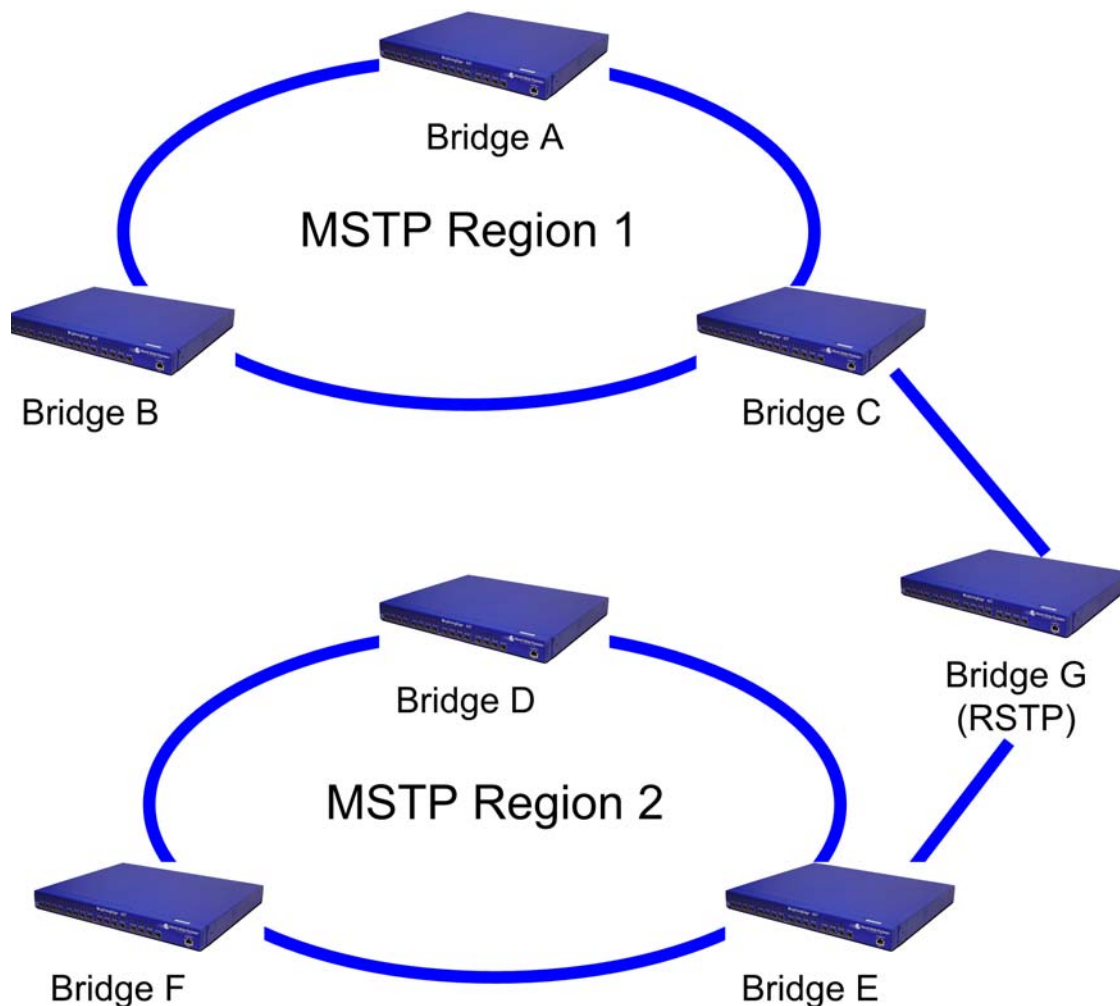


Figure 20-1: Sample Network Segment

The general steps for configuring MSTP in a network are as follows:

1. Configure one bridge in the network as the CIST root bridge.
2. Configure the CIST port settings.
3. For each region, configure the unique MST Identifiers.
4. For each MSTP bridge, configure the mode to MSTP.
5. Configure the bridge settings.
6. Configure port settings.
7. Enable MSTP on all bridges.

Configuring the CIST Root Bridge

For all bridges in the network, pick a bridge as the root bridge of the CIST. Assign the lowest number of priority to the root bridge. The bridge-priority assigned to the CIST for the bridge is used in the priority component of the CIST Bridge Identifier of BPDUs transmitted from this bridge. The supported range is 0-15. The value entered is multiplied by 4096 to conform with the standard as shown in **Table 20-2**, in this chapter.

Table 20-2: CIST Root Bridge Priority Mapping

Bridge Priority Entered Value	Maps to Standard Value
0	0
1	4096
2	8192
3	12288
4	16384
5	20480
6	24576
7	28672
8	32768
9	36864
10	40960
11	45056
12	49152
13	53248
14	57344
15	61440

To set the CIST root bridge priority:

```
mstp set cist bridge-priority <NUMBER: 0-15>
```

Example:

Assume for the network segment shown in **Figure 20-1** that Bridge A is the CIST Root bridge.

1. For Bridge A, set the CIST bridge priority as follows:

```
> mstp set cist bridge-priority 1
```

2. To verify the priority:

```
> mstp show cist
```

+--- MSTP CIST Info -----+	
Parameter	Value
+-----+	
CIST Bridge Id	
Priority	1 (0x1000)
Mac Address	00-02-A1-30-7C-40
CIST Bridge Priority Vector	
Root Port Id	
Priority	1 (0x1000)
Mac Address	00-02-A1-30-7C-40
External Path Cost	0
Regional Root Id	
Priority	1 (0x1000)
Mac Address	00-02-A1-30-7C-40
Internal Path Cost	0
Designated Bridge Id	
Priority	1 (0x1000)
Mac Address	00-02-A1-30-7C-40
Designated Root Id	(0x0000)
Priority	0
Port	0
CIST Bridge Times	
Message Age	0
Max Age	20
Forward Delay	15
Max Hops	20
CIST Root Priority Vector	
Root Port Id	
Priority	1 (0x1000)
Mac Address	00-02-A1-30-7C-40
External Path Cost	0
Regional Root Id	
Priority	1 (0x1000)
Mac Address	00-02-A1-30-7C-40
Internal Path Cost	0
Designated Bridge Id	
Priority	1 (0x1000)
Mac Address	00-02-A1-30-7C-40
Designated Root Id	(0x0000)
Priority	0
Port	0
CIST Root Port ID	(0x0000)
Priority	0
Port	0
CIST Root Times	
Message Age	0
Max Age	20
Forward Delay	15
Remaining Hops	20
+-----+	

Configuring CIST ports

If desired, you can individually configure priority and path cost settings for CIST ports manually. These configurable settings are:

- **Port Priority (`port-priority`)** - Port priority is the priority component of the CIST Port Identifier field of BPDUs transmitted from the specified port(s). The supported range is 0-15. The value entered is multiplied by 16 to conform with the standard as shown in **Table 20-3**, in this chapter.

Table 20-3: CIST Port Priority Mapping

Port Priority Entered Value	Maps to Standard Value
0	0
1	16
2	32
3	48
4	64
5	80
6	96
7	112
8	128
9	144
10	160
11	176
12	192
13	208
14	224
15	240

- **Internal Path Cost (`int-path-cost`)** - Sets the CIST internal root path cost for the specified port(s). Allowable path cost values are 1-200000000. This sets the CIST Internal Root Path Cost field in BPDUs transmitted from the specified port(s). This value will not be used in the BPDU if dynamic internal path cost is enabled for the CIST on the specified port(s). The default is 20000.
- **Dynamic Internal Path Cost (`dynamic-int-path-cost`)** - Enables or disables dynamic internal port path cost calculations for the CIST for the specified port(s). When enabled, the CIST Internal Root Path Cost field of BPDUs from the specified port(s) will use a value internally calculated based on link rate (and possibly other factors). When disabled, the configured `int-path-cost` value for the CIST for the specified port(s) will be used.

To configure the CIST ports:

```
mstp set cist-port {[port-priority <NUMBER: 0-15>],[int-path-cost <NUMBER: 1-200000000>],[dynamic-int-path-cost <on|off>]}.{port <PortNameList>}
```

Configuring the MST Identifier

To more easily identify BPDUs sent from an MST Region, you can configure the following:

- **Configuration Name (mst-cfg-id-name)** - The configuration name is used for calculating the MST Configuration Identifier for the bridge.
- **Revision Level (mst-cfg-id-rev-level)** - The revision level for calculating the MST Configuration Identifier for the bridge. The numeric value is transmitted in MST BPDUs in the Revision Level of the MST Configuration Identifier field. Since this is limited to 2 octets, the range of this value is 0-65535. The default value is '0'.

To configure the MST Identifier:

```
mstp set [mst-cfg-id-name <String[32]>] [mst-cfg-id-rev-level <NUMBER: 0-65535>]
```

To display the MST Identifier:

```
mstp show mst-cfg-id
```

Example:

For the network segment shown in **Figure 20-1**:

1. Set the MST Identifier for Bridges A, B, and C as follows:

```
> mstp set mst-cfg-id-name "MST Region 1" mst-cfg-id-rev-level 1
```

2. Verify the MST Identifier.

```
> mstp show mst-cfg-id
+--- MSTP MST Configuration Id Info -----+
| Parameter                               | Value                               |
+-----+-----+
| Configuration Name                     | MST Region 1 |
| Revision Level                         | 1 |
| Configuration Digest                   | 6EDEDDB2C31B7A50DCEBFB6FFE47D5766 |
+-----+-----+
```

3. Set the MST Identifier for Bridges D, E, and F as follows:

```
> mstp set mst-cfg-id-name "MST Region 2" mst-cfg-id-rev-level 2
```

4. Verify the MST Identifier.

```
> mstp show mst-cfg-id
+--- MSTP MST Configuration Id Info -----+
| Parameter                               | Value                               |
+-----+-----+
| Configuration Name                     | MST Region 2 |
| Revision Level                         | 2 |
| Configuration Digest                   | 6F696C6D9DD9032F8FEDA4DD25AC021B |
+-----+-----+
```

Configuring Bridge Global Settings

You can manually configure global settings for all network bridges, including:

- **Forward Delay (forward-delay)** - Forward delay is the time taken before a root or designated port starts forwarding after being selected and determined not to satisfy the rapid transition condition. The operational value is set to the value distributed by the root bridge via BPDU and the configured value is not set until this bridge becomes the elected root bridge. The default value is '15'.

- **Hello Time (hello-time)** - Hello time is the time between two consecutive periodic BPDUs. The operational value is set to the value distributed by the root bridge via BPDU and the configured value is not set until this bridge becomes the elected root bridge. The minimum value of '1' is not recommended because the periodic BPDU sending takes up the 1 per second transmit hold count allowance. When rapid convergence takes place, only one BPDU is allowed to send within a second for a port delaying the explicit handshake and rapid topology change. The default value is '2'.
- **Loopback Blocking (loopback-blocking)** - Loopback port blocking prevents data loops by detecting their own BPDUs being looped back to them on the same port. The default value is 'off', which is shown as 'disabled' with the `mstp show bridge` command.
- **Maximum Age (max-age)** - Maximum age limits the BPDU life span to limit the size of the spanning tree. The default value is '20'.
- **Maximum Hops (max-hops)** - Maximum hops limits the number of hops for BPDUs. The default is '20'.
- **Path Cost Default (path-cost-def)** - Path cost default controls the type of internal and external path costs for the bridge. MSTP supports default path costs defined in IEEE802.1D-1998 and IEEE802.1t-2001. The default value is 'stp8021t2001'.
- **Transmit Hold Count (tx-hold-count)** - Transmit hold count limits the number of BPDUs a bridge can send per second. The default value is '6'.

To configure bridge global settings:

```
mstp set {[forward-delay <NUMBER: 4-30>], [hello-time <NUMBER: 1-10>], [loopback-
blocking <on|off>], [max-age <NUMBER: 6-40>], [max-hops <NUMBER: 6-40>], [path-cost-
def <stp8021d1998|stp8021t2001>], [tx-hold-count <NUMBER: 1-10>]}
```

To verify bridge global settings:

```
mstp show [bridge]
```

Configuring Ports

You can manually adjust individual port settings, such as:

- **Dynamic External Path Cost (dynamic-ext-path-cost)** - Turns on or off dynamic calculation of the external path cost. When set to 'on', the external port path cost is calculated dynamically based on the port speed. When set to 'off', the external port path cost is the value configured in the 'ext-path-cost' parameter.
- **Edge Port (edge-port)** - Setting the specified port to be consider an edge port allows for rapid port state transition to the forwarding state. For 10/100 ports, the default value for edge-port is 'on'. For other ports, the default is 'off'. Always configure GIG link edge ports explicitly as edge ports. Rapid transition will fail otherwise. Another alternative is to disable MSTP on the GIG link edge ports, though this is not the preferred method.
- **Migration Check (migration-check)** - Triggers a migration check by the MSTP Port Protocol Migration State Machine. This is a momentary configuration parameter, setting it to 'on' will initiate the migration check and setting it to 'off' will have no effect.
- **External Path Cost (ext-path-cost)** - Sets the external port path cost for the specified port, which takes effect only if 'dynamic-ext-path-cost' is set to 'off'. The default value is '20000'. Rather than configure the port path cost, it is recommended that you turn on dynamic path cost to have MSTP select the best link(s) for forwarding.
- **Point to Point MAC (point-point-mac)** - Sets how to determine the link for the specified port: auto (automatic mechanisms determine the link), force-true (connected to a point-to-point link) or force-false (not connected to a point-to-point link).
- **Automatic Edge (auto-edge)** - Sets MSTP to automatically identify the edge ports.

- **Restricted Role (restricted-role)** - When set to on, this attribute restricts the port from becoming a root port, even if it has the best priority. The default is 'off'.
- **Restricted Topology Change Notice (restricted-tcn)** - When set to on, this attribute restricts the port from forwarding topology change notices.

To configure ports:

```
mstp set port <PortNameList> [dynamic-ext-path-cost <on|off>][edge-port  
<on|off>][migration-check][ext-path-cost <NUMBER: 1-200000000>][point-point-mac  
<auto|force-false|force-true>][auto-edge <on|off>][restricted-role  
<on|off>][restricted-tcn <on|off>]
```

To disable MSTP on specified ports:

```
mstp disable port <PortNameList>
```

To enable MSTP on specified ports:

```
mstp enable port <PortNameList>
```

To verify port settings:

```
mstp show port <PortNameList>
```

Enabling MSTP and Saving Configuration

After completing the MSTP configuration, enable MSTP on all bridges and save the configuration.

To globally enable MSTP and save the configuration:

```
mstp enable  
configuration save
```

Troubleshooting

Disabling and Enabling MSTP on a bridge

In general, it is best never to disable Spanning Tree on any bridge in the network as data loops might exist, rendering part or whole of the network useless. However, there may be occasions during troubleshooting that require you to globally disable MSTP on a bridge.

To disable MSTP:

```
mstp disable
```

To enable MSTP:

```
mstp enable
```

Clearing and Viewing MSTP Statistics

MSTP statistics track the number of received and transmitted topology change notification (TCN), configuration (CFG), RSTP, and MSTP BPDUs.

To view statistics for all ports:

```
mstp show statistics
```

Example:

```
> mstp show statistics
+--- MSTP Statistics -----+
| Port | Port Receive Statistics |
| Name | rxTcnBpdu| rxCfgBpdu| rxRstBpdu| rxMstBpdu|
+-----+-----+-----+-----+
| 1 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 |
+-----+-----+-----+-----+
| Port | Port Transmit Statistics |
| Name | txTcnBpdu| txCfgBpdu| txRstBpdu| txMstBpdu|
+-----+-----+-----+-----+
| 1 | 0 | 0 | 0 | 120889 |
| 2 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 120891 |
+-----+-----+-----+-----+
```

To view statistics for specific ports:

```
mstp show port <PortNameList> statistics
```

Example:

```
> mstp show port 1 statistics
+--- MSTP Port 1 Statistics -----+
| Statistic | Value |
+-----+-----+
| Received TCN BPDUs | 0 |
| Received CFG BPDUs | 0 |
| Received RST BPDUs | 3 |
| Received MST BPDUs | 3 |
| Transmitted TCN BPDUs | 0 |
| Transmitted CFG BPDUs | 0 |
| Transmitted RST BPDUs | 0 |
| Transmitted MST BPDUs | 36627 |
+-----+-----+
```

To clear statistics for all or specified ports:

```
mstp clear [port <PortNameList>] statistics
```

Viewing Port State Machine Information

MSTP port and CIST state machine information includes variables, timers, and states.

To view state machine information:

```
mstp show port <PortNameList> state-machine
```

Example:

```
> mstp show port 1 state-machine
```

+--- MSTP Port 1 Info ---+	
Parameter	Value
Name	1
Port Status	up
Port Uptime	0000D19:52:40
MSTP Enable	enabled
External Path Cost	
Admin Value	20000
Oper Value	200000
Dynamic Ext Path Cost	on
Edge Port	
Auto Edge	true
Admin Value	true
Oper Value	false
Point-to-Point MAC	
Admin Value	auto
Oper Value	true
Restricted Role	false
Restricted Tcn	false
Port State Machine Info	
Port State Machine Variables	
txCount	1
operEdge	false
portEnabled	true
infoInternal	false
newInfo	false
newInfoMsti	false
rcvdInternal	false
rcvdBpdu	false
rcvdRSTP	false
rcvdSTP	false
rcvdTcAck	false
rcvdTcn	false
sendRSTP	true
tcAck	false
mcheck	false
autoEdge	true
Port State Machine Timers	
mdelayWhile	0
helloWhen	2
edgeDelayWhile	0
Port State Machine States	
Port Protocol Migration State	SENSING
Port Receive State	RECEIVE
Port Transmit State	IDLE
Bridge Detection State	NOT_EDGE
+--- MSTP Port 1 CIST Info ---+	
MSTP State	forwarding
Role	designated
Port Priority	8
Internal Path Cost	
Admin Value	20000
Oper Value	200000
Dynamic Int Path Cost	on
CIST Designated Times	
Message Age	0
Max Age	20
Forward Delay	15
Remaining Hops	20
CIST Designated Priority Vector	
Root Port Id	

Priority	1 (0x1000)
Mac Address	00-02-A1-30-7C-40
External Path Cost	0
Regional Root Id	
Priority	1 (0x1000)
Mac Address	00-02-A1-30-7C-40
Internal Path Cost	0
Designated Bridge Id	
Priority	1 (0x1000)
Mac Address	00-02-A1-30-7C-40
Designated Root Id	(0x8001)
Priority	8
Port	1
CIST Message Times	
Message Age	1
Max Age	20
Forward Delay	15
Hello Time	2
Remaining Hops	20
CIST Message Priority Vector	
Root Port Id	
Priority	15 (0xFFFF)
Mac Address	FF-FF-FF-FF-FF-FF
External Path Cost	4294967295
Regional Root Id	
Priority	15 (0xFFFF)
Mac Address	FF-FF-FF-FF-FF-FF
Internal Path Cost	4294967295
Designated Bridge Id	
Priority	15 (0xFFFF)
Mac Address	FF-FF-FF-FF-FF-FF
Designated Root Id	(0xFFFF)
Priority	15
Port	4095
CIST Port Times	
Message Age	0
Max Age	20
Forward Delay	15
Hello Time	2
Remaining Hops	20
CIST Port Priority Vector	
Root Port Id	
Priority	1 (0x1000)
Mac Address	00-02-A1-30-7C-40
External Path Cost	0
Regional Root Id	
Priority	1 (0x1000)
Mac Address	00-02-A1-30-7C-40
Internal Path Cost	0
Designated Bridge Id	
Priority	1 (0x1000)
Mac Address	00-02-A1-30-7C-40
Designated Root Id	(0x8001)
Priority	8
Port	1
CIST Root Path Priority Vector	
Root Port Id	
Priority	1 (0x1000)
Mac Address	00-02-A1-30-7C-40
External Path Cost	0
Regional Root Id	
Priority	1 (0x1000)
Mac Address	00-02-A1-30-7C-40
Internal Path Cost	0
Designated Bridge Id	
Priority	1 (0x1000)

Mac Address	00-02-A1-30-7C-40
Designated Root Id	(0x8001)
Priority	8
Port	1
CIST State Machine Info	
CIST State Machine Variables	
forward	true
forwarding	true
infoIs	Mine
learn	true
learning	true
proposed	false
proposing	false
rcvdTc	false
reRoot	false
reselect	false
selected	true
tcProp	false
updtInfo	false
agreed	true
portId	0x8001-->priority 8, portnum 1
rcvdInfo	InferiorRootAlternateInfo
role	designated
selectedRole	designated
sync	false
synced	true
agree	true
disputed	false
fdbFlush	false
rcvdMsg	false
CIST State Machine Timers	
fdWhile	0
rrWhile	0
rbWhile	0
tcWhile	0
rcvdInfowhile	0
CIST State Machine States	
Port Information State	CURRENT
Port Role Transitions State	DESIGNATED_PORT
Port State Transition State	FORWARDING
Topology Change State	ACTIVE

Chapter Event Logging



At a Glance:

- Overview
- Principles of Operation
- Syslog
- Flash Log
- RAM Log
- Command Log
- Troubleshooting

This chapter provides explanations for how events generate messages to different types of logs on a Ciena device and describes the various options available to view and/or configure these event logging messages.

Overview

The system software supports the following types of logs SAOS:

- Syslog: Messages sent to collectors which are added (configured) via the SAOS CLI.
- Flash log: Text messages written to flash files.
- RAM log: Text messages written to RAM files.
- Command log: Entries of commands issued from the CLI.

Messages are written to the logs with timestamps based upon the system time settings, of local or UTC. A variety of log filters can be created to specify which events need to be logged and where they should be logged to.

Principles of Operation

In SAOS, every event can be logged to the logs listed above. An event manager converts events to messages and traps.

Events are generated by any component of the software that is programmed to generate logging information.

To display a list of system events, run any of the following CLI commands:

- > syslog show system-events
- > log flash show system-events

- > log ram show system events



NOTE: The log flash show system-events, log ram show system events, and the syslog show system-events commands list system events that apply to multiple platforms, including events that are not supported by devices running this system software.

Example:

```
> syslog show system-events
```

```
+ EVENTS -----+
| Mgr: bcastContainment
| Event Sev | Syslog Sev| Event # | Event
+-----+-----+-----+
| warning   | warning   | 0x10001 | Broadcast containment filter %d(%s) is dro
| warning   | warning   | 0x10002 | Broadcast containment filter %d(%s) has st
+-----+-----+-----+
| Mgr: blade
| Event Sev | Syslog Sev| Event # | Event
+-----+-----+-----+
| info      | info      | 0x20001 | Blade Operational State changed
| major     | alert     | 0x20003 | Line Blade Faulted
| info      | info      | 0x20004 | Blade Admin State Changed on Slot %d
| info      | info      | 0x20005 | Blade package version incorrect
| minor     | error     | 0x20006 | POST Error code 0x%08x : %s
| config    | notice    | 0x20007 | Blade manager config entry add slot: %d ca
| config    | notice    | 0x20008 | Blade manager config entry remove slot: %d
| config    | notice    | 0x20009 | Blade manager set slot: %d, admin state to
| config    | notice    | 0x2000B | Blade manager set installed image slot: %d
| config    | notice    | 0x2000C | Blade manager set installed slot: %d, pac
+-----+-----+-----+
...
+-----+-----+-----+
```

To display the event severity to Syslog severity mapping, run any of the following CLI commands:

- > syslog show severity-mapping
- > log flash show severity-mapping
- > log ram show severity-mapping

Example:

```
> syslog show severity-mapping
```

```
+--- SEVERITY MAPPING ---+
| Event | Syslog |
+-----+-----+
| critical | emergency |
| major    | alert     |
| minor    | error     |
| warning  | warning   |
| config   | notice    |
| info     | info      |
| debug    | debug     |
+-----+-----+
```

Comparing Log Types

Some differences between the log types can be found. These differences will guide the configuration of the event logging process. Users are encouraged to review the next paragraphs to identify the most appropriate log or combination of logs that will best meet their needs.

For example, flash logs may contain up to 4000 messages and messages are persistent across reboots up to a maximum of 4 reboots.

Syslog collectors and trap servers have configuration options external to SAOS that may include how many messages are retained and for how long.

Flash and RAM logs have a great deal of configuration flexibility because multiple filters may be created specifying the severity range, source manager and port, and the information specified by all of the filters is logged.

Because of the more permanent properties of flash logs, users can review the flash logs to identify or review older events.

Syslog has a more limited configuration capability. Multiple collectors can be configured but only one min-max severity range per collector. A syslog message facility number and prefix string can be specified per CLI-configured collector.

Command logs are persistent across reboots and can contain up to 2500 entries.

System Failure Notification

The purpose of the “System Failure Notification” is to notify the network operator that a device is going off-line. There are two major means of notification:

- if the system is able to detect failure and transmit a notification, a “dying gasp” will be transmitted.
- on power-up, the system will provide notification regarding the reason for the failure.

The “dying gasp” behavior is highly desirable. The capability to differentiate at the Network Operations Center between a power failure and a device failure is important for the operator.

If a system failure occurs, devices will do the following:

- Generate an event on any administrative reboot, either forced reboot or reset to factory defaults and indicate the reason.
- Attempt to generate an event on any system crash or unexpected reboot. There will be some conditions where transmitting a notification is not possible.
- Attempt to generate an event when a power failure occurs.

The “dying gasp” event will have critical severity. The event can be saved to the internal flash. The event will also generate a syslog message that will be delivered based on the users syslog configuration. In addition, the system will generate an associated SNMP trap (`wwwLeosChassisDyingGaspNotification`).

On system start-up a Cold Start trap is generated that includes the reason for the previous shutdown. An event is generated at start-up to indicate that the system has started up.

Syslog

Syslog messages can be sent to the Syslog Server or a standard UNIX or NT-type Syslog daemon. Configuring Syslog enables configuration events, system error messages, interface status, security alerts, and environmental conditions to be centrally logged and analyzed.

The Syslog server, if operationally enabled will transmit Syslog messages to the specified IP address(es) and port numbers. It will only transmit messages greater than or equal to the minimum severity and less than or equal to the maximum severity. The user can also specify which Syslog facility they wish system events to be generated for. This is typically used on the server side to separate events arriving at the server from multiple sources.

Since Syslog servers can be configured via DHCP, the user can also configure the default collector attributes for minimum severity, maximum severity, UDP port, and facility.

These defaults are applied to the user and DHCP configured collectors.

Each event generated by the SAOS software has a severity and a manager, and possibly a port associated with it. Next is the type of information selected and/or filtered sent to the syslog:

- Multiple collectors (external systems with IP address) may be configured (added) via the SAOS CLI and/or via DHCP.
- Each collector added via the CLI has a configurable min-max severity range.
- Each collector added via the CLI has a configurable facility number.
- All events in the min-max range are sent to the collector.
- Each CLI configured collector may have a different min-max range.
- Collectors added via DHCP have a default min-max range which cannot be configured.
- Each collector can have only one min-max range.

The device allows configuration of the Syslog collector and global parameters shown in the tables that follow.

Table 21-1 defines event severities.

Table 21-1: Event Severity Mapping

Syslog Severity	Definition
Critical	This indicates a condition in the device that is service affecting and requires immediate corrective action. It may indicate a catastrophic condition that affects multiple subscribers/customers.
Major	This indicates a condition in the device that is service affecting and requires urgent corrective action. It may indicate a condition that affects a very small number of customers.
Minor	This indicates the existence of a non-service affecting fault condition and that corrective action should be taken in order to prevent a more serious (for example, service affecting) fault. Such a severity can be reported, for example, when the detected alarm condition is not currently degrading the capacity of the managed object.
Warning	The Warning severity level indicates the detection of a potential or impending service affecting fault, before any significant effects have occurred. Action should be taken to further diagnose (if necessary) and correct the problem in order to prevent it from becoming a more serious service affecting fault.
Informational	The informational severity level indicates an occurrence on the device which is in no way associated with a performance degradation. No action is required by the operator. One example of this may be an event indicating that the configuration was saved to the flash file system.
Debug	The debug severity level indicates a class of events that are not intended for normal operation of the device and are merely used for troubleshooting. In general it is expected that these would be filtered.
Cleared	The Cleared severity level indicates the clearing of one or more previously reported alarms. An alarm with severity level "Cleared" can clear the corresponding Critical, Major or Minor alarm.
Config	The Config event indicates a configuration change. It is primarily used for communicating configuration changes through the system and to external entities.

Table 21-2 summarizes the mapping of SAOS event severities to standard Syslog severities.

Table 21-2: Event Severity Mapping			
Syslog Severity (numerical Value)	Event Severity	Syslog Severity	Syslog Severity Value
0	none	debug	7
1	cleared	debug	7
2	indeterminate	debug	7
3	critical	emergency	0
4	major	alert	1
5	minor	error	3
6	warning	warning	4
7	config	notice	5
8	info	informational	6
9	debug	debug	7
10	local	debug	7

Table 21-3 provides a description of Syslog attributes.

Table 21-3: Syslog Attributes			
Field	Default	Range (min. max.)	Description
Admin State	Enable	Enable, Disable	The administrative state of this collector
Oper State		Enable, Disable, Unresolved	The operational state is Enabled if both the global Admin State for Syslog is Enabled, and the Admin state of this collector is Enabled
Collector	None	x.x.x.x or valid hostname	This identifies the IP Address of the Syslog collector where the syslog messages will be sent.
Custom Prefix	Empty	String [15]	This value is included as a prefix in the syslog message
Facility	3	Integer (0-23)	Defines the facility code that will be sent on each message for this collector
Min. Severity	Alert	Other, Debug, Informational, Notice, Warning, Error, Alert, Emergency	Defines the minimum severity that a message must be to be sent to this collector
Max. Severity	Emergency	Other, Debug, Informational, Notice, Warning, Error, Alert, Emergency	Defines the maximum severity that a message can be to be sent to this collector
UDP Port	514	Integer (0-65535)	The UDP port that the syslog message will be transmitted to on the collector IP Address

A mnemonic field has been added to syslog messages to help quantify events. This field consists of three parts separated by dashes:

1. Source of the event
2. Event severity
3. Abbreviation of the event

For example, the mnemonic XCVR-3-OPTIC_REMOVED identifies that the source is the Transceiver manager (XCVR) with an event severity of Error (3) and the event is that a pluggable transceiver has been removed (OPTIC_REMOVED).

To enable and configure Syslog

Step #	Description	Command
Step 1	Enables syslog globally.	<code>syslog enable</code>
Step 2	Adds a syslog server.	<code>syslog add collector <IpAddress> <'emergency' 'alert' 'critical' 'error' 'warning' 'notice' 'info' 'debug' 'other'></code>
Step 3	Enables syslog on the specified server.	<code>syslog enable collector <IpAddress></code>

Example:

1. `> syslog enable`
2. `> syslog add collector 12.14.16.12 min-severity error max-severity info udp-port 560 facility 1`
3. `> syslog enable collector 12.14.16.12`

Flash Log

The system software logs various events (critical, reboot, power failure) to local flash files.

The default severities for flash filtering are as follows:

- minimum: major
- maximum: critical

Each event generated by the system has a severity and a manager, and possibly a port associated with it. You can configure flash log filters to select the type of events to be sent to the flash log:

- Only one flash log exists.
- Multiple filters may be created for the flash log.
- Each filter specifies the min-max range, the source software manager and the source port.
- All events in the min-max range that match the manager and port are sent to the collector.

Table 21-4 provides a description of event filter attributes.

Table 21-4: Event Filter Attributes			
Field	Default	Range (min. max.)	Description
Admin State	Enable	Enable, Disable	The administrative state of this collector
Operational State		Enable, Disable	The operational state is Enabled if both the global Admin State for Syslog is Enabled, and the Admin state of this collector is Enabled
Min. Severity	Major	Debug, Info, Config, Warning, Minor, Major, Critical	Defines the minimum severity that a message must be to be included in the log.
Max. Severity	Critical	Debug, Info, Config, Warning, Minor, Major, Critical	Defines the maximum severity that a message must be to be included in the log
Port List	Empty	List of Port IDs	This is a list of ports. For events generated on ports, only events on the ports in this list will be included in the log
Category List	Empty	List of Categories	This is a list of categories. All events in the listed categories will be included in the log as long as the port and severity criteria also match.

Configuring flash log filters

A default flash filter is automatically created and is named “default”. You can update the default filter or create new filters to limit or increase the events you want to log. The 1,000 most recent events are logged into flash memory, and will survive a system reboot.

To create a flash log filter:

```
log flash create filter <LogFlashFilterName[15]> {[all-mgrs], [arp-mgr <all|info>], [blade-mgr
<all|config|info>], [bcast-containment-mgr <all|info>], [cfm-mgr <all|info>], [chassis-mgr
<all|info>], [config-mgr <all|info>], [dnld-mgr <all|info>], [dnsc-mgr all|info], [dhcp-mgr
<all|debug|error|info|options|pkt|sm|timers>], [dot1x <all|info>], [event-mgr <all|info>],
[interface-mgr <all|debug|info>], [lacc-mgr <all|error|info|notif|mux-sm|ptx-ss-pkt>],
[lldp-mgr <all|error|info|notif|other|pdu|sm>], [max-severity
<critical|major|minor|warning|config|info|debug>], [min-severity
<critical|major|minor|warning|config|info|debug>], [ntpc-mgr <all|config|debug|info>], [port
<PortNameList>], [port-mgr <all|config|info|state-change>], [snmp-mgr <all|info>], [software-
mgr <all|info>], [tacacs-mgr <all|info>], [xcvr-mgr <all|debug|info>]}
```

To add events to an existing flash log filter:

```
log flash add filter <LogFlashFilterName[15]> {[all-mgrs], [arp-mgr <all|info>], [blade-mgr
<all|config|info>], [bcast-containment-mgr <all|info>], [cfm-mgr <all|info>], [chassis-mgr
<all|info>], [config-mgr <all|info>], [dnld-mgr <all|info>], [dnsc-mgr all|info], [dhcp-mgr
<all|debug|error|info|options|pkt|sm|timers>], [dot1x <all|info>], [event-mgr <all|info>],
[interface-mgr <all|debug|info>], [lacc-mgr <all|error|info|notif|mux-sm|ptx-ss-pkt>],
[lldp-mgr <all|error|info|notif|other|pdu|sm>], [ntpc-mgr <all|config|debug|info>], [port
<PortNameList>], [port-mgr <all|config|info|state-change>], [snmp-mgr <all|info>], [software-
mgr <all|info>], [tacacs-mgr <all|info>], [xcvr-mgr <all|debug|info>]}
```

To remove events from an existing flash log filter:

```
log flash remove filter <LogFlashFilterName[15]> {[all-mgrs], [arp-mgr <all|info>], [blade-mgr
<all|config|info>], [bcast-containment-mgr <all|info>], [cfm-mgr <all|info>], [chassis-mgr
<all|info>], [config-mgr <all|info>], [dnld-mgr <all|info>], [dnsc-mgr all|info], [dhcp-mgr
<all|debug|error|info|options|pkt|sm|timers>], [dot1x <all|info>], [event-mgr <all|info>],
[interface-mgr <all|debug|info>], [lacc-mgr <all|error|info|notif|mux-sm|ptx-ss-pkt>],
[lldp-mgr <all|error|info|notif|other|pdu|sm>], [ntpc-mgr <all|config|debug|info>], [port
<PortNameList>], [port-mgr <all|config|info|state-change>], [snmp-mgr <all|info>], [software-
mgr <all|info>], [tacacs-mgr <all|info>], [xcvr-mgr <all|debug|info>]}
```

To set the severities for a flash log filter:

```
log flash set filter <LogFlashFilterName[15]> {[max-severity
<critical|major|minor|warning|config|info|debug>], [min-severity
<critical|major|minor|warning|config|info|debug>]}
```

To delete a custom flash log filter:

```
log flash delete filter <LogFlashFilterName[15]>
```

To enable flash logging globally or for a specific flash log filter:

```
log flash enable [filter <LogFlashFilterName[15]>]
```

To disable flash logging globally or for a specific flash log filter:

```
log flash disable [filter <LogFlashFilterName[15]>]
```

Configuration Example:

This example shows how to create and enable a flash log filter for DHCP options:

```
> log flash create filter dhcpOptions
> log flash add filter dhcpOptions dhcp-mgr options
> log flash set filter dhcpOptions min-severity debug
> log flash enable filter dhcpOptions
> log flash enable
```

Configuring flash log packet filters

In addition to the flash log filters for events based on specific managers and severities, you can create flash log packet filters to enable logging based on specific packet types or ports. For each flash log packet filters, you can enable or disable packet decoding. When packet decoding is enabled, only the decoded packet is logged.



NOTE: Creating a packet filter for all, ingress, or egress ip-pkt types can use 100% of the CPU resulting in lockup and reboot.

Table 21-5 provides a description of packet filter attributes.

Table 21-5: Packet Filter Attributes

Field	Default	Range (min. max.)/Value	Description
Admin State	Enable	Enable, Disable	The administrative state of this collector
Operational State		Enable, Disable	The operational state is Enabled if both the global Admin State for Syslog is Enabled, and the Admin state of this collector is Enabled
Packet Decode	Off	On, Off	When this attribute is On the packets will be included in the log in decoded format. This is less space efficient, but much easier to read
Packet Groups		IGMP, IP, LACP, LLDP, RSTP	Defines the maximum severity of messages to be included in the log
Port List	Empty	List of Port IDs	This is a list of ports. For events generated on ports, only events on the ports in this list will be included in the log

To create a packet filter:

```
log flash create pkt-filter <LogFlashPacketFilterName[15]> {[cfm-pkt <all|egress|ingress>],  
[igmp-pkt <all|egress|ingress>], [ip-pkt <all|egress|ingress>],[larp-pkt  
<all|egress|ingress>], [lldp-pkt <all|egress|ingress>], [mstp-pkt <all|egress|ingress>],  
[pkt-decode <on|off>], [port <PortNameList>], [rstp-pkt <all|egress|ingress>]}
```

To add a packet type or port to a packet filter:

```
log flash add pkt-filter <LogFlashPacketFilterName[15]> {[cfm-pkt <all|egress|ingress>],  
[igmp-pkt <all|egress|ingress>], [ip-pkt <all|egress|ingress>],[larp-pkt  
<all|egress|ingress>], [lldp-pkt <all|egress|ingress>], [mstp-pkt <all|egress|ingress>],  
[port <PortNameList>], [rstp-pkt <all|egress|ingress>]}
```

To remove a packet type from a packet filter:

```
log flash remove pkt-filter <LogFlashPacketFilterName[15]> {[cfm-pkt <all|egress|ingress>],  
[igmp-pkt <all|egress|ingress>], [ip-pkt <all|egress|ingress>],[larp-pkt  
<all|egress|ingress>], [lldp-pkt <all|egress|ingress>], [mstp-pkt <all|egress|ingress>],  
[port <PortNameList>], [rstp-pkt <all|egress|ingress>]}
```

To set the packet decoding attribute for a packet filter:

```
log flash set pkt-filter <LogFlashPacketFilterName[15]> {pkt-decode <on|off>}
```

To delete a packet filter:

```
log flash delete pkt-filter <LogFlashPacketFilterName[15]>
```

To enable a packet filter:

```
log flash enable pkt-filter <LogFlashPacketFilterName[15]>
```

To disable a packet filter:

```
log flash disable pkt-filter <LogFlashPacketFilterName[15]>
```

Configuration Example:

This example shows how to configure a flash log packet filter for LLDP.

```
> log flash create pkt-filter myLLDPPktFilter  
> log flash add pkt-filter myLLDPPktFilter lldp-pkt all  
> log flash set pkt-filter myLLDPPktFilter pkt-decode on  
> log flash enable pkt-filter myLLDPPktFilter
```

Displaying flash log and flash log packet filter configuration

You can display the global state configuration with a summarized list of flash log and flash log packet filters, a summary of flash log filters only, or a summary of packet filters only or details for a specific flash log or flash log packet filters.

To display flash log filter configuration:

```
log flash show [filter <LogFlashFilterName>] | [pkt-filter <LogFlashPktFilter>] | [log-  
summary] | [pkt-summary]
```

Example of a summarized list of both flash log and flash log packet filters:

```
> log flash show  
+----- FLASH LOG STATE CONFIGURATION -----+  
| Admin State      | enabled  
+-----+  
  
+----- FLASH LOG FILTER CONFIGURATION -----+  
| Filter Name      | Admin | Oper | Severity | Minimum | No. Ports |  
| State            | State | State |           |          |           |  
+-----+-----+-----+-----+-----+-----+  
| default          | enabled | enabled | critical | critical | 28  
| dhcpOptions      | enabled | enabled | critical | debug   | 0  
+-----+-----+-----+-----+-----+-----+  
  
+----- FLASH PKT FILTER CONFIGURATION -----+  
| Filter Name      | Admin | Oper | Pkt | No. Frame |  
| State            | State | State | Decode | Types | No. Ports |  
+-----+-----+-----+-----+-----+-----+  
| No Pkt Filters   |      |      |      |      |      |  
+-----+-----+-----+-----+-----+-----+
```

Example of the default flash log filter configuration:

> log flash show filter default

+----- LOG FLASH FILTER CONFIGURATION -----+		
Name	default	
Index	1	
Admin State	enabled	
Oper State	enabled	
Maximum Severity	critical	
Minimum Severity	major	
Categories	blade-mgr - config - info chassis-mgr - info config-mgr - info dnld-mgr - info dhcp-mgr - debug - error - info - options - pkt - sm - timers dnsc-mgr - resolve - monitor - info event-mgr - info igmp-mgr - events - egress-pkt - ingress-pkt - info interface-mgr - debug - info unknown - info lldp-mgr - error - notif - other - pdu - sm - info ntpc-mgr - config - debug - info port-mgr - config - info - state-change snmp-mgr - info software-mgr - info xcvr-mgr - info - debug	
Port List	1	2 3
	12345678901234567890123456789012	XXXXXXX-----
+-----		

Displaying the flash log

You can display the entries made to flash based upon the configured flash log and flash log packet filters. Specifying the 'tail' attribute will display the last number of lines specified and the keyword string will search for the keyword in entries and display the corresponding lines.

To display the flash log:

```
log flash view [tail <NUMBER: 1-100>][keyword <String[16]>]
```

Example:

```
> log flash view tail 5
January 2, 2000 17:02:09.000 ntwrk: :Vlan add port vlan 200 added port 3
January 2, 2000 17:02:09.000 ntwrk: :Vlan add port vlan 200 added port 4
January 2, 2000 17:02:16.000 chassis: DHCP IP 172.25.0.2 User dhcp:DHCP System
Time Offset Set, tJanuary 2, 2000 17:02:16.000 chassis: DHCP IP 172.25.0.2 User
dhcp:DHCP System Time Offset Set, tJanuary 2, 2000 17:02:28.000 snmp: :Cannot
ping gateway, cannot send cold trap but making an attempt
```

In addition, you can display the log files located in the /mnt/sysfs/log directory. These default system event logs are accessible using the following CLI commands. In this example, we can see at what time and for which reason the unit was reset.

Example:

```
> file
(file)> cd /mnt/sysfs/log
(file)> ls
Directory '/mnt/sysfs/log'
pdtrc.lo0
ipstrc.lo0
eventLog.6
eventLog.5
(file)> cat eventLog.5
----- > BOOTING < -----
21:55:50.252 chassis: Cli requested device REBOOT, Rebooting now
```

To clear the log flash file:

```
log flash clear
```

RAM Log

The system software logs events to local RAM files in addition to the local flash. The default severities for RAM filter are as follows:

- minimum: major
- maximum: critical

The configuration and attributes of RAM log filters are similar to flash log filters:

- Only one RAM log exists.
- Multiple filters may be created for the RAM log.
- Each filter specifies the min-max range, the source software manager and the source port.
- All events in the min-max range that match the manager and port are sent to the collector.



NOTE: The RAM log is a temporary storage log file that will be erased when the unit is rebooted.

You can configure event and packet filters for the RAM log with the same attributes described for the flash log. With RAM logs, you can set a global notification attribute to broadcast new entries to all active CLI sessions.

To configure the global notification:

```
log ram set global-notify <on|off>
```

Creating a RAM log filter

A default RAM log filter is automatically created and is named “default”. You can update the default filter or create new filters to limit or increase the events you want to log.

To create a RAM log filter:

```
log ram create filter <LogFlashFilterName[15]> {[all-mgrs], [arp-mgr <all|info>], [blade-mgr
<all|config|info>], [bcast-containment-mgr <all|info>], [cfm-mgr <all|info>], [chassis-mgr
<all|info>], [config-mgr <all|info>], [dnld-mgr <all|info>], [dnsc-mgr all|info], [dhcp-mgr
<all|debug|error|info|options|pkt|sm|timers>], [dot1x <all|info>], [event-mgr <all|info>],
[interface-mgr <all|debug|info>], [lcp-mgr <all|error|info|notif|mux-sm|ptx-ss-pkt>],
[lldp-mgr <all|error|info|notif|other|pdu|sm>], [max-severity
<critical|major|minor|warning|config|info|debug>], [min-severity
<critical|major|minor|warning|config|info|debug>], [ntpc-mgr <all|config|debug|info>], [port
<PortNameList>], [port-mgr <all|config|info|state-change>], [snmp-mgr <all|info>], [software-
mgr <all|info>], [tacacs-mgr <all|info>], [xcvr-mgr <all|debug|info>]}
```

To add events to an existing RAM log filter:

```
log ram add filter <LogFlashFilterName[15]> {[all-mgrs], [arp-mgr <all|info>], [blade-mgr
<all|config|info>], [bcast-containment-mgr <all|info>], [cfm-mgr <all|info>], [chassis-mgr
<all|info>], [config-mgr <all|info>], [dnld-mgr <all|info>], [dnsc-mgr all|info], [dhcp-mgr
<all|debug|error|info|options|pkt|sm|timers>], [dot1x <all|info>], [event-mgr <all|info>],
[interface-mgr <all|debug|info>], [lcp-mgr <all|error|info|notif|mux-sm|ptx-ss-pkt>],
[lldp-mgr <all|error|info|notif|other|pdu|sm>], [ntpc-mgr <all|config|debug|info>], [port
<PortNameList>], [port-mgr <all|config|info|state-change>], [snmp-mgr <all|info>], [software-
mgr <all|info>], [tacacs-mgr <all|info>], [xcvr-mgr <all|debug|info>]}
```

To remove events from an existing RAM log filter:

```
log ram remove filter <LogFlashFilterName[15]> {[all-mgrs], [arp-mgr <all|info>],[blade-mgr  
<all|config|info>], [bcast-containment-mgr <all|info>], [cfm-mgr <all|info>], [chassis-mgr  
<all|info>], [config-mgr <all|info>], [dnld-mgr <all|info>], [dnsc-mgr all|info], [dhcp-mgr  
<all|debug|error|info|options|pkt|sm|timers>], [dot1x <all|info>], [event-mgr <all|info>],  
[interface-mgr <all|debug|info>], [lcp-mgr <all|error|info|notif|mux-sm|ptx-ss-pkt>],  
[lldp-mgr <all|error|info|notif|other|pdu|sm>], [ntpc-mgr <all|config|debug|info>], [port  
<PortNameList>], [port-mgr <all|config|info|state-change>], [snmp-mgr <all|info>], [software-  
mgr <all|info>], [tacacs-mgr <all|info>], [xcvr-mgr <all|debug|info>]}
```

To set the severities for a RAM log filter:

```
log ram set filter <LogFlashFilterName[15]> {[max-severity  
<critical|major|minor|warning|config|info|debug>], [min-severity  
<critical|major|minor|warning|config|info|debug>]}
```

To delete a custom RAM log filter:

```
log ram delete filter <LogFlashFilterName[15]>
```

To enable flash logging globally or for a specific ram log filter:

```
log ram enable [filter <LogFlashFilterName[15]>]
```

To disable flash logging globally or for a specific ram log filter:

```
log ram disable [filter <LogFlashFilterName[15]>]
```

Configuration Example:

This example shows how to create and enable a RAM log filter for DHCP options:

```
> log ram create filter dhcpOptions  
> log ram add filter dhcpOptions dhcp-mgr options  
> log ram set filter dhcpOptions min-severity debug  
> log ram enable filter dhcpOptions  
> log ram enable
```

Configuring RAM log packet filters

In addition to the RAM log filters for events based on specific managers and severities, you can create RAM log packet filters to enable logging based on specific packet types or ports. For each RAM log packet filters, you can enable or disable packet decoding. When packet decoding is enabled, only the decoded packet is logged.



NOTE: Creating a packet filter for all, ingress, or egress ip-pkt types can use 100% of the CPU resulting in lockup and reboot.

To create a packet filter:

```
log ram create pkt-filter <LogramPacketFilterName[15]> {[cfm-pkt <all|egress|ingress>],  
[igmp-pkt <all|egress|ingress>], [ip-pkt <all|egress|ingress>],[lcp-pkt  
<all|egress|ingress>], [lldp-pkt <all|egress|ingress>], [mstp-pkt <all|egress|ingress>],  
[pkt-decode <on|off>], [port <PortNameList>], [rstp-pkt <all|egress|ingress>]}
```


To add a packet type or port to a packet filter:

```
log ram add pkt-filter <LogramPacketFilterName[15]> {[cfm-pkt <all|egress|ingress>], [igmp-
pkt <all|egress|ingress>], [ip-pkt <all|egress|ingress>], [lcp-pkt <all|egress|ingress>],
[lldp-pkt <all|egress|ingress>], [mstp-pkt <all|egress|ingress>], [port <PortNameList>],
[rstp-pkt <all|egress|ingress>]}
```

To remove a packet type from a packet filter:

```
log ram remove pkt-filter <LogramPacketFilterName[15]> {[cfm-pkt <all|egress|ingress>],
[igmp-pkt <all|egress|ingress>], [ip-pkt <all|egress|ingress>], [lcp-pkt
<all|egress|ingress>], [lldp-pkt <all|egress|ingress>], [mstp-pkt <all|egress|ingress>],
[port <PortNameList>], [rstp-pkt <all|egress|ingress>]}
```

To set the packet decoding attribute for a packet filter:

```
log ram set pkt-filter <LogramPacketFilterName[15]> {pkt-decode <on|off>}
```

To delete a packet filter:

```
log ram delete pkt-filter <LogramPacketFilterName[15]>
```

To enable a packet filter:

```
log ram enable pkt-filter <LogramPacketFilterName[15]>
```

To disable a packet filter:

```
log ram disable pkt-filter <LogramPacketFilterName[15]>
```

Configuration Example:

This example shows how to configure a ram log packet filter for LLDP.

```
> log ram create pkt-filter myLLDPPktFilter
> log ram add pkt-filter myLLDPPktFilter lldp-pkt all
> log ram set pkt-filter myLLDPPktFilter pkt-decode on
> log ram enable pkt-filter myLLDPPktFilter
```

Displaying RAM log and RAM log packet filter configuration

You can display the global configuration with a summarized list of RAM log and RAM log packet filters, a summary of flash log filters only, or a summary of packet filters only or details for a specific flash log or flash log packet filters.

To display flash log filter configuration:

```
log flash show [filter <LogFlashFilterName>] | [pkt-filter <LogFlashPktFilter>] | [log-
summary] | [pkt-summary]
```

Example of a summarized list of both flash log and flash log packet filters:

> log ram show

```
+----- RAM LOG STATE CONFIGURATION -----+
| Admin State      | enabled      |
| Global-notify    | disabled     |
+-----+-----+
```

```
+----- RAM LOG FILTER CONFIGURATION -----+
| Filter Name      | Admin        | Oper         | Severity      |
|                  | State        | State        | Maximum       | Minimum       | No. Ports    |
+-----+-----+-----+-----+-----+-----+
| default          | enabled      | enabled      | critical      | info          | 12           |
+-----+-----+-----+-----+-----+-----+
```

```
+----- RAM PKT FILTER CONFIGURATION -----+
| Filter Name      | Admin        | Oper         | Pkt           | No. Frame    |
|                  | State        | State        | Decode        | Types        | No. Ports    |
+-----+-----+-----+-----+-----+-----+
| No Filters       |              |              |               |              |              |
+-----+-----+-----+-----+-----+-----+
```

Example of the default flash log filter configuration:

> log ram show filter default

LOG RAM FILTER CONFIGURATION	
Name	default
Index	1
Admin State	enabled
Oper State	enabled
Maximum Severity	critical
Minimum Severity	major
Categories	blade-mgr - config - info chassis-mgr - info config-mgr - info dnld-mgr - info dhcp-mgr - debug - error - info - options - pkt - sm - timers dnsc-mgr - resolve - monitor - info event-mgr - info igmp-mgr - events - egress-pkt - ingress-pkt - info interface-mgr - debug - info unknown - info lldp-mgr - error - notif - other - pdu - sm - info ntpc-mgr - config - debug - info port-mgr - config - info - state-change snmp-mgr - info software-mgr - info xcvr-mgr - info - debug
Port List	1 2 3 12345678901234567890123456789012 XXXXXXXXXX-----

Displaying the RAM log

You can display all RAM log entries or monitor entries as they occur. To stop monitoring the RAM log, press Ctrl+C.

To display RAM log entries:

```
log ram trace [all]
```

Example of monitoring entries:

```
> log ram trace
(trace activated)
May 6, 2009 14:14:26.604 chassis: Telnet IP 1.90.90.24 User su:System Session More Enable
<Ctrl+C>
--break--
```

Example of all:

```
> log ram trace all
January 1, 2000 00:00:50.488 interface: :local interface is operationally enabled
January 1, 2000 00:00:51.038 interface: :local interface is operationally enabled
January 1, 2000 00:00:51.081 chassis: :AC power supply 1 failure
January 1, 2000 00:00:51.097 interface: :remote interface is operationally enabled
January 1, 2000 00:00:56.952 lacpOptCheck() Total 0 signal sent
January 1, 2000 00:01:15.151 LLDP: lldpBAadmStateSET() to state 0
January 1, 2000 00:01:15.759 interface: :remote interface is operationally enabled
January 1, 2000 00:01:15.798 interface: :remote interface is operationally enabled
January 1, 2000 00:01:22.410 Software: saos-06-05-00-0027 Build 27
May 10, 2009 07:05:05.890 [UTC] config: Local RS-232 User gss:Config Save
May 10, 2009 07:05:46.971 [UTC] config: Local RS-232 User gss:Config Save
May 10, 2009 07:05:55.112 [UTC] chassis: Telnet IP 10.25.42.9 User su:System Session More Disable
May 10, 2009 07:05:55.316 [UTC] chassis: Telnet IP 10.25.42.9 User su:System Global Inactivity Timer Disable
May 11, 2009 16:55:55.139 [UTC] chassis: Telnet IP 10.25.42.9 User su:System Session More Disable
May 11, 2009 16:55:55.343 [UTC] chassis: Telnet IP 10.25.42.9 User su:System Global Inactivity Timer Disable
-----
```

To clear the log ram file:

```
log ram clear
```

Command Log

The system logs user command history for monitoring system configuration performed from the CLI. Each time a system goes into service, a header is written to the log containing the system identifier and a timestamp. All subsequent commands (with some exceptions) issued from the CLI are entered in chronological order up to 2500 entries, and then the entries wrap to the beginning of the command log file. When commands contain a password, the password will be masked to maintain security. This command log is stored in the local flash file system, and each entry includes:

- **Log ID** - sequence identifier of the entry.

- **User** - Session, IP address of the user session, or user ID to indicate who issued the command.
- **User privilege level** - access level of the user who issued the command.
- **Timestamp** - Timestamp of when the command was issued. This timestamp is stored in UTC format, but the display format is determined by the system timestamp as set with the system set timestamp command.

Currently, the system does not write entries to the command log for the following:

- Log on attempts, successful or failed.
- Commands run from the configuration file during startup.
- Commands contained within a file used in configuration augment commands.

You can display the command log, rerun commands entered into the log file, specify to repeat a specific command, and disable or enable command logging.



NOTE: Limited users cannot display or repeat commands requiring super user access.

Displaying the command log

You can display all entries in the command log in the default format with sequence ID and command. Also, you can apply multiple options to display specific information and to change the format, such as:

- **[destination]** - Location of the command log file.
- **[recent]** - Recent entries.
- **[last <DurationString>]** - Entries from the specified time interval in the format N[yMwdhms]. If you specify a number only, the interval will be shown in seconds.
- **[today]** - Entries from today.
- **[yesterday]** - Entries from yesterday.
- **[from-date <DateString>]** - Entries from specified date (yyyy-mm-dd or yy-mm-dd or mm-dd).
- **[to-date <DateString>]** - Entries to specified date (yyyy-mm-dd or yy-mm-dd or mm-dd).
- **[from-time <TimeString>]** - Entries from specified time (hh:mm or hh:mm:ss)
- **[to-time <TimeString>]** - Entries to specified time (hh:mm or hh:mm:ss)
- **[tail <NUMBER: 1-4290261631>]** - Latest number of entries
- **[containing <String>]** - Entries containing a specific string.
- **[mine]** - Displays entries for current user.
- **[since-activated]** - Entries since system startup.
- **[user <String[16]>]** - Displays entries for the specified user.
- **[privilege <limited|super>]** - Limits to users with the specified privilege.
- **[on-terminal <TerminalString>]** - Entries of commands run from a specific terminal ID.
- **[sequence-id <NUMBERList>]** - Entries with the specified sequence identifier(s).
- **[verbose]** - Displays the command log in a table format with headings, timestamp, and user information. Without the verbose option, the command log is displayed with sequence ID and command only.

To display the command log:

```
command-log show [destination] [recent] [last <String>] [today] [yesterday] [from-date <String>] [to-date <String>] [from-time <String>] [to-time <String>] [tail <#>] [containing <String>] [mine] [since-activated] [user <String>] [privilege <limited|super|diag>] [on-terminal <String>] [sequence-id <#List>][verbose]
```

Examples:

```
> command-log show destination
Command Log Destination: flash

> command-log show recent
8180: command-log show last 6h
8181: command-log show last 6h verbose
8182: command-log show last 30m verbose
8183: command-log show destination
8184: command-log show today
8185: command-log show yesterday
8189: command-log show from-date 2009-05-04 to-date 2009-05-06
8190: command-log show on-terminal /telnet_10.25.42.9:4682
8194: command-log show tail 10 verbose

> command-log show recent verbose
```

COMMAND LOG				
ID	Date & Time (UTC)		User(privilege) on Terminal	
8274	Wed May 6	19:37:22 2009	su(super) /telnet_1.90.90.24:3935	
command-log show today from-time 13:34:00 to-time 19:34:00 verbose				
	Wed May 6	19:37:28 2009		

Repeating commands

If you need to rerun a command listed in the command log, you can repeat it by specifying a sequence ID or repeat your last command. Also, you can repeat a specific command without having to look up a sequence Identifier. When repeating commands, you can specify a time interval (in the format N[yMwdhms]) and number of times to run the command.



NOTE: The system does not support rerunning the `command-log repeat` command. If you run `command-log repeat my-last-command` and the last command run was `command-log repeat`, the system will rerun the command you ran prior to it. Also, if you run `command-log repeat` and specify a sequence ID for the `command-log repeat` command, it will fail with the error message “Cannot repeat command: command-log repeat.”

To repeat a command

```
command-log repeat {sequence-id <numbers>|my-last-command|command <String>} [every <DurationString>] [times <NUMBER: 1-4290261631>]
```

Example of my-last-command:

```
> command-log repeat my-last-command times 2
command-log show last 1m
8281: command-log show last 1m
8282: command-log show last 1m
command-log show last 1m
8281: command-log show last 1m
8282: command-log show last 1m
```

Example of sequence-id list:

```
> command-log repeat sequence-id 8360,8196,8042
cli show object command-log full
command-log disable
command-log enable
command-log show
command-log show destination
command-log show recent
command-log show last <String>
command-log show today
command-log show yesterday
command-log show from-date <String>
command-log show to-date <String>
command-log show from-time <String>
command-log show to-time <String>
command-log show tail <#>
command-log show containing <String>
command-log show mine
command-log show since-activated
command-log show user <String>
command-log show privilege <limited|super|diag>
command-log show on-terminal <String>
command-log show sequence-id <#List>
command-log show verbose
command-log repeat my-last-command
command-log repeat command <String>
command-log repeat every <String>
command-log repeat times <#>
command-log show tail 7
8448: broadcast-containment show port 1
8479: cli show object broadcast-containment full
8939: command-log show
8943: command-log repeat sequence-id 8409,8205,8210
8944: command-log show
8945: command-log repeat sequence-id 8210
8946: broadcast-containment show
system shell set more on
```

Example of a specific command:

```
> command-log repeat command "port show port 1 statistics active" every 10s times 2
port show port 1 statistics active
```

```
+----- PORT 1 STATISTICS -----+
| Statistic           | Value                |
+-----+-----+
| TxBytes             | 14790225612          |
| TxPkts              | 119276013            |
| TxBcastPkts         | 119276013            |
+-----+-----+
port show port 1 statistics active
```

```
+----- PORT 1 STATISTICS -----+
| Statistic           | Value                |
+-----+-----+
| TxBytes             | 14791312968          |
| TxPkts              | 119284782            |
| TxBcastPkts         | 119284782            |
+-----+-----+
```

Disabling and enabling command logging

Command logging is enabled by default. You can disable it to conserve space on the local flash file system. The commands to disable and enable are logged.

To disable command logging:

```
command-log disable
```

To enable command logging:

```
command-log enable
```

Troubleshooting

Sending log test messages

You can test the configuration of log flash and RAM filters by sending a test message.

To send a test message:

```
log send msg <String[127]> severity <critical|major|minor|warning|config|info|debug>
```

Example:

```
> log send msg "This is a test message." severity critical
```

Resetting log file configuration to defaults

You can reset the configuration of flash and RAM log filters to the default settings and clear the flash and RAM log files.

To reset the configuration and clear the log files:

```
log reset-to-factory-defaults
```


Chapter Configuring SNMP

22

At a Glance:

- Overview
- Benefits
- Configuring Global Attributes
- Configuring SNMPv1/v2c Community Based Security
- Configuring Port Traps and Servers
- Configuring SNMPv3
- Configuring RMON
- Troubleshooting

This chapter describes Simple Network Management Protocol (SNMP) and how to configure it.

Overview

Simple Network Management Protocol (SNMP) governs the functions and management of network devices and components called managed objects. SNMP provides the ability to administer managed objects using a Network Management System (NMS) interface, instead of the CLI. Examples of NMS interfaces are a Management Information Base (MIB) browser or Ethernet Services Manager (ESM). The NMS interface acts as an SNMP manager and sends messages to the device in the form of an SNMP Protocol Description Unit (PDU). These messages are processed by the SNMP agent on the device.



NOTE: To optimize performance when retrieving large table views while browsing MIBs, use SNMP v2 Get Bulk instead of SNMP Get.

SNMP Architecture

The system software supports SNMP versions v1, v2c, and v3. The SNMP architecture includes the following components:

- **Message dispatcher** - The message dispatcher is responsible for sending and receiving SNMP messages. When an SNMP request message is received, the Dispatcher determines the SNMP version and then passes the message to the appropriate Message Processing Model (SNMPv1, SNMPv2c, or SNMPv3). The Dispatcher is also responsible for dispatching SNMP response messages to the NMS interface application.
- **Community authentication** - SNMPv1 and SNMPv2c support a community-based security model. This model provides limited security based upon the configured community name. No encryption or user authentication is provided. All SNMP messages between Agent and manager contain "Community Name" in the plain text.
- **User-based authentication** - SNMPv3 supports a user-based security model. This model requires users to provide a secret key for authentication and privacy. The supported authentication protocols are Keyed Hashing for Message Authentication

Message Digest 5 (HMAC-MD5) and HMAC Secure Hash Algorithm 1 (SHA-1) algorithms. Privacy is accomplished by encrypting and decrypting SNMPv3 packets with the Cipher Block Chaining mode to the Data Encryption Standard (CBC-DES) algorithm.

- **View-based access control**- SNMPv3 provides additional security by limiting access to specific managed objects.
- **Protocol PDU operations** - The Message Processing Subsystem handles the Protocol PDU operations of preparing messages for sending and extracting data from received messages. This system software version supports the SNMPv1 Message Processing Model for SNMPv1 and SNMPv2 protocol operations.
- **MIBs** - The system software supports both standard and proprietary MIBs that store configuration, operational state, and statistics information in the form of managed objects. Each managed object is identified by an Object Identifier (OID) and exchanges information between the MIB and the system software modules through an Application Programming Interface (API). MIB files supported in this release include:
 - BRIDGE-MIB.my
 - ETHERLIKE-MIB.my
 - IANA-ADDRESS-FAMILY-NUMBERS-MIB.my
 - IANAifType-MIB.my
 - IEEE8021-PAE-MIB.my
 - IF-MIB.my
 - LLDP_DOT1-MIB.my
 - LLDP_DOT3-MIB.my
 - RFC1213-MIB.my
 - rfc1215.mib
 - RFC-1215.my
 - RMON2-MIB.my
 - RMON-MIB.my
 - SNMP-NOTIFICATION-MIB.my
 - SNMPv2-MIB.my
 - WWP-LEOS-8021X-MIB.my
 - WWP-LEOS-BLADE-MIB.my
 - WWP-LEOS-BROADCAST-CONTAINMENT-MIB.my
 - WWP-LEOS-CFM-MIB.my
 - WWP-LEOS-CHASSIS-MIB.my
 - WWP-LEOS-COMMUNITY-MIB.my
 - WWP-LEOS-DATAPLANE-MIB.my
 - WWP-LEOS-DHCP-CLIENT-MIB.my
 - WWP-LEOS-DNS-CLIENT-MIB.my
 - WWP-LEOS-EXT-LAG-MIB.my
 - WWP-LEOS-FEATURE-LICENSE-MIB.my
 - WWP-LEOS-FILE-TRANSFER-MIB.my
 - WWP-LEOS-FLOW-MIB.my
 - WWP-LEOS-IGMP-MIB.my
 - WWP-LEOS-IP-INTERFACE-MIB.my
 - WWP-LEOS-L2CFT-MIB.my
 - WWP-LEOS-LLDP-MIB.my
 - WWP-LEOS-MSTP-MIB.my

- WWP-LEOS-MULTICAST-FILTER-MIB.my
- WWP-LEOS-NTP-CLIENT-MIB.my
- WWP-LEOS-OAM-MIB.my
- WWP-LEOS-PBT-MIB.my
- WWP-LEOS-OAM-MIB-MODULE.my
- WWP-LEOS-PING-MIB.my
- WWP-LEOS-PORT-MIB.my
- WWP-LEOS-PORT-STATS-MIB.my
- WWP-LEOS-PORT-XCVR-MIB.my
- WWP-LEOS-RADIUS-CLIENT.my
- WWP-LEOS-SSH-MIB.my
- WWP-LEOS-SW-XGRADE-MIB.my
- WWP-LEOS-SYSLOG-COLLECTOR-MIB.my
- WWP-LEOS-SYSTEM-CONFIG-MIB.my
- WWP-LEOS-SYSTEM-CONTROL-MIB.my
- WWP-LEOS-TACACS-CLIENT-MIB.my
- WWP-LEOS-TRAFFIC-PROFILE-MIB.my
- WWP-LEOS-TWAMP-MIB.my
- WWP-LEOS-USER-MIB.my
- WWP-LEOS-VLAN-TAG-MIB.my
- WWP-LEOS-VPLS-MIB.my
- WWP-PRODUCTS-MIB.my

Figure 22-1 illustrates the SNMPv1 & SNMPv2c agent and the SNMPv3 Engine Architecture.

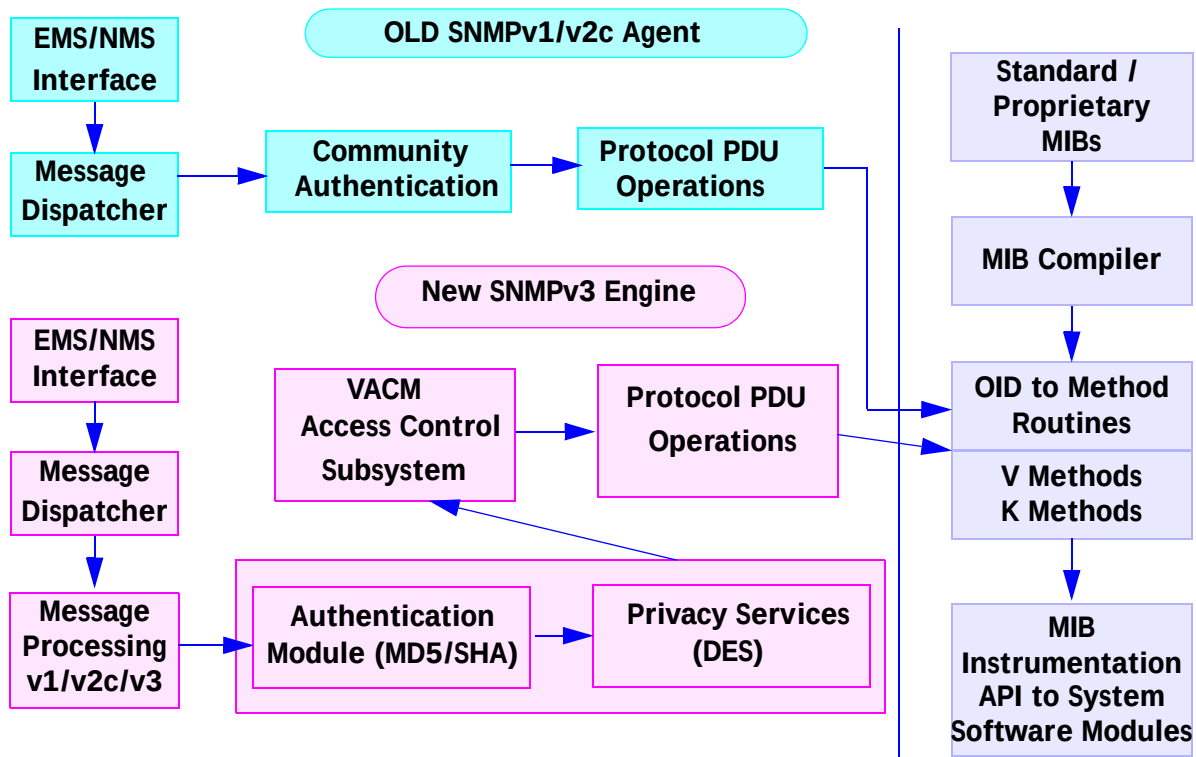


Figure 22-1: SNMPv1 & SNMPv2c Agents / SNMPv3 Engine Architecture

SNMPv1

SNMPv1 is defined by RFC1157 (SNMPv1), RFC1155 Structure of Management Information Version 1 (SMIv1), RFC1212 and RFC1215. This version supports primitive data types based on SMIv1 with the following operations:

- **Get Request** - manager requests the current value of a specified managed object from the agent.
- **Get Next Request** - manager requests the current value of the next managed object in the MIB from the agent.
- **Set Request** - manager requests the agent to set the value of the specified managed object.
- **Get Response** - agent responds to a Get-Request, Get-Next-Request, or Set-Request with the value of the managed object.
- **Trap** - agent notifies manager of system event.

The SNMPv1 message and Protocol Description Unit (PDU) format is shown in **Figure 22-2**:

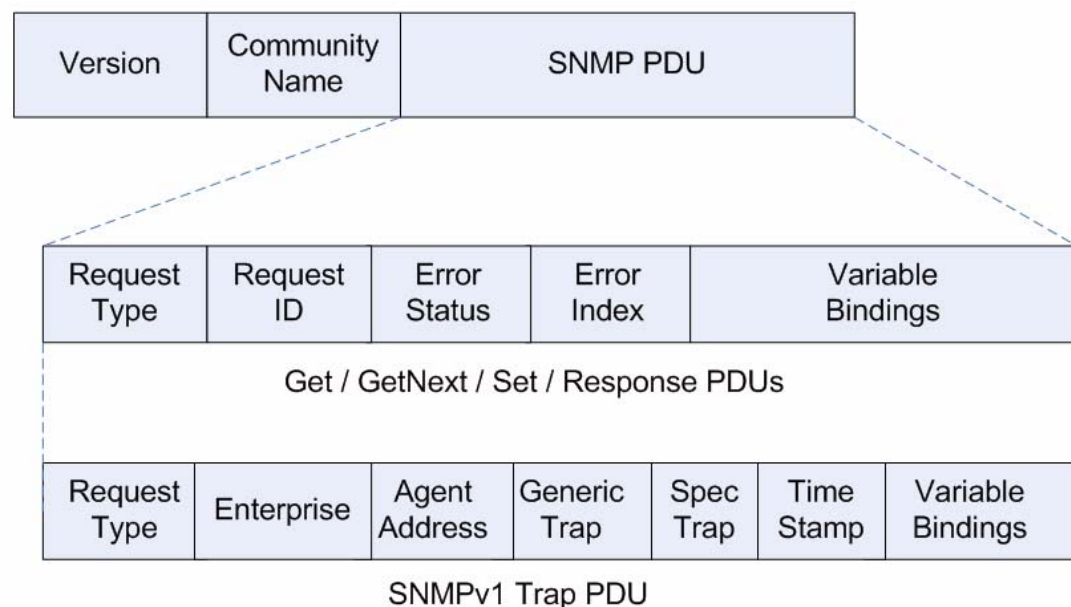


Figure 22-2: SNMPv1 Message and PDU Format

SNMPv2c

SNMPv2c is defined by RFC1901, RFC3416 (SNMPv2), RFC2578 (SMIv2) and RFC2579. It supports the same operations as SNMPv1 with additional support for the Get Bulk (RFC3616) operation for efficient retrieval of large amounts of data. This version defines a newer SNMPv2 Trap PDU format and supports data types based on SMIv2 including 64 bit counters.

The SNMPv2c message and PDU format is shown in **Figure 22-3**:

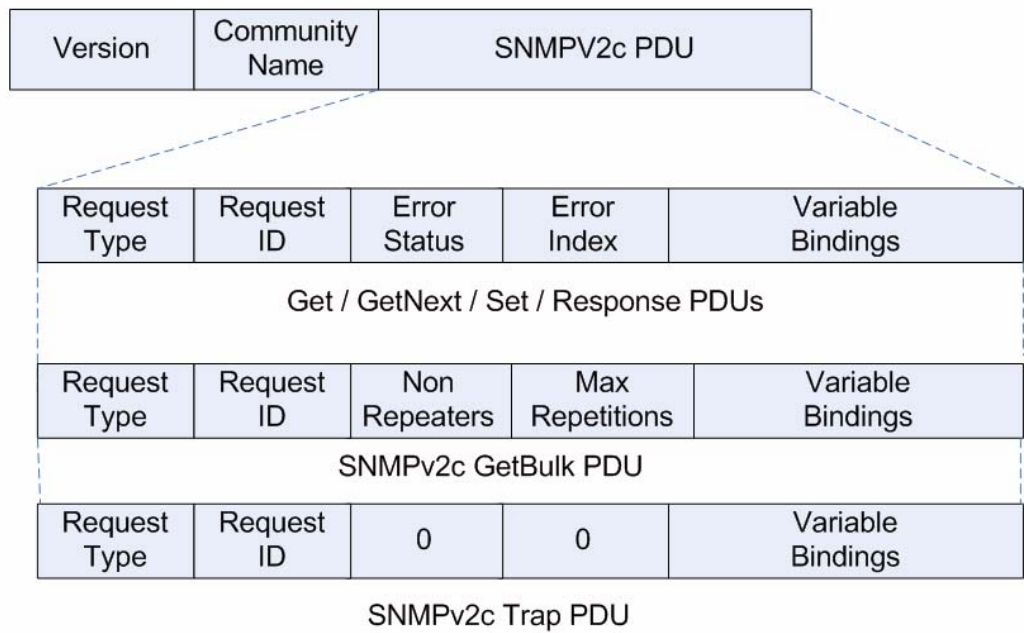


Figure 22-3: SNMPv2c Message and PDU Format

SNMPv3

SNMPv3 uses the same PDU format and supports all operations that are defined in SNMPv2c, but it is *not* considered a stand-alone protocol. Instead, it employs an extensible framework that uses SNMPv2c information that is encapsulated in the SNMPv3 packet format.

Packet Format

The SNMPv3 packet format includes a message header, security parameters, and PDU information as shown in **Figure 22-4**:

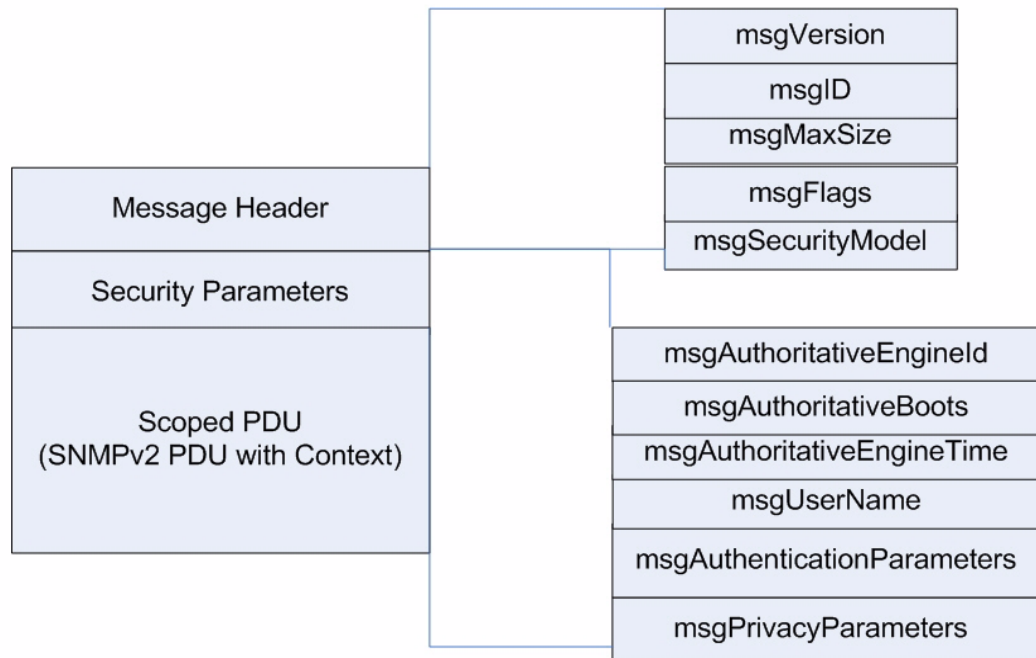


Figure 22-4: SNMPv3 Packet Format

Following is a list of the supported SNMPv3 fields:

Table 22-1: SNMPv3 Packets

Packet Name	Description
msgVersion	Displays the SNMP version of the packet (e.g. 1, 2, or 3).
msgID	Used to coordinate request and response messages between manager and agent. A <i>msgID</i> in a response must be the same as the <i>msgID</i> received in the request.
msgMaxSize	Indicates the maximum message size that the sender can support.
msgFlags	Indicates how the message is to be processed and contains the following flags: • reportableFlag • authFlag • privFlag
msgSecurityModel	Contains the security model that was used for security processing upon message reception.
msgSecurityParameters	Contains the security model specific data. This data is defined and used only by the security model specified by <i>msgSecurityModel</i> .
scopedPDU	Contains the normal PDU and information for identifying the administratively unique context for processing the PDU.

Security License Key

A valid security license key is required to allow SNMPv3 packets with an authentication only security level setting (*authNoPriv*) or an authentication with privacy security level setting (*authPriv*).



CAUTION: SNMP will not respond to requests and will drop packets if a valid security license key is not installed.

Once a valid security license key is installed, SNMP will enable encryption and authentication. It will then accept SNMPv3 packets and allow the user to access the device.



NOTE: A valid security license key is not required to allow SNMPv1, SNMPv2c, or SNMPv3 packets with a no authentication and privacy (*noAuthNoPriv*) security level setting.

For information on SNMP security levels, see the **snmpSecurityLevel** section on page 315.

Supported Concepts

Following is a list of the supported SNMPv3 concepts:

Table 22-2: SNMPv3 Concepts

Concept	Description

Table 22-2: SNMPv3 Concepts

snmpEngineID	A unique identifier for an SNMP engine within an administrative domain. The <i>snmpEngineID</i> is computed using the chassis MAC address and an administratively assigned string.
snmpEngineBoots	Counts the number of times an SNMP engine has re-booted or re-initialized since the <i>snmpEngineID</i> was last set. This counter is initially set to zero.
snmpEngineTime	Specifies the number of seconds since the <i>snmpEngineBoots</i> counter was last incremented. This counter is initially set to zero. If the <i>snmpEngineTime</i> reaches its maximum (2147483647), then the <i>snmpEngineBoots</i> is incremented by one and the <i>snmpEngineTime</i> starts counting again from zero.
snmpSecurityLevel	Contains three security levels that rank from highest to lowest respectively: • authPriv • authNoPriv • noAuthNoPriv
Authoritative SNMP Engine	Protects against message replay, message delay, and message redirection.
Agent Discovery	Used to first determine the <i>snmpEngineID</i> of the agent, and then determines the <i>snmpEngineBoots</i> and <i>snmpEngineTime</i> .

Supported Table Entries

Following is a list of the supported SNMPv3 table entries:

Table 22-3: SNMPv3 Table Entries

Table Name	Description
usmUserTable	Specifies the creation of new users who are allowed to access SNMP supported devices. This table is only used when an ingress SNMP packet utilizes SNMPv3. <i>usmUserTable</i> includes the following information: • usmUserEngineID • usmUserName • usmUserAuthProtocol • usmUserPrivProtocol
vacmSecurityToGroupTable	Attaches a security model to a group that is defined in <i>usmUserTable</i> . This table does not, however, validate whether or not a user ID specified in the table exists in <i>usmUserTable</i> . <i>vacmSecurityToGroupTable</i> includes the following information: • vacmSecurityModel • vacmSecurityName • vacmGroupName

Table 22-3: SNMPv3 Table Entries

vacmAccessTable	Specifies either a read view, write view, or notify view access policy for the group specified in <i>vacmSecurityToGroupTable</i>. <i>vacmAccessTable</i> includes the following information: • <i>vacmGroupName</i> • <i>vacmAccessSecurityModel</i> • <i>vacmAccessSecurityLevel</i> • <i>vacmAccessReadViewName</i> • <i>vacmAccessWriteViewName</i> • <i>vacmAccessNotifyViewName</i> <i>vacmAccessSecurityLevel</i> contains three security levels that rank from highest to lowest respectively: • <i>authPriv</i> • <i>authNoPriv</i> • <i>noAuthNoPriv</i>
vacmViewTreeFamilyTable	Specifies the following three views that are used in <i>vacmAccessTable</i>: • <i>vacmViewTreeFamilyViewName</i> • <i>vacmViewTreeFamilySubtree</i> • <i>vacmViewTreeFamilyType</i>
snmpTargetAddrTable	Specifies the transport addresses that can either be used when generating SNMP traps or allow SNMP requests that come from specified IP addresses. <i>snmpTargetAddrTable</i> includes the following information: • <i>snmpTargetAddrName</i> • <i>snmpTargetAddrTAddress</i> • <i>snmpTargetAddrTagList</i> • <i>snmpTargetAddrParams</i>
snmpTargetParamTable	Specifies additional information about the <i>snmpTargetAddrTable</i>. This additional information includes what security model, security level, and trap type is to be used when generating SNMP traps. <i>snmpTargetParamTable</i> includes the following information: • <i>snmpTargetParamsName</i> • <i>snmpTargetParamsSecurityModel</i> • <i>snmpTargetParamsSecurityName</i> • <i>snmpTargetParamsSecurityLevel</i>
snmpCommunityTable	Used to map earlier SNMPv1 and SNMPv2c communities, notifications, and configurations into the SNMPv3 framework. <i>snmpCommunityTable</i> includes the following information: • <i>snmpCommunityIndex</i> • <i>snmpCommunityName</i> • <i>snmpCommunitySecurityName</i> • <i>snmpCommunityTransportTag</i>

Following is a list of the maximum number of SNMPv3 table entries that are supported

Table 22-4: SNMPv3 Maximum Number Of Table Entries

Table Name	Maximum Entries Supported
usmUserTable	20
vacmSecurityToGroupTable	15
vacmAccessTable	15
vacmViewTreeFamilyTable	20
snmpTargetAddrTable	17
snmpTargetParamTable	15
snmpCommunityTable	18

Supported SNMP Traps

Following is a list of supported SNMP traps:

Table 22-5: SNMP Traps

SNMP Trap Name	Associated MIB File
authenticationFailure	SNMPv2-MIB.my
coldStart	SNMPv2-MIB.my
fallingAlarm	RMON-MIB.my
linkDown	IF-MIB.my
linkUp	IF-MIB.my
IldpRemTablesChange	LLDP-MIB.my
risingAlarm	RMON-MIB.my
wwpFTransferCompletion	WWP-LEOS-FILE-TRANSFER-MIB.my
wwpLeosBcastThresholdExceed	WWP-LEOS-BROADCAST-CONTAINMENT-MIB.my
wwpLeosBladeStateChange	WWP-LEOS-BLADE-MIB.my
wwpLeosCfmFaultTrap	WWP-LEOS-CFM-MIB.my
wwpLeosCfmPbtFaultTrap	WWP-LEOS-CFM-MIB.my
wwpLeosChassisDoorStatusChangeNotification	WWP-LEOS-CHASSIS-MIB.my
wwpLeosChassisDyingGaspNotification	WWP-LEOS-CHASSIS-MIB.my
wwpLeosChassisPowerSupplyStatusNotification	WWP-LEOS-CHASSIS-MIB.my
wwpLeosChassisRebootNotification	WWP-LEOS-CHASSIS-MIB.my
wwpLeosChassisTempNotification	WWP-LEOS-CHASSIS-MIB.my
wwpLeosChassisSnmpStateNotification	WWP-LEOS-CHASSIS-MIB.my
wwpLeosDhcpClientOptionDisabledNotification	WWP-LEOS-DHCP-CLIENT-MIB.my
wwpLeosEthLinkUp	WWP-LEOS-PORT-MIB.my
wwpLeosEthLinkDown	WWP-LEOS-PORT-MIB.my
wwpLeosFlowL2SacHighThreshold	WWP-LEOS-FLOW-MIB.my
wwpLeosFlowL2SacNormalThreshold	WWP-LEOS-FLOW-MIB.my
wwpLeosImproperCmdInConfigFile	WWP-LEOS-SYSTEM-CONFIG-MIB.my
wwpLeosIpInterfaceAddrChgNotification	WWP-LEOS-IP-INTERFACE-MIB.my
wwpLeosMstpBridgeRootPortLostNotification	WWP-LEOS-MSTP-MIB.my
wwpLeosMstpNewRootNotification	WWP-LEOS-MSTP-MIB.my
wwpLeosMstpPortBackupNotification	WWP-LEOS-MSTP-MIB.my

Table 22-5: SNMP Traps

wwpLeosMstpPortFlapNotification	WWP-LEOS-MSTP-MIB.my
wwpLeosMstpPortOperEdgeNotification	WWP-LEOS-MSTP-MIB.my
wwpLeosMstpPvstBpduReceivedNotification	WWP-LEOS-MSTP-MIB.my
wwpLeosMstpSelfLoopNotification	WWP-LEOS-MSTP-MIB.my
wwpLeosMstpTopologyChangeNotification	WWP-LEOS-MSTP-MIB.my
wwpLeosOamLinkEventTrap	WWP-LEOS-OAM-MIB.my
wwpLeosPbtTunnelReversionNotification	WWP-LEOS-PBT-MIB.my
wwpLeosCfmFaultTrapSet	WWP-LEOS-CFM-MIB.my
wwpLeosCfmFaultTrapClear	WWP-LEOS-CFM-MIB.my
wwpLeosSwXgradeBladePkgIncorrect	WWP-LEOS-SW-XGRADE-MIB.my
wwpLeosSwXgradeOpCompletion	WWP-LEOS-SW-XGRADE-MIB.my
wwpLeosSystemServiceModeChange	WWP-LEOS-SYSTEM-CONFIG-MIB.my

RMON

With remote monitoring (RMON), you can enable a device to gather information related to groups defined in the IEEE RFC 1757 and RFC 2021. Using a network monitoring device, you can probe the network to retrieve this information by sampling SNMP MIB objects. RMON supports four of the groups defined in IEEE RFC 1757:

- **Alarm** - The alarm group monitors system variables periodically, taking samples and comparing them to the configured thresholds (rising and/or falling). A user defined event is generated when a threshold has been crossed.
- **Event** - With the event group you can create an event and define an action to take when an alarm occurs. RMON on all devices supports the configuration of up to 28 entries for statistics, alarms, events, and history.
- **History** - The history group is a set of periodical statistical samples saved during a defined period of time for a port. Data provided can subsequently be reviewed.
- **Statistics** - Ethernet statistics are retrieved and measured by the probes for each of the configured Ethernet ports on the device.

RMON supports one of the groups defined in IEEE RFC 2021:

- **User History** - Periodic samples of user specified history.

Benefits

SNMP provides the basis to manage network devices through interfaces other than the CLI, including configuration, notification of system events, and RMON.

Configuring Global Attributes

You can set and display global SNMP attributes including:

- Operational status
- System contact information

- System location
- Link up and down traps status
- CFM fault traps status

Setting Operational Status

The operational status is either enabled or disabled. When the operational status is disabled, attempts to connect to the SNMP agent will timeout. By default, the status is enabled.

To enable SNMP status:

```
snmp enable
```

To disable SNMP status:

```
snmp disable
```

Setting Contact, Location, Link Up and Down Traps, and CFM Fault Traps

In addition to the operational status, you can set the following attributes:

- **Contact** - The contact field is a 1-63 character string, such as a department name and phone number. If the string includes spaces, enclose it with quotes. By default, the contact is "Customer Support, World Wide Packets".
- **Location** - The location field is a 1-63 character string, such as an address. If the string includes spaces, enclose it with quotes. By default, the location is "Not Specified".
- **Enhanced link up and link down trap** - When enabled, proprietary link up and down traps are sent by the device. By default, the proprietary link up and link down traps are disabled.
- **Standard link up and link down trap** - When enabled, standard link up and down traps are sent by the device. By default, standard link up and link down traps are enabled.
- **CFM fault trap** - When enabled, CFM faults are sent by the device. By default, the CFM fault traps are disabled.

To set SNMP contact, location, and trap attributes:

```
snmp set {[contact <String[255]>], [enhancement-link-up-down-trap <disable|enable>]}  
[location <String[255]>], [std-link-up-down-trap <disable|enable>], [cfm-fault-trap  
<disable|enable>]}
```

Example:

```
> snmp set contact "Customer Support, World Wide Packets" enhancement-link-up-down-trap  
disable location "Spokane Valley, USA" std-link-up-down-trap enable
```

Displaying SNMP Global Attributes

To display SNMP global attributes:

```
snmp show
```

Example:

```
> snmp show
```

-----SNMP GLOBAL CONFIGURATION-----	
Parameter	Value
Operational status	Enable
System Contact	Customer Support, World Wide Packets
System Location	Not Specified
Standard link-up-down trap	Enable
Enhanced link-up-down trap	Disable

Configuring SNMPv1/v2c Community Based Security

SNMP communities provide limited security for SNMP access to the device. The default community configuration shown in **Table 22-6**, in this chapter allows any IP address within the network to access the device via SNMP.

Table 22-6: Default SNMP Communities		
IP Address	Community	Permissions
0.0.0.0	public	read-only
0.0.0.0	private	read-write



NOTE: SNMPv1/v2c community based security are deprecated. Deprecated commands are still supported by the CLI and work for configuration. However, in a future release, deprecated commands will no longer be supported.

Creating a Community and Adding Members

Whether you want to add a member to an existing community or create a new one, the command is the same. If the community does not exist, it is created. If it already exists, the IP address and permission is added to the community. You can add up to 18 entries to the community table.

To create a community or add members to an existing community:

```
snmp add community <String[64]> ip <IpAddress> permission <read-only|read-write>
```

Example:

```
> snmp add community MyCommunity ip 1.1.1.1 permission read-write
```

Removing a Community and Removing Members

Whether you want to remove a member from a community or remove a community, the command is the same. If the community has more than one member, you must run the command to remove all IP addresses from the community.

To remove a community or remove members from a community:

```
snmp remove community <CommunityName> ip <IpAddress>
```

Example:

```
> snmp remove community MyCommunity ip 1.1.1.1
```

Updating Community Permissions

To update the permissions for a community entry:

```
snmp set community <CommunityName> ip <IpAddress> permission <read-only|read-write>
```

Example:

```
> snmp set community MyCommunity ip 1.1.1.1 permission read-only
```

Displaying SNMP Communities

To display all SNMP communities:

```
snmp show communities
```

Example:

```
> snmp show communities
```

IP Address	Host Name	Community Name	Permissions
0.0.0.0		public	read-only
0.0.0.0		private	read-write
1.1.1.1		MyCommunity	read-only

Configuring Trap Servers

You can configure the device to transmit any SNMP traps to a designated trap server.

Adding a Trap Server

To add a trap server:

```
snmp add trap-server <IpAddress> community <CommunityName>
```

Example:

```
> snmp add trap-server 1.1.1.4 community MyCommunity
```


Removing a Trap Server

To remove a trap server:

```
snmp remove trap-server <IpAddress> community <CommunityName>
```

Example:

```
> snmp remove trap-server 1.1.1.4 community MyCommunity
```

Displaying Trap Servers

To display all trap servers:

```
snmp show trap-server
```

Example:

```
> snmp show trap-server
```

```
+----- TRAP SERVER TABLE -----+
| IP Address      | Host Name          | Community Name      |
+-----+-----+-----+
| 1.1.1.4         |                    | MyCommunity         |
+-----+-----+-----+
```

Configuring Port Traps and Servers

When the port trap is disabled, any traps generated by the port will not be transmitted to a configured trap server. By default, port traps are enabled for all ports.

To disable port traps:

```
snmp port-traps disable port <PortNameList>
```

Example:

```
> snmp port-traps disable port 10
```

To enable port traps:

```
snmp port-traps enable port <PortNameList>
```

Example:

```
> snmp port-traps enable port 10
```

To display all port traps:

```
snmp show port-traps
```

Example:

```
> snmp show port-traps
+-----PORT TRAP TABLE-----+
| PortName | State |
+-----+-----+
| 1 | Enable |
| 2 | Enable |
| 3 | Enable |
| 4 | Enable |
| 5 | Enable |
| 6 | Enable |
| 7 | Enable |
| 8 | Enable |
| 9 | Enable |
| 10 | Enable |
+-----+-----+
```

Configuring SNMPv3

This section identifies default table entries and sample configurations that are supported.



NOTE: To configure SNMPv3 encryption and authentication, the Advanced Security feature license must be installed with the software license install command.

SNMPv3 Default Table Entries

Following is a list of the SNMPv3 default table entries that are supported :

Table 22-7: Default SNMP User Table Entries

User Name	AuthProtocol	PrivProtocol
Public	noAuth	noPriv
Private	noAuth	noPriv

Table 22-8: Default SNMP Security Map Table Entries

User Name	SecModel	GroupName
Public	V1	Public
Private	V1	Private
Public	V2	Public
Private	V2	Private

Table 22-9: Default SNMP VACM Access Table Entries

GroupName	SecModel	SecLevel	ReadView	WriteView	NotifView
Public	V1	noAuth	V12cView		V12cView

Table 22-9: Default SNMP VACM Access Table Entries

Public	V2c	noAuth	V12cView		V12cView
Private	V1	noAuth	V12cView	V12cView	V12cView
Private	V2	noAuth	V12cView	V12cView	V12cView

Table 22-10: Default SNMP VACM View Tree Table Entries

ViewTreeName	SubTree	Type
V12cView	iso	include
V12cView	snmpResearch	exclude

Table 22-11: Default SNMP Target Table Entries

Target Name	IP Address	Param Name	Tags	UDP Port
Anywhere	0.0.0.0	None	AnywhereTag	0

Table 22-12: Default SNMP Community Map Table Entries

Community Index	Community Name	SecName	Transport Tag
T0000000	Public	Public	AnywhereTag
T0000001	Private	Private	AnywhereTag

Table 22-13: Default SNMP Notification Table Entries

Notification Name	Notification Tag	Notification Type
Traps	TrapTag	1

Creating SNMP Users

You can create users with an authentication protocol, privacy protocol, authentication password, privacy password, authentication secret key, and privacy secret key.

To create a user:

```
snmp create user <String[32]> {auth-protocol <noauth|md5|sha>} [priv-protocol  
<nopriv|des>] [priv-password <String[64]>] [auth-password <String[64]>] [auth-  
secret <String[40]>] [priv-secret <String[40]>]
```

Example:

```
> snmp create user user1 auth-protocol md5 priv-protocol noPriv auth-password mypassword
```

To display users:

```
snmp show user
```

Example:

```
> snmp show user
```

UserName	AuthProt	PrivProt
user1	md5	noPriv
public	noAuth	noPriv
private	noAuth	noPriv

To delete a user:

```
snmp delete user <String[32]>
```

Example:

```
> snmp show user
```

Configuring SNMP Community Mapping

1. Create an entry in the *snmpCommunityTable*.

```
snmp create community-index <String[32]> {community <String[64]>} {sec-name <String[32]>}
```

Example:

```
> snmp create community-index comm1 community mycommunity sec-name user1
```

2. Validate that the new entry was created.

```
> snmp show community-map
```

CommunityIndex	CommunityName	SecName	TransportTag
comm1	mycommunity	user1	
t0000000	public	public	anywhereTag
t0000001	private	private	anywhereTag

3. Create an entry in the *vacmSecurityToGroupTable*.

```
snmp security-to-group attach user <String[32]> {sec-model <v1|v2c|v3>} {group <String[32]>}
```

Example:

```
> snmp security-to-group attach user user1 sec-model v1 group group1
```

4. Validate that the new entry was created.

```
> snmp show security-to-group
```

UserName	SecModel	GroupName
user1	v1	group1
public	v1	public
private	v1	private
public	v2c	public
private	v2c	private

5. Create an entry in the *vacmAccessTable*.

```
snmp create access-entry <String[32]> {sec-model <v1|v2c|v3>}{sec-level  
<noAuth|authNoPriv|authWithPriv>}[read-view <String[64]>][write-view  
<String[64]>][notify-view <String[64]>]
```

Example:

```
> snmp create access-entry group1 sec-model v1 sec-level noAuth read-view viewtree1
```

6. Validate that the new entry was created.

```
> snmp show access-entry
```

GroupName	SecModel	SecLevel	ReadView	WriteView	NotifView
group1	v1	noAu	viewtree1		
public	v1	noAu	V12cView		V12cView
public	v2c	noAu	V12cView		V12cView
private	v1	noAu	V12cView	V12cView	V12cView
private	v2c	noAu	V12cView	V12cView	V12cView

7. Create an entry in the *vacmViewTreeFamilyTable*.

```
snmp create viewtree <String[32]> {sub-tree <String[64]>} {type <include|exclude>}
```

Example:

```
> snmp create viewtree viewtree1 sub-tree mgmt type include
```

8. Validate that the new entry was created.

```
> snmp show viewtree
```

ViewTreeName	SubTree	Type
V12cView	iso	include
V12cView	snmpResearch	exclude
viewtree1	mgmt	include

Configuring a Trap Server

1. Create an SNMP trap server entry using the default SNMPv1 / SNMPv2c configuration.

```
snmp create target <String[32]>{addr <IpAddress>}{param-name <String[32]>}[tag <String[32]>][udp-port <NUMBER: 1-65535>]
```

Example:

```
> snmp create target TRAPS addr 10.10.10.10 param-name TRAPS
```

2. Validate that the new entry was created.

```
> snmp show target
```

TargetName	IPAddress	ParamName	Tags	Udp Port
TRAPS	10.10.10.10	TRAPS	TrapTag	162
anywhere	0.0.0.0	none	anywhereTag	0

3. Create a target parameter and security name.

```
snmp create target-param <String[32]> {sec-name <String[32]>}
```

Example:

```
> snmp create target-param TRAPS sec-name public
```

4. Validate that the new entry was created.

```
> snmp show targetParams
```

TargetParamName	SecurityName	Sec Model	MP Model
TRAPS	public	v1	0

Configuring Traps

1. Create an entry in the *snmpTargetAddrTable*.

```
snmp create target <String[32]>{addr <IpAddress>}{param-name <String[32]>}{tag
<String[32]>}[udp-port <NUMBER: 1-65535>]
```

Example:

```
> snmp create target target1 addr 192.168.15.30 param-name param1 tag TrapTag
```

2. Validate that the new entry was created.

```
> snmp show target
```

TargetName	IPAddress	ParamName	Tags	Udp Port
anywhere	0.0.0.0	none	anywhereTag	0
target1	192.168.15.30	param1	TrapTag	162

3. Create an entry in the *snmpTargetParamTable*.

```
snmp create target-param <String[32]> {sec-name <String[32]>}
```

Example:

```
> snmp create target-param param1 sec-name user1
```

4. Validate that the new entry was created.

```
> snmp show targetparams
```

TargetParamName	SecurityName	Sec Model	MP Model
param1	user1	v1	0

5. Create an entry in the *vacmSecurityToGroupTable*.

```
snmp security-to-group attach user <String[32]> {sec-model <v1|v2c|v3>} {group
<String[32]>}
```

Example:

```
> snmp security-to-group attach user user1 sec-model v1 group group1
```

6. Validate that the new entry was created.

```
> snmp show security-to-group
```

UserName	SecModel	GroupName
user1	v1	group1
public	v1	public
private	v1	private
public	v2c	public
private	v2c	private

7. Create an entry in the *vacmViewTreeFamilyTable*.

```
snmp create viewtree <String[32]> {sub-tree <String[64]>} {type <include|exclude>}
```

Example:

```
> snmp create viewtree trap sub-tree mgmt type include
```

8. Validate that the new entry was created.

```
> snmp show viewtree
```

ViewTreeName	SubTree	Type
trap	mgmt	include
V12cView	iso	include
V12cView	snmpResearch	exclude

9. Create an entry in the *vacmAccessTable*.

```
snmp create access-entry <String[32]> {sec-model <v1|v2c|v3>}{sec-level  
<noAuth|authNoPriv|authWithPriv>}[read-view <String[64]>][write-view  
<String[64]>][notify-view <String[64]>]}
```

Example:

```
> snmp create access-entry group1 sec-model v1 sec-level noAuth read-view trap  
notify-view trap
```

10. Validate that the new entry was created.

```
> snmp show access-entry
```

GroupName	SecModel	SecLevel	ReadView	WriteView	NotifView
group1	v1	noAuth	trap		trap
public	v1	noAuth	V12cView		V12cView
public	v2c	noAuth	V12cView		V12cView
private	v1	noAuth	V12cView	V12cView	V12cView
private	v2c	noAuth	V12cView	V12cView	V12cView

11. Create an entry in the *snmpCommunityTable*.

```
snmp create community-index <String[32]> {community <String[64]>} {sec-name <String[32]>}
```

Example:

```
> snmp create community-index target1 community comm1 sec-name user1 transport-tag TrapTag
```

12. Validate that the new entry was created.

```
> snmp show community-map
```

CommunityIndex	CommunityName	SecName	TransportTag
t00000000	public	public	anywhereTag
t00000001	private	private	anywhereTag
target1	comm1	user1	TrapTag

Modifying Community Map Attributes

You can modify the attributes of a community map, including the community name, security name, and transport tag.

To modify community map attributes:

```
snmp set community-index <String[32]> {community <String[64]>} {sec-name <String[32]>} [transport-tag <String[32]>}
```

Example:

```
> snmp set community-index target1 community comm1 sec-name user1 transport-tag anywhereTag
```

Creating and Attaching an SNMPv3 User to an SNMPv3 Access Entry Group

1. Create an SNMPv3 user with an authentication protocol, privacy protocol, authentication password, and privacy password.

```
snmp create user <String[32]> {auth-protocol <noauth|md5|sha>} [priv-protocol
<nopriv|des>] [priv-password <String[64]>] [auth-password <String[64]>] [auth-
secret <String[40]>] [priv-secret <String[40]>]
```

Example:

```
> snmp create user SNMPv3_User auth-protocol md5 priv-protocol des auth-password
SNMPv3_password1 priv-password SNMPv3_password2
```

2. Validate that the new entry was created.

```
> snmp show user
```

UserName	AuthProt	PrivProt
public	noAuth	noPriv
private	noAuth	noPriv
SNMPv3_User	md5	des

3. Create a view tree entry in the *vacmViewTreeFamilyTable* with a sub-tree that can be viewed.

```
snmp create viewtree <String[32]> {sub-tree <String[64]>} {type <include|exclude>}
```

Example:

```
> snmp create viewtree SNMPv3_view sub-tree mgmt type include
```

4. Validate that the new entry was created.

```
> snmp show viewtree
```

ViewTreeName	SubTree	Type
V12cView	iso	include
V12cView	snmpResearch	exclude
SNMPv3_view	mgmt	include

5. Create an access policy in the *vacmAccessTable* with a v3 security model. Include a security level with authorization and privileges. Also include a read view, write view, and notify view.

```
snmp create access-entry <String[32]> {sec-model <v1|v2c|v3>} {sec-level
<noAuth|authNoPriv|authWithPriv>} [read-view <String[64]>] [write-view
<String[64]>] [notify-view <String[64]>]
```

Example:

```
> snmp create access-entry SNMPv3_Group sec-model v3 sec-level authWithPriv read-view V3View write-view V3View notify-view V3View
```

6. Validate that the new entry was created.

```
> snmp show access-entry
```

GroupName	SecModel	SecLevel	ReadView	WriteView	NotifView
public	v1	noAuth	V12cView		V12cView
public	v2c	noAuth	V12cView		V12cView
private	v1	noAuth	V12cView	V12cView	V12cView
private	v2c	noAuth	V12cView	V12cView	V12cView
SNMPv3_Group	usm	AuthWtPv	V3View	V3View	V3View

7. Attach the SNMPv3 user to an SNMPv3 access group using the *vacmSecurityToGroupTable*.

```
snmp security-to-group attach user <String[32]> {sec-model <v1|v2c|v3>} {group <String[32]>}
```

Example:

```
> snmp security-to-group attach user SNMPv3_User sec-model v3 group SNMPv3_Group
```

8. Validate that the new entry was created.

```
> snmp show security-to-group
```

UserName	SecModel	GroupName
public	v1	public
private	v1	private
public	v2c	public
private	v2c	private
SNMPv3_User	v3	SNMPv3_Group

Modifying User Attributes

You can modify the attributes of an existing SNMPv3 user, including: authentication protocol, privacy protocol, authentication password, and privacy password.

To modify user attributes:

```
snmp set user <SnmpUser> {[auth-protocol <noauth|md5|sha>], [auth-password <String>], [priv-protocol <nopriv|des>], [priv-password <String>]}
```

Example:

```
> snmp set user SNMPv3_User auth-protocol md5 priv-protocol des auth-password SNMPv3_password1 priv-password SNMPv3_password2
```

Configuring Notification Entries

You can create, modify, delete, and display entries in the *snmpNotifTable* specified in *SNMP-NOTIFICATION-MIB.my*. The *snmpNotifTable* contains a default entry tag called the Trap Tag that is used to qualify entries in the *snmpTargetTable* for SNMPv1 traps.

To create notification entries:

```
snmp create notify <String[32]> {notify-tag <String[32]>} [notify-type  
<trap|notification>]
```

Example:

```
> snmp create notify myNotifyName notify-tag myNotifyTag notify-type trap
```

To modify notification entries:

```
snmp set notify <String[32]> {[notify-tag <String[32]>], [notify-type  
<trap|notification>]}
```

Example:

```
> snmp set notify notify myNotifyName notify-tag myNotifyTag notify-type  
notification
```

To delete notification entries:

```
snmp delete notify <String[32]>
```

Example:

```
> snmp delete notify myNotification
```

To display a list of notification entries:

```
snmp show notify
```

Example:

```
> snmp show notify
```

```
+-----+-----+-----+  
|NotificationName| Notification Tag | Notification Type |  
+-----+-----+-----+  
|Traps          | TrapTag          | 1                 |  
|myNotifyName   | myNotifyTag      | 2                 |  
+-----+-----+-----+
```

Configuring RMON

Configuring Alarms

When you configure alarms, you define a set of parameters that will be compared to object values and network activities. When the alarm threshold is crossed, an event is generated and the samples will be written to a log.

Two types of sampling can be configured: absolute sampling which compares the data to the set threshold; delta sampling which compares two consecutive samplings and compares the difference against the threshold.

Rising and falling thresholds allow the administrator to define boundaries (high and low) and create a warning if these boundaries are crossed. For example, an alarm will be triggered if the amount of packets going through a port is higher than expected (rising threshold) or below normal (falling threshold).

A number of attributes need to be defined in order to describe an alarm:

- **data source** - indicate the interface OID (example: 1.3.6.1.2.1.16.1.1.1.5).
- **index** - the index in the alarm table.
- **owner** - name of the owner (optional).
- **sample-type** - absolute or delta.
- **interval** - time interval in seconds used to compare samples and send alarm.
- **startup-alarm** - defines the condition required to trigger alarm (rising, falling or both).
- **falling-event-index** - set index for falling event.
- **rising-event-index** - set index for rising event.
- **falling-threshold** - minimum value (related to the particular interface MIB object being monitored) against which samplings are compared.
- **rising-threshold** - maximum value (related to the particular interface MIB object being monitored) against which samplings are compared.

To add an alarm entry:

```
rmon alarm add {data-source <String[127]>} {falling-event-index <NUMBER:1-65535>} {falling-  
threshold <NUMBER:0-999999999>} {index <NUMBER:1-65535>} {interval <NUMBER:1-3600>} [owner  
<String[127]>] {rising-event-index <NUMBER:1-65535>} {rising-threshold <NUMBER:0-999999999>}  
{sample-type <absolute|delta>} {startup-alarm <rising|falling|both>}
```

Example:

This example adds an alarm entry to monitor the amount of traffic entering a port and create an event when the throughput is under 100 Mbps or above 900 Mbps:

```
> rmon alarm add data-source 1.3.6.1.2.1.16.1.1.1.5 index 1 interval 30 owner Admin  
sample-type absolute startup-alarm both falling-event-index 1 falling-threshold 100  
rising-event-index 1 rising-threshold 900
```

To display an alarm entry:

```
rmon show alarm-index <NUMBER:1-65535>
```

Example:

```
> rmon show alarm-index 1  
+-----RMON ALARM STATISTICS-----+  
| Index | Parameter | Value |  
+-----+-----+-----+  
| 1 | OID | etherStatsPkts |  
| | Type | Absolute |  
| | Interval (sec) | 30 |  
| | Rising Limit | 900 |  
| | Falling Limit | 100 |  
| | Rising Index | 1 |  
| | Falling Index | 1 |  
| | Owner | Admin |  
+-----+-----+-----+
```

To delete an alarm entry:

```
rmon alarm remove index <NUMBER:1-65535>
```

Example:

```
> rmon alarm remove alarm-index 1
```

Configuring Events

An event notifies you when an alarm is triggered. When you create an event, the following attributes apply:

- **index** - creates an index for the event in the event table
- **description** - describe the event
- **type** - indicate the type of event created and where the information is sent: none, log snmp-trap, log-and-snmptrap.
- **community** - create a community or refer to an existing community (optional)
- **owner** - indicate event's owner (optional)

To add an event entry:

```
rmon event add [community <String[127]>] [owner <String[127]>] {description <String[127]>}  
{index <NUMBER:1-65535>} {type <none|log|snmp-trap|log-and-snmptrap>}
```

Example:

```
> rmon event add index 1 description Test type log community Network1 owner Admin
```

To display event entries:

```
rmon show event-table
```

Example:

```
> rmon show event-table  
+-----+-----RMON EVENT STATISTICS-----+  
| Index | Description          | Event Type   | Community   | Owner   |  
+-----+-----+-----+-----+-----+  
| 1      | Test                  | log          | Network1    | Admin   |  
+-----+-----+-----+-----+-----+
```

To delete an event entry:

```
rmon event remove index <NUMBER:1-65535>
```

Example:

```
> rmon event remove index 1
```

Configuring History

With the history group, you can monitor and store port Ethernet statistics. A bucket is one sample of data collection during a distinct time interval. A number of attributes need to be defined to configure the history group:

- **data source** - indicate the interface OID (example: 1.3.6.1.2.1.16.1.1.1.5).
- **index** - the index in the history table.

- **interval** - indicates in seconds the sampling interval.
- **num-buckets** - number of buckets to use.
- **owner** - indicate history entry's owner (optional)
- **file-logging** - enables or disables saving the history to a file.

To add an history entry:

```
rmon history add {data-source <String[127]>} {index <NUMBER:1-65535>} [interval <NUMBER:1-3600>] [num-buckets <NUMBER:1-65535>] [owner <String[127]>] [file-logging <on | off>]
```

Example:

```
> rmon history add data-source 1.3.6.1.2.1.16.1.1.1.5 index 1 interval 12 num-buckets 78 owner Admin
```

To display event entries:

```
rmon show history
```

Example:

```
> rmon show history
+-----RMON HISTORY STATISTICS-----+
| Index | OID                      | Req-buckets | Interval | Owner  |
+-----+-----+-----+-----+
| 1      | etherStatsPkts           | 78          | 12       | Admin  |
+-----+-----+-----+-----+
```

To delete a history entry:

```
rmon history remove index <NUMBER:1-65535>
```

Example:

```
> rmon history remove index 1
```

Configuring Statistics

The statistics group (defined in RFC1757) provides information about data received over a device ports. This information is a list of raw statistics. These statistic counters are either based on frames or bytes passing through the port.

Statistics attributes include:

- **data source** - indicate the interface OID in the format ifIndex.100xx where xx is the port number (example: ifindex.10001).
- **index** - the index is a unique number corresponding to a row in the table.
- **owner** - indicate history entry's owner (optional).

To add a statistics entry:

```
rmon statistics add {data-source <String[127]>} {index <NUMBER:1-65535>} [owner <String[127]>]
```

Example:

```
> rmon statistics add index 1 data-source ifIndex.10001 owner Admin
```

To display a statistics entry:

```
rmon show statistics
```

Example:

```
> rmon show statistics
+-----RMON STATISTICS-----+
| Index | OID           | Owner   |
+-----+-----+-----+
| 1     | ifIndex.10001 | Admin   |
+-----+-----+-----+
```

To delete a statistics entry:

```
rmon statistics remove index <NUMBER 1-65535>
```

Example:

```
> rmon statistics remove index 1
```

Configuring User History

The user history provides a way to specify the MIB information to be collected. When configuring user history, you need to define an SNMP object along with a control entry.

The object attributes include:

- **sample-type** - sample type, absolute or delta.
- **object** - OID name.
- **index** - the index is a unique number corresponding to a row in the table.
- **control-index** - maps to the associated control entry.

The control entry includes:

- **file-logging** - Enables or disables file-logging which makes the history persistent (optional).
- **index** - Index in the history table (optional).
- **interval** - Interval used for monitoring (optional).
- **num-buckets** - Number of buckets to use (optional).
- **owner** - Name of the owner (optional).

To add a user history object entry:

```
rmon usr-history add-object {sample-type absolute|delta} {object <String[127]>} {index  
<NUMBER: 1-1200>} control-index <NUMBER: 1-1200>}
```

Example:

```
> rmon usr-history add-object index 1 control-index 1 sample-type absolute object snmpInPkts.0
```

To add a user history control entry:

```
rmon usr-history add-control [file-logging <on|off>] {index <NUMBER:1-1200>} [interval  
<NUMBER:1-65535>] [num-buckets <NUMBER:1-65535>] [owner <String[127]>]
```


Example:

```
> rmon history add data-source 1.3.6.1.2.1.16.1.1.1.5 index 1 interval 12 num-buckets 78 owner
Admin
```

To display user history object and control entries:

```
rmon show user-history
```

Example:

```
> rmon show user-history
+-----RMON USER HISTORY CONTROL TABLE-----+
| index | object | requested | granted | interval | owner          | File |
|        |        | buckets  | buckets |          |                | Logging|
+-----+-----+-----+-----+-----+-----+-----+
|      1 |      1 |        50 |        50 |       1800 |                |    no |
+-----+-----+-----+-----+-----+-----+-----+

+-----RMON USER HISTORY OBJECT TABLE-----+
| object | control |      data source      | sample-type |
| index  | index   |                      |             |
+-----+-----+-----+-----+
|      1 |      1 |      snmpInPkts.0    |   Absolute  |
+-----+-----+-----+-----+
```

To delete a user history object entry:

```
rmon usr-history remove-object {index <NUMBER 1-65535>} {control-index <NUMBER: 1-1200>}
```

Example:

```
> rmon usr-history remove-object index 1 control-index 1
```

To delete a user history control entry:

```
rmon usr-history remove-control index <NUMBER 1-65535>
```

Example:

```
> rmon usr-history remove-control index 1
```

Troubleshooting

Displaying SNMP Configuration in the Configuration File

SNMP and RMON configuration is saved to the configuration file in the SNMP CONFIG: section.

Example:

```
> configuration show
```

```
...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! SNMP CONFIG:
!
snmp port-traps disable port 1
snmp port-traps disable port 2
snmp port-traps disable port 3
snmp port-traps disable port 4
snmp port-traps disable port 5
snmp port-traps disable port 6
snmp port-traps disable port 7
snmp port-traps disable port 8
snmp port-traps disable port 9
snmp port-traps disable port 10
snmp set contact "Customer Support, Ciena +1 (509) 242-9000"
snmp set location "Spokane Valley, USA"
snmp set enhancement-link-up-down-trap enable
rmon usr-history add-control index 1
rmon usr-history add-object index 1 object snmpInPkts.0 control-index 1 sample-type absolute

!
```

Chapter Provider Backbone Transport



At a Glance:

- Overview
- Connectivity Fault Management
- Benefits
- Configuration

This chapter details the implementation of Provider Backbone Transport (PBT) in the core of a Ciena network. A basic understanding of the IEEE 802.1Q, 802.1ad, and 802.1ah standards is assumed. In addition, it is highly recommended that CFM (IEEE 802.1ag) be used to monitor the PBT service to warn if any faults occur in the service.

A software license key is required to activate PBT. Contact Ciena Sales to obtain a license key.

NOTE: PBT is not supported on the CN 3911 and CN 3920.

Overview

Provider Backbone Transport (PBT) can be considered as an extension to what is known as Provider Backbone Bridging (PBB) or Carrier Ethernet. PBT allows providers to create point-to-point, primary and backup Ethernet tunnels and specify the path that traffic will take across their Ethernet metro networks. These paths reserve appropriate bandwidth and support the provisioned QoS metrics. However, PBT is unique in that it actually disables some Ethernet features in order to accomplish its goal of delivering traffic.

VLAN Tagging

The IEEE 802.1Q standard specifies a mechanism for adding tags to Ethernet frames. This tagging allows an Ethernet network to be divided into virtual networks or VLANs. Generally, individual customers in a provider's network are identified by unique VLAN IDs. Additionally, each customer typically uses VLAN IDs in their own network to differentiate between service types (for example, data or VoIP) and possibly to distinguish between departments. This three-tier hierarchy allows separate domains for the service provider, customer and individual enterprise departments.

Given the 12-bit size of the VLAN field in an Ethernet frame, the number of available VLAN IDs is limited to 4,096. In a large provider network, the number of customers could easily exceed 4,000, exhausting the available VLAN IDs very quickly. To help improve network scalability, two standards have been introduced to support this hierarchical approach, IEEE 802.1ad and IEEE 802.1ah.

Q-in-Q

The IEEE 802.1ad (also known as Q-in-Q, stacked VLANs, or Provider Bridges), extends the original concept of VLAN tags by specifying a new provider-administered 802.1Q tag (Q-tag) that wraps or encapsulates the original customer packet in an additional header. This allows the service provider to administer their own tags to identify individual customer networks, while the first (original) Q-tag is unique within the customer's own network. This then allows for overlap between the customer and provider VLAN IDs since the customer Q-tag is hidden while it is transported through the provider network. However, while this Q-in-Q approach supports a three-tiered hierarchy and frees up additional VLAN IDs, the service provider can still only create 4,094 customer VLANs. Scalability is still an issue as 4,000 tags is simply insufficient for large metropolitan networks. This shortcoming is addressed by the second standard, IEEE 802.1ah.

MAC Header Encapsulation

The IEEE 802.1ah standard, also known as MAC header encapsulation (MAC-in-MAC) or Provider Backbone Bridging, encapsulates the customer MAC header with a MAC header for the service provider. A 24-bit service tag that identifies individual subscribers, is also used in the service provider MAC header. This enables a maximum of 16 million service instances to be supported, thus alleviating the scalability issue entirely.

With IEEE 802.1ah, the overall network is treated as separate service provider and end customer domains. In the service provider domain, the network switches on the service provider MAC header and the customer MAC is not even visible. This introduces strict demarcation between the customer and service provider, enabling a truly hierarchical approach to the network. MAC-in-MAC greatly improves the scalability of Layer 2 networks.

This approach also alleviates another limitation to traditional Ethernet; learning. Traditional Ethernet switch-based networks have two defining characteristics that limit their topological size, namely learning and loop avoidance. When a switch receives a packet destined for an end station it does not yet know about, it floods the packet down every link on which it is connected. This is referred to as Flood for Unknown. As the switch inspects every packet it receives, it remembers or learns the association of sending stations and ingress links. Each switch in the layer 2 domain learns the address and associated link for every other device in the network.

While many metro and core devices may be able to support hundreds of thousands of addresses, requiring each device in a provider's network to handle this number of addresses is cost prohibitive and impacts protection switching schemes. MAC-in-MAC encapsulation solves this Layer 2 scalability problem since there are now fewer MAC addresses to learn at the core.

The IEEE 802.1ah MAC header, specifies that a backbone VLAN tag (B-tag), and an instance service VLAN tag (I-tag) be added to packets traversing the provider backbone bridge. This extended service VLAN tag is mapped from the Service VLAN ID tag and is longer than a normal VLAN tag. The additional B-tag is then added to ensure that the switches in the middle of the 802.1ah core do not need to know about the 802.1ah functions, thus ensuring backward compatibility. The backbone MAC header is then removed at the other end of the provider's 802.1ah backbone bridge. A big advantage of 802.1ah is that it works in conjunction with the 802.1ad Provider Bridges VLAN stacking standard to allow both techniques to be used simultaneously.

Provider Backbone Transport



NOTE: When using PBT, MSTP should not be enabled as all PBT ports need to be in the forwarding state. For example, if MSTP is enabled it could block one of the PBT ports and thus remove the backup tunnel.

PBT has emerged to further address limitations related to scalability and reliability. PBT may be deployed in place of PBB or may run in parallel with PBB. In both cases, PBT eliminates the need for backbone core devices to perform learning and flooding. Instead, point-to-point tunnels to transport L2VPNs are provisioned. Rather than using MSTP to prevent loops, the tunnels are used to traffic engineer the provider backbone network. A PBT tunnel is unidirectional and is set up to ingress on a local node at one edge of the provider backbone and to terminate on a remote device at the other end of the backbone. This tunnel transports encapsulated subscriber frames from the local node to the remote node. A second tunnel is then configured in the opposite direction to ingress the remote node and terminate on the local node. This serves as the transport for the reverse traffic. A tunnel pair together make a bidirectional pipe referred to as a PBT trunk.

PBT tunnels are set up to transport Ethernet Virtual Circuits (IEEE 802.1ad), with the subscriber frames encapsulated using 802.1ah MAC-in-MAC encapsulation. Tunnels are then identified by the Backbone Destination Address (B-DA) and the Backbone Tag (B-Tag). In **Figure 23-1**, the highlighted fields are added to the frame to identify tunnels and to identify flood domains and interconnects.

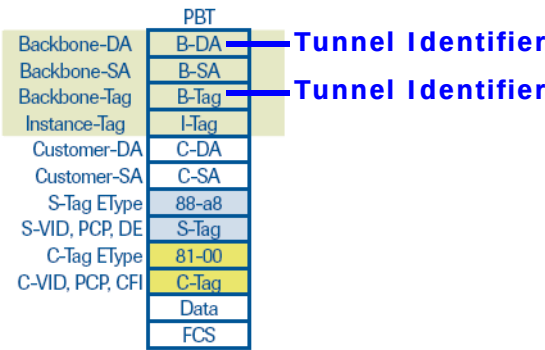


Figure 23-1: PBT Frame Format

Since the tunnels are point-to-point, PBT can also achieve recovery times approaching 50 ms. Providers can set up primary and protection PBT paths and then leverage Carrier Ethernet OAM standard CFM (IEEE 802.1ag) to monitor the tunnels. This provides fault notifications in milliseconds and thus carrier-grade failover times can be achieved.

Figure 23-2 shows an example PBT network with the core provider network in the center and 3 access networks attached to the core. In the core, primary tunnels are configured (solid lines) as well as backup tunnels (dotted lines) in order to provide resiliency and greater utilization of the backbone network. Again, in the core, there is no loop detection and no learning.

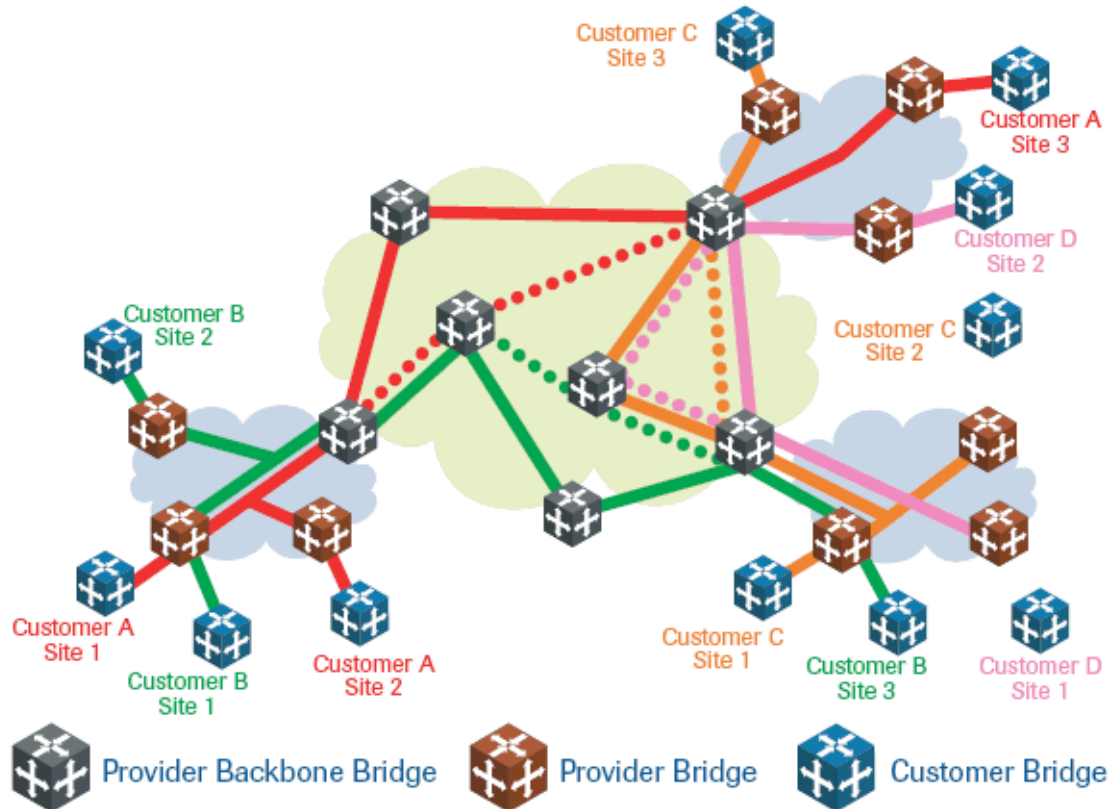


Figure 23-2: Example of a PBT Network

The system software supports configuration of a maximum of 64 PBT trunks. This allows for 32 ingress tunnels and 32 egress tunnels. However, one PBT tunnel may be used to transport multiple subscriber services. In addition, one virtual circuit must be created for each service instance. A maximum of 127 virtual circuits are supported by one PBT tunnel. PBT tunnels may also be configured across link aggregation ports.

Figure 23-3 depicts two Provider Bridged networks interconnected by a PBT network. Two customer Layer 2 Virtual Private networks are shown traversing primary and backup PBT tunnels through the core network.

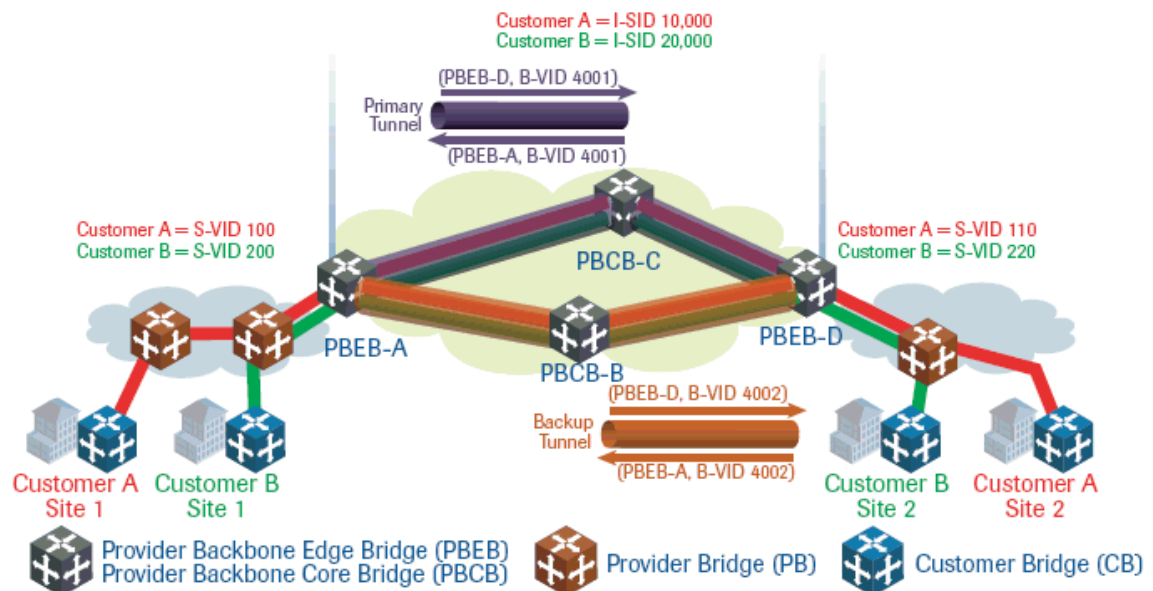


Figure 23-3: A PBT Network with Primary and Backup Tunnels

Traffic from Customer A originates at its Site 1. The Provider Bridge encapsulates the customer traffic by adding a Subscriber S-Tag containing the configured S-VID value of 100 reserved for Customer A within its domain. This traffic is then sent to the Provider Backbone Edge Bridge A (PBEB-A).

PBEB-A has been configured to assign Customer A traffic (S-VID=100) to a 24-bit Instance Service Identifier (I-SID) value of 10,000. This I-SID value is associated with a primary and a backup PBT tunnel. Each primary and backup tunnel is identified using the combination of a PBEB Destination MAC address and a Backbone-VID (B-VID). This is a significant difference between PBT and PBB. In PBB, B-VIDs represent flood domains that interconnect multiple Provider Bridged networks. In PBT, B-VIDs together with B-DAs identify which tunnel the frame will use.

In our example, the PBEB-A encapsulates S-VID 100 traffic by adding the B-DA value for PBEB-D, a B-SA value for PBEB-A, a B-VID value of 4001 (primary tunnel), and the I-SID value of 10,000. This MAC header encapsulated traffic is forwarded to Provider Backbone Core Bridge-C (PBCB-C). PBCB-C has been configured to not learn or flood traffic on B-VID 4001, which has been reserved for PBT use. The fact that PBT does not learn or flood is an important point. Each PBCB device must be provisioned with forwarding database entries in order to properly forward traffic within the tunnels.

The PBCB-C forwarding table learns an entry for the combination of PBEB-D, B-VID 4001 and the traffic is forwarded on the particular port in the direction of PBEB-D. PBEB-D receives the traffic and removes the MAC header encapsulation. Since the S-VID values are only locally significant to the Provider Bridged network, a provider has the flexibility to translate the S-VID value. In our example, PBEB-D has been configured to associate I-SID 10,000 with S-VID 110.

In this illustration, traffic from the tunnel is de-encapsulated and the S-VID is remapped to the value of 110. The traffic is forwarded to the provider bridge attached to Customer A's Site 2. The S-Tag encapsulation is removed by the PB device and the original customer frame from Site 1 is delivered to Site 2.



NOTE: It should also be noted that the PBT service tag is 22 Bytes in length and this needs to be taken into account when calculating available bandwidth. For example, when sending a 64-Byte packet at 100% of line rate through a PBT tunnel, each 64-Byte frame is actually 86 Bytes long (64 + 22).

Connectivity Fault Management

PBT virtual switches and tunnels are monitored through the use of IEEE 802.1ag Connectivity Fault Management (CFM) Continuity Check Messages (CCM). When CFM services are configured for PBT virtual switches, CCM control frames are sent and received within the PBT tunnels and monitor faults based on the associated PBT virtual circuit events. For CFM services that monitor PBT tunnels, CCM control frames are sent and received regularly along the PBT tunnels. If the primary tunnel should experience a fault, the tunnel endpoints automatically begin using the backup tunnel. The forwarding database entries are pre-configured along the backup path to minimize the failover and restoration times. Only one backup tunnel can be created.

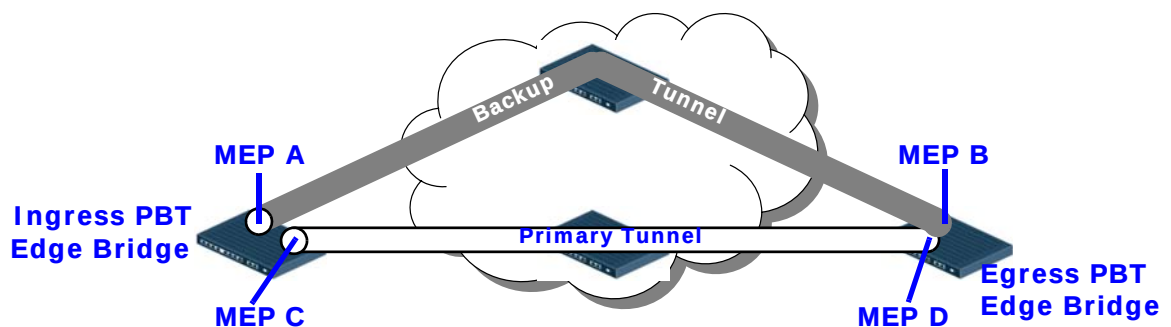


Figure 23-4: PBT with CFM

It should be noted that once a failover occurs (switching the path from the primary to the backup tunnel), the default behavior is for the provisioned primary tunnel to become the backup tunnel unless tunnel reversion is configured using the `pbt set tunnel-reversion` command. The `tunnel-reversion` command will automatically revert traffic back to the provisioned primary tunnel once it is up and the reversion hold timer is completed (`pbt set reversion-hold-time`).

Example:

```
> pbt set tunnel-reversion off
> pbt set reversion-hold-time 3000
```


Manual reversion allows the network operator to control when or if the reversion will take place (such as late at night or on a weekend) so that the impact to the service is minimum. Manual reversion also prevents flapping between the two tunnels if the primary is not entirely stable. Automatic tunnel reversion is useful if the backup tunnel is inferior to the primary tunnel. Thus, failback occurs automatically.



NOTE: Please note that when configuring PBT reversion, tunnel reversion must be enabled on all remote bridges and the reversion hold time must be set to the same value. If reversion settings are not symmetrical, it can cause issues with indicating the primary/backup tunnel and can cause delays in reversions.

Ciena supports the draft IEEE 802.1ag CFM including MAC ping, MAC traceroute, and CCM. Using these powerful CFM tools, both service connectivity and PBT tunnel resiliency is enhanced. In addition, CCM thresholds can be configured to fine-tune protection switching.

PBT Dual Homing

The system software also supports the dual homing of primary and backup tunnels. This enables PBT tunnels to terminate on entirely separate devices. This offers device redundancy and path diversity for upstream connections.

In **Figure 23-5**, device A is dual homed to device B and device C. This offers link resiliency, such that if device B fails, traffic is then diverted to the backup tunnel terminating at device C.

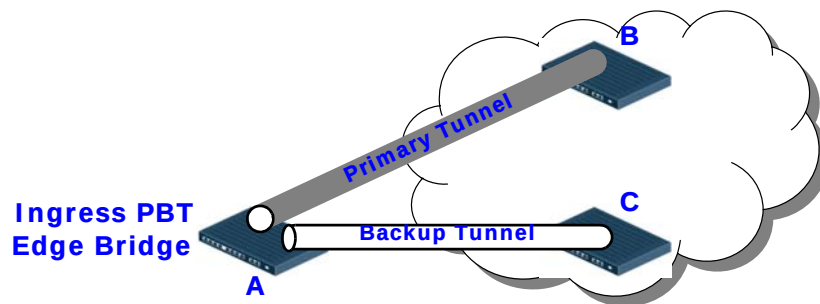


Figure 23-5: PBT Dual Homing

Dual homing is configured by specifying a unique MAC address and bridge name when using the `pbt remote-bridge create bridge-name` command. This second remote bridge is then specified when creating the backup tunnel.

Tunnel Pairing and Synchronization

Although PBT tunnels are set up as trunks, and both an encapsulation and a decapsulation tunnel are required for traffic transport, the tunnel states are not automatically linked together. This makes it possible for the encap and decap tunnels to have different operational states.

For example, if the encap tunnel was down due to misconfiguration, the decap tunnel could still be up and running. This would allow incoming traffic to be decapsulated, thus providing only unidirectional traffic on the circuit. This creates a problem with devices on the terminating end of the tunnels. They would accept all frames regardless of their B-VID value.

To avoid this behavior, encap and decap tunnels should be tied together using the `tunnel pair create` command. By pairing encap and decap tunnels, traffic on an interface is dropped unless the B-VID is specifically configured. In addition, it synchronizes the operational state of the two tunnels. When one tunnel goes down, encap or decap, CCMs are sent over the interface to ensure that the device on the other end takes both tunnels down. The tunnel state will remain down until the MEPs on the other devices have verified connectivity.

In **Figure 23-6**, the encap tunnel on device B goes down. Device B then sends a CCM error code to device A. Device A then takes down both the primary encap and decap tunnels and a failover occurs to the backup tunnel.

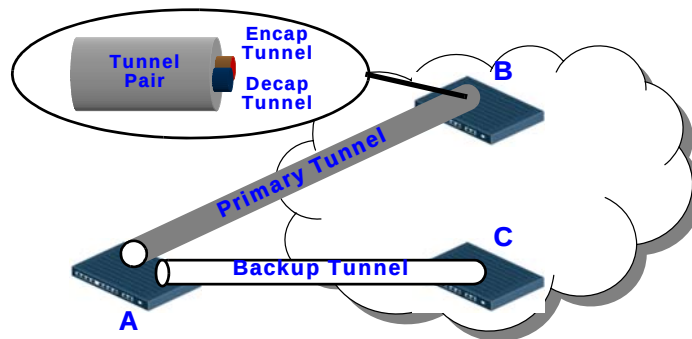


Figure 23-6: Tunnel Pairing Example

To ensure synchronization between primary and backup tunnels, you can enable tunnel synchronization. When tunnel synchronization is turned on for the primary tunnel, a deactivation of either the primary or backup tunnel causes CCMs to be transmitted to the inactive tunnel. This feature enables interoperability with devices running system software 5.x. By default, tunnel synchronization is disabled.

To enable or disable tunnel synchronization when creating a tunnel:

```
tunnel encap create static-pbt <String> tunnel-sync <on|off>
```

To enable or disable tunnel synchronization for an existing tunnel:

```
tunnel encap set static-pbt <TunnelPbtPriTunnel> tunnel-sync <on|off>
```

Benefits

The main benefits of PBT include:

- Removing the 4,000 tag limitation, enabling 16 million distinct services to be configured.
- No learning or flooding in the core of the network for a reduction in complexity and cost.

- Customer MAC address and other information is tunneled through the provider's network, enhancing security and scalability.
- Using specifically engineered paths or tunnels allows the provider to target maximum utilization of the core network devices.
- The customer and Provider control domains are separated, allowing layer 2 control frames to be transported through the provider's network.
- 802.1ag CFM can be used to monitor tunnels and provide carrier-grade failover detection.

Configuration

The following steps are used to configure PBT:

1. Prepare the device for PBT
2. PBT general configuration
3. Tunnel configuration
4. Tunnel protection (optional)
5. VC configuration
6. VS configuration
7. VS subscribers
8. CFM configuration (optional)
9. QoS (optional)



NOTE: On the CN 3960, only ports 11 and 12 can be used to configure tunnels for PBT.

Preparing the device for PBT

To use PBT, a license key is required in order to enable PBT features. PBT license keys can be purchased by contacting Ciena customer support.

To prepare the device for PBT:

1. > software license show

Feature Name	Status	License Domain	Admin	Sequence Number	Days Remain
Base-Features	enable		00000	00000000000	00000
Advanced-Security	enable	CN 3140	00001	00000000020	00000
Advanced-Ethernet	enable	CN 3140	00001	00000000175	00000
Advanced-OAM	enable	CN 3140	00001	00000000190	00000
PBB-TE	disable		00000	00000000000	00000

Feature Name	License Key
Base-Features	
Advanced-Security	W6F6H8C7N3ZPLQ
Advanced-Ethernet	W9F6H8C7N330Q4
Advanced-OAM	WAF6H8C7N34FQK
PBB-TE	

2. > software license install file myLicenseFile.txt license-key A1BCD2E3F4GHIZ

3. >software license show

Feature Name	Status	License Domain	Admin	Sequence Number	Days Remain
Base-Features	enable		00000	00000000000	00000
Advanced-Security	enable	CN 3140	00001	00000000020	00000
Advanced-Ethernet	enable	CN 3140	00001	00000000175	00000
Advanced-OAM	enable	CN 3140	00001	00000000190	00000
PBB-TE	enable	CN 3140	00001	00000000200	00000

Feature Name	License Key
Base-Features	
Advanced-Security	W6F6H8C7N3ZPLQ
Advanced-Ethernet	W9F6H8C7N330Q4
Advanced-OAM	WAF6H8C7N34FQK
PBB-TE	A1BCD2E3F4GHIZ

NOTE: Please note that the license key used here is only an example. Contact Ciena Sales to obtain a proper license key.

4. Make sure that MSTP is disabled either globally or on the individual encap and decap tunnel ports.

```
> mstp disable
> mstp show
===== Bridge MSTP is DISABLED !!! =====
```

Configuring PBT

The following configurations are set on a single device as an example of configuring PBT general parameters.

Configuring general PBT parameters:

1. Display the current PBT settings

```
> pbt show

+----- PBT Attributes -----+
| PBT Bridge MAC           | 00:02:a1:30:7d:60 |
| PBT Service E-type       | 0x88c8             |
| PBT Tunnel E-type        | 0x88a8             |
| PBT Tunnel Reversion     | Off                |
| PBT Reversion Hold Time  | 3000              milli secs |
+-----+-----+

+----- PBT Reserved B-VIDs -----+
| B-VID                     | In Use             |
+-----+-----+
| No entries found          |
+-----+-----+

+----- PBT Remote Bridges -----+
| Bridge Name | Index | Bridge MAC | In use |
+-----+-----+-----+-----+
| No entries found |
+-----+-----+-----+-----+
```

2. Configure the PBT bridge MAC that will be used as the B-SA in the frames.

```
> pbt set bridge-mac 00:02:a1:30:7c:80
```



NOTE: It is recommended that you manually set the B-SA PBT bridge MAC address. If you do not set the B-SA PBT bridge MAC address, the system software will send the chassis base MAC address as the B-SA. In the event of a hardware failure, the chassis base MAC would change, requiring configuration changes on other devices configured to use this device as a remote bridge. This setting needs to be unique from the B-SA for all devices.

3. Set the Ethertypes if needed. Ethertypes for services and PBT tunnels are configurable for interoperability. The default is 0x88a8 for PBT tunnels and 0x88c8 for services.

```
> pbt set tunnel-tag-ethertype 0x88a8
> pbt set service-tag-ethertype 0x88c8
```



NOTE: Please note that in order for PBT frames to be transmitted through a device, the PBT ethertype must be set to 0x8100 (33024 decimal).

4. Reserve Bridge VLAN IDs (B-VIDs). Each incoming tunnel requires a unique B-VID.

```
> pbt reserve bvid 112-115
```



NOTE: The maximum number of B-VIDs that can be reserved is equal to the maximum number of PBT tunnels, which is 32. If trying to reserve more than 32, the system software generates the following error message: ERROR: reserving B-Vid, No more resources available.

5. Configure remote bridge names for use in tunnels and virtual circuits. For operator convenience, tunnel endpoints can be identified with names by associating a MAC address with name. The subsequent Tunnel and VC configurations refer to the nodes by these names.

```
> pbt remote-bridge create bridge-name sw1 bridge-mac 00:02:a1:37:bc:60
```

Configuring PBT tunnels:

Both an encapsulation (egressing) and a decapsulation (ingressing) tunnel are required for connectivity.

1. Configure the encap tunnel, providing the tunnel destination node, the B-VID to be used, and the NNI port that the tunnel will egress traffic on.

```
> tunnel encap create static-pbt to_sw1 b-vid 115 dest-bridge-name sw1 port 21
tunnel-sync on
```



NOTE: Optionally a CoS policy and a Primary Code Point (PCP) value for the encapsulated frames can also be configured using the `tunnel encap set encap-cos-policy` and `tunnel encap set encap-fixed-pcp` commands.

2. Configure the decapsulation tunnel, providing the tunnel source node, the B-VID to be used, and the NNI port on which the tunnel will ingress.

```
> tunnel decap create static-pbt frm-sw1 b-vid 115 src-bridge-name sw1 port 21
```

3. Pair the primary encapsulation and decapsulation tunnels together.

```
> tunnel pair create tnl-pair myPair encap-pbt to_sw1 decap-pbt frm-sw1
```

Configuring the PBT backup tunnels:

Note that configuration of the backup tunnel is optional, but recommended. The tunnel name must also be the same as the primary tunnel.

1. Configure the backup encap tunnel.

```
> tunnel encap create static-backup-pbt to_sw1 b-vid 116 dest-bridge-name sw1 port 23
```

2. Configure the backup decap tunnel.

```
> tunnel decap create static-pbt bkp_sw1 b-vid 116 src-bridge-name sw1 port 23
```

3. Pair the backup encapsulation and decapsulation tunnels together.

```
> tunnel pair create tnl-pair backup_pair encap-backup-pbt to_sw1 decap-pbt bkp_sw1
```

4. Display the tunnels to verify the configuration.

```
> tunnel encap show
```

ENCAP TUNNEL TABLE							
Name	Type	Oper	Admin	Destination	B-VID	Role	Active
tunnel1	encap-pbt	En	En	sw1	115	pri	Yes
tunnel1	encap-pbt	En	En	sw1	116	bkp	No

Configuring the virtual circuit:

Configuring a virtual circuit for PBT involves setting the ingress I-SID for service identification, the egress I-SID, the destination node, and the PBT tunnels to be used.

1. Configure the VC.

```
> virtual-circuit pbt create static-vc vc1 dest-bridge-name sw1 egress-isid 1001 ingress-isid 1002 tunnel tunnel1
```

Configuring the virtual switch:

Configuring a virtual switch for PBT involves creating reserved VLANs, designating the PBT VC to be used with the VS, and adding subscriber ports/VLANs. Optionally, Encap CoS policies may also be set for CoS mapping between the customer frames and the encapsulation PBT tunnel header.

1. Reserve VLANs for the virtual switch.

```
> virtual-switch add reserved-vlan 3100-3105
```

2. Create the virtual switch naming it and associating it with the PBT virtual circuit.

```
> virtual-switch ethernet create vs vs1 vc vc1
```

3. Add the subscriber port and VLAN to the virtual switch.

```
> virtual-switch ethernet add vs vs1 port 1 vlan 10
```

Configuring CFM on a PBT tunnel (optional):

Configuring CFM for the PBT tunnels requires enabling CFM globally, creating a CFM service using the PBT tunnel, and then enabling the service.

1. Enable CFM globally.

```
> cfm enable
```

2. Create the CFM service for the PBT tunnel.

```
> cfm service create static-pbt pbt1 name pbt1 next-mepid 2
```

3. If desired, the CCM interval can be configured, but the interval must be the same on both sides of the tunnel endpoints. The default is 1 second.



NOTE: Setting the CCM Interval to 4 milliseconds is not recommended for a production environment, although it can be used for testing.

```
> cfm service set service pbt1 ccm-interval 4
```

or

```
> cfm service set service pbt1 ccm-interval 1sec
```

4. Enable the CFM PBT service.

```
> cfm service enable service pbt1
```

5. Verify that the MEP IDs at both ends of the tunnel are different. If they are the same, change one of the MEP IDs.

```
> cfm mep show
```

```
> cfm remote-mep show
```

```
> cfm mep set service pbt1 port 21 mepid 2
```

Configuring QoS on a PBT tunnel (optional):

Configuring QoS for PBT involves setting any traffic metering required at the ingress (UNI), configuring a flow service level, then configuring a flow service mapping using the configured VS and the service level.

1. Set up ingress metering.

```
> traffic-profiling standard-profile create port 1 profile 1 cir 15040 pir 15040
```

```
> traffic-profiling set port 1 mode standard-diffserv
```

2. Configure Egress traffic shaping.

```
> flow service-level create port 21 slid 9 cir 15040 pir 15040
```

```
> flow service-mapping create vs pbt1 dst-port 21 slid 9
```

3. Set CoS marking.

```
> tunnel encap set static-pbt pbt1 encap-cos-policy fixed encap-fixed-pcp 3
```

```
> virtual-switch ethernet set vs pbt1 encap-cos-policy fixed encap-fixed-dot1dpri 4
```


Sample Configuration

The following configuration example displays the steps to configure a primary and a backup PBT tunnel over the devices shown in **Figure 23-7**. It also employs CFM to monitor the connection.

The following configuration assumes PBT mode has been enabled on the device and that a valid PBT license key has been entered.

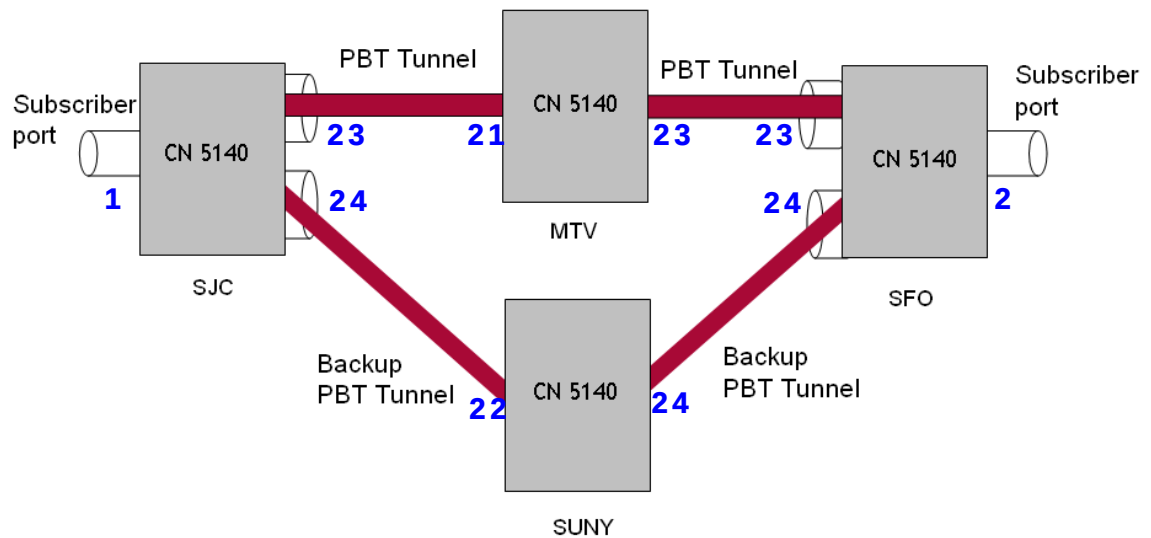


Figure 23-7: PBT Configuration Example

Configuration for device 1 SJC:

1. SJC> mstp disable
2. SJC> pbt set bridge-mac 00:02:a1:30:7c:80
3. SJC> pbt reserve bvid 2000,3000
4. SJC> pbt remote-bridge create bridge-name SFO bridge-mac 00:02:a1:30:7c:c0
5. SJC> tunnel encap create static-pbt to_SFO b-vid 2000 dest-bridge-name SFO port 23 tunnel-sync on
6. SJC> tunnel decap create static-pbt frm_SFO b-vid 2000 src-bridge-name SFO port 23
7. SJC> tunnel pair create tnl-pair SJC encap-pbt to_SFO decap-pbt frm_SFO
8. SJC> tunnel encap create static-backup-pbt to_SFO b-vid 3000 dest-bridge-name SFO port 24
9. SJC> tunnel decap create static-pbt bkp_SFO b-vid 3000 src-bridge-name SFO port 24
10. SJC> tunnel pair create tnl-pair SJC-Backup encap-backup-pbt to_SFO decap-pbt bkp_sfo

11. SJC> virtual-circuit pbt create static-vc pbt dest-bridge-name SF0 egress-isid 1 ingress-isid 2 tunnel to_SF0
12. SJC> virtual-switch add reserved-vlan 1000
13. SJC> virtual-switch ethernet create vs pbt vc pbt
14. SJC> virtual-switch ethernet add vs pbt port 1 vlan 10
15. SJC> cfm service create static-pbt to_SF0 name PBT level 7 next-mepid 100
16. SJC> cfm service set service PBT alarm-time 0
17. SJC> cfm service enable service PBT
18. SJC> cfm service create static-backup-pbt to_SF0 name PBT_BKP level 7 next-mepid 101

Configuration for device 2 SF0:

1. SF0> mstp disable
2. SF0> pbt set bridge-mac 00:02:a1:30:7c:c0
3. SF0> pbt reserve bvid 2000,3000
4. SF0> pbt remote-bridge create bridge-name SJC bridge-mac 00:02:a1:30:7c:80
5. SF0> tunnel encap create static-pbt to_SJC b-vid 2000 dest-bridge-name SJC port 23 tunnel-sync on
6. SF0> tunnel decap create static-pbt to_SJC b-vid 2000 src-bridge-name SJC port 23
7. SF0> tunnel pair create tnl-pair SF0 encap-pbt to_SJC decap-pbt to_SJC
8. SF0> tunnel encap create static-backup-pbt to_SJC b-vid 3000 dest-bridge-name SJC port 24
9. SF0> tunnel decap create static-pbt to_SJC b-vid 3000 src-bridge-name SJC port 24
10. SF0> tunnel pair create tnl-pair SF0-Backup encap-backup-pbt to_SJC decap-pbt to_SJC
11. SF0> virtual-circuit pbt create static-vc pbt dest-bridge-name SJC egress-isid 2 ingress 1 tunnel to_SJC
12. SF0> virtual-switch add reserved-vlan 1000
13. SF0> virtual-switch ethernet create vs pbt vc pbt
14. SF0> virtual-switch ethernet add vs pbt port 1 vlan 10
15. SF0> cfm service create static-pbt to_SJC name PBT level 7 next-mepid 200
16. SF0> cfm service set service PBT alarm-time 0
17. SF0> cfm service enable service PBT
18. SF0> cfm service create static-backup-pbt to_SJC name PBT_BKP level 7 next-mepid 201
19. SF0> cfm service enable service PBT_BKP

Configuration for device 3 MTV:

1. MTV> mstp disable
2. MTV> vlan create vlan 2000,3000
3. MTV> vlan add vlan 2000,3000 port 21,23
4. MTV> cfm mip create vlan 2000 port 21 level 6
5. MTV> cfm mip create vlan 2000 port 23 level 6
6. MTV> cfm mip create vlan 3000 port 21 level 6
7. MTV> cfm mip create vlan 3000 port 23 level 6

Configuration for device 4 Sunny:

1. Sunny> mstp disable
2. Sunny> vlan create vlan 2000,3000
3. Sunny> vlan add vlan 2000,3000 port 22,26
4. Sunny> cfm mip create vlan 2000 port 22 level 6
5. Sunny> cfm mip create vlan 2000 port 24 level 6
6. Sunny> cfm mip create vlan 3000 port 22 level 6
7. Sunny> cfm mip create vlan 3000 port 24 level 6

Chapter

Link Layer Discovery Protocol

24

At a Glance:

- Overview
- Principles of Operation
- Feature Benefits
- Configuring Link Layer Discovery Protocol
- Troubleshooting

This chapter provides an overview of the Link Layer Discovery Protocol (LLDP) and describes how to configure 802.1AB LLDP.

Overview

The Link Layer Discovery Protocol allows network equipment (i.e., stations, switches, bridges, routers, etc.) to advertise their parameters for network topology discovery and management. Traditional network management protocols, such as SNMP, running at key locations, use layer 3 protocols to identify the devices connected to the network. The Link Layer Discovery Protocol is a layer 2 protocol, allowing precise discovery of the physical-link topology of the network. Devices act as LLDP agents, which drastically increases the network discovery performance of SNMP applications, as well as any system capable of accessing standard LLDP MIBs.

Principles of Operation

The system software supports LLDP as specified in the IEEE 802.1AB-2005 standard. Like Rapid Spanning Tree Protocol (RSTP), LLDP is a link-constrained, layer 2 protocol. This means that the exchange of LLDP messages only takes place between adjacent LLDP agents (devices) on the network, unless control frame tunneling is used to tunnel the LLDP PDUs through another device. LLDP agents communicate basic management information with each other by exchanging Link Layer Discovery Protocol Data Units (LLDPDUs). The information about a device, and its immediate neighbors is then retrievable through the standard LLDP MIBs using SNMP. It is important to note that LLDP operates only on physical ports.

As illustrated in **Figure 24-1**, LLDP Agent A exchanges LLDPDUs with LLDP Agent B and Agent C, but not with Agent D since it is not directly connected to Agent A.

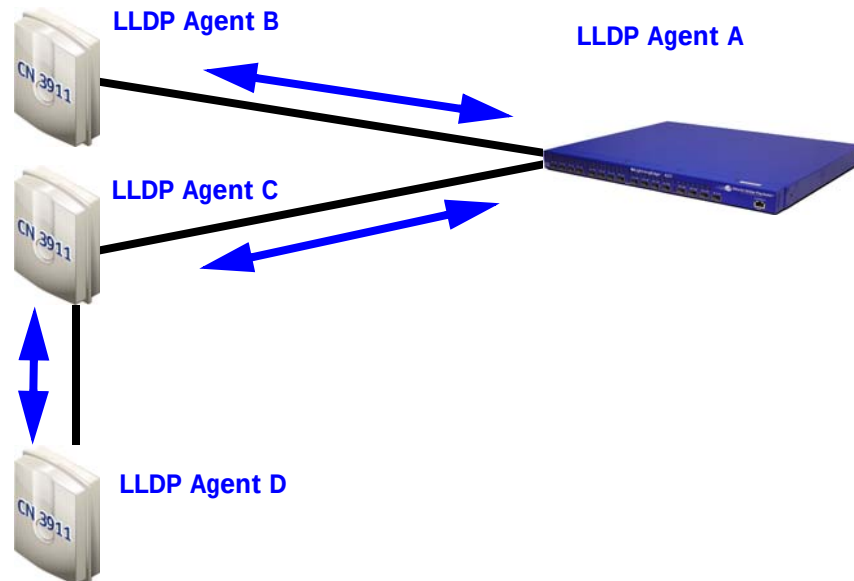


Figure 24-1: Example of Architectural Relationship Between LLDP Agents



NOTE: Link Layer Discovery Protocol does not configure or control any traffic or devices on the network. Its primary role is to report discovered information to higher-layer management tools. It is not intended to act as a configuration protocol for remote systems nor as a mechanism to signal control information between ports.

LLDP TLVs

The LLDPDU is a layer 2 packet that consists of an L2 source, destination, and an EtherType field, and 4 or more Type Length and Value fields (TLVs). The LLDP standard specifies 9 common TLV fields, 4 of which are mandatory TLVs and the remaining 5 are optional TLVs to carry information for broadcasting sender information.

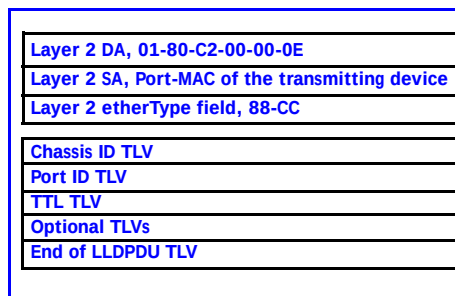


Figure 24-2: LLDPDU Packet

Periodic LLDPDUs are sent out at a user defined interval, however, LLDPDUs are also sent whenever LLDP TLV data has changed. An SNMP notification is then generated after changed data is received from a neighboring device. Upon receipt of this notification the SNMP management application polls the LLDP MIB objects to determine what information has changed.

Common TLVs

The system software supports all of the 9 common TLVs specified by the standard:

- **Chassis ID TLV-** The first TLV in an LLDPDU is mandatory and identifies the chassis. It contains the 802 LAN station associated with the transmitting LLDP agent and supports the "MAC Address" chassis ID subtype.
- **Port ID TLV-** The second TLV in an LLDPDU is mandatory and identifies the port component that transmits the TLV. It supports the "Interface Alias" port ID subtype.
- **Time To Live (TTL) TLV-** The third TLV in an LLDPDU is mandatory and indicates the number of seconds that the recipient LLDP agent is to regard the information associated with this LLDPDU to be valid.
- **Port Description TLV-** This optional TLV is an alpha-numeric string that indicates the port's description.
- **System Name TLV-** This optional TLV is an alpha-numeric string that indicates the assigned name.
- **System Description TLV-** This optional TLV is an alpha-numeric string that indicates the system description.
- **System Capabilities TLV-** This optional TLV identifies the primary functions of the system and whether or not these primary functions are enabled. It supports the bridge capability.
- **Management Address TLV(s)-** This optional TLV identifies the address associated with the local LLDP agent that may be used to reach higher layer entities to assist discovery by network management.
- **End of LLDPDU TLV-** This mandatory 2 octet TLV defines the end of LLDPDU with all 0 values.

802.1 Organizationally Specific TLVs

- **Port VLAN ID TLV-** allows a port to advertise its VLAN ID (PVID) that will be associated with untagged or priority tagged frames.
- **Port and Protocol VLAN ID TLV-** The system software stores values received from the remote partner for this TLV but does not transmit this TLV.
- **VLAN Name TLV-** The system software stores values received from the remote partner for this TLV but does not transmit this TLV.
- **Protocol ID TLV-** allows an 802 LAN station to advertise particular protocols that are accessible through the port. Currently, the system software advertises the following protocols: RSTP and 802.3ah OAM.

802.3 Organizationally Specific TLVs

- **MAC/PHY Configuration/Status TLV-** advertises Auto-negotiation support and status, PMD auto-negotiation capability, and Operational MAU type.
- **Power via MDI TLV-** The system software stores values received from the remote partner for this TLV but does not transmit this TLV.

- **Link Aggregation TLV-** advertises whether the link is capable of being aggregated, whether the link is currently in an aggregation, and the port ID of the aggregation if it is in an aggregation. LLDP advertises Link Agg TLV in the PDU but Link Aggregation is not currently supported and is disabled.
- **Maximum Frame Size TLV-** advertises the maximum frame size capability.

Ciena Organizationally Specific TLVs

- **Unknown TLVs-** the LLDP standard specifies that unknown TLVs need to be stored locally if memory can be allocated. The system software stores all unknown TLVs for all valid LLDP PDUs for retrieval.
- **LLDP Graceful Shut Down-** When an LLDP agent is administratively disabled, it executes a graceful shut down handshake. It sends out the last LLDP PDU that specifies the TTL as zero in TTL TLV. When its counterpart receives this LLDPDU, it cleans up all the LLDP information received.

Feature Benefits

Using LLDP for network topology discovery offers the following benefits to the network provider:

- Accurate network topology discovery and management
- Support of standard tools using SNMP
- Multi-vendor interoperability.

Accurate Network Topology Discovery and Management

Many network management tools use layer 3 protocols to automate the discovery process and track topology configurations and changes. The use of layer 2 LLDP allows network management tools to quickly and accurately discover current network topologies and to track both intentional and unintentional topology changes. Network administrators and technicians can use the accurate and up to date topology information to more quickly diagnose network problems in the field.

Support of Standard Tools

Each LLDP agent maintains its own per-port table of information in a standard SNMP MIB. Updates are sent as needed to the closest connected device on the network. Through the Command Line Interface (CLI), a user can access the device and manage LLDP information. General information, such as Chassis ID and port configuration can be displayed. Users with su security privileges can configure LLDP options and manipulate TLVs. For example, a specific port could be configured to only transmit or receive LLDPDUs.

LLDPDUs are used to update standard LLDP Management information Databases (MIBs) allowing any standard SNMP application to monitor the information as it changes.

Multi-vendor Interoperability.

LLDP is a standards-based protocol. Using LLDP rather than a proprietary topology discovery protocol allows the network provider to interoperate with non-Ciena devices that also support LLDP.

Configuring Link Layer Discovery Protocol

LLDP is enabled by default on all ports, but can be enabled or disabled on a per-port basis. In addition, some optional TLVs can be excluded from transmission in the LLDP PDU on a per-port basis.

For a complete list of the available LLDP commands refer to the **lldp** section on page 441 in Appendix , “ ”.



CAUTION: The default settings for LLDP should be sufficient to ensure proper topology discovery in most networks. Since LE-NS ESM topology discovery relies on LLDP for higher performance topology discovery, care should be taken when modifying the LLDP configuration. In certain topologies, LLDP does not need to be forwarded (e.g., when using non-LLDP devices such as hubs).

In the following configuration example, the user displays the state of port 10, then disables LLDP on this port.

It should be noted as well that by using the `lldp show port` command, information about the remote port (neighbor) can be seen in the LLDP Remote Port TLV section of the output. This displays the MAC address, port number, and other information of the connected remote port.

Configuration steps:

Step #	Description	Location/Command
Step 1	Display the current state of port 10.	<code>lldp show [configuration] [statistics][port <PhyPortNameList> [configuration statistics]]</code>
Step 2	Set port 10 to disable.	<code>lldp set port <PhyPortNameList> {[mode rx-only tx-only tx- rx disable],[notification <on off>]}</code>
Step 3	(Optional) Verify the configuration of the port.	<code>lldp show [configuration] [statistics][port <PhyPortNameList> [configuration statistics]]</code>

CLI Example:

1. > lldp show port 10

```
>lldp show port 10
+----- LLDP Port Configuration -----+
|      |      |      |      |      |      |      |      |
|  Port | Admin | TLV  | Dot1 | Dot3 |      | Notif |
|      | State | Type |      |      |      |      |
+-----+-----+-----+-----+-----+-----+
| 10    | Tx-Rx | 111111111 | 1 1111 | 1111 |      | Off |
+-----+-----+-----+-----+-----+-----+

Where:
Dot3 Type      ||||| +-- 4 Maximum Frame Size      TlvTx
Dot3 Type      ||||| +-- 3 Link Aggregation      TlvTx
Dot3 Type      ||||| +-- 2 Power via MDI      TlvTx
Dot3 Type      ||||| +-- 1 MacPhy Config      TlvTx
Dot1 Type      ||||| +-- 7 Protocol ID OAM      TlvTx
Dot1 Type      ||||| +-- 6 Protocol ID Dot1X      TlvTx
Dot1 Type      ||||| +-- 5 Protocol ID STP      TlvTx
Dot1 Type      ||||| +-- 4 Protocol ID LACP      TlvTx
Dot1 Type      ||||| +-- 3 VLAN Name      TlvTx
Dot1 Type      ||||| +-- 2 Port&Protocol VLAN ID TlvTx
Dot1 Type      ||||| +-- 1 Port VLAN ID      TlvTx
Basic Type     ||||| +-- 9 Local Mgmt Address      TlvTx
Basic Type     ||||| +-- 8 Remote Mgmt Address      TlvTx
Basic Type     ||||| +-- 7 System Capabilities      TlvTx
Basic Type     ||||| +-- 6 System Description      TlvTx
Basic Type     ||||| +-- 5 System Name      TlvTx
Basic Type     ||||| +-- 4 Port Description      TlvTx
Basic Type     ||||| +-- 3 Time-to-Live      TlvTx
Basic Type     ||||| +-- 2 Port ID      TlvTx
Basic Type     ||||| +-- 1 Chassis ID      TlvTx

+----- LLDP Port Statistics -----+
| Port | Out  | In  | InErrPkt | InError | Tlv  | Unknown | AgedOut |
|      | TotalPkt | TotalPkt | Discarded | Tlv  | Discarded | Tlv  | Total  |
+-----+-----+-----+-----+-----+-----+-----+
| 10    | 7    | 8    | 0         | 0        | 0      | 0        | 0        |
+-----+-----+-----+-----+-----+-----+

+----- LLDP Local Bridge TLV -----+
| TLV | Type | Value |
+-----+-----+-----+
| Chassis ID | MacAddr | % 0x0002A107A4A0 |
| TimeToLive |         | 120 (second) |
| System Name |         | CN 3911 |
| System Desc |         | CN 3911 Service Delivery Switch |

| System Cap | Capabilities | Bridge |
| Mgmt Addr  | Enabled Cap  | Bridge |
|            |              | No Data |

+-----+-----+-----+
+ Port 10 ----- LLDP Local Port TLV -----+
| TLV | Type | Value |
+-----+-----+-----+
| Port ID | IfAlias | 1 10 |
| Port Desc |         | 10/100/G Port |
| 802.1 | PortVlanId | 1 |
| 802.1 | PortProtVlanId | NotSupt Disable ProtVid:0 |
| 802.1 | ProtocolId | LACP (operationally disabled) |
|         |         | STP |
|         |         | Dot1X (operationally disabled) |
|         |         | OAM (operationally disabled) |
| 802.3 | MacPhyConfig | AutoNeg:Support Enable |
|         |         | PmdAutoNegAdCap:Unknown |
|         |         | OperMauType:Unknown |
| 802.3 | PowerViaMDI | PortClass:PD MDI:NotSupt |
|         |         | MDI:Disable PairCtrl:Can't |
|         |         | PwrPair:NotSupt PwrClass:NotSupt |
| 802.3 | LinkAgg | Capable Disable |
| 802.3 | MaxFrameSize | 1526 |
+-----+-----+-----+
```

+ Port 10 ----- LLDP Remote Port TLV -----+		
TLV	Type	Value
Chassis ID	MacAddr	0x0002A1307D60
Port ID	IfAlias	10
TimeToLive		120 (second)
Port Desc		Fast Ethernet Port
System Name		311v-Src
System Desc		LE-311v Access Concentrator
System Cap	Capabilities	Bridge
	Enabled Cap	Bridge
Mgmt Addr	IPv4	192.168.054.242
AddrIf	ifIndex/if#2	1.3.6.1.2.1.2.2.1.1.2
802.1	PortVlanId	1
802.1	ProtocolId	LACP
		OAM
802.3	MacPhyConfig	AutoNeg:Support Enable
		PmdAutoNegAdCap:Unknown
		OperMauType:Unknown
802.3	PowerViaMDI	PortClass:PD MDI:NotSupt
		MDI:Disable PairCtrl:Can't
		PwrPair:NotSupt PwrClass:NotSupt
802.3	LinkAgg	Capable Disable
802.3	MaxFrameSize	1526

2. > lldp set port 10 mode disable

```
>lldp set port 10 disable
```

3. > lldp show port 10 configuration

```
>lldp show port 10 configuration
```

+----- LLDP Port Configuration -----+						
		Basic	Org Specific			
	Admin	TLV Type	Dot1	Dot3		
Port	State	123456789	1234567	1234		Notif
10	Disable	111111111	1 1111	1111		Off

Where:

Dot3	Type				+-- 4 Maximum Frame Size	TlvTx
Dot3	Type			+-- 3 Link Aggregation		TlvTx
Dot3	Type			+-- 2 Power via MDI		TlvTx
Dot3	Type			+-- 1 MacPhy Config		TlvTx
Dot1	Type			+-- 7 Protocol ID OAM		TlvTx
Dot1	Type			+-- 6 Protocol ID Dot1X		TlvTx
Dot1	Type			+-- 5 Protocol ID STP		TlvTx
Dot1	Type			+-- 4 Protocol ID LACP		TlvTx
Dot1	Type			+-- 3 VLAN Name		TlvTx
Dot1	Type			+-- 2 Port&Protocol VLAN ID		TlvTx
Dot1	Type			+-- 1 Port VLAN ID		TlvTx
Basic	Type		+-- 9 Local Mgmt Address			TlvTx
Basic	Type		+-- 8 Remote Mgmt Address			TlvTx
Basic	Type		+-- 7 System Capabilities			TlvTx
Basic	Type		+-- 6 System Description			TlvTx
Basic	Type	+-- 5 System Name				TlvTx
Basic	Type	+-- 4 Port Description				TlvTx
Basic	Type	+-- 3 Time-to-Live				TlvTx
Basic	Type	+-- 2 Port ID				TlvTx
Basic	Type	+-- 1 Chassis ID				TlvTx

Troubleshooting

Displaying LLDP neighbors

To display neighboring devices including the local port, remote port, remote management address, chassis identification, and system name:

```
>lldp show neighbors
```

LLDP Neighbors			
Remote Addr: 10.26.193.79			
System Name: 3911-Center-Ematar			
System Desc: CN 3911 Service Delivery Switch			
Local	Remote		
Port	Port	Info	
5	27	Chassis Id: 0002A1306B40	
		Mgmt Addr: 172.16.233.214	
		System Name: LE311-Center-Ematar	
		System Desc: LightningEdge (tm) LE-311v Access Concentrator	
6	8	Chassis Id: 0002A107B010	
		Mgmt Addr: 10.26.193.56, 10.26.193.56	
		System Name: 3920-Right-Ematar	
		System Desc: CN 3920 Service Delivery Switch	
8	8	Chassis Id: 0002A107AFC0	
		Mgmt Addr: 10.26.193.55	
		System Name: 3920-Left-Ematar	
		System Desc: CN 3920 Service Delivery Switch	

Chapter System Software Management

25

At A Glance:

- Overview
- Network connectivity
- Release Compatibility
- Preparing Files for Upgrade
- Upgrading from a Previous Version of SAOS
- Backup Software Images

This chapter describes the procedure for upgrading and downgrading system software.

Overview

The upgrade of system software is driven by the use of software configuration files created by the network administrator. The actual upgrade process takes about 10 minutes for the device to execute. Device upgrades should take place in an organized manner, for example, starting from the edge of the network and working toward the core, or starting from the core and working toward to the edge.

Network connectivity

The system software upgrade process requires the device to have network connectivity in order to download files and send notifications. You can use the serial console or the remote interface for the upgrade. The remote interface must be configured properly before the upgrade is started. The device must be able to communicate with the TFTP server.

Release Compatibility

The following rules apply to software upgrade and downgrade:

- Release 6.1 can upgrade to 6.2.x but not to any other releases.
- Release 6.2.x can upgrade to 6.3.x but not to any other releases.
- Release 6.3.x will not downgrade to any other release.
- Release 6.4.x can downgrade to 6.3.1 but cannot downgrade to any other release.
- Release 6.3.1 can upgrade to any other software version.
- The device will not install unsupported software.
- Attempting to install unsupported software will cause an error message

Preparing Files for Upgrade

Installing the Software Package

SAOS system software is released in the form of a software package. All files needed for the upgrade are contained in the package. Compatibility information is found in the software package readme file. The software package must be decompressed to the TFTP root directory. The ZIP file is created so that all files will be contained in a subfolder named <tftpboot>/ciena/packages/saos-<build> directory on the TFTP server (where <build> is the actual build number of the system software, for example, saos-06-05-00-0043).

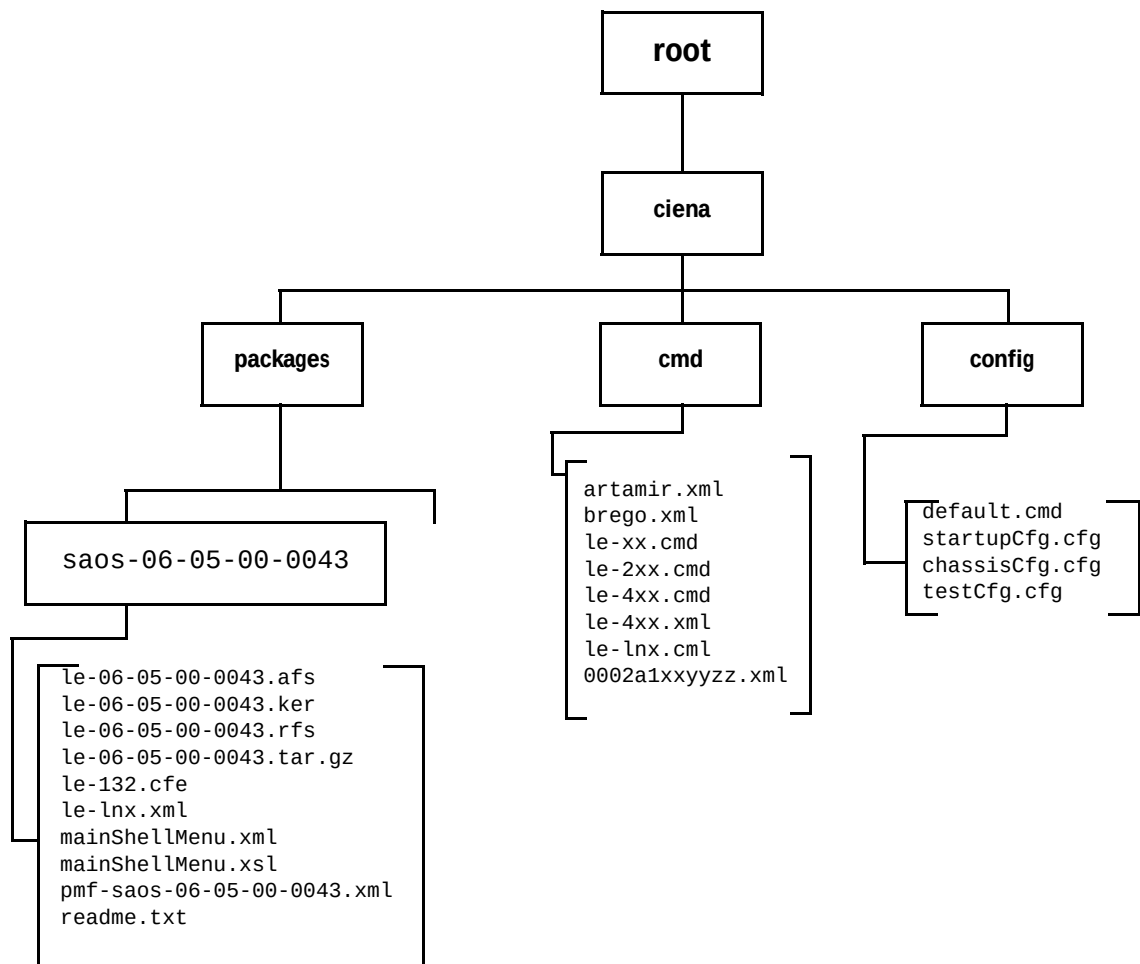


Figure 25-1: Sample TFTP Directory Structure

In **Figure 25-1**, the root directory refers to the directory that was chosen as the root directory for the TFTP server. Operators are free to define the root directory however they wish. All files and folders will be stored in one sub-directory off the root directory named "ciena". This directory has three sub-directories:

- **packages:** This directory has one sub-directory for each software package. Each directory contains all the image files for all device types supported by the software package. This folder also contains platform or board capability files. File names may be changed, but the extensions may not be changed (i.e., .xml).
- **cmd:** Device command files. This directory contains command files and package meta files for each platform class. Command files for specific devices may also exist in this directory, such as <MACAddress>.xml.
- **config:** This directory contains configuration files such as startup-config, chassis-config, etc.

Several files are required for the upgrade, which are summarized in the following table. Also note that all file locations in this table are specified relative to the TFTP root folder.

Table 25-1: Table 1 Upgrade Files

Filename	Description
ciena/packages/saos-<build>.rfs	Root file.
ciena/packages/saos-<build>.afs	Application file.
ciena/packages/le-lnx.xml	Device class command file.
ciena/packages/pmf-saos-<build>.xml	Package command file.
ciena/packages/readme.txt	Package readme file.
ciena/cmd/<MACAddress>.xml	Device specific command file.

Command File

The software package contains a generic platform class command file named le-lnx.xml. This is a fully functional command file that does not require any modifications in order to install the software package on the device. Command files can also be used to upgrade or configure one or more devices.

The following is an example of a SAOS Command file:

```
<!--
```

```
README:  SAOS Command File
```

```
This is a sample command file.  
This file will activate package saos-06-05-00-0043 on your device(s).  
You can modify this file, rename it, and copy it as you wish.
```

```
Command files are used to install new software and/or load new configuration  
files to one or many devices.  Definitions in the command file are organized  
by platform-class.  You may define as many platform classes as you like  
in a single command file.
```

The following example defines two platform classes and uses all possible attributes:

```
<XmlWwpCommandFile>  
  <XmlCmdPlatformClass name="CN3911"  
    version="saos-06-05-00-0043"  
    operation="upgrade"  
    serviceAffecting="yes">  
  </XmlCmdPlatformClass>  
  <XmlCmdPlatformClass name="brego"  
    configFilePath="myFolder/my-config-file.txt"  
    configFileRule="activate"  
    welcomeBanner="myBannerFile.txt"  
    licenseFile="myLicenseFile.txt"  
    <SshKeyFile name="user1.pk2"></SshKeyFile>  
    <SshKeyFile name="user2.pk2"></SshKeyFile>  
    <SshKeyFile name="user3.pk2"></SshKeyFile>  
    version="saos-06-05-00-0043"  
    packagePath="folder1/folder2/folder3"  
    operation="install"  
    serviceAffecting="no" >  
  </XmlCmdPlatformClass>  
</XmlWwpCommandFile>
```

The following attributes are MANDATORY:

platformClass
in order of preference, the most specific match (eg, CN3911), then the class
match (eg, artamir for CN3911 and CN3920, brego for CN3940 and 5140 etc)
The class "le-lnx" must be there if upgrade from 6.3.1 or earlier (for
CN3911 and CN3920 only)

Possible values for platformClass:

le-lnx, CN3911, CN3920, CN3940, CN5140, CN3960, artamir, brego.

The following attributes are OPTIONAL:

configFilePath	(path and filename, path is relative to tftpboot)
configFileRule	(see note #1 below)
welcomeBanner	(path and filename, path is relative to tftpboot)
licenseFile	(path and filename, path is relative to tftpboot)
SshKeyFile	(path and filename, path is relative to tftpboot)
version	(leos-xx-yy-zz-abcd)
packagePath	(complete path to the package directory relative to the tftp-root directory)
operation	(upgrade or xgradei or install)
serviceAffecting	(yes or no)

Possible values for the attribute: configFileRule

install
- Download the config file from the server.
- Store the file in the directory '/flash0/config'
- Store the new filename as 'default-load-file'
- Store the new filename as 'last-config-file'
- This file will be loaded when the device is rebooted.
activate
- Same behavior as install.
- In addition, the file is activated (loaded) immediately.

- This may require a reboot.
 - Reboot will not occur unless "serviceAffecting" is specified.
- augment
- Download the config file.
 - Augment the current system configuration with the commands in this file.
- augmentAndSave
- Download the config file.
 - Augment the current system configuration with the commands in this file.
 - Save the resulting configuration to the file default-save-filename.

Possible values for the attribute: operation

- upgrade
- Download & install image files if necessary.
 - Activate the new image files.
 - This operation may require a reboot.
 - Reboot will not occur unless serviceAffecting="yes"
- install
- Download & install image files if necessary
 - Do not activate the new image files
 - This option is not available for CN3911 and CN3920
- x-grade
- Exact same behavior as 'upgrade'
 - It is supported for backwards compatibility with previous release.

Possible values for the attribute: serviceAffecting

- yes (The device is allowed to reboot if necessary)
- no (The device is NOT allowed to reboot)

NOTE #1

DHCP can be used to run a command file. If a command file request comes in from DHCP, the device will only run the command file once. If another request comes in with the same command file name, the device will ignore the request from DHCP. The name of the command file is saved (last-command-file) and it may be reset by the user via the shell or SNMP. The same is true for the configuration file.

NOTE #2

The License file format is shown here. Lines may appear in any order. Any text following ! will be considered a comment. Whitespace is ignored.

```
! This is my example license file
install <license key>
uninstall <feature name>
install <license key>
```

-->

```
<XmlWwpCommandFile>
  <XmlCmdPlatformClass name="le-lnx"
    version="saos-06-05-00-0043"
    packagePath="ciena/packages/saos-06-05-00-0043"
    operation="upgrade"
    serviceAffecting="yes"
  ></XmlCmdPlatformClass>
  <XmlCmdPlatformClass name="artamir"
    version="saos-06-05-00-0043"
    packagePath="ciena/packages/saos-06-05-00-0043"
    operation="upgrade"
    serviceAffecting="yes"
  ></XmlCmdPlatformClass>
  <XmlCmdPlatformClass name="brego"
    version="saos-06-05-00-0043"
    packagePath="ciena/packages/saos-06-05-00-0043"
    operation="upgrade"
    serviceAffecting="yes"
  ></XmlCmdPlatformClass>
</XmlWwpCommandFile>
```

Command file types

You can create additional command files for specific devices or platform classes. Device specific command files are named with the device MAC address, such as:

- 0002a1010203.xml

Platform class command files are named as follows:

- artimir.xml - for CN 3911 and CN 3920 platforms.
- brego.xml - for CN 3940, CN 3960, and CN 5140 platforms.

You can run command files from the CLI or with a DHCP server. To run the command file from the command line:

```
> software run command-file <FileName> server <IpAddress>
```

Configure the DHCP server settings as follows:

- Next Server (option -14): Specifies the IP address of the TFTP server.
- Boot File (option -1): Specifies the path to the command file directory or the full path to the command file itself.

CORRECT:

```
ciena/cmd/  
ciena/packages/saos-<build>/  
ciena/cmd/0002a1010203.xml
```

INCORRECT:

```
ciena/cmd (missing the slash "/" at the end of the path
```

If you specify only the path of the command file, the device will search the directory for the most specific command file in the following order.

1. Device specific file named with its MAC address.
2. Platform class file for its platform, artimir.xml or brego.xml
3. Generic platform class file, le-lnx.xml

Once the most specific command file has been selected, the device runs the section of the command file with the most specific platform class. So, if the command file has an artimir section and an le-lnx section, the device will process the artimir section, and skip the le-lnx section.



NOTE: For CN 3911 or CN 3920 devices running system software 6.3.1 or earlier, only the device specific and generic platform files are supported. Also, the le-lnx platform class must exist within the command file.

Upgrading from a Previous Version of SAOS

There are several methods to upgrade the system software. The upgrade process can be triggered by a DHCP server or from the CLI. In addition, the upgrade process can be accomplished without the use of a command file.



CAUTION: The instructions in this section assume you are upgrading from 6.3.1 or higher.



NOTE: After upgrading SAOS, configuration changes that are saved to the configuration file may not be backwards compatible. If a downgrade occurs, such changes can cause configuration errors after a re-boot.



NOTE: Packages must be located in the <tftpboot>/ciena/packages/saos-<build> directory on the TFTP server or the upgrade will fail.

The following is an example of a SAOS Command File for upgrading:

```
<XmlWwpCommandFile>
  <XmlCmdPlatformClass name="le-lnx"
    version="saos-06-05-00-0043"
    packagePath="ciena/packages/saos-06-05-00-0043"
    operation="upgrade"
    serviceAffecting="yes"
  ></XmlCmdPlatformClass>
  <XmlCmdPlatformClass name="artamir"
    version="saos-06-05-00-0043"
    packagePath="ciena/packages/saos-06-05-00-0043"
    operation="upgrade"
    serviceAffecting="yes"
  ></XmlCmdPlatformClass>
  <XmlCmdPlatformClass name="brego"
    version="saos-06-05-00-0043"
    packagePath="ciena/packages/saos-06-05-00-0043"
    operation="upgrade"
    serviceAffecting="yes"
  ></XmlCmdPlatformClass>
</XmlWwpCommandFile>
```

The following is a list of the Command File Syntax.
Possible values for the configFileRule attribute:

- install
 - Download the config file from the server.
 - Store the file in the directory '/flash0/config'
 - Store the new filename as 'default-load-file'
 - Store the old file as 'last-config-file'
 - This file will be loaded when the device is rebooted.
- activate
 - Same behavior as install.
 - In addition, the file is activated (loaded) immediately.
 - This may require a reboot.
 - Reboot will not occur unless "serviceAffecting" is specified.
- augment
 - Download the config file.
 - Augment the current system configuration with the commands in this file.

- Configuration is NOT saved.
- augmentAndSave
 - Download the config file.
 - Augment the current system configuration with the commands in this file.
 - Save the resulting configuration to the file 'default-save-filename'.
 - No backup configuration is saved, the configuration that is updated.

Possible values for the operation attribute:

- upgrade
 - Download and install image files if necessary.
 - Activate the new image files.
 - This operation may require a reboot.
 - Reboot will not occur unless serviceAffecting="yes"
- x-grade
 - Download package PMF file from TFTP server.
 - Download all images files specified in the PMF file.
These files are stored in the RAM disk.
 - No further action is taken until the reboot command is given.
 - Erase flash and burn new image files into flash.
 - Supported for backwards compatibility with previous release.



NOTE: If you intend to upgrade software AND system configuration with the same command file, do NOT use 'activate' for the configFileRule.

Instead of using activate for the configFileRule when upgrading software AND system configuration with the same command file, use one of the following combinations:

1. configFileRule="install" operation="install"
This combination installs a new configuration file in flash, installs new software, then stops. The user must then activate the new software by rebooting device.
2. configFileRule="install" operation="activate"
Installs a new configuration file, installs the new software, then reboots the device.
3. configFileRule="augmentAndSave" operation="activate"
Augments the configuration, saves it, upgrades the software, then reboots the device.

Upgrading Using the CLI and a Command File

The following commands can be run using any user account with a privilege level of super-user.

1. Ensure that the device has access to the TFTP server.
2. Using the CLI, perform a configuration save using the configuration save command.
3. Enter the following command to run the command file, specifying the desired directory, command file, and TFTP server IP address:

```
> software run command-file ciena/packages/saos-##-##-##-####/xx.xml server <TFTP Server IP>
```

The upgrade process begins immediately and may take up to 10 minutes to complete.

Upgrading Using the CLI without a Command File

The following commands can be run using any user account with a privilege level of super-user.



CAUTION: The upgrade process described in this section will cause the system to reboot automatically.

1. Ensure that the device has access to the TFTP server.
2. Using the CLI, perform a configuration save using the `configuration save` command.
3. Enter the following command:
 - To cause the device to upgrade the system software and to reboot automatically, enter the following command, specifying the desired software package and TFTP server IP address:

```
> software upgrade package saos-##-##-##-#### server 1.2.3.4 service-disruption allow
```



NOTE: The upgrade process may take up to 10 minutes to complete.

Upgrading Using a DHCP server

This method of upgrade uses a DHCP server to trigger the upgrade process through the use of a command file.

1. Configure the DHCP server according to the instructions found in the **Configuring DHCP** section on page 23.
2. Enable the DHCP client on the SAOS device using the CLI command `dhcp client enable`.
3. Perform a configuration save (e.g., from the CLI use the `configuration save` command).
4. The upgrade process will begin as soon as a DHCP renew occurs and may take up to 10 minutes to complete.

Use the DHCP option 'bootfile' to run a command file. A fully qualified filename (path1/path2/file.xml) can be used or a directory name such as "Path1/path2/" can be specified. Path names **MUST** end with a slash to distinguish them from a file name. Some examples:

- bootfile = "ciena/packages/saos-06-04-00-0032/"
- bootfile = "ciena/packages/saos-06-04-00-0032/command-06-03-00-0032.xml"
- bootfile = "cmd/my-command-file.xml"

If you specify a directory as the bootfile, the device will try to download the file MAC.xml where MAC is the Ethernet MAC address of the device (i.e. 0002a1010203.xml). If that fails, the device will try to download the file le-lnx.xml file.



NOTE: When a configuration file is processed due to a request from DHCP, the device will save the filename (last-config-file) and it will not process the same file name twice. You need to reset this file name in order to process the same configuration file a second time. The same is true for the command file name as well.

Backup Software Images

The CN 3940, CN 3960, and CN 5140 have two flash image banks instead of a single flash image bank. The second image bank holds a backup copy of the system software. If the primary image bank becomes corrupted, the system will automatically switch to the backup bank.

When the software upgrade command is used, the new software is installed in one image bank only. The old software remains in the other image bank. Once the new software is installed and running, the user can backup the new software as follows:

```
> software protect
```

It is highly recommended (but not required) to run the protect command after each upgrade.

The software show command displays information for both flash image banks:

```
> software show
```

```
+-----+
| Installed Package   : saos-06-05-00-0040 |
| Running Package    : saos-06-05-00-0040 |
| Application Build   : 3507               |
| Package Build Info  : Wed Feb 11 02:50:42 2009 shdbuilder tango.ciena.com |
| Running Kernel      : 2.6.26.6-3507      |
| Running MIB version : 02-03-07-0005      |
+-----+
| Running bank        : B                   |
| Bank package version: saos-06-05-00-0040 |
| Bootloader version  : 3454               |
| Bootloader status   : valid              |
| Standby bank        : A                   |
| Bank package version: saos-06-05-00-0040 |
| Bootloader version  : 3516               |
| Bootloader status   : valid              |
+-----+
| Last command file: unknown                |
| Last configuration file: unknown           |
+-----+
```

The following command will download and install software into flash but will not reboot the device. The system will load the new software when the device is later rebooted or power cycled:

```
> software install package saos-06-04-00-0134 server 1.2.3.4
```

Appendix Command Line Interface

26

This appendix describes the operating system commands and syntax.

Overview

The Command Line Interface (CLI) is a text-based command interface used to configure the device and to view system information.



NOTE: The CLI hides commands depending on user access level, installed licenses, and platform.

This appendix includes the following topics:

- **Access Levels**
- **Accessing the CLI**
- **Navigating the CLI**
- **Deprecated Commands**
- **Global Commands**
- **Protocol/Manager Commands**



CAUTION: Commands not documented in this appendix should not be used. If you choose to use them, you do so at your own risk as they can cause severe interruption of delivered services and access to the device.

Access Levels

When a user account is created, it is assigned an access level. The CLI provides two access levels, including:

- **Limited User** (lu) - able to execute commands that do not change the state of the system in a significant way or change the configuration of the device.
- **Super User** (su) - includes all the privileges of the limited user and can make significant system state changes, modify the device configuration, and perform execute commands including creating user accounts.

The CLI provides two default user names/passwords:

User Name	Access Level	Password	Access Rights
su	Super User (su)	wwp	Read/Write
user	Limited User (lu)	<empty>	Read-Only

Accessing the CLI

To access CLI commands, a session must first be established with the device by establishing a Telnet session or through direct connection to the serial console port.



NOTE: A maximum of 6 Telnet sessions can be connected at the same time.

Accessing the CLI Using Telnet

To access the device through Telnet, the device must have an IP address, the Telnet client must have a route set up to allow access to the device, and the user must have a valid user name and password to log into the system.

All devices coming out of manufacturing have a hard coded IP address, 172.16.233.214. This IP address should be used when connecting to a device that has not gone through a DHCP process.

If the device has gone through the DHCP process, the DHCP server assigns an IP address based on the device's MAC address. The MAC address is the same as the device's serial number.

To access the CLI using Telnet:

1. Determine the IP address for the device.
2. Obtain a valid user name and logon password.
3. Configure default gateway setup to access the device.
4. Use a Telnet client to connect to the device.
5. At the logon prompt, enter a user name and then a password to access the prompt, for example:

```
username: su
password:
```

```
>
```


Accessing the CLI Using the Serial Console Port

By default, the serial console port is enabled.

1. Connect a terminal or PC running terminal emulation software to the serial console port using an RJ-45 cable.
2. Configure the connected terminal with the following settings:
 - Character size = 8
 - Parity = None
 - Stop Bit = 1
 - Baud Rate = 9600 bps
 - Control = None
3. At the logon prompt, enter a user name and then a password to access the prompt, for example:

```
username: su
password:
```

```
>
```

Navigating the CLI

When entering a command at the prompt, ensure that you have the appropriate access level. Most configuration commands require the super-user access level. At any prompt, press the **Tab** key for a list of commands in alphabetical order available from the current prompt. For example, pressing tab on the main level menu lists the following:

```
>
arp                - arp
blade              - blade management
chassis            - chassis management
cli                - cli shell special functions
configuration      - configuration
device-archive     - device archive
dhcp               - dhcp commands
file               - file submenu
flow               - flow management
interface          - ip interface management
lldp               - Link Layer Discovery Protocol
log                - log
logout             - Log off this system
ntp-client          - ntp-client
ping               - ping
port               - port
reboot             - reboot system
snmp               - SNMP
software           - software version management
syslog             - syslog
system             - system management
traceroute         - traceroute a packet
user               - user management
vlan               - vlan
```

Command Schema

In order to provide consistency across all the commands, all CLI commands follow a basic underlying schema or syntax:

```
<object> [<subobject>] <action> [instance] [<attributes>]
```

An <object> can identify a feature (e.g. multicast, epr, radius etc.) or a basic object (e.g. module, VLAN, port, etc.). On the surface, these seem like completely mismatched entities, however, if a device is considered to have an instance of each of these entities, then both features and the basic system objects can be considered as objects.

A <subobject> subdivides a feature. For example, multicast has many sub-features in it such as umf, epf, channel-stream, etc.

An <action> is a verb that describes the type of action that will occur on the object/instance that is specified. Examples of actions are:

- create
- delete
- add
- remove
- set
- unset
- enable
- disable
- attach
- detach

An <instance> defines an recurrence of an object. For example, ports have multiple instances. A feature like radius is an object but there is only a single instance of it. An instance is identified by a keyword and a value, such as “port 3/1.”

<attributes> are always a pairing of a keyword and a value. For example, the keyword “port” is followed by a value such as 3/1. A command may take multiple attributes and the attributes can be specified in any order relative to one another.

As an example, breaking down the command grammar of a command such as “aggregation add agg Lag1 port 7/2” yields the following:

- object = aggregation
- subobject = none
- action = add
- instance = agg Lag1
- attribute = port 7/2

Sub-menus

Objects and sub-objects have sub-menus. For example, from the top-level prompt, if you enter `system`, the prompt changes to the system sub-menu and displays, `(system)>`. The same is true for sub-features, such as system shell. At the `(system)>` prompt, entering `shell` the prompt changes to the shell sub-menu under system and displays `(system/shell)>`. To return to the top-level prompt from any sub-menu, type `exit`, and press **Enter**.

Command Completion

The CLI supports partial command recognition. This means that you can enter the first few characters that uniquely identify a command for the system to recognize it. For example, for the sub-port commands, you can enter:

```
> vl
```

and the prompt will then change to:

```
CLI(vlan)>
```

If you do not enter enough characters to uniquely identify the command, a shell parser error will occur. For example:

```
> s
SHELL PARSER FAILURE: 's' - ambiguous input
```

This error occurs, because multiple commands begin with “s”. Pressing the **Tab** key partially completes the command and displays the available commands. For example,:

```
>s

snmp                software                system
```

In addition, pressing space and then **Tab** twice at the end of the command string displays available actions, objects, or sub-objects, for example:

```
>arp <Tab>
arp
>arp <Tab>
delete                - delete arp entry
flush                 - flush arp cache for all interfaces
for                   - check if the ip address is in use
in-use                - check if the ip address is in use
show                  - show arp information
```

After specifying the object, action, instance, and even attributes, you can press space and then **Tab** to display additional parameters. For example,

```
>arp for
ip                    - IP address
```

Getting Help

To get more detail about available commands, enter `?` or `help` at any prompt. A command can also be followed by a space and a `?` or `help` to get a list of valid parameters for that command. For example, the following command lists all the valid parameters for the `arp` command:

```
>arp
delete                - delete arp entry
flush                 - flush arp cache for all interfaces
for                   - check if the ip address is in use
in-use                - check if the ip address is in use
show                  - show arp information
```

In addition, you can display specific objects or search on specific keywords with the `cli` search and show commands described in the `cli` command section of this chapter.

Command Response

In general, errors are generated for a configuration command only when the command is unsuccessful. For example, if you run a delete command, the CLI responds without any message and returns to the CLI prompt. Even if the object does not exist, the command does not end in error, because the end result is that the specified object does not exist in the system. Similarly, if you attempt set an attribute that is already set, the CLI responds by returning you to the CLI prompt. If you attempt to create an object that already exists, the CLI responds with an error to show the duplication.

Understanding Command Syntax

A variety of symbols are used to indicate CLI command syntax. These symbols describe how to enter a command. They are not entered as part of the command itself. Table 1 summarizes command syntax symbols.

Table 26-1: Command Syntax Symbols

Symbol	Description
< >	Encloses a variable or literal value that must be specified. Some examples include: <pre>server <IpAddress> priority <NUMBER: 1-7> dns <on off> description <String[31]></pre> For <code>server <IpAddress></code>, the attribute could be entered as <code>server 10.10.11.100</code> or <code>server www.ciena.com</code>. With <code>priority <NUMBER: 1-7></code> the text within <> indicates that 1 - 7 are valid values. In the example of <code>dns <on off></code>, either the literal value of on or off is valid, such as <code>dns on</code>. For <code>description <String[31]></code>, any string of up to 31 characters is entered.
{ }	Encloses a required value or list of required arguments. One or more values or arguments can be specified. For example, in the syntax: <pre>flow access-control create {port <PortName>} {max-dynamic-macs <NUMBER>} [forward-unlearned <on off>]</pre> The port and max-dynamic-max arguments are required. The forward-unlearned argument is optional.
	Separates mutually exclusive items in a list, only one of which can be entered. For example, in the syntax: <pre>dhcp client options set subnet <on off></pre> either on or off must be specified, for example: <pre>dhcp client options set subnet on</pre>
[]	Encloses an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the syntax: <pre>arp show [interface <Interface>]</pre> you can enter a value for interface <Interface> or not. For example: <code>arp show</code>
{ [], [], [] }	Specifies a list of optional items where at least one must be specified.

Table 26-1: Command Syntax Symbols

...	Indicates the example has been abbreviated and that the actual display contains more information.
*	Indicates zero or more occurrences of what is preceding.

Specifying Multiple Objects with Lists and Ranges

To simplify configuration of multiple objects, some CLI commands allow actions to be specified on multiple ports or slots at once. This is done using object lists and ranges. Each command specifies the CLI variables it accepts.

A list of objects can be specified using a comma-delimited list (for example, x, y, z). A range of objects can be specified using a dash (-). For example, "x-z" would properly specify a range.

On a multi-module device, a command can apply to multiple modules by specifying a slot list or range. For example, "1,2,3" or "1-3". Ports on the module are then specified relative to the module. For example, port 1/1 identifies the first port on module in slot 1. Port ranges are generally specified as: <port a>-<port b>. This range specifies all the ports between and including ports 'a' and 'b'. So the range "1/1 - 4/3" would include all the ports present on modules in slots 1, 2, 3 as well as the first 3 ports on the module in slot 4. Lists of ports can be specified as being comma delimited, e.g. "1/1, 1/3, 1/5". Port lists and ranges can also be combined so that the following is valid, "1/1-1/5,1/7". For a single module device, ports are enumerated with a single ID, e.g. 1, 2, and 3. Lists of ports can be specified as being comma delimited, e.g. "1, 3, 5." Port lists and ranges can also be combined so that the following is valid, "1-4, 7."

For example, the vlan command could be used as follows:

```
> vlan add vlan 400 port 2,4
```

Or each command could be entered individually:

```
> vlan add vlan 400 port 2
```

```
> vlan add vlan 400 port 4
```

Specifying IP Addresses

The format for the IpAddress is:

<IpAddress>=<NUMBER STRING: xxx.xxx.xxx.xxx, 0<=xxx<=255>

The syntax description from RFC 1035 is as follows:

<domain>::= <subdomain>| ""

<subdomain>::= <label>|<subdomain> "." <label>

<label>::= <letter> [[<ldh-str>] <let-dig>]

<ldh-st> ::= <let-dig-hyp>|<let-dig-hyp> <ldh-str>

<let-dig-hyp> ::= <let-dig>| "-"

<let-dig> ::= <letter>|<digit>

<letter> ::= any one of the 52 alphabetic characters A through Z in upper case and a through z in lower case

<digit> ::= any one of the ten digits 0 through 9

RFC 3696 (Application Techniques for Checking and Transformation of Names) describes the above situation as follows:

“The LDH rule, as updated, provides that the labels (words or strings separated by periods) that make up a domain name must consist of only the ASCII [ASCII] alphabetic and numeric characters, plus the hyphen. No other symbols or punctuation characters are permitted, nor is blank space. If the hyphen is used, it is not permitted to appear at either the beginning or end of a label. There is an additional rule that essentially requires that top-level domain names not be all- numeric.”

Additionally a fully qualified domain name may contain up to 255 characters including '.' and must not be all digits.

Entering Names

When entering names or description the following rules apply:

- String length > 0
- First character may not be a space
- Last character may not be a space
- All characters are in the ASCII range 32...126
- The following characters are not allowed:
 - "
 - %
 - *
 - ?
 - !
- Names are case-sensitive

Specifying Common Objects and Attributes

<FileName>= <String> for example, /flash0/file.txt

<DirName> = <String[127]>

<MacAddress>= <xx:xx:xx:xx:xx:xx>

Deprecated Commands

Some commands are designated as deprecated (obsolete). Deprecated commands are still supported by the CLI and work for configuration. However, in a future release, deprecated commands will no longer be supported. These commands can be identified in the command list with the text “(DEPRECATED)”. In addition to commands, parameters for some commands are designated as deprecated.



NOTE: All commands deprecated in past releases have been removed from this release and are no longer supported.

Global Commands

Various global commands are supported that are common to the computing industry. These commands do not follow the defined schema and use a standard UNIX-type implementation. You can run these commands from any menu shell. Some global commands related to file management are listed under the “file” command menu, however, you do not have to type “file” preceding the commands.

Command	Description	Access Level	Release Introduced
clear	Clears the terminal screen.	su/lu	6.0
Example:			
> clear			
exit	Log off and end the Telnet session.	su/lu	6.2
Example:			
> exit			
Goodbye.			
Connection to host lost.			
ping [ip] <IpAddress>	Ping the specified IP address. Attributes are expressed as integers in the following units:	su/lu	6.0
[count <NUMBER: 1-100000>]	number of packets to send		6.0
[interval <NUMBER: 1-100000>]	interval (in milliseconds)		6.0
[packet-size <NUMBER: 1-1464>]	packet-size (in kilobytes)		6.0
[timeout <NUMBER: 1-100000>]	timeout (in milliseconds).		6.0

Command	Description	Access Level	Release Introduced

Example:

```
>ping ip 192.168.76.100
PING 192.168.76.100 (192.168.76.100): 56 data bytes

ping: sendto: Network is unreachable
```

reboot	Performs a soft reset of the system including the kernel.	su	6.0
telnet	Establishes Telnet client session to the specified IP address.	su/lu	6.3
[-l <UserName>]	Logs in with the specified user. If left unspecified, the remote system prompts for the user name.		6.3
{<IpAddress>}	IP address to Telnet to.		6.3
[<port>]	TCP port. By default, the port is 23.		6.3

Example:

```
> telnet 10.10.121.19

Entering character mode
Escape character is '^]'.

3911 00:02:A1:24:0E:30
SAOS is True Carrier Ethernet TM software.

3911 login: su
Password:

SAOS is True Carrier Ethernet TM software.

Welcome to the shell.
> exit

Goodbye.
>
```

traceroute [ip] <IpAddress>	Performs a standard traceroute for the specified ip address.	su/lu	6.0
[-F]	Set the don't fragment bit.		6.0
[-I]	Use ICMP ECHO instead of UDP datagrams.		6.0
[-l]	Display the ttl value of the returned packet.		6.0
[-d]	Set SO_DEBUG options to socket.		6.0
[-n]	Print hop addresses numerically rather than symbolically.		6.0
[-r]	Bypass the normal routing tables and send directly to a host.		6.0

Command	Description	Access Level	Release Introduced
[-v]	• Verbose.		6.0
[-m max_ttl]	• Max time-to-live (max number of hops).		6.0
[-p port#]	• Base UDP port number used in probes (default is 33434).		6.0
[-q nqueries]	• Number of probes per 'ttl' (default is 3).		6.0
[-s src_addr]	• IP address to use as the source address.		6.0
[-t tos]	• Type-of-service in probe packets (default 0).		6.0
[-w wait]	• Time in seconds to wait for a response (default is 3 seconds).		6.0
[-g]	• Loose source route gateway (8 max).		6.0

Example:

```
> traceroute ip 192.168.54.241
traceroute to 192.168.54.241 (192.168.54.241), 30 hops max, 40 byte packets
 1: 192.168.54.241 4087 us 1811 us 1811 us
```

Protocol/Manager Commands

Protocol/Manager commands are those commands that configure system operation.

Table 26-2: Summary of Protocol/Manager Commands

Command	Description	Release Introduced
aggregation	Enter the link aggregation menu	6.4
arp	Enter the ARP menu	6.0
blade	Enter the blade menu	6.0
broadcast-containment	Enter the broadcast containment menu	6.2
cfm	Enter the Connectivity Fault Management (CFM) menu	6.2
chassis	Enter the chassis menu	6.0
cli	Search or display CLI shell commands	6.0
command-log	Enter the command logging menu	6.5
configuration	Applies, saves, resets, and displays configuration	6.0
device-archive	Enters the device-archive menu	6.0
dhcp	Enter the DHCP menu	6.0

Table 26-2: Summary of Protocol/Manager Commands

dns client	Enter the DNS menu	6.2
dot1x	Enter the 802.1x menu	6.4
eoam	Enter the OAM menu	6.2
file	Enter the file menu	6.0
flow	Enter flow menu	6.0
interface	Enter the interface menu	6.0
lldp	Enter the LLDP menu	6.0
log	Enter the logging menu	6.0
mstp	Enter the MSTP menu	6.3
multicast-services	Enter the Multicast Services menu	6.0
ntp-client	Enter the NTP menu	6.0
PBT	Enter the PBT menu	6.4
port	Enter the port menu	6.0
radius	Enter the RADIUS menu	6.3
rmon	Enter the RMON menu	6.2
snmp	Enter the SNMP menu	6.0
software	Enter the software management menu	6.0
ssh	Enter the Secure Shell (SSH) menu	6.2
system	Enter the system menu	6.0
tacacs	Enter the TACACS+ menu	6.3
telnet-server	Enter the Telnet server menu	6.3
traffic-profiling	Enter the traffic profiling menu	6.2
twamp	Enter the TWAMP menu	6.2
user	Enter the user menu	6.0
virtual-circuit	Enter the virtual circuit menu	6.0
virtual-switch	Enter the virtual switch menu	6.0
vlan	Enter the VLAN menu	6.0

aggregation

Command	Description	Security Level	Release Introduced
aggregation add agg <LagPortName[7]> [[port <PhyPortNameList>] [protection-port <PhyPortNameList>]]	Adds a port and protection port to an aggregation.	su	6.4
Example:			
> aggregation add agg lag21 port 1-4			
aggregation create agg <LagPortName[7]>	Creates an aggregation group.	su	6.4
Example:			
> aggregation create agg lag22			
aggregation delete agg <LagPortName[7]>	Deletes an aggregation.	su	6.4
Example:			
> aggregation delete agg lag22			
aggregation disable	Disables aggregation globally. Note that remote connections between Juniper devices are lost after disabling link aggregation. Juniper devices should be set to manual mode with the interfaces <agg group> aggregated-ether-options lacp command.	su	6.4
Example:			
> aggregation disable			
aggregation enable	Enables aggregation globally. Aggregation is enabled by default.	su	6.4
Example:			
> aggregation enable			
aggregation lacpmib set agg <LagPortName[7]>	Sets the LACP MIB attributes for the specified aggregator port, including:	su	6.4
[[admin-key <NUMBER: 0 - 4095>],	• Administrator key		6.4
[system-priority <NUMBER: 0 - 65535>]]	• System priority.		6.4
Example:			
> aggregation lacpmib set agg ManLag1 admin-key 2050			
aggregation lacpmib set port <PhyPortName>	Sets LACP MIB group attributes for the specified physical ports, including:	su	6.4
[[actor-admin-key <NUMBER: 0-4095>]	• Actor Administrator key.		6.4

[actor-admin-state <NUMBER: 0-255>]	• Actor Administrator state.	6.4
[actor-port-priority <NUMBER: 0-65535>]	• Actor port priority.	6.4
[actor-system-priority <NUMBER: 0-65535>]	• Actor system priority.	6.4
[partner-admin-key <NUMBER: 0-4095>]	• Partner administrator key.	6.4
[partner-admin-state <NUMBER: 0-255>]	• Partner administrator state.	6.4
[partner-port-priority <NUMBER: 0-65535>]	• Partner port priority.	6.4
[partner-system-id <MacAddress>]	• Partner system identification, MAC address.	6.4
partner-system-priority <NUMBER: 0-65535>	• Partner system priority.	6.4

Example:

```
> aggregation lacpmib set port 5 actor-admin-key 2050
```

aggregation remove agg <LagPortName[7]> port <PhyPortNameList>	Removes physical ports from an aggregation	su	6.4

Example:

```
> aggregation remove agg lag21 port 4
```

aggregation set marker-timeout <NUMBER: 0-1000>	Sets the marker timeout in milliseconds. The default is 50(ms).	su	6.4

Example:

```
> aggregation set marker-timeout 100
```

aggregation set agg <LagPortName[7]>	Displays the aggregation attributes for the aggregator port.	su	6.4

mode <lacp manual>	• Mode.	6.4

revert-delay <NUMBER: 0-60000>	• Revert delay, default: 5000(ms).	6.4

revert-protection <on off>	• Revert protection.	6.4

Example:

```
> aggregation set agg ManLag1 mode manual
```

aggregation set port <PhyPortNameList> agg-mode <lacp manual>	Sets the aggregation mode for the specified list of physical ports.	su	6.4

Example:

```
> aggregation set port 7 agg-mode lacp
```

aggregation show [member] [state]	Shows general aggregation information. Optionally, displays aggregation member information and state.	su/lu	6.4

Example:

```
> aggregation show state
```

Parameter	Aggregation State	Value
Bridge Aggregation Admin	Disabled	
Aggregation Group Created	0	
Time Since Last Update	003 days 19:56:01	
Time Since Last Selection	001 days 21:37:11	
Marker Frame Timeout	50 (ms)	
Total Selection Sm Called	21	

aggregation show agg <LagPortName[7]> [info] [mode]	Displays information and mode for the specified aggregator port.	su/lu	6.4

Example:

```
> aggregation show
```

aggregation show port <PhyPortNameList> [agg-mode] [info]	Displays information and aggregation mode for the specified list of physical ports.	su/lu	6.4

Example:

```
> aggregation show port 1 agg-mode
Physical Port configured in LACP mode
```

arp

Address resolution protocol (ARP) maps an IP address to a physical MAC address.

Command	Description	Access Level	Release Introduced
arp delete ip <IpAddress>	Deletes the specified IP address from the ARP table. This command checks for entries in both tables.	su	6.0
Example:			
<pre>>arp delete ip 1.1.1.1</pre>			
arp flush [intf <remote>]	Flush the specified ARP entry from the ARP table.	su	6.0
Example:			
<pre>>arp flush interface remote</pre>			
arp for ip <IpAddress> [interface <remote>]	Checks to see if the specified IP address is in use.	su/lu	6.0
Example:			
<pre>>arp for ip 1.1.1.1</pre>			
arp in-use ip <IpAddress> [interface <remote>]	Checks to see if the specified IP address is in use.	su/lu	6.0

Example:

```
>arp in-use ip 1.1.1.1
```

arp set cachetime <60-3600>	Configure the ARP timeout.	su/lu	6.4.1

Example:

```
>arp set cachetime 200
```

arp show [intf <remote>]	Shows ARP information with the optional ability to specify an interface.	su/lu	6.0

Example:

```
> arp show
```

```

+----- ARP TABLE -----+
| IP Address      | MAC Address      | Type | Interface |
+-----+-----+
| 172.26.0.1      | 00:01:f4:06:52:c0 | dyn  | tap1 (0)  |
+-----+-----+

```

blade

Command	Description	Access Level	Release Introduced
blade show	Displays a summary of blade information, optionally displays details, including:	su/lu	6.0
[attributes]	Attributes for hardware device identification.		6.0
[capabilities]	Capabilities of the board, ports, and global flow and core switch.		6.0
[information]	General blade information		6.0
[state]	Administrative and operational states.		6.0

Example:

```
>blade show
```

```

+----- BLADE SUMMARY -----+
| Slot | Ports | PortBaseMac      | BladeType | OperState |
+-----+-----+
| 1    | 10    | 00:02:a1:07:a4:a2 | Single    | Enabled   |
+-----+-----+

```

broadcast-containment



NOTE: To enable broadcast containment commands, the Advanced Ethernet feature license must be installed with the software license install command.

Command	Description	Access Level	Release Introduced
broadcast-containment enable	Enables broadcast containment.	su	6.2
Example:			
> broadcast-containment enable			
broadcast-containment disable	Disables broadcast containment.	su	6.2
Example:			
> broadcast-containment disable			
broadcast-containment add	Adds ports to an existing broadcast containment filter specified by:	su	6.2
{filter <String>}	Filter name.		6.2
{port <PortNameList>}	Port name list.		6.2
Example:			
> broadcast-containment disable			
broadcast-containment create	Creates a broadcast containment filter specified by:	su	6.2
{filter <String>}	Filter name.		6.2
[kbps <NUMBER: 0-10000000>]	Rate from 0-10000000 in kilobits per second.		6.2
[port <PortNameList>]	Port name list.		6.2
[containment-classification <bcast l2-mcast unknown-ucast>]	Specifies a flood traffic type to filter, Unknown unicast traffic (unknown-ucast), Layer 2 Broadcast traffic (bcast), or Layer 2 Unknown Multicast traffic (l2-mcast). By default, the filtered traffic types are Layer 2 Broadcast traffic (bcast) and Layer 2 Unknown Multicast traffic (l2-mcast).		6.5
Example:			
> broadcast-containment create filter denial kbps 2000 port 1			
broadcast-containment delete	Deletes an existing broadcast containment filter specified by:	su	6.2
{filter <String>}	Filter name.		6.2
Example:			
> broadcast-containment delete filter			

broadcast-containment remove	Removes ports from a broadcast containment filter specified by:	su	6.2
{filter <String>}	Filter name.		6.2
[port <PortNameList>]	Port name list.		6.2

Example:

```
> broadcast-containment remove filter denial port 1
```

broadcast-containment set	Sets the attributes for a broadcast containment filter:	su	6.2
{filter <String>}	Filter name.		6.2
[kbps <NUMBER: 0-10000000>]	Rate from 0-10000000 in kilobits per second.		6.2
[port <PortNameList>]	Port name list.		6.2
[containment-classification <[bcast],[l2-mcast],[unknown-ucast]>]	Specifies a flood traffic type to filter, Unknown unicast traffic (unknown-ucast), Layer 2 Broadcast traffic (bcast), or Layer 2 Unknown Multicast traffic (l2-mcast). By default, the filtered traffic types are Layer 2 Broadcast traffic (bcast) and Layer 2 Unknown Multicast traffic (l2-mcast).		6.5

Example:

```
> broadcast-containment create filter denial kbps 2000 port 1
```

broadcast-containment show	Displays global broadcast containment status along with a summary of the configured broadcast containment filter. Optionally, displays:	su	6.2
[filter <String>]	Details about a specific filter.		6.2
[port <PortNameList>]	Filter membership for specified ports.		6.2

Example:

```
> broadcast-containment show
+----- Broadcast Containment Globals -----+
|      Parameter      |      Value      |
+-----+-----+
| Admin Status        | Enabled          |
+-----+-----+

+----- Broadcast Containment Filters -----+
|      Filter      | ID | Kbps | Dropping |
+-----+-----+-----+-----+
| Denial            | 1  | 2000 | No        |
+-----+-----+-----+-----+
```


cfm



NOTE: To enable CFM commands, the Advanced OAM feature license must be installed with the software license install command.

Command	Description	Security Level	Release Introduced
cfm clear statistics	Clears CFM statistics.	su	6.2
Example:			
> cfm clear statistics			
cfm disable	Globally disable CFM.	su	6.2
Example:			
> cfm disable			
cfm enable	Globally enable CFM.	su	6.2
Example:			
> cfm enable			
cfm set	Set global CFM attributes:	su	6.2
[[dot1ad-strict <on off>],	When enabled, only CFM frames that contain a single VLAN tag or are untagged are recognized as CFM frames. A double-tagged CFM frame will be forwarded as a normal data frame on interfaces containing MEPs and/or MIPs, and CFM processing is bypassed.		6.5
[ethertype <NUMBER: 2048...65535>],	CFM frame Ethertype.		6.2
[mip-level-enforcement <on off>],	Set MIPs to only process CFM frames at their configured MD level (on) or at all levels (off). Default is off.		6.5
[rmep-hold-time <NUMBER: 10-300000>],	MEP inactive state hold-time (ms).		6.2
[y1731ethertype <NUMBER: 2048...65535>]]	CFM Y.1731 Ethertype.		6.5
Example:			
> cfm set ethertype 35272 rmep-hold-time 300000			
cfm linktrace clear [service <CFMServiceName>]	Clears CFM linktrace statistics. Optionally, clears statistics for a specific service.	su	6.2
[statistics]	Clears all statistics		6.2

[port <PortName>][mepid <NUMBER: 1-8191>][statistics][vlan <Vlan>]] [statistics]	• Clears statistics for a specific MEP.	6.2

Example:

```
> cfm linktrace clear
> cfm linktrace clear service CFM-1 mepid 12 statistics
```

cfm linktrace send service <CFMServiceName> {local-mepid <NUMBER: 1-8191> port <PortName> [vlan <Vlan>]]	Sends a Linktrace Request message from a CFM service to a remote MEP. Command attributes include:	su	6.2
{mepid <NUMBER: 1-8191>}	• Remote MEP identifier to send to.		6.2
[ttl <NUMBER: 1-255>]	• Initial value for the Time To Live (TTL) field, which limits the number of hops that the Linktrace Request message can propagate through the network.		6.2
[priority <NUMBER: 0-7>]	• Priority value used in the VLAN tag of the transmitted frame.		6.2
[fdb-only]	• Flag indicating that only the normal forwarding database should be used to look up the target MAC, and not the MEP CCM and MIP CCM databases that would also be used otherwise.		6.3.1

Example:

```
> cfm linktrace send service CFM-1 port 1 mepid 100
```

cfm linktrace send-mac service <CFMServiceName> {local-mepid <NUMBER: 1-8191> port <PortName> [vlan <Vlan>]]	Sends a Linktrace Request message from a CFM service to a MAC address. Command attributes include:	su	6.2
{mac <MacAddress>}	• MAC address to send to.		6.2
[ttl <NUMBER: 1-255>]	• Initial value for the Time To Live (TTL) field, which limits the number of hops that the Linktrace Request message can propagate through the network.		6.2
[priority <NUMBER: 0-7>]	• Priority value used in the VLAN tag of the transmitted frame.		6.2
[fdb-only]	• Flag indicating that only the normal forwarding database should be used to look up the target MAC, and not the MEP CCM and MIP CCM databases that would also be used otherwise.		6.3.1

Example:

```
> cfm linktrace send service CFM-1 mac 01:02:03:04:05:06
```

cfm linktrace show [service <String[16]> [port <PortName>][mepid <NUMBER: 1-8191>] [vlan <Vlan>]]	Show the Linktrace Replies associated with a previously transmitted Linktrace Request.	su	6.2

[order-by-mepid]	• Sort the results by MEP ID.	6.2
[exclude-evpl]	• Exclude EVPL entries.	6.2

Example:

```
> cfm link-trace show
```

```
+----- Linktrace Message -----+
--+
|      Service Name      |MepId|Logical Intf Name |  Target Mac  |Tr-Id|TxLtm|RxLtr|
|-----+-----+-----+-----+-----+-----+
--|
|Remote      |    66|      |      |      |    1|    0|    0|
|-----+-----+-----+-----+-----+
--|
|      Remote MP      |Relay |      Ingress TLV      |      Egress TLV      |
|Ttl| Mac Address |Action | Mac Address |Port |Action | Mac Address |Port |Action |
|-----+-----+-----+-----+-----+-----+
--+
| 63|00:B0:C7:07:E9:8C|FDB |      |    11|    0k|      |    11|    0k|
|-----+-----+-----+-----+-----+
--+
```

cfm loopback clear [service <CFMServiceName>]	Clears CFM loopback statistics. Optionally, clears statistics for a specific service.	su	6.2
[statistics]	• Clears all statistics		6.2
[port <PortName>][mepid <NUMBER: 1-8191>][statistics][vlan <Vlan>]] [statistics]	• Clears statistics for a specific MEP.		6.2

Example:

```
> cfm loopback clear
> cfm loopback clear service CFM-1 mepid 12 statistics
```

cfm loopback send service <CFMServiceName> {local-mepid <NUMBER: 1-8191> port <PortName> [vlan <Vlan>]}	Sends a Loopback message from a CFM service and port to a remote MEP. Command attributes include:	su	6.2
{mepid <NUMBER: 1-8191>}	• Remote MEP identifier to send to.		6.2
[count <NUMBER: 1-255>]	• Number of Loopback messages to send.		6.2
[priority <NUMBER: 0-7>]	• Priority value used in the VLAN tag of the transmitted frame.		6.2
[data <String [128]>]	• Loopback data to be included in each.		6.2

Example:

```
> cfm loopback send service CFM-1 port 1 mepid 100
```

cfm loopback send-mac service <String[16]> {local-mepid <NUMBER: 1-8191> port <PortName> [vlan <Vlan>]}	Send a Loopback Request message from a CFM service and port to a MAC address.	su	6.2
{mac <MacAddress>}	• MAC address to send to.		6.2

[count <NUMBER: 1-255>]	Number of Loopback messages to send.	6.2
[priority <NUMBER: 0-7>]	Priority value used in the VLAN tag of the transmitted frame.	6.2
[data <String [128]>]	Loopback data to be included in each.	6.2

Example:

```
> cfm loopback send service CFM-1 port 1 mac 01:02:03:04:05:06
```

cfm loopback show [service <String[16]>]	Displays Loopback Reply counters. Loopback Reply counters reflect success or failure of previously transmitted Loopback Request messages.	su	6.2
[order-by-mepid]	Sort the results by MEP ID.		6.2
[exclude-evpl]	Exclude EVPL entries.		6.2

Example:

```
> cfm loopback show
```

LOOPBACK MESSAGE INFORMATION						
Service Name	Interface	Remote Mac Address	Next LBM TransId	Tx LBM	Rx Order	LBR 000
Remote	rmtEgress		1	0	0	0

cfm delay clear [service <CFMServiceName>]	Clears CFM delay statistics. Optionally, clears statistics for a specific service.	su	6.2
[statistics]	Clears all statistics		6.2
[port <PortName>][mepid <NUMBER: 1-8191>][statistics][vlan <Vlan>]] [statistics]	Clears statistics for a specific MEP.		6.2

Example:

```
> cfm delay clear
> cfm delay clear service CFM-1 mepid 12 statistics
```

cfm delay cancel service <CFMServiceName> {local-mepid <NUMBER: 1-8191> port <PortName> [vlan <Vlan>]}	Cancels DMM to a remote MEP.	su	6.3
{mepid <NUMBER: 1-8191>}	Remote MEP identifier.		6.3

Example:

```
> cfm delay cancel service Remote local-mepid 1 mepid 100
```

cfm delay cancel-mac service <CFMServiceName> {local-mepid <NUMBER: 1-8191> port <PortName> [vlan <Vlan>]}	Cancels Delay Measurement Messages (DMMs) to a target MAC.	su	6.3
{mac <MacAddress>}	MAC address.		6.3

Example:

```
> cfm delay cancel service Remote local-mepid 1 mac 01:02:03:04:05:06
```

cfm delay send service <CFMServiceName> {local-mepid <NUMBER: 1-8191> port <PortName> [vlan <Vlan>]}	Sends DMMs to a remote MEP, specified by the following attributes:	su	6.3
[count <NUMBER: 2-600>]	• Number of DMMs to transmit.		6.3
[priority <NUMBER: 1-7>]	• DMM message priority.		6.3
[repeat <NUMBER: 1-7>]	• DMM test repeat time in minutes.		6.3
[delay-threshold <NUMBER>]	• Delay error threshold in microseconds.		6.3
[jitter-threshold <NUMBER>]	• Jitter error threshold in microseconds.		6.3

Example:

```
> cfm delay send service CFM-1 local-mepid 1 mepid 100
```

cfm delay send-mac service <CFMServiceName> {local-mepid <NUMBER: 1-8191> port <PortName> [vlan <Vlan>]}	Sends DMMs to a remote MAC, specified by the following attributes:	su	6.3
[count <NUMBER: 2-600>]	• Number of DMMs to transmit.		6.3
[priority <NUMBER: 1-7>]	• DMM message priority.		6.3
[repeat <NUMBER: 1-7>]	• DMM test repeat time in minutes.		6.3
[delay-threshold <NUMBER>]	• Delay error threshold in microseconds.		6.3
[jitter-threshold <NUMBER>]	• Jitter error threshold in microseconds.		6.3

Example:

```
> cfm delay send-mac service CFM-1 local-mepid 1 mac 01:02:03:04:05:06
```

cfm delay show	Displays DMM statistics.	su	6.3
[order-by-mepid]	• Sort the results by MEP ID.		
[exclude-evpl]	• Exclude EVPL entries.		
[service <CFMServiceName> [order-by- mepid][exclude-evpl]]	• Display DMM statistics for a specific service.		

Example:

```
> cfm delay show
```

```

+----- DELAY MEASUREMENT MESSAGE INFORMATION -----
+-----+
|          |Local| Remote      |Remote|Repeat| Delay  | Jitter | Tx  | Rx  | Rx  | Tx  |
| Service Name |MepId| Mac Address  |MepId |in min| in us  | in us  | Dmm | Dmr | Dmm | Dmr |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
|427_3300    |  200|00:00:00:00:00:00|    0|    0|    0|    0|  0|  0|  0|  0|
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+

```

cfm frame-loss clear [service <CFMServiceName>]	Clears CFM frame-loss statistics. Optionally, clears statistics for a specific service.	su	6.2
[statistics]	Clears all statistics		6.2
[port <PortName>][mepid <NUMBER: 1-8191>][statistics][vlan <Vlan>]] [statistics]	Clears statistics for a specific MEP.		6.2

Example:

```
> cfm frame-loss clear
> cfm frame-loss clear service CFM-1 mepid 12 statistics
```

cfm frame-loss cancel service <CFMServiceName> {local-mepid <NUMBER: 1-8191> port <PortName> [vlan <Vlan>]}	Cancels Loss Measurement Messages (LMMs) to a remote MEP specified by:	su	6.3
{mepid <NUMBER: 1-8191>}	Remote MEP identifier.		6.3

Example:

```
> cfm frame-loss cancel service CFM-1 local-mepid 1 mepid 100
```

cfm frame-loss cancel-mac service <CFMServiceName> {local-mepid <NUMBER: 1-8191> port <PortName> [vlan <Vlan>]}	Cancels LMMs to a target MAC address specified by:	su	6.3
{mac <MacAddress>}	MAC address.		6.3

Example:

```
> cfm frame-loss cancel
```

cfm frame-loss send service <CFMServiceName> {local-mepid <NUMBER: 1-8191> port <PortName> [vlan <Vlan>]}	Sends LMMs to a remote MEP specified by:	su	6.3
{mepid <NUMBER: 1-8191>}	Remote MEP identifier		6.3
[count <NUMBER: 2-600>]	Number of LMMs to transmit.		6.3
[priority <NUMBER: 1-7>]	LMM message priority.		6.3
[repeat <NUMBER: 0-1440>]	LMM test repeat time in minutes.		6.3
[fln-threshold <NUMBER: 0-600>]	Frame loss near error threshold.		6.3
[flf-threshold <NUMBER: 0-600>]	Frame loss far error threshold.		6.3

Example:

```
> cfm frame-loss send service CFM-1 local-mepid 1 mepid 100
```

cfm frame-loss send-mac service <CFMServiceName> {local-mepid <NUMBER: 1-8191> port <PortName> [vlan <Vlan>]}	Sends LMM to target MAC address specified by:	su	6.3
{mac <MacAddress>}	MAC address for the target.		6.3
[count <NUMBER: 2-600>]	Number of LMMs to transmit.		6.3
[priority <NUMBER: 1-7>]	LMM message priority.		6.3

[repeat <NUMBER: 0-1440>]	• LMM test repeat time in minutes.	6.3
[fln-threshold <NUMBER: 0-600>]	• Frame loss near error threshold.	6.3
[flf-threshold <NUMBER: 0-600>]	• Frame loss far error threshold.	6.3

Example:

```
> cfm frame-loss send-mac service CFM-1 local-mepid 1 mac 00:11:22:33:44:55
```

cfm frame-loss show	Displays LMM information:	su	6.3
[order-by-mepid]	• Sort the results by MEP ID.		
[exclude-evpl]	• Exclude EVPL entries.		
[service <CFMServiceName> [order-by-mepid][exclude-evpl]]	• Display LMM information for a specific service.		

Example:

```
> cfm frame-loss show
```

```
+----- LOSS MEASUREMENT MESSAGE INFORMATION -----
-+
| Service Name | Local | Remote | Remote | Repeat | Loss | Tx | Rx | Rx | Tx |
| |MepId| Mac Address |MepId | in min| Near | Far | Lmm | Lmr | Lmm | Lmr |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
-+
| 427_3300 | 200 | 00:00:00:00:00:00 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
+-----+-----+-----+-----+-----+-----+-----+-----+
-+
```

cfm md set	Sets the name for a Maintenance Domain. Command attributes include:	su	6.2
{level <NUMBER: 0-7>}	• Maintenance Domain level to name.		6.2
{name <String [31]>}	• Name for the Maintenance Domain. If a Maintenance Domain name is changed, it must be changed on all other units. The name must be the same on each end point.		6.2

Example:

```
> cfm md set level 7 CustomerMD7
```

cfm md show	Displays a summary list of all Maintenance Domains. Optionally, displays:	su/lu	6.2
[level <NUMBER: 0-7>]	• Summary for the specific Maintenance Domain level		6.2
[services]]	• Services for the specified Maintenance Domain level.		6.2

Example:

```
> cfm md show
```

```
+---- CFM MAINTENANCE DOMAINS ----+
|Level|Name          |Services|
+-----+-----+
|0     |md0            |0       |
|1     |md1            |0       |
|2     |md2            |0       |
|3     |md3            |0       |
|4     |md4            |0       |
|5     |md5            |0       |
|6     |md6            |0       |
|7     |md7            |0       |
+-----+-----+
```

cfm mep clear [service <CFMServiceName>]	Clears CFM mep statistics. Optionally, clears statistics for a specific service.	su	6.2
[statistics]	Clears all statistics		6.2
[port <PortName>][mepid <NUMBER: 1-8191>][statistics][vlan <Vlan>] [statistics]	Clears statistics for a specific MEP.		6.2

Example:

```
> cfm mep clear
> cfm mep clear service CFM-1 mepid 12 statistics
```

cfm mep create {service <String[16]>} {port <PortName>}	Manually create a Maintenance End Point (MEP) on a CFM Service port for VLAN or VS CFM services. Options include:	su	6.2
[vlan <Vlan>]	Default VLAN is 0.		6.3.1
[type <up down>]	Default type is 'up'.		6.2
[mepid <NUMBER: 1-8191>]	Default MEPID is 1.		6.2

Example:

```
> cfm mep create service CFM-1 port 1 type down mepid 200
```

cfm mep delete {service <String[16]>} {port <PortName>}	Deletes a MEP.	su	6.2
[vlan <Vlan>]	VLAN.		6.3.1
[mepid <NUMBER: 1-8191>]	Default MEPID is 1.		6.2

Example:

```
> cfm mep delete service CFM-1 port 1
```

cfm mep disable {service <String[16]>} {port <PortName>}	Disables a MEP.	su	6.2
[vlan <Vlan>]	VLAN.		6.3.1
[mepid <NUMBER: 1-8191>]	Default MEPID is 1.		6.2

Example:

```
> cfm mep disable service CFM-1 port 1
```

cfm mep enable {service <String[16]>} {port <PortName>}	Enables a MEP.	su	6.2
[vlan <Vlan>]	VLAN.		6.3.1
[mepid <NUMBER: 1-8191>]	Default MEPID is 1.		6.2

Example:

```
> cfm mep enable service CFM-1 port 1
```

cfm mep set {local-mepid <NUMBER: 1-8191> port <PortName> [vlan <Vlan>]}	Set MEP attributes for the specified service and port, including:	su	6.2
[ccm-priority <NUMBER: 1-5>]	CCM message priority.		6.2
[ccm-state <on off>]	Enables or disables transmission of CCMs. Default is enabled. For troubleshooting purposes, you can set the state to disabled, and the MEP will process the CCMs that it receives, but will not transmit any.		6.2
[lrm-priority <NUMBER: 1-5>]	LTM message priority.		6.2
[mepid <NUMBER: 1-8191>]	Set a new MEP ID.		6.2
[tag-vid <0-4095>]	The VLAN ID of the additional tag. This tag is pushed onto the frame prior to any other tags that it would normally contain. Default 0.		6.4.1
[tag-priority <0-7>]	The dot1p priority encoded in the additional tag. Default 7.		6.4.1
[tag-mode <on off>]	When the tag-mode is on, the MEP originates all frames with an additional inner-most tag, typically to transmit double-tagged CFM frames from a Down MEP.		6.4.1
[type <up down>]	MEP type.		6.2

Example:

```
> cfm mep set service CFM-1 port 1 type up
```

cfm mep show	Show MEP information.	su	6.2
[order-by-mepid]	Sort the results by MEP ID.		
[exclude-evpl]	Exclude EVPL entries.		

[service <CFMServiceName> port <PortName> vlan <Vlan> mepid <#>][order-by-mepid][exclude-evpl]]

- Show MEP information for a specific service.

Example:

```
> cfm mep show
```

CFM MEPS							
Service	Port	Mepid	Type	Mac Address	Admin State	CCM State	CCM Pri
CFM_VLAN_777	1	3	down	00:02:A1:15:56:E2	en	on	7
CFM_VLAN_777	2	4	down	00:02:A1:15:56:E3	en	on	7
CFM_VLAN_777	3	5	down	00:02:A1:15:56:E4	en	on	7
CFM_VLAN_777	5	5	down	00:02:A1:15:56:E6	en	on	7

cfm mip-ccm-db		su	6.5
[enable disable]	• Enable or disable the MIP CCM database.		6.5
[show <vlan <VlanId>>]	• Display MIP CCM database details.		6.5

Example:

```
> cfm mip-ccm-db enable
```

cfm mip clear	Clears MIP statistics for all or a specific CFM service.	su	6.2
[service <String[16]>			
port <PortName>]			
statistics			

Example:

```
> cfm mip clear statistics
```

cfm mip create	Creates a Maintenance Intermediate Point (MIP) on a VLAN at one or more ports and levels.	su	6.2
{vlan <VlanId>}	• VLAN ID.		6.2
{port <PortNameList>}	• Port names.		6.2
[level <NUMBER: 0-7>]	• Maintenance Domain Level. If a MEP exists at the specified level or higher, the MIP will not be created.		6.2

Example:

```
> cfm mip create vlan 1001 port 5
```

cfm mip delete	Delete an Maintenance Intermediate Point specified by:	su	6.2
{vlan <VlanId>}	• VLAN ID.		6.2
{port <PortNameList>}	• Port names.		6.2

Example:

```
> cfm mip delete vlan 1001 port 5
```

cfm mip set	Sets the MD level for the specified MIP.	su	6.2
{vlan <VlanId>}	VLAN ID.		6.2
{port <PortNameList>}	Port names.		6.2
[level <NUMBER: 0-7>]	Maintenance Domain Level. If a MEP exists at the specified level or higher, the MIP will not be created.		6.2

Example:

```
> cfm mip set vlan 1001 port 5 level 1
```

cfm mip show [vlan <VlanId> port <PortName>]	Show a list of all MIP, or the MIPs for a specific VLAN and port.	su	6.2

Example:

```
> cfm mip show
```

```
+----- CFM MIPS -----+
| Service Instance |Vlan Id |Port   |Level |Mac Address |
+-----+-----+-----+-----+-----+
| VLAN#1001       |1001   |1      |3     |00:02:A1:24:0E:32 |
+-----+-----+-----+-----+-----+
```

cfm mip-ccm-db show [vlan <VlanId>]	Shows the MIP CCM database records for all or the specified VLAN.	su/lu	6.2

Example:

```
> cfm mip-ccm-db show
No MIP CCM database records found
```

cfm remote-mep clear {service <String[16]>} {mepid <NUMBER: 1-8191>} {statistics}	Clear all or specific remote MEP statistics.	su	6.2

Example:

```
> cfm remote-mep clear service VLAN#1001 mepid 100 statistics
```

cfm remote-mep create {service <String[16]>}	Manually create a remote MEP on a CFM Service port.	su	6.2

[mepid <NUMBER: 1-8191>]	Default MEPID is 1.		6.2

Example:

```
> cfm remote-mep create service CFM-1 mepid 200
```

cfm remote-mep delete {service <String[16]>} {mepid <NUMBER: 1-8191>}	Deletes a Remote MEP.	su	6.2

Example:

```
> cfm remote-mep delete service VLAN#1001 mepid 100
```

cfm remote-mep disable {service <String[16]>} {mepid <NUMBER: 1-8191>}	Disables a Remote MEP.	su	6.2

Example:

```
> cfm remote-mep disable service VLAN#1001 mepid 100
```

cfm remote-mep enable {service <String[16]>} {mepid <NUMBER: 1-8191>}	Enables a Remote MEP.	su	6.2

Example:

```
> cfm remote-mep enable service VLAN#1001 mepid 100
```

cfm remote-mep set {service <String[16]>} {mepid <NUMBER: 1-8191>}	Sets Remote MEP attributes.	su	6.3.1

[hold-state <enabled|disabled|lock>]

- Remote MEP hold state:
enabled - remain in an operational "hold" state until the MEP remains fault free for a time interval equal to (Remote MEP Hold Time + (CCM Interval * CCM Loss Count)).
disabled - the operational state will directly reflect its administrative state.
lock - in a hold state regardless of fault state.

[mac <MacAddress>]

- MAC address. If the remote MEP is not configured with a fixed MAC address, then the CCM source-address is used.

Example:

```
> cfm remote-mep set service VLAN#1001 mepid 100 hold-state lock
```

cfm remote-mep show	Show a list of all Remote MEPs. Optionally, displays:	su/lu	6.2

[service<CFMServiceName>]	• All Remote MEPs in a single CFM Service.	6.2

[mepid <NUMBER: 1-8191>]	• A specific remote MEP.	6.2

[y1731]	• Y.1731 frame Ethertype.	6.3

Example:

```
> cfm remote-mep show
```

```

+----- CFM REMOTE MEPS -----+
|Service      |Mepid|Mac Address      |State|Total  |Seq  |Last  |Fault|
|-----|-----|-----|-----|-----|-----|-----|
|VS-CFM-1     |2    |00:00:00:00:00:00|en|hd|0    |0    |0    |X| | |
+-----+-----+-----+-----+-----+-----+-----+

```

cfm remote-mep unset service <CfmService>	Clear a Remote MEP mac address.	su	6.3.1

mepid <#> mac

Example:

```
> cfm service clear statistics
```

cfm service clear	Clear CFM service statistics for all or a	su	6.2

[service <String[16]>]
statistics

specified service.

Example:

```
> cfm service clear statistics
```

cfm service create	Create a CFM Service with the following attributes:	su	6.2, 6.5

{static-backup-pbt <TunnelPbtBackup> static-pbt <TunnelPbtPriTunnel> vlan <VlanId> vs <VirtualSwitchName[15]>}	Name or ID of the static backup PBT, static PBT, VLAN, or virtual switch to monitor.		
[level <NUMBER>]	Maintenance Domain Level - The default value for level is 3.		
[name <String[16]>]	Service Name- If unspecified, the new CFM service has the same name as its PBT static backup tunnel, PBT static primary tunnel, VLAN, or VS.		
[next-mepid <NUMBER>]	Next mep ID - The default value for next-mepid is 1. Note that since next-mepid is used to generate default MEPIDs, it is important to set it to a unique value on each device in the service instance.		

Example:

```
> cfm service create vlan 1001
```

cfm service delete	Delete a CFM Service.	su	6.2

{service <String[16]>}

Example:

```
> cfm service delete service VLAN#1001
```

cfm service disable	Disable a CFM Service	su	6.2

{service <String[16]>}

Example:

```
> cfm service disable service VLAN#1001
```

cfm service enable {service <String[16]>}	Enable a CFM Service	su	6.2

Example:

```
> cfm service enable service VLAN#1001
```

cfm service set {service <String[16]>}	Set CFM Service attributes:	su	6.2
{[alarm-priority <NUMBER: 1-5>],	• Service fault alarm priority. Default is 1.		6.2
[alarm-time <NUMBER: 0-36000>],	• Service fault alarm time. Default is 3000.		6.2
[ccm-interval <NUMBER: 0-7 off 4ms 10ms 100ms 1sec 10sec 1min 10min>],	• CCM transmission interval 0 or off - No CCMs sent 1 or 4ms - 4 milliseconds 2 or 10ms - 10 milliseconds 3 or 100ms - 100 milliseconds 4 or 1sec - 1 second default 5 or 10sec - 10 seconds 6 or 1min - 1 minute 7 or 10min - 10 minutes For PBT tunnels, the smallest CCM interval value recommended is Index 2 (10 ms).		6.2
[ccm-interval <NUMBER: 0-7 4msecCCM 100msecCCM 10secCCM 10minCCM 10msecCCM 1secCCM 1minCCM>]	• CCM transmission interval: 0 or off - No CCMs sent 1 or 4msecCCM - 4 milliseconds 2 or 10msecCCM - 10 milliseconds 3 or 100msecCCM - 100 4 or milliseconds 4 or 1secCCM - 1 second default value 5 or 10secCCM - 10 seconds 6 or 1minCCM - 1 minute 7 or 10minCCM - 10 minutes		6.3
[ccm-loss-bucket-size <NUMBER: 1-60>],	• CCM loss bucket size.		6.2
[ccm-loss-num <NUMBER: 1-255>],	• CCM loss number. Applicable when the CFM service is for a PBT tunnel, this attribute defines the allowable CCM loss number before a tunnel is deemed to have failed. The default is 3.		6.2
[ccm-loss-stats <enable disable>],	• Enables or disables CCM loss statistics.		6.2

[dmm-interval <NUMBER: 0-7 4msecCCM 100msecCCM 10secCCM 10minCCM 10msecCCM 1secCCM 1minCCM>]	- DMM transmission interval: - off - No CCMs sent 4msecCCM - 4 milliseconds 10msecCCM - 10 milliseconds 100msecCCM - 100 milliseconds 1secCCM - 1 second default value 10secCCM - 10 seconds 1minCCM - 1 minute 10minCCM - 10 minutes	6.3
[level <NUMBER: 0-7>],	MD Level.	6.2
[lmm-interval <NUMBER: 0-7 4msecCCM 100msecCCM 10secCCM 10minCCM 10msecCCM 1secCCM 1minCCM>]	- LMM transmission interval: - off - No CCMs sent 4msecCCM - 4 milliseconds 10msecCCM - 10 milliseconds 100msecCCM - 100 milliseconds 1secCCM - 1 second default value 10secCCM - 10 seconds 1minCCM - 1 minute 10minCCM - 10 minutes	6.3
[encapsulation <dot1q dot1ad>],	CFM encapsulation mode -802.1q compliant (single tagged) or 802.1ad compliant (Q-in-Q, etc.).	6.2
[name <String[16]>],	CFM service name.	6.2
[next-mepid <NUMBER: 1-8191>],	MEPID of next MEP created.	6.2
[reset-time <NUMBER: 10-36000>]]	Service fault reset time.	6.2
[remote-mep-aging-time <NUMBER: 10-36000>]]	Remote MEP aging time.	6.2
[remote-mep-discovery <NUMBER: 10-36000>]]	Remote MEP discovery interval.	6.2
[sender-id-type]	Sender ID type.	6.2

Example:

```
> cfm service set service VLAN#1001 ccm-interval 1min
```

cfm service show	Show a list of all CFM Services, or detailed information for a single CFM Service.	su/lu	6.2
[service <CFMServiceName>	Specified CFM service.		6.2
[mep	MEPs for the specified CFM service.		6.2
remote-mep	Remote MEP for the specified CFM service.		6.2
statistics]]	Statistics for the specified CFM service.		6.2

Example:

```
> cfm service show
```

CFM SERVICES													
Name	Type	Service Network	Vid	Lvl	Adm	Loc	Rem	XC	CC	RM	PS	RD	IS
VLAN#1001	VLAN	VLAN#1001	1001	3	dis	0	0						

cfm stack show [vlan <VlanId>]	Display CFM port stacks for all or the specified VLAN.	su	6.2

Example:

```
> cfm stack show
```

CFM Interface Stacks									
Service Inst	Vlan	Port	Type	L	Mep	Adm	Service	MAC Address	
VLAN#1001	1001	1	Down	3	1	en	VLAN#1001	00:02:A1:24:0E:32	

cfm show [statistics]	Show the global CFM configuration or statistics.	su/lu	6.2

Example:

```
> cfm stack show
```

CFM GLOBAL CONFIGURATION	
Parameter	Value
Admin State	Disabled
Ethertype	0x8902
Remote MEP Hold Time (ms)	10000
CCMs/sec Avail	4998
Total Rx Frames	0
Total Tx Frames	0

chassis

Command	Description	Access Level	Release Introduced
chassis post disable	Disables Power On Self Tests (POST).	su	6.0
Example:			
>chassis post enable			
chassis post enable	Enables Power On Self Tests (POST).	su	6.0
Example:			
>chassis post enable			
chassis post show	Displays POST status.	su	6.0

Example:

```
>chassis post show
POST is enabled.
POST Results: No errors detected.
```

chassis set	Set chassis temperature thresholds, including:	su	6.0
{[dying gasp <on off>],	Sets whether or not to send the dying gasp TLV when the system detects a failure.		6.4.1
[temperature-high-threshold <NUMBER: 0-65>],	High temperature threshold. Default is 50 degrees Celsius.		6.0
[temperature-low-threshold <NUMBER: 0-65>],	Low temperature threshold. Default is 0 degrees Celsius.		6.0
[power <AC DC>]]	Displays the selected power type. The default is AC, and it will revert to this setting if reset to factory defaults.		6.4.1

Example:

```
>chassis set temperature-high-threshold 45
```

chassis show	Displays all or the specific chassis information. Options include:	su/lu	6.0
[attributes]	Device identification attributes.		6.0
[capabilities]	Platform capabilities.		6.0
[mac]	MAC address of the chassis.		6.0
[power]	Power supply status.		6.0
[temperature]	Temperature threshold and current status.		6.0

Example:

```
> chassis show attributes
```

```
+----- CHASSIS DEVICE ID -----+
| Parameter                        |
+-----+-----+
| Chassis Device Type              | 007 |
| Chassis Hardware Version         | 0   |
| Chassis Serial Number            | 0   |
| Chassis MAC Address              | 00:02:a1:07:a4:a0 |
| Manufactured Date                | 25-10-2007 |
| Param Version                    | 005 |
+-----+-----+
```

cli

Command	Description	Access Level	Release Introduced
cli search keyword <String[63]> [object <String[63]>][full]	Searches the CLI for the specified text string. Optionally, the search can be limited to a specific main level command object and expanded to show full attributes.	su/lu	6.0
Example:			
<pre>> cli search keyword password user create user <String> password <String> user set user <String> nopassword user set user <String> password <String></pre>			
cli show	Displays all available commands.	su/lu	6.0

Example:

```
>cli show
arp delete ip
arp flush intf remote
arp for ip interface remote
arp in-use ip interface remote
arp show intf remote
blade show
chassis post disable
chassis post enable
chassis post show
chassis set
chassis show
clear
cli search keyword
cli show
configuration augment
configuration install
configuration list
configuration reset-config-restore-warning
configuration reset-to-factory-defaults
configuration save filename
configuration set
configuration show
device-archive save
device-archive show
Press any key to continue (Q to quit)
```

command-log

Command	Description	Access Level	Release Introduced
command-log disable	Disables logging of CLI commands run on the system.	su	6.5

Example:

```
>command-log disable
```

command-log enable	Enables logging of CLI commands run on the system.	su	6.5

Example:

```
>command-log enable
```

command-log show	Displays the CLI command log with the following options:	su/lu	6.5
[destination]	Location of the entries.		6.5
[recent]	Recent entries.		6.5
[last <DurationString>]	Entries from the specified time interval in the format N[yMwdhms].		6.5
[today]	Entries from today.		6.5
[yesterday]	Entries from yesterday.		6.5
[from-date <DateString>]	Entries from specified date (yyyy-mm-dd or yy-mm-dd or mm-dd)		6.5
[to-date <DateString>]	Entries to specified date (yyyy-mm-dd or yy-mm-dd or mm-dd)		6.5
[from-time <TimeString>]	Entries from specified time (hh:mm or hh:mm:ss)		6.5
[to-time <TimeString>]	Entries to specified time (hh:mm or hh:mm:ss)		6.5
[tail <NUMBER: 1-4290261631>]	Latest number of entries		6.5
[containing <String>]	Entries containing a specific string.		6.5
[mine]	Displays entries for current user.		6.5
[since-activated]	Entries since the system was activated.		6.5
[user <String[16]>]	Displays entries for the specified user.		6.5
[privilege <limited super>]	Limits to users with the specified privilege.		6.5
[on-terminal <TerminalString>]	Entries of commands run from a specific terminal ID.		6.5
[sequence-id <NUMBERList>]	Entries of a specific sequence identifier.		6.5

[verbose]	Displays the command log in a table format with headings, timestamp, and user information. Without the verbose option, the command log is displayed with sequence ID and command only.	6.5

Example:

```
> command-log show recent
8274: command-log show today from-time 13:34 to-time 19:34:00 verbose
8275: command-log show recent verbose
8279: command-log repeat my-last-command times 2
8280: command-log repeat my-last-command times 2
8281: command-log show last 1m
8282: command-log show last 1m
8283: command-log repeat my-last-command times 2
8287: command-log repeat sequence-id 8279
8297: dhcp client lease renew
8301: command-log show
```

command-log repeat	Re-runs a command or sequence of commands from the command log:	su/lu	6.5
{sequence-id <numbers> my-last-command command <String>}	Specifies the sequence identifier of command(s), the last command of the user issuing the repeat command, or the command to repeat. When specifying multiple sequence identifiers, separate each item with a comma. Duplicate sequence identifiers are not supported.		6.5
[every <Duration>]	Specifies an interval in the format N[yMwdhms to rerun the command.		6.5
[times <NUMBER: 1-4290261631>]	Specifies the number of times to rerun the command. Note: “More” processing will be disabled for all but the last run of the command.		6.5

Example:

```
> command-log repeat my-last-command times 2
command-log show last 1m
8281: command-log show last 1m
8282: command-log show last 1m
command-log show last 1m
8281: command-log show last 1m
8282: command-log show last 1m
```

configuration

Command	Description	Access Level	Release Introduced
configuration augment	Augments the currently running configuration with commands from the specified configuration file.	su	6.0

{filename <FileName>}	Specifies the filename to use to augment the configuration.	6.0
[server <IpHost>]	TFTP server where the file is located.	6.0

Example:

```
> configuration augment filename myConfig.cfg server 192.168.76.100
```

configuration install	Installs the specified configuration file.	su	6.0
{filename <FileName>}	• Specifies the filename to use to augment the configuration.		6.0
[server <IpHost>]	• TFTP server where the file is located.		6.0

Example:

```
> configuration install filename myConfig.cfg server 192.168.76.100
```

configuration list	Lists all configuration files.	su/lu	6.0

Example:

```
> configuration list
```

```
+-----+
|      Configuration Files      |
+-----+
| startup-config                |
+-----+
| Default Save File: startup-config |
| Default Load File: startup-config |
+-----+
```

configuration reset-config-restore-warning	Reset the configuration restore warning flag.	su	6.0

Example:

```
> configuration reset-config-restore-warning
```

configuration reset-to-factory-defaults	The system will restore the configuration to the factory defaults, including clearing all configuration files, license key, and log files.	su	6.0

Example:

```
> configuration reset-to-factory-defaults
```

configuration save	Saves current system configuration to the specified file on the flash disk.	su	6.0
[filename <FileName>]	Optionally, saves the current system configuration to a specified file.		6.0

Example:

```
> configuration save
```

configuration search	Search for a specific string in a configuration file. This command is similar to the unix grep command.	su/lu	6.0
[file <FileName>]	• Specifies the file to search. If a file is not specified, then the default file is searched.		6.0
[lines <NUMBER: 0 - 40>]	• Indicates how many text lines you want to view above and below the search line.		6.0
{string <String[255]>}	• String to search for.		6.0

Example:

```
> configuration search string aging lines 5
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! AGING and LEARNING CONFIG:
!
flow aging set time 1800
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! STATIC MAC CONFIG:
!
!
```

configuration set	Set the default configuration file names for:	su	6.0
{[default-save-filename <FileName>],	• File name for saving configuration.		6.0
[default-load-filename <FileName>],	• File name for loading configuration.		6.0

Example:

```
> configuration set default-save-filename myConfig default-load-filename myConfig
```

configuration show	Displays the current running configuration.	su/lu	6.0

Example:

```
>configuration show
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! NETWORK CONFIG:  vlans
!
vlan create vlan 69
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! EVENT LOG MANAGER:
!
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! CHASSIS CONFIG:
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! SYSTEM CONFIG:
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! INTERFACE CONFIG:
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! PORT CONFIG: ports
!
port set port 9 speed hundred auto-neg off
port set port 10 speed hundred auto-neg off
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Press any key to continue (Q to quit)
```

device-archive

Command	Description	Access Level	Release Introduced

device-archive clear	Clears the device archive.	su/lu	6.0

Example:

```
> device-archive clear
```

device-archive save	Writes the device archive parameters the default device archive file	su/lu	6.0

Example:

```
> device-archive save
```

device-archive show	Displays the contents of the device archive that is stored as parameters in the boot flash	su/lu	6.0

Example:

```
> device-archive show
```

```
+-----+-----+
| Parameter                                     | Value                                     |
+-----+-----+
| Cumulative system uptime (seconds)           | 0                                         |
| Cumulative system uptime (days:hh:mm:ss)    | 0:00:00:00                              |
| Highest Temperature (degrees Celsius)        | 0 (50 MAX)                              |
| Number of High Temperature Violations        | 0                                         |
| Lowest Temperature (degrees Celsius)         | 50 ( 0 MIN)                             |
| Number of Low Temperature Violations         | 0                                         |
| Number of Soft Resets                        | 0                                         |
| Total Number of Resets                      | 0                                         |
| Last Reset Reason                           | Unknown                                  |
+-----+-----+
```

dhcp

Command	Description	Access Level	Release Introduced

dhcp client disable	Globally disables DHCP.	su	6.0

Example:

```
> dhcp client disable
```

dhcp client enable	Globally enables DHCP.	su	6.0

Example:

```
> dhcp client enable
```

dhcp client lease renew	Renews the lease for the DHCP client.	su	6.0

Example:

```
> dhcp client lease renew
```

dhcp client options set	Sets the DHCP options.	su	6.0
{[subnet <on off>],	• Subnet DHCP option (1).		6.0
[time-offset <on off>],	• Time offset DHCP option (2).		6.0
[router <on off>],	• Router DHCP option (3).		6.0
[dns <on off>],	• DNS DHCP option (6).		6.0
[log-server <on off>],	• Log server DHCP option (7).		6.0
[host-name <on off>],	• Host name DHCP option (12).		6.0
[domain-name <on off>],	• Domain name DHCP option (15).		6.0

[ntp <on off>],	• NTP DHCP option (42).	6.0
[lease-time <on off>],	• Lease time option (51)	6.0
[tftp-server <on off>],	• TFTP server DHCP option (66).	6.0
[boot-file <on off>]}	• Boot file DHCP option (-1 or 67).	6.0

Example:

```
> dhcp client options set tftp-server off
```

dhcp client set	Sets the DHCP client global attributes:	su	6.0
{[interface <remote>],	• Interface on which to run DHCP.		6.0
[discovery-interval <NUMBER: 1-60>]}	• DHCP discovery interval in seconds.		6.0

Example:

```
> dhcp client set discovery-interval 10
```

dhcp client show	Displays the current DHCP client state and DHCP/BOOTP options state. Optionally, displays one or more of the following:	su	6.0
[config]	• Configuration from enabled DHCP options.		6.0
[options]	• DHCP/BOOTP options state.		6.0

[state] • DHCP client state. 6.0

Example:

```
> dhcp client show
```

```
+----- DHCP CLIENT STATE -----+
| Parameter | Value |
+-----+-----+
| Interface Name | remote |
| Admin State | Enabled |
| Oper State | Enabled |
| DHCP State | Disabled |
| Discovery Interval | 3 |
| Lease Time (days hh:mm:ss) | 000:01:00:00 |
| Lease Remaining (seconds) | 3600 |
| Renewal (T1) Time (seconds) | 0 |
| Rebinding (T2) Time (seconds) | 0 |
| DHCP Server | 0.0.0.0 |
+-----+-----+

+----- DHCP/BOOTP OPTIONS STATE -----+
| Option | Description | State |
+-----+-----+-----+
| 1 | Subnet Mask Option | On |
| 2 | Time Offset Option | On |
| 3 | Router Option | On |
| 6 | Domain Name Server Option | On |
| 7 | Log Server Option | On |
| 12 | Host Name Option | On |
| 15 | Domain Name Option | On |
| 42 | Network Time Protocol Servers Option | On |
| 51 | Lease Time Option | On |
| 66 | Tftp Server Name Option | On |
| 67 | Bootfile Name Option | On |
+-----+-----+-----+
```

dns client

Command	Description	Security Level	Release Introduced
dns-client add server <IpAddress>	Adds DNS Client server IP address to the DNS list.	su	6.2

Example:

```
> dns-client add server 10.10.10.12
```

dns-client disable [server <IpAddress>]	Disables DNS Client globally or for the specified server.	su	6.2

Example:

```
> dns-client add server 10.25.34.11
```

dns-client enable [server <IpAddress>]	Enables DNS Client globally or for the specified server.	su	6.2

Example:

```
> dns-client enable server 10.25.34.11
```

dns-client remove server <IpAddress>	Removes DNS Client server IP address from the DNS list.	su	6.2

Example:

```
> dns-client remove server 10.25.34.13
```

dns-client resolve ip <IpHost>	Resolves an IP address or host name.	su/lu	6.2

Example:

```
> dns-client resolve ip ciena.com
```

dns-client set {{domain-name <String[63]>}} [server <IpAddress> priority <NUMBER: 1-3>]}	Sets the DNS domain name or server IP address and priority.	su/lu	6.2

Example:

```
> dns-client set domain-name ciena.com server 10.25.34.11 priority 1
```

dns-client show	Displays the DNS clients operational state. Optionally, displays:	su/lu	6.2

[domain-name] Domain name configuration.

[servers] Server configuration information.

Example:

```
> dns-client sh ser
```

DNS CLIENT SERVER CONFIGURATION						
IP Address	Config State	Admin State	Oper State	User Priority	DHCP Priority	
10.25.34.11	dhcp	Enabled	Enabled		1	
10.25.34.12	dhcp	Enabled	Enabled		2	

dns-client unset domain-name	Clears the DNS Client attributes.		6.2

Example:

```
> dns-client unset domain-name ciena.com
```

dot1x

Command	Description	Security Level	Release Introduced
dot1x auth clear [port <PhyPortNameList>] statistics	Clears all dot1x authenticator statistics globally or for the specified ports.	su	6.4
Example:			
> dot1x auth clear port 16 statistics			
dot1x auth disable port <PhyPortNameList>	Disables dot1x authenticator on the specified ports.	su	6.4
Example:			
> dot1x auth disable port 16			
dot1x auth enable port <PhyPortNameList>	Enables dot1x authenticator on the specified ports.	su	6.4
Example:			
> dot1x auth enable port 16			
dot1x auth pae-port-reauth port <PhyPortNameList>	Causes the PAE state machine to re-authenticate the port.	su	6.4
Example:			
> dot1x auth pae-port-reauth port 16			
dot1x auth set port <PhyPortNameList>	Sets 802.1x authenticator port attributes, including:	su	6.4
{[eapol-version <NUMBER: 1...2>]}	Sets the EAPOL version.		6.4.1
[max-reauth-req <NUMBER: 1-10>]	Maximum number of times the EAP Request Packet would be sent to a supplicant before the authenticator times out the authentication process. The default is 2.		
[mode <auto force-auth force-unauth>]	Authenticator PAE mode. In 'auto' mode, the port state depends on the result of the authentication process. In 'forceauth' mode the port dot1x state is authorized and the port state is UP. In 'forceunauth' mode, the dot1x state is always un-authorized and the operational state is 'Nau' (Not Authenticated). The default is 'auto'.		
[reauthentication on off>]	Causes the authenticator to challenge the supplicant. Not saved in the config file.		

[reauth-period <NUMBER: 0-65535>]	Reauthentication period - number of seconds between periodic reauthentication of the supplicant.	
[quiet-period <NUMBER: 1...65535>]	Sets the quiet period.	6.4.1
[server-timeout <NUMBER: 0-180>]	Server timeout - number of seconds allowed for server authentication. The default is 30.	
[supp-timeout <NUMBER: 1-180>]	Supplicant timeout - the initialization value in seconds for the timer used to timeout a supplicant.	
[tx-period <NUMBER: 0-65535>]	Transmit period- the time interval in seconds in which EAPOL-PDU is sent. The default is 30.	
[quiet-period <NUMBER: 0-65535>]}	Quiet period - number of seconds during which the authenticator will not try to acquire a supplicant. The default is 60.	

Example:

```
> dot1x auth set port 16 mode auto
```

dot1x auth show [stats] [[port <PhyPortNameList>]	Shows 802.1x authenticator information for all or the specified ports. Optionally, shows authenticator statistics for all ports.	su	6.4

Example:

```
> dot1x auth show stats
```

dot1x disable	Disable all dot1x authenticators and supplicants on all ports system wide.	su	6.4

Example:

```
> dot1x disable
```

dot1x enable	Enables dot1x globally. Individual dot1x port settings are honored.	su	6.4

Example:

```
> dot1x enable
```

dot1x pae-port-initialize port <PhyPortNameList>	Initializes the specified port.	su	6.4

Example:

```
> dot1x pae-port-initialize port 16
```

dot1x show	Shows dot1x global information.	su/lu	6.4

Example:

```
> dot1x show
```

dot1x supp clear [port <PhyPortNameList>] statistics	Clears all dot1x supplicant statistics or for the specified ports.	su	6.4

Example:

```
> dot1x supp clear port 10 statistics
```

dot1x supp disable port <PhyPortNameList>	Disable dot1x supplicant on the specified ports.	su	6.4

Example:

```
> dot1x supp disable port 10
```

dot1x supp enable port <PhyPortNameList>	Enable dot1x supplicant on the specified ports.	su	6.4

Example:

```
> dot1x supp enable port 10
```

dot1x supp set port <PhyPortNameList>	Set the attributes for the supplicant, including:	su	6.4

{[authentication-period <NUMBER: 1-65535>]}	• Authentication period - number of seconds the supplicant waits for a response from the authenticator before timing out. The default is 30.		
[eapol-version <NUMBER: 1...2>]	• Sets the EAPOL version.		6.4.1
[held-period <NUMBER: 1-65535>]	• Held period -number of seconds during which a supplicant does not try to acquire an authenticator. The default is 60.		
[password <String[15]>]	• Password - used with the user name to gain access on port.		
[max-start <NUMBER: 1-65535>]	• Max start - maximum number of successive EAPOL start messages after which the supplicant assumes there is no authenticator present. The default is 3 attempts.		
[secret <String[32]>]	• The password in MD5 encrypted format. The password can be set using a pre-encrypted string as opposed to a clear text password string.		6.4
[start-period <NUMBER: 1-65535>]	• Start period - time interval (in seconds) in which an EAPOL start PDU is transmitted by the supplicant. The default is 30.		
[username <String[15]>]}	• User name used with the password to gain access to the PAE resources.		

Example:

```
> dot1x supp set port 10 authentication-period 50
```

dot1x supp show [stats] [port <PhyPortNameList>]	Shows 802.1x supplicant information for all or the specified ports. Optionally, shows supplicant statistics for all ports.	su/lu	6.4

Example:

```
> dot1x supp show stats
```

dot1x supp unset port <PhyPortNameList> {[password], [username]}	Clears supplicant user name and/or password.	su	6.4

Example:

```
> dot1x supp unset port 10 username User1 password mysecret
```

eoam

NOTE: To enable EOAM commands, the Advanced OAM feature license must be installed with the software license install command.

Command	Description	Security Level	Release Introduced
eoam clear statistics	Resets all statistics in the statistics table.	su	6.2

Example:

```
> eoam clear statistics
```

eoam disable [port <PhyPortNameList>]	Disables EOAM globally or, if a list of ports is specified, the administrative state of the specified ports is set to Disabled.	su	6.2

Example:

```
> eoam disable port 15
```

eoam enable [port <PhyPortNameList>]	Enables EOAM globally. If a list of ports is specified the administrative state of the specified ports is set to Enabled.	su	6.2

Example:

```
> eoam enable port 15
```

eoam loopback stop port <PhyPortNameList>	Stops OAM loopback on the specified port. This command is not saved as part of configuration.	su	6.2

Example:

```
> eoam loopback stop port 15
```

eoam loopback start port <PhyPortNameList>	Starts OAM loopback on the specified port. The port may or may not successfully enter loopback, because it depends on negotiation with the peer. This command not saved as part of configuration.	su	6.2

Example:

```
> eoam loopback start port 15
```

eoam loopback ignore port <PhyPortNameList>	Sets OAM loopback commands to be ignored on the specified port to prevent disruption.	su	6.2

Example:

```
> eoam loopback ignore port 7
```

eoam loopback process port <PhyPortNameList>	Sets OAM loopback commands to be processed.	su	6.2

Example:

```
> eoam loopback process port 15
```

eoam loopback show [port <PhyPortNameList>]	Show the current loopback statistics for the entire switch or the specified ports.	su/lu	6.2

Example:

```
> eoam loopback show port 15
```

eoam set port <PhyPortNameList>	Sets the port attributes, including:	su	6.2
{[critical-event <on off>],	• Critical event notification.		6.2
[dying-gasp <on off>],	• Sets whether or not to send the dying gasp TLV when the system detects a failure.		6.2
[mode <active passive>],	• Active or passive mode.		6.2
[errd-frame-ev-notify <on off>],	• Error frame event notification.		6.2
[errd-frame-window <NUMBER: 10-600 >],	• Error frame window (default is 10).		6.2
[errd-frame-threshold <NUMBER: 0-4294967295 >],	• Error frame threshold (default is 1).		6.2
[errd-frame-period-ev-notify <on off>],	• Error frame period event notification		6.2
[errd-frame-period-window <NUMBER: 14880-8928000>]	• Error frame period window. Value depends on the interface speed, i.e. the number of frames that can be received in a second:, 100Mbps:, 1Gbps:, 10Gbps.		6.2

[errd-frame-period-threshold <NUMBER: 0-4294967295 >],	• Error frame period threshold (default is 1).	6.2
[errd-frame-secs-summary <on off>],	• Error frame seconds summary event notification.	6.2
[errd-frame-secs-window <NUMBER: 10-900>],	• Error frame seconds summary window in seconds (default is 60).	6.2
[errd-frame-secs-threshold <NUMBER: 0-65535 >]]	• Error frame seconds summary threshold (default is 1).	6.2

Example:

```
> eoam set port 15 dying-gasp on
```

eoam show	Shows global OAM status and port statistics. Options include:	6.2
[port <PhyPortNameList>]	• When only ports are specified, displays global OAM status, specified port statistics and specified peer port information.	6.2
[link-events]	• Link-event configuration, globally or for specified ports.	6.2
[errd-events-statistics]	• Error statistics, Error frame event TLV, Error frame period event TLV, and Error frame seconds summary event TLV, globally or for specified ports.	6.2
[event-log]	• OAM event log for the specified ports. Only valid with the port option.	6.2

Example:

```
> eoam show link-events
```

file

The CLI includes several commands for directory/file manipulation. These commands do not follow the defined CLI schema but instead use a standard UNIX-type implementation: FileName = <String[127]>

DirName = <String[127]>

Command	Description	Access Level	Release Introduced

file cat <FileName> [<FileName>]	Displays the contents of the specified file(s).	su/lu	6.0

Example:

```
> file cat /mnt/sysfs/archive/default.arc
SYSTEM_UPTIME_SEC=1359

HIGH_TEMP_DEGC=0

HIGH_TEMP_VIOLATIONS=0

LOW_TEMP_DEGC=50

LOW_TEMP_VIOLATIONS=0

SOFT_REBOOT_COUNT=0

TOTAL_REBOOT_COUNT=0

UNKNOWN_ARCHIVE_PARAM=2
```

file cd [<DirName>]	Changes the working directory	su/lu	6.0

Example:

```
> file cd /mnt/sysfs/archive
```

file chmod <NUMBER: 0,2,4,6> <FileName>	Changes the access mode of the specified file.	su	6.0

Valid options are:

- 0 - No access allowed
- 2 - Write
- 4 - Read only
- 6 - Read/write

Example:

```
> file cd /mnt/sysfs/archive
```

file cp <SourceFileName> <DestinationFileName>	The copy command is used to copy files to/from a file server or to/from the device's file system.	su	6.0

Example:

```
> file cp /mnt/sysfs/archive/default.arc /mnt/sysfs/archives/02-14-08.arc
```

file ls [-la] [<DirName>]	Lists files in the working directory or a specific directory.	su/lu	6.0

Command	Description										Access Level	Release Introduced
Example:												
<pre>> file ls drwxr-xr-x 2 root root 445 Feb 12 2008 bin drwxr-xr-x 4 root root 759 Feb 12 2008 dev drwxr-xr-x 3 root root 191 Feb 12 2008 etc drwxr-xr-x 3 root root 398 Feb 12 2008 lib lrwxrwxrwx 1 root root 11 Feb 12 2008 linuxrc -> bin/busybox drwxr-xr-x 6 root root 51 Feb 12 2008 mnt dr-xr-xr-x 64 root root 0 Jan 1 00:00 proc drwxr-xr-x 2 root root 463 Feb 12 2008 sbin drwxr-xr-x 9 root root 0 Jan 1 00:00 sys drwxr-xr-x 2 root root 3 Feb 12 2008 tmp drwxr-xr-x 5 root root 39 Feb 12 2008 usr -r--r--r-- 1 root root 14 Feb 12 2008 version</pre>												
file mkdir <DirName>	The mkdir command creates a directory or multiple directories.										su	6.0
Example:												
<pre>> file mkdir myDir</pre>												
file mv <SourceFileName> <DestinationFileName>	Renames/move files										su	6.0
Example:												
<pre>> file mv /mnt/sysfs/archives/02-14-08.arc /tmp/02-14-08.arc</pre>												
file pwd	The pwd command displays the present working directory.										su/lu	6.0
Example:												
<pre>> file pwd /</pre>												
file rm [-f] <FileName>	The remove command removes a file or list of files.										su	6.0
Example:												
<pre>> file rm /mnt/sysfs/archives/02-14-08.arc</pre>												
file rmdir [-f] <DirName>	The rmdir command removes a directory or multiple directories.										su	6.0
Example:												
<pre>> file rmdir myDir</pre>												
file rmtree	Removes a directory tree.										su	6.0
Example:												
<pre>> file rmtree myDirTree</pre>												
file tget <IpHost> <RemoteFileName> <LocalFileName>	Gets a file from a TFTP server.										su	6.0

Command	Description	Access Level	Release Introduced

Example:

```
> file tget 192.168.10.161 myFile.txt myFile.txt
```

file tput <IpHost> <RemoteFileName> <LocalFileName>	Sends a file to a remote TFTP server.	su/lu	6.0

Example:

```
> file tput 192.168.10.161 default.arc default.arc
```

flow

Command	Description	Access Level	Release Introduced

flow aging disable	Disables MAC aging.	su	6.0

Example:

```
> flow aging disable
```

flow aging enable	Enables MAC aging.	su	6.0

Example:

```
> flow aging enable
```

flow aging set	Sets MAC aging timeout in seconds.	su	6.0
{time <NUMBER: 10-1000000>}			6.0

Example:

```
> flow aging set time 300
```

flow aging show	Display aging time/status.	su/lu	6.0

Example:

```
> flow aging show
```

```
+----- AGING-INFO -----+
| Parameter      | Value      |
+-----+-----+
| Status        | Enabled    |
| Time (Seconds) | 300        |
+-----+-----+
```

flow bw-calculation-mode	Sets the bandwidth calculation mode. This determines whether or not the 20-byte inter-frame-gap (IFG) is used in calculations for ingress metering and egress shaping.	su	6.4

set mode <payload transport>	- payload—do not use IFG in the calculations. - transport—use IFG in the calculations.	6.4

Example:

```
> flow bw-calculation-mode set mode payload
```

flow mac-addr find mac <MacAddress>	Finds the specified MAC address. Options include:	su/lu	6.0
[vlan <Vlan>]	Find in a specified VLAN.		6.0
[all-occurrences]	Find all occurrences that are VLAN independent.		6.0

Example:

```
> flow mac-addr find mac 00:01:aa:bb:dd:ff
```

```
+----- FLOW MAC-FIND TABLE -----+
| Address          | VLAN  | Port  |
+-----+-----+-----+
| 00:01:AA:BB:DD:FF | 127   | 5     |
+-----+-----+-----+
```

flow access-control create	Creates an access control entry. With an Advanced Ethernet license, a maximum of 16,000 MAC entries can be learned on the device.	su	6.3
{port <PortNo>}	The port number.		6.3
{max-dynamic-macs <NUMBER: 0...16000>}	The maximum number of dynamic MACs.		6.3
[forward-unlearned <on off>]	Flood (forward-unlearned on) or drop (forward-unlearned off) unknown DA MAC addresses once the MAC Learning threshold has been reached.		6.3.1

Example:

```
> flow access-control create port 5 max-dynamic-macs 16000 forward-unlearned on
```

flow access-control delete	Deletes an access control entry.	su	6.3
{port <PortNo>}	The port number.		6.3

Example:

```
> flow access-control delete port 5
```

flow access-control show	Displays access control for all ports.	su	6.3

Example:

```
> flow access-control show
```

Access Control		
Port Name	MAC Limit	Learned
1	16000	0
2	16000	0
3	16000	0
4	16000	0
5	16000	0
6	16000	0
7	16000	0
8	16000	0
9	16000	0
10	16000	0

flow cpu-rate-limit clear	Clears CPU rate limiting statistics for the specified port.	su	6.4
{port <PhyPortNameList>}			6.4
{statistics}			6.4

Example:

```
> flow cpu-rate-limit clear port 15 statistics
```

flow cpu-rate-limit disable	Disables CPU rate limiting globally. Optionally:	su	6.4
[port <PhyPortNameList>]	Disables CPU rate limiting for the specified port.		6.4

Example:

```
> flow cpu-rate-limit disable port 15
```

flow cpu-rate-limit enable	Enables CPU rate limiting globally. Optionally:	su	6.4
[port <PhyPortNameList>]	Enables CPU rate limiting for the specified port.		6.4

Example:

```
> flow cpu-rate-limit enable port 15
```

flow cpu-rate-limit set	Sets the CPU rate limits, in Packets Per Second (PPS), for the port and packet classes, including the following parameters:	su	6.4
{port <PhyPortNameList>}	Physical port name(s) to set.		6.4
{[bootp <NUMBER: 0-500>],	Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP) control frames. The default rate limit is 5 PPS.		6.4

[cfm <NUMBER: 0-500>],	Connectivity Fault Management (CFM) control frames. The default rate limit is 50 PPS.	6.4
[cft <NUMBER: 0-500>],	Tunneled control frames. The default rate limit is 250 PPS.	6.4
[dot1x <NUMBER: 0-500>],	802.1x port-based network access control frames. The default rate limit is 5 PPS.	6.4
[eoam <NUMBER: 0-500>],	Operation, Administration, and Maintenance (EOAM) control frames. The default rate limit is 5 PPS.	6.4
[eprarp <NUMBER: 0-500>],	Egress Port Restriction (EPR) Address Resolution Protocol (ARP) control frames. The default rate limit is 5 PPS.	6.4
[igmp <NUMBER: 0-500>],	Internet Group Management Protocol (IGMP) control frames. The default rate limit is 5 PPS.	6.4
[inet <NUMBER: 0-1000>],	Generic Internet Protocol control frames. The default rate limit is 700 PPS.	6.4
[lACP <NUMBER: 0-500>],	Link Aggregation Control Protocol (LACP) control frames. The default rate limit is 5 PPS.	6.4
[lldp <NUMBER: 0-500>],	Link Layer Discovery Protocol (LLDP) control frames. The default rate limit is 5 PPS.	6.4
[mpls <NUMBER: 0-500>],	Multi-Protocol Label Switching (MPLS) control frames. The default rate limit is 5 PPS.	6.4
[pearp <NUMBER: 0-500>],	Provider Edge (PE) ARP control frames. The default rate limit is 5 PPS.	6.4
[pvst <NUMBER: 0-500>],	Per VLAN Spanning Tree (PVST) control frames. The default rate limit is 5 PPS.	6.4
[rstp <NUMBER: 0-500>],	Rapid Spanning Tree Protocol (RSTP) control frames. The default rate limit is 5 PPS.	6.4
[lpbk <NUMBER: 0-500>],	Loopback (used for debug). The default rate limit is 5 PPS.	6.4
[rmtlpbk <NUMBER: 0-500>],	Remote loopback (used for debug). The default rate limit is 5 PPS.	6.4
[twamp <NUMBER: 0-500>],	Two-Way Active Measurement Protocol (TWAMP) test frames. The default rate limit is 100 PPS.	6.4

[twampRsp <NUMBER: 0-500>],	Two-Way Active Measurement Protocol (TWAMP) response frames. The default rate limit is 250 PPS.	4.6.2
[dfilt <NUMBER: 0-2000>]]	Unknown control frames (do not match other packet classes). The default rate limit is 500 PPS.	6.4

Example:

```
> flow cpu-rate-limit set port 15 twamp 300
```

flow cpu-rate-limit show	Displays CPU rate limiting global status. Optionally, displays:	su/lu	6.4
[port <PhyPortNameList	Configuration for the specified port.		6.4
[statistics]]	Statistics for the specified port.		6.4

Example:

```
> flow cpu-rate-limit show port 1
```

Packets Per Second Rate Limits		
Port	Packet Class	PPS Rate
15	Bootp/DHCP	5
15	CFM	50
15	CFT	250
15	Dot 1X	5
15	EOAM	5
15	EPR ARP	5
15	IGMP	5
15	INET/IP	700
15	LACP	5
15	LLDP	5
15	MPLS	5
15	MSTP	5
15	PE ARP	5
15	PVST	5
15	RSTP	5
15	Loopback	5
15	Remote Loopback	5
15	TWAMP TST	100
15	TWAMP RSP	250
15	Default	500

flow cpu-rate-limit unset	Resets CPU rate limits to the default rates:	su	6.4
{port <PhyPortNameList}	Specifies port(s) to reset. If you do not specify a packet class, all packet classes are reset to their default values for the specified port(s).		6.4
[bootp]	Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP) control frames. The default rate limit is 5 PPS.		6.4

[cfm]	Connectivity Fault Management (CFM) control frames. The default rate limit is 50 PPS.	6.4
[cft]	Tunneled control frames. The default rate limit is 250 PPS.	6.4
[dot1x]	802.1x port-based network access control frames. The default rate limit is 5 PPS.	6.4
[eoam]	Operation, Administration, and Maintenance (EOAM) control frames. The default rate limit is 5 PPS.	6.4
[eprarp]	Egress Port Restriction (EPR) Address Resolution Protocol (ARP) control frames. The default rate limit is 5 PPS.	6.4
[igmp]	Internet Group Management Protocol (IGMP) control frames. The default rate limit is 5 PPS.	6.4
[inet]	Generic Internet Protocol control frames. The default rate limit is 700 PPS.	6.4
[lACP]	Link Aggregation Control Protocol (LACP) control frames. The default rate limit is 5 PPS.	6.4
[lldp]	Link Layer Discovery Protocol (LLDP) control frames. The default rate limit is 5 PPS.	6.4
[mpls]	Multi-Protocol Label Switching (MPLS) control frames. The default rate limit is 5 PPS.	6.4
[mstp]	Multiple Spanning Tree Protocol (MSTP) control frames. The default rate limit is 5 PPS.	6.4
[pearp]	Provider Edge (PE) ARP control frames. The default rate limit is 5 PPS.	6.4
[pvst]	Per VLAN Spanning Tree (PVST) control frames. The default rate limit is 5 PPS.	6.4
[rstp]	Rapid Spanning Tree Protocol (RSTP) control frames. The default rate limit is 5 PPS.	6.4
[lpbk]	Loopback (used for debug). The default rate limit is 5 PPS.	6.4
[rmtlpbk]	Remote loopback (used for debug). The default rate limit is 5 PPS.	6.4

[twamp]	Two-Way Active Measurement Protocol (TWAMP) test frames. The default rate limit is 100 PPS.	6.4
[twampRsp]	Two-Way Active Measurement Protocol (TWAMP) response frames. The default rate limit is 100 PPS.	4.6.2
[dfilt]	Unknown control frames (do not match other packet classes). The default rate limit is 500 PPS.	6.4

Example:

```
> flow cpu-rate-limit unset port 15 twamp
```

flow mac-addr flush	Flushes all MAC addresses for:	su	6.0
{port <PortNo>	Port number.		6.0
{vlan <VlanId>}	VLAN identifier.		6.0

Example:

```
> flow mac-addr flush vlan 127
```

flow mac-addr show	Displays all dynamic and static MAC address entries. Optionally, displays:	su/lu	6.0
[mac <MacAddress>]	Entries for a specific MAC address.		6.0
[port <PortNo>]	Entries for a specific port.		6.0
[vlan <VlanList> [mac <MacAddress> table-count]]	All entries for a specific VLAN, a specific MAC address within the specified VLAN, or a count of all entries for the specified VLAN.		6.0

Example:

```
> flow mac-addr show
```

```
+----- FLOW MAC-LEARN TABLE -----+
| VLAN | Address (SA) | Port | Type |
+-----+-----+-----+-----+
| 1     | 00:BB:CC:DD:EE:FF | 1     | Dyna |
| 127   | 00:AA:CC:DD:EE:FF | 1     | Dyna |
| 300   | AA:BB:CC:DD:EE:FF | 5     | Stat |
+-----+-----+-----+-----+
```

flow show	Displays high level flow information, including:	su/lu	6.0
{[aging],	Aging information.		6.0
[mac-addr]}	MAC learning table, includes static and dynamic entries.		6.0

Example:

```
> flow show aging
```

```
+----- AGING-INFO -----+
| Parameter      | Value      |
+-----+-----+
| Status         | Enabled    |
| Time (Seconds) | 400        |
+-----+-----+
```

flow static-mac add	Adds a static mac entry to the table with the following attributes:	su	6.0
{mac <MacAddress>}	• MAC address.		6.0
{port <PortNo>}	• Port number.		6.0
{vlan <VlanId>}	• VLAN ID.		6.0

Example:

```
> flow static-mac add mac 00:11:22:33:44:55 port 5 vlan 127
```

flow static-mac remove	Adds a static mac entry to the table with the following attributes:	su	6.0
{mac <MacAddress>}	• MAC address.		6.0
{vlan <VlanId>}	• VLAN ID.		6.0

Example:

```
> flow static-mac remove mac 00:11:22:33:44:55 port 5 vlan 127
```

flow static-mac show	Adds a static mac entry to the table with the following attributes:	su	6.0
{mac <MacAddress>}	• MAC address.		6.0
{vlan <VlanId>}	• VLAN ID.		6.0

Example:

```
> flow static-mac show
```

```
+----- FLOW STATIC-MAC TABLE -----+
| VLAN | Address          | Port |
+-----+-----+
| 127   | 00:11:22:33:44:55 | 5     |
| 127   | 00:33:33:33:33:33 | 3     |
+-----+-----+
```

interface

Command	Description	Access Level	Release Introduced
interface ip-acl add	Adds an IP-ACL entry and optionally specifies which physical ports the entry is restricted to accepting frames from.	su	6.4

{ip <IPAddress>}	6.4
{netmask <IPAddress>}	6.4
[port <PortNameList>]	6.4

Example:

```
> interface ip-acl add ip 10.10.10.100 netmask 255.255.255.255
```

interface ip-acl clear statistics	Clears the global and IP-ACL entry statistics counters.	su	6.4

Example:

```
> interface ip-acl clear statistics
```

interface ip-acl enable	Enables processing IP-ACL entries.	su	6.4

Example:

```
> interface ip-acl enable
```

interface ip-acl disable	Disables processing IP-ACL entries.	su	6.4

Example:

```
> interface ip-acl disable
```

interface ip-acl import	Import IP addresses and IP mask of configured interfaces into the IP ACL list.	su	6.4

Example:

```
> interface ip-acl import
```

interface ip-acl remove [ip <IPAddress>] [netmask <IPAddress>]	Removes an IP-ACL entry.	su	6.4

Example:

```
> interface ip-acl remove ip 10.10.10.100 netmask 255.255.255.255
```

interface ip-acl set [ip <IPAddress>] [netmask <IPAddress>] [port <PortNameList>]	Updates an IP-ACL entry.	su	6.4

Example:

```
> interface ip-acl remove ip 10.10.10.100 netmask 255.255.255.0
```

interface ip-acl show	Displays the current state of the IP-ACL facility and the individual IP-ACL entries.	su/lu	6.4

Example:

```
> interface ip-acl show
```

interface local disable	Disables the local management interface.	su	6.4

Example:

```
> interface local disable
```

interface local enable	Enables the local management interface. (Applicable to the CN 3920 only.)	su	6.3

Example:

```
> interface local enable
```

interface local set	Updates the local management interface attributes. Note that the local and remote management interfaces cannot be configured to the same IP subnet.	su	6.3

{[ip <IpAddress>],	• IP address.	6.3

[subnet <SubnetMask>],	• Subnet mask in dotted decimal format.	6.3

(The CN 3911 does not support the local management interface.)

Example:

```
> interface local set ip 1.2.3.4
```

interface remote disable	Disables the remote management interface.	su	6.0

Example:

```
> interface remote disable
```

interface remote enable	Enables the remote management interface.	su	6.0

Example:

```
> interface remote enable
```

interface remote set	Updates the remote management interface attributes. Note that the local and remote management interfaces cannot be configured to the same IP subnet.	su	6.0

{[ip <IpAddress>],	• IP address.	6.0

[subnet <SubnetMask>],	• Subnet mask in dotted decimal format.	6.0

[vlan <VlanID>]}	• VLAN.	6.0

Example:

```
> interface remote set ip 1.2.3.4
```

interface remote show	Displays the remote management interface configuration.	su/lu	6.0

Example:

```
> interface remote show
```

tap1				
Parameter	Operational	User	DHCP	
IP Address	172.26.0.26	0.0.0.0	172.26.0.26	
Subnet Mask	255.255.0.0	0.0.0.0	0.0.0.0	
Index	2			
Admin State	Enabled			
Oper State	Enabled			
Broadcast Address	172.26.255.255			
MAC Address	00:02:a1:07:a4:a0			
VLAN	127			
Priority	7			
MTU	1500			

interface route add	Adds a route to the routing table with the following attributes:	su	6.0
{[destination <IpAddress>],	• Destination IP address.		6.0
[gateway <IpAddress>],	• Gateway IP address.		6.0
[genmask <Mask>],	• Route Mask in dotted decimal format.		6.0
[metric <NUMBER>]}	• Interface metric.		6.0

Example:

```
> interface route add gateway 172.16.233.0 genmask 255.255.255.0
```

interface route remove	Removes a route from the routing table specified by the following attributes:.	su	6.0
[destination <IpAddress>]	• Destination IP address.		6.0
[gateway <IpAddress>]	• Gateway IP address.		6.0
[genmask <Mask>]	• Route Mask in dotted decimal format.		6.0

Example:

```
> interface route remove gateway 172.16.233.0
```

interface route show	Displays the routing table.	su	6.0

Example:

```
> interface route show
```

ROUTING TABLE							
	Act	User	Destination	Gateway	Genmask	Metric	Intf
1	*		172.26.0.0	0	0.0.0.0	0	2
2	*		0.0.0.0	172.26.0.1	0.0.0.0	0	2

interface serial-console disable	Disables login access to the serial console interface.	su	6.0

Example:

```
> interface serial-console disable
```

interface serial-console enable	Enables login access to the serial console interface.	su	6.0

Example:

```
> interface serial-console enable
```

interface serial-console show	Displays the status of the serial console interface.	su/lu	6.0

Example:

```
> interface serial-console show
+-----serial console-----+
| Parameter      | Value                |
+-----+-----+
| serial login   | disabled             |
+-----+-----+
```

interface show	Displays all or the specified interface configurations for the following:	su/lu	6.0
[gateway]	• Default gateway.		6.0
[local]	• Local interface. (Applicable to the CN 3920 only.)		6.3
[remote]	• Remote interface.		6.0

Example:

```
> interface show gateway
```

```
+----- GATEWAY STATUS -----+
| Type   | Address      | Arp Status      | Oper Status |
+-----+-----+-----+-----+
| DHCP   | 0.0.0.0      | N/A             | Disabled    |
| User   | 192.168.54.1 | Present         | Selected    |
+-----+-----+-----+-----+
```

lldp

Link Layer Discovery Protocol (LLDP) commands.

Commands	Description	Access Level	Release Introduced
lldp clear [port <PhyPortNameList>] statistics	Clears the LLDP statistics on the specified ports or for all ports if no ports are specified.	su	6.1
Example:			
>lldp clear port 1 statistics			
lldp disable	Globally disables LLDP.	su	6.1

Example:

```
>lldp disable
```

lldp enable [port <PhyPortNameList>]	Globally enables LLDP.	su	6.1

Example:

```
>lldp enable
```

lldp set	Sets LLDP global parameters, including:	su	6.1

{[msg-interval <NUMBER: 5-3600>],	msg-interval - Sets the interval (in seconds) between successive LLDP transmissions. The range is 5 to 3600, default is 30.		6.1

[msg-tx-hold <NUMBER: 2-10>],	msg-tx-hold - Sets the transmit hold multiplier, which is multiplied times the message interval setting to populate the Time to Live (TTL) TLV. The range is 2 to 10, default is 4 seconds.		6.1

[notif-interval <NUMBER: 5-3600>],	notif-interval - Controls the transmission of LLDP notifications. No more than 1 notification may be sent within this throttling period. The range is 5 to 3600 seconds, default is 5 seconds.		6.1

[reinit-delay <NUMBER: 1-10>],	reinit-delay - Defines the number of seconds that must pass after the LLDP operation for a port has been disabled before any further LLDP activity can occur on that port. The range is 1 to 10 seconds, default is 2.		6.1

[tx-delay <NUMBER:1 - 8192>}}	tx-delay - Sets the re-initialization delay parameter value. This value defines the number of seconds that must pass after LLDP operation for a port has been disabled before any further LLDP activity can occur on that port. The range is 1 to 8192 seconds: default is 2.		6.1

Example:

```
>lldp set msg-interval 60
```

lldp set port <PhyPortNameList>	Sets the per port attributes, including:	su	6.1

{[mode rx-only tx-only tx-rx disable],	Mode		6.1

[notification <on off>}}	Notification		6.1

Example:

```
>lldp set port 3/1 mode disable notification off
```


lldp show	Displays bridge configuration, port configuration, statistics, and TLVs. Optionally, displays:	su/lu	6.1
[configuration]	Bridge and port configuration only.		6.1
[statistics]	Bridge statistics only.		6.1
[neighbors]	LLDP neighboring devices.		6.1
[port <PhyPortNameList> [configuration statistics]]	Configuration and detailed statistics for a specified port. Optionally, displays configuration or statistics only for the specified port.		6.1

Example:

```
>lldp show port 1 configuration
+----- LLDP Port Configuration -----+
|      |      | Basic | Org Specific |      |
|      | Admin| TLV  | Dot1  | Dot3 |      |
| Port | State| 123456789|1234567|1234|  |Notif|
+-----+-----+-----+-----+-----+
| 1    | Tx-Rx| 111111111|1 1111|1111|  | Off |
+-----+-----+-----+-----+-----+
Where:
Dot3 Type  |||+-- 4 Maximum Frame Size  TlvTx
Dot3 Type  |||+-- 3 Link Aggregation  TlvTx
Dot3 Type  |||+-- 2 Power via MDI  TlvTx
Dot3 Type  |||+-- 1 MacPhy Config  TlvTx
Dot1 Type  |||+-- 7 Protocol ID OAM  TlvTx
Dot1 Type  |||+-- 6 Protocol ID Dot1X  TlvTx
Dot1 Type  |||+-- 5 Protocol ID STP  TlvTx
Dot1 Type  |||+-- 4 Protocol ID LACP  TlvTx
Dot1 Type  |||+-- 3 VLAN Name  TlvTx
Dot1 Type  |||+-- 2 Port&Protocol VLAN ID  TlvTx
Dot1 Type  |||+-- 1 Port VLAN ID  TlvTx
Basic Type  |||+-- 9 Local Mgmt Address  TlvTx
Basic Type  |||+-- 8 Remote Mgmt Address  TlvTx
Basic Type  |||+-- 7 System Capabilities  TlvTx
Basic Type  |||+-- 6 System Description  TlvTx
Basic Type  |||+-- 5 System Name  TlvTx
Basic Type  |||+-- 4 Port Description  TlvTx
Basic Type  |||+-- 3 Time-to-Live  TlvTx
Basic Type  |||+-- 2 Port ID  TlvTx
Basic Type  |||+-- 1 Chassis ID  TlvTx
```

lldp tlvtx set port <PhyPortNameList>	Sets the per port TLV transmit parameters, including:	su	6.1
{[mgmt-addr-remote <on off>],	Remote management address.		6.1
[port-descr <on off>],	Port description.		6.1
[system-cap <on off>]]	System capabilities.		6.1
[system-descr <on off>],	System description.		6.1
[system-name <on off>],	System name.		6.1

Example:

```
> lldp tlvtx set port 1 system-cap on
```

lldp tlvtx show [port <PhyPortNameList>]	Displays the LLDP TLV transmit configuration information for all or specified ports.	su/lu	6.1

Example:

```
>lldp tlvtx show
+- LLDP  Config -+
|      | Basic |
|      | TLV  Type|
| Port |123456789|
+-----+-----+
|1      |111111111|
|2      |111111111|
|3      |111111111|
|4      |111111111|
|5      |111111111|
|6      |111111111|
|7      |111111111|
|8      |111111111|
|9      |111111111|
|10     |111111111|
+-----+-----+
```

```
Where: |||||
|||+-- 9 Local Mgmt Address   TlvTx
|||+-- 8 Remote Mgmt Address TlvTx
|||+-- 7 System Capabilities  TlvTx
|||+-- 6 System Description   TlvTx
|||+-- 5 System Name          TlvTx
|||+-- 4 Port Description     TlvTx
||+-- 3 Time-to-Live          TlvTx
||+-- 2 Port ID               TlvTx
||+-- 1 Chassis ID            TlvTx
```

lldp tlvtx-dot1 set port <PhyPortNameList>	Sets the 802.1 per port TLV transmit parameters, including:	su	6.1
{[port-vlan-id <on off>],	• Port VLAN ID. Default is on.		6.1
[protocol-id-dot1<on off>],	• 802.1x		6.4
[protocol-id-lacp <on off>],	• LACP		6.4
[protocol-id-oam <on off>],	• 802.3ah OAM		6.3
[protocol-id-stp <on off>]}	• Rapid Spanning Tree Protocol		6.3

Example:

```
> lldp tlvtx-dot1 set port 1 port-vlan-id off
```

lldp tlvtx-dot1 show [port <PhyPortNameList>]	Displays the LLDP 802.1 TLV transmit configuration information for all or specified ports.	su/lu	6.2

Example:

```
>lldp tlvtx-dot1 show
```

```
+ LLDP Config +
|   | Org Spe |
|   | Dot1   |
| Port | 1234567 |
+-----+
| 1 | 1 1111 |
| 2 | 1 1111 |
| 3 | 1 1111 |
| 4 | 1 1111 |
| 5 | 1 1111 |
| 6 | 1 1111 |
| 7 | 1 1111 |
| 8 | 1 1111 |
| 9 | 1 1111 |
|10 | 1 1111 |
+-----+
```

```
Where: | | | | | | |
        | | | | | | | +-- 7 Protocol ID OAM      TlvTx
        | | | | | | | +-- 6 Protocol ID Dot1X    TlvTx
        | | | | | | | +-- 5 Protocol ID STP      TlvTx
        | | | | | | | +-- 4 Protocol ID LACP     TlvTx
        | | | | | | | +-- 3 VLAN Name           TlvTx
        | | | | | | | +-- 2 Port&Protocol VLAN ID TlvTx
        +-- 1 Port VLAN ID                     TlvTx
```

lldp tlvtx-dot3 set port <PhyPortNameList>	Sets the 802.1 per port TLV transmit parameters, including:	su	6.2
{[mac-phy-config <on off>],	MAC/PHY Configuration/Status TLV- advertises Auto-negotiation support and status, PMD auto-negotiation capability, and Operational MAU type.		6.2
[power-via-mdi <on off>],	Power via MDI TLV- The system software stores values received from the remote partner for this TLV but does not transmit this TLV.		6.3
[link-agg <on off>],	Link Aggregation TLV- advertises whether the link is capable of being aggregated, whether the link is currently in an aggregation, and the port ID of the aggregation if it is in an aggregation. LLDP advertises Link Agg TLV in the PDU but Link Aggregation is not currently supported and is disabled.		6.2
[[max-frame-size <on off>]]	Maximum Frame Size TLV- advertises the maximum frame size capability.		6.2

Example:

```
> lldp tlvtx-dot3 set port 1 link-agg off
```

```
lldp tlvtx-dot3 show
[port <PhyPortNameList>]
```

Displays the LLDP 802.3 TLV transmit configuration information for all or specified ports.

su/lu

6.1

Example:

```
> lldp tlvtx-dot3 show
```

```
+ LLDP Config +
```

```
|      |Org Spe|
|      |Dot3   |
| Port |1234    |
+-----+
```

```
|1      |1111    |
|2      |1111    |
|3      |1111    |
|4      |1111    |
|5      |1111    |
|6      |1111    |
|7      |1111    |
|8      |1111    |
|9      |1111    |
|10     |1111    |
+-----+
```

Where:

```
||||
|||+-- 4 Maximum Frame Size      TlvTx
||+-- 3 Link Aggregation         TlvTx
|+-- 2 Power via MDI             TlvTx
+-- 1 MacPhy Config              TlvTx
```

log

Command	Description	Access Level	Release Introduced
log flash add filter <LogFlashFilterName[15]>	Adds attributes to a flash log filter, including:	su	6.1
[all-mgrs],	All logging categories		6.3
[arp-mgr <all info>],	ARP logging categories.		6.3
[blade-mgr <all config info>],	Categories for module (blade) management.		6.1
[bcast-containment-mgr <all info>],	Broadcast containment categories.		6.3
[chassis-mgr <all info>],	Categories for chassis management.		6.1
[cfm-mgr <all info>],	CFM categories.		6.3
[config-mgr <all info>],	Categories for configuration management.		6.1
[dhcp-mgr <all debug error info options pkt sm timers>],	Categories for DHCP client management.		6.1
[dnld-mgr <all info>],	Categories for download management.		6.1
[dnsc-mgr <all info monitor resolve>],	DNS client categories.		6.3
[dot1x <all info>],	802.1x categories.		6.4
[event-mgr <all info>],	Categories for event management.		6.1
[flow-mgr <all info>],	Flow management categories.		6.3
[igmp-mgr <all events egress-pkt info ingress-pkt>],	IGMP and multicast services categories.		6.3
[interface-mgr <all debug info>],	Categories for interface management.		6.1
[lACP-mgr <all error info notif mux-sm ptx-ss-pkt>]	Categories for LACP management.		6.4
[lldp-mgr <all error info notif other pdu sm>],	Categories for LLDP management.		6.1
[max-severity <critical major minor warning config info debug>]	Maximum severity to log.		6.1
[min-severity <critical major minor warning config info debug>]	Minimum severity to log.		6.1
[mstp-mgr <all info>],	MSTP categories.		6.3

[ntpc-mgr <all config debug info>],	• Categories for NTPC management.	6.1
[ntwrk-mgr <all info>],	• Network categories.	6.3
[oam-mgr <all info>],	• OAM categories.	6.3
[port <PortNameList>],	• List of port names to log.	6.1
[port-mgr <all config info state-change>],	• Categories for port management.	6.1
[radius-mgr <all info>],	• RADIUS categories.	6.3
[security-mgr <all info>],	• Security management categories.	6.3
[ssh-mgr <all info>],	• SSH categories.	6.3
[snmp-mgr <all info>],	• Categories for SNMP management.	6.1
[software-mgr <all info>],	• Categories for software management.	6.3
[tacacs-mgr <all info>],	• Categories for TACACS+.	6.4.1
[traffic-profiling-mgr <all info>],	• Traffic profiling categories.	6.3
[twamp-mgr <all info>],	• TWAMP categories.	6.3
[virtual-circuit-mgr <all info>],	• Virtual circuit categories	6.3
[xcvr-mgr <all debug info>]}	• Categories for transceiver management.	6.1

Example:

```
> log flash add filter myFilter blade-mgr all
```

log flash add pkt-filter <LogFlashPacketFilterName[15]>	Adds packet types or ports to a flash log pkt-filter, including:	su	6.1
[igmp-pkt <all egress ingress>],	• IGMP packet types.		6.1
[ip-pkt <all egress ingress>],	• IP packet types.		6.1
[larp-pkt <all egress ingress>],	• LACP packet types.		6.1
[lldp-pkt <all egress ingress>],	• LLDP packet types.		6.1
[mstp-pkt <all egress ingress>],	• MSTP packet types.		6.1
[port <PortNameList>],	• List of ports to log.		6.1
[rstp-pkt <all egress ingress>]}	• RSTP packets.		6.1

Example:

```
> log flash add pkt-filter myPktFilter lldp-pkt all
```

log flash clear	Clears the flash log.	su

Example:

```
> log flash clear
```

log flash log flash create filter <LogFlashFilterName[15]>	Creates a flash log filter with the following attributes:	su	6.1
{[blade-mgr <all config info>],	Categories for module (blade) management.		6.1
[chassis-mgr <all info>],	Categories for chassis management.		6.1
[config-mgr <all info>],	Categories for configuration management.		6.1
[dnld-mgr <all info>],	Categories for download management.		6.1
[dhcp-mgr <all debug error info options pkt sm timers>],	Categories for DHCP client management.		6.1
[dot1x <all info>],	802.1x categories.		6.4
[event-mgr <all info>],	Categories for event management.		6.1
[interface-mgr <all debug info>],	Categories for interface management.		6.1
[lACP-mgr <all error info notif mux-sm ptx-ss-pkt>]	Categories for LACP management.		6.4
[lldp-mgr <all error info notif other pdu sm>],	Categories for LLDP management.		6.1
[max-severity <critical major minor warning config info debug>]	Maximum severity to log.		6.1
[min-severity <critical major minor warning config info debug>]	Minimum severity to log.		6.1
[ntpc-mgr <all config debug info>],	Categories for NTPC management.		6.1
[port <PortNameList>],	List of port names to log.		6.1
[port-mgr <all config info state-change>],	Categories for port management.		6.1
[snmp-mgr <all info>],	Categories for SNMP management.		6.1
[software-mgr <all info>],	Categories for software management.		6.1
[tacacs-mgr <all info>],	Categories for TACACS+.		6.4.1
[xcvr-mgr <all debug info>]}	Categories for transceiver management.		6.1

Example:

```
> log flash create filter myFilter min-severity debug
```

log flash create pkt-filter <LogFlashPacketFilterName[15]>	Creates a flash log packet filter with the following packet types:	su	6.1

{[igmp-pkt <all egress ingress>],	• IGMP packet types.	6.1
[ip-pkt <all egress ingress>],	• IP packet types.	6.1
[lacp-pkt <all egress ingress>],	• LACP packet types.	6.1
[lldp-pkt <all egress ingress>],	• LLDP packet types.	6.1
[mstp-pkt <all egress ingress>],	• MSTP packet types.	6.1
[pkt-decode <on off>]	• Enables or disables packet decoding.	6.1
[port <PortNameList>],	• List of ports to log.	6.1
[rstp-pkt <all egress ingress>}}	• RSTP packets.	6.1

Example:

```
> log flash create pkt-filter myPktFilter
```

log flash delete filter <LogFlashFilterName[15]>	Deletes a flash log filter.	su	6.1

Example:

```
> log flash delete filter myFilter
```

log flash delete pkt-filter <LogFlashPacketFilterName[15]>	Deletes a flash log packet filter.	su	6.1

Example:

```
> log flash delete pkt-filter myPktFilter
```

log flash disable	Globally disables logging to flash. Optionally, disables logging for a specified:	su	6.1
[filter <LogFlashFilterName[15]>]]	• Filter.		6.1
[pkt-filter <LogFlashPacketFilterName[15]>]	• Packet filter.		6.1

Example:

```
> log flash disable pkt-filter myPktFilter
```

log flash enable	Globally enables logging to flash. Optionally, enables logging for a specified:	su	6.1
[filter <LogFlashFilterName[15]>]]	• Filter.		6.1
[pkt-filter <LogFlashPacketFilterName[15]>]	• Packet filter.		6.1

Example:

```
> log flash enable pkt-filter myPktFilter
```

log flash remove filter <LogFlashFilterName[15]>	Removes attributes from a log flash filter, including:	su	6.1
{[blade-mgr <all config info>],	• Categories for module (blade) management.		6.1

[chassis-mgr <all info>],	• Categories for chassis management.	6.1
[config-mgr <all info>],	• Categories for configuration management.	6.1
[dnld-mgr <all info>],	• Categories for download management.	6.1
[dhcp-mgr <all debug error info options pkt sm timers>],	• Categories for DHCP client management.	6.1
[dot1x <all info>],	• 802.1x categories.	6.4
[event-mgr <all info>],	• Categories for event management.	6.1
[interface-mgr <all debug info>],	• Categories for interface management.	6.1
[lACP-mgr <all error info notif mux-sm ptx-ss-pkt>]	• Categories for LACP management.	6.4
[lldp-mgr <all error info notif other pdu sm>],	• Categories for LLDP management.	6.1
[max-severity <critical major minor warning config info debug>]	• Maximum severity to log.	6.1
[min-severity <critical major minor warning config info debug>]	• Minimum severity to log.	6.1
[ntpc-mgr <all config debug info>],	• Categories for NTPC management.	6.1
[port <PortNameList>],	• List of port names to log.	6.1
[port-mgr <all config info state-change>],	• Categories for port management.	6.1
[snmp-mgr <all info>],	• Categories for SNMP management.	6.1
[software-mgr <all info>],	• Categories for software management.	6.1
[tacacs-mgr <all info>],	• Categories for TACACS+.	6.4.1
[xcvr-mgr <all debug info>]	• Categories for transceiver management.	6.1

Example:

```
> log flash remove filter myFilter blade-mgr all
```

log flash remove pkt-filter <LogFlashPacketFilterName[15]>	Remove packet types from a packet filter, including:	su	6.1
{[igmp-pkt <all egress ingress>],	• IGMP packet types.		6.1
[ip-pkt <all egress ingress>],	• IP packet types.		6.1
[lACP-pkt <all egress ingress>],	• LACP packet types.		6.1
[lldp-pkt <all egress ingress>],	• LLDP packet types.		6.1

[mstp-pkt <all egress ingress>],	• MSTP packet types.	6.1
[port <PortNameList>],	• List of ports to log.	6.1
[rstp-pkt <all egress ingress>]]	• RSTP packets.	6.1

Example:

```
> log flash create pkt-filter myPktFilter
```

log flash set filter <LogFlashFilterName[15]>	Set severity attributes for a flash log filter, including:	su	6.1
{[max-severity <critical major minor warning config info debug>],	• Maximum severity to log.		6.1
[min-severity <critical major minor warning config info debug>]]	• Minimum severity to log.		6.1

Example:

```
> log flash set filter filter myFilter min-severity info
```

log flash set pkt-filter <LogFlashPacketFilterName[15]>	Set attributes for a flash log pkt-filter	su	6.1
{pkt-decode <on off>}	• Enables or disables packet decoding.		6.1

Example:

```
> log flash set pkt-filter myFilter min-severity info
```

log flash show	Displays a summary of global flash log configuration. Optionally, displays:	su/lu	6.1
[filter <LogFlashFilterName[15]>]]	• Detailed configuration of the specified log flash filter.		6.1
[pkt-filter <LogFlashPacketFilterName[15]>]]	• Detailed configuration of the specified packet filter.		6.1
[log-summary]]	• Summary of log flash filters only.		6.1
[pkt-summary]]	• Summary of log flash packet filters only.		6.1
[severity-mapping]]	• Mapping of event severity values to Syslog severity values.		6.1
[system-events]	• Lists descriptions of potential system events with event ID number, event severity, and Syslog severity. Note that this option lists system events that apply to multiple platforms, including events that are not supported by devices running this system software.		6.1

Example:

```
> log flash show
```

```
+----- FLASH LOG STATE CONFIGURATION -----+
| Admin State      | enabled |
+-----+-----+-----+-----+-----+-----+
```

```
+----- FLASH LOG FILTER CONFIGURATION -----+
| Filter Name      | Admin   | Oper    | Severity | Minimum | No. Ports |
| State            | State   | State   |           |          |           |
+-----+-----+-----+-----+-----+-----+
| default          | enabled | enabled | critical | major   | 10        |
| myFilter         | enabled | enabled | critical | debug   | 1         |
+-----+-----+-----+-----+-----+-----+-----+
```

```
+----- FLASH PKT FILTER CONFIGURATION -----+
| Filter Name      | Admin   | Oper    | Pkt       | No. Frame | No. Ports |
| State            | State   | State   | Decode    | Types     |           |
+-----+-----+-----+-----+-----+-----+
| myPktFilter      | enabled | enabled | off       | 1         | 1         |
+-----+-----+-----+-----+-----+-----+-----+
```

log flash view	Display the entries made to flash since the last time this command was entered. Options include:	su/lu	6.1
[tail <NUMBER: 1-100>]	The 'tail' attribute will display the last number of lines specified.		6.1
[keyword <String[16]>]	The keyword string will search for the keyword in entries and display the corresponding lines.		6.1

Example:

```
> log flash view tail 5
January 2, 2000 17:02:09.000 ntwrk: :Vlan add port vlan 200 added port 3
January 2, 2000 17:02:09.000 ntwrk: :Vlan add port vlan 200 added port 4
January 2, 2000 17:02:16.000 chassis: DHCP IP 172.25.0.2 User dhcp:DHCP System
Time Offset Set, tJanuary 2, 2000 17:02:16.000 chassis: DHCP IP 172.25.0.2 User
dhcp:DHCP System Time Offset Set, tJanuary 2, 2000 17:02:28.000 snmp: :Cannot
ping gateway, cannot send cold trap but making an attempt
```

log ram add filter <LogRamFilterName[15]>	Adds attributes to a ram log filter, including:	su	6.2
[all-mgrs],	All logging categories		6.3
[arp-mgr <all info>],	ARP logging categories.		6.3
[blade-mgr <all config info>],	Categories for module (blade) management.		6.2
[bcast-containment-mgr <all info>],	Broadcast containment categories.		6.3
[cfm-mgr <all info>],	CFM categories.		6.3
[chassis-mgr <all info>],	Categories for chassis management.		6.2

[config-mgr <all info>],	• Categories for configuration management.	6.2
[dhcp-mgr <all debug error info options pkt sm timers>],	• Categories for DHCP client management.	6.2
[dnld-mgr <all info>],	• Categories for download management.	6.2
[dnsc-mgr <all info monitor resolve>],	• DNS client categories.	6.3
[dot1x <all info>],	• 802.1x categories.	6.4
[event-mgr <all info>],	• Categories for event management.	6.2
[flow-mgr <all info>],	• Flow management categories.	6.3
[igmp-mgr <all events egress-pkt info ingress-pkt>],	• IGMP and multicast services categories.	6.3
[interface-mgr <all debug info>],	• Categories for interface management.	6.2
[lACP-mgr <all error info notif mux-sm ptx-ss-pkt>]	• Categories for LACP management.	6.4
[lldp-mgr <all error info notif other pdu sm>],	• Categories for LLDP management.	6.2
[mstp-mgr <all info>],	• MSTP categories.	6.3
[ntpc-mgr <all config debug info>],	• Categories for NTPC management.	6.2
[ntwrk-mgr <all info>],	• Network categories.	6.3
[oam-mgr <all info>],	• OAM categories.	6.3
[port <PortNameList>],	• List of port names to log.	6.2
[port-mgr <all config info state-change>],	• Categories for port management.	6.2
[radius-mgr <all info>],	• RADIUS categories.	6.3
[security-mgr <all info>],	• Security management categories.	6.3
[ssh-mgr <all info>],	• SSH categories.	6.3
[snmp-mgr <all info>],	• Categories for SNMP management.	6.2
[software-mgr <all info>],	• Categories for software management.	6.3
[tacacs-mgr <all info>],	• Categories for TACACS+.	6.4.1
[traffic-profiling-mgr <all info>],	• Traffic profiling categories.	6.3
[twamp-mgr <all info>],	• TWAMP categories.	6.3
[virtual-circuit-mgr <all info>],	• Virtual circuit categories	6.3
[xcvr-mgr <all debug info>]]	• Categories for transceiver management.	6.2

Example:

```
> log ram add filter myFilter blade-mgr all
```

log ram add pkt-filter <LogRamPacketFilterName[15]>	Adds packet types or ports to a ram log pkt-filter, including:	su	6.2
[igmp-pkt <all egress ingress>],	• IGMP packet types.		6.2
[ip-pkt <all egress ingress>],	• IP packet types.		6.2
[lACP-pkt <all egress ingress>],	• LACP packet types.		6.2
[lldp-pkt <all egress ingress>],	• LLDP packet types.		6.2
[mstp-pkt <all egress ingress>],	• MSTP packet types.		6.2
[port <PortNameList>],	• List of ports to log.		6.2
[rstp-pkt <all egress ingress>]]	• RSTP packets.		6.2

Example:

```
> log ram add pkt-filter myPktFilter lldp-pkt all
```

log ram clear	Clears the ram log.	su	6.2

Example:

```
> log ram clear
```

log ram log ram create filter <LogRamFilterName[15]>	Creates a ram log filter with the following attributes:	su	6.2
{[blade-mgr <all config info>],	• Categories for module (blade) management.		6.2
[chassis-mgr <all info>],	• Categories for chassis management.		6.2
[config-mgr <all info>],	• Categories for configuration management.		6.2
[dnld-mgr <all info>],	• Categories for download management.		6.2
[dhcp-mgr <all debug error info options pkt sm timers>],	• Categories for DHCP client management.		6.2
[dot1x <all info>],	• 802.1x categories.		6.4
[event-mgr <all info>],	• Categories for event management.		6.2
[interface-mgr <all debug info>],	• Categories for interface management.		6.2
[lACP-mgr <all error info notif mux-sm ptx- ss-pkt>]	• Categories for LACP management.		6.4
[lldp-mgr <all error info notif other pdu sm>],	• Categories for LLDP management.		6.2

[max-severity <critical major minor warning config info debug>]	• Maximum severity to log.	6.2
[min-severity <critical major minor warning config info debug>]	• Minimum severity to log.	6.2
[ntpc-mgr <all config debug info>],	• Categories for NTPC management.	6.2
[port <PortNameList>],	• List of port names to log.	6.2
[port-mgr <all config info state-change>],	• Categories for port management.	6.2
[snmp-mgr <all info>],	• Categories for SNMP management.	6.2
[software-mgr <all info>],	• Categories for software management.	6.2
[tacacs-mgr <all info>],	• Categories for TACACS+.	6.4.1
[xcvr-mgr <all debug info>]}	• Categories for transceiver management.	6.2

Example:

```
> log ram create filter myFilter min-severity debug
```

log ram create pkt-filter <LogRamPacketFilterName[15]>	Creates a ram log packet filter with the following packet types:	su	6.2
{[igmp-pkt <all egress ingress>],	• IGMP packet types.		6.2
[ip-pkt <all egress ingress>],	• IP packet types.		6.2
[larp-pkt <all egress ingress>],	• LACP packet types.		6.2
[lldp-pkt <all egress ingress>],	• LLDP packet types.		6.2
[mstp-pkt <all egress ingress>],	• MSTP packet types.		6.2
[port <PortNameList>],	• List of ports to log.		6.2
[rstp-pkt <all egress ingress>]}	• RSTP packets.		6.2

Example:

```
> log ram create pkt-filter myPktFilter
```

log ram delete filter <LogRamFilterName[15]>	Deletes a ram log filter.	su	6.2

Example:

```
> log ram delete filter myFilter
```

log ram delete pkt-filter <LogRamPacketFilterName[15]>	Deletes a ram log packet filter.	su	6.2

Example:

```
> log ram delete pkt-filter myPktFilter
```

log ram disable	Globally disables logging to ram. Optionally, disables logging for a specified:	su	6.2
[filter <LogRamFilterName[15]>]	• Filter.		6.2
[pkt-filter <LogRamPacketFilterName[15]>]	• Packet filter.		6.2

Example:

```
> log ram disable pkt-filter myPktFilter
```

log ram enable	Globally enables logging to ram. Optionally, enables logging for a specified:	su	6.2
[filter <LogRamFilterName[15]>]	• Filter.		6.2
[pkt-filter <LogRamPacketFilterName[15]>]	• Packet filter.		6.2

Example:

```
> log ram enable pkt-filter myPktFilter
```

log ram remove filter <LogRamFilterName[15]>	Removes attributes from a log ram filter, including:	su	6.2
{[blade-mgr <all config info>],	• Categories for module (blade) management.		6.2
[chassis-mgr <all info>],	• Categories for chassis management.		6.2
[config-mgr <all info>],	• Categories for configuration management.		6.2
[dnld-mgr <all info>],	• Categories for download management.		6.2
[dhcp-mgr <all debug error info options pkt sm timers>],	• Categories for DHCP client management.		6.2
[dot1x <all info>],	• 802.1x categories.		6.4
[event-mgr <all info>],	• Categories for event management.		6.2
[interface-mgr <all debug info>],	• Categories for interface management.		6.2
[lACP-mgr <all error info notif mux-sm ptx-ss-pkt>]	• Categories for LACP management.		6.4
[lldp-mgr <all error info notif other pdu sm>],	• Categories for LLDP management.		6.2
[max-severity <critical major minor warning config info debug>]	• Maximum severity to log.		6.2
[min-severity <critical major minor warning config info debug>]	• Minimum severity to log.		6.2

[ntpc-mgr <all config debug info>],	• Categories for NTPC management.	6.2
[port <PortNameList>],	• List of port names to log.	6.2
[port-mgr <all config info state-change>],	• Categories for port management.	6.2
[snmp-mgr <all info>],	• Categories for SNMP management.	6.2
[software-mgr <all info>],	• Categories for software management.	6.2
[tacacs-mgr <all info>],	• Categories for TACACS+.	6.4.1
[xcvr-mgr <all debug info>]}	• Categories for transceiver management.	6.2

Example:

```
> log ram remove filter myFilter blade-mgr all
```

log ram remove pkt-filter <LogRamPacketFilterName[15]>	Remove packet types from a packet filter, including:	su	6.2
{[igmp-pkt <all egress ingress>],	• IGMP packet types.		6.2
[ip-pkt <all egress ingress>],	• IP packet types.		6.2
[lacp-pkt <all egress ingress>],	• LACP packet types.		6.2
[lldp-pkt <all egress ingress>],	• LLDP packet types.		6.2
[mstp-pkt <all egress ingress>],	• MSTP packet types.		6.2
[port <PortNameList>],	• List of ports to log.		6.2
[rstp-pkt <all egress ingress>]}	• RSTP packets.		6.2

Example:

```
> log ram create pkt-filter myPktFilter
```

log ram set filter <LogRamFilterName[15]>	Set severity attributes for a ram log filter, including:	su	6.2
{[max-severity <critical major minor warning config info debug>],	• Maximum severity to log.		6.2
[min-severity <critical major minor warning config info debug>]}	• Minimum severity to log.		6.2

Example:

```
> log ram set filter filter myFilter min-severity info
```

log ram set pkt-filter <LogRamPacketFilterName[15]>	Set attributes for a ram log pkt-filter	su	6.2
{pkt-decode <on off>}	• Enables or disables packet decoding.		6.2

Example:

```
> log ram set pkt-filter myFilter min-severity info
```

log ram set global-notify <on off>	Enables or disables broadcasting of RAM log entries to all active CLI sessions.	su	6.5

Example:

```
> log ram set global-notify on
```

log ram show	Displays a summary of global ram log configuration. Optionally, displays:	su/lu	6.2
[filter <LogRamFilterName[15]>]	Detailed configuration of the specified log ram filter.		6.2
[pkt-filter <LogRamPacketFilterName[15]>]	Detailed configuration of the specified packet filter.		6.2
[log-summary]	Summary of log ram filters only.		6.2
[pkt-summary]	Summary of log ram packet filters only.		6.2
[severity-mapping]	Mapping of event severity values to Syslog severity values.		6.2
[system-events]	Lists descriptions of potential system events with event ID number, event severity, and Syslog severity. Note that this option lists system events that apply to multiple platforms, including events that are not supported by devices running this system software.		6.2

Example:

```
> log ram show
```

```
+----- ram LOG STATE CONFIGURATION -----+
| Admin State      | enabled                                     |
+-----+-----+-----+-----+-----+-----+

+----- ram LOG FILTER CONFIGURATION -----+
| Filter Name      | Admin | Oper | Severity | No. Ports |
|                  | State | State | Maximum | Minimum   |
+-----+-----+-----+-----+-----+-----+
| default          | enabled | enabled | critical | major     |
| myFilter         | enabled | enabled | critical | debug     |
+-----+-----+-----+-----+-----+-----+

+----- ram PKT FILTER CONFIGURATION -----+
| Filter Name      | Admin | Oper | Pkt | No. Frame | No. Ports |
|                  | State | State | Decode | Types     |           |
+-----+-----+-----+-----+-----+-----+
| myPktFilter      | enabled | enabled | off   | 1         | 1         |
+-----+-----+-----+-----+-----+-----+
```

log ram trace	Activates and displays the RAM trace buffer to monitor current entries as they occur. To exit the RAM trace buffer commands, press Ctrl+C.	su/lu	6.2
[all]	Optionally, displays all entries.		6.2

Example:

```
> log ram trace
(trace activated)
May 6, 2009 14:14:26.604 chassis: Telnet IP 1.90.90.24 User su:System Session More Enable

--break--
> log ram trace all
January 1, 2000 00:00:39.880 interface: :local interface is operationally enabled
January 1, 2000 00:00:40.344 interface: :remote interface is operationally enabled
January 1, 2000 00:00:40.882 interface: :local interface is operationally enabled
January 1, 2000 00:00:46.121 Software: saos-06-03-00-0091 Build 91
January 1, 2000 00:00:48.632 interface: :remote interface is operationally enabled
January 1, 2000 00:00:56.045 interface: DHCP IP 10.10.121.2 User root:remote interface is
operationally enabled
January 1, 2000 00:01:01.069 chassis: DHCP IP 10.10.121.2 User root:DC power supply 1 failure
-----
```

log send	Sends a message for flash and RAM log files to test filters, specified by:	su	6.4
{[msg <String[127]>	• Message string.		6.4
[severity <critical major minor warning config info debug>]	• Severity of the message.		6.4

Example:

```
> log reset-to-factory-default
```

log reset-to-factory-defaults	Resets all log configuration to default and clears the flash and RAM log files.	su	6.1

Example:

```
> log reset-to-factory-default
```

mstp

NOTE: To enable MSTP commands, the Advanced Ethernet feature license must be installed with the software license install command.

Command	Description	Security Level	Release Introduced
mstp clear [port <PortNameList>] statistics	Clears Multiple Spanning Tree Protocol (MSTP) statistics for all or specified ports.	su	6.3

Example:

```
> mstp clear port 1 statistics
```

mstp disable	Disables MSTP globally within the bridge. Use caution when disabling MSTP as data loops may exist in the network topology. If specified, disables MSTP for the following:	su	6.3
[port <PortNameList>]	List of ports.		6.3

Example:

```
> mstp disable port 1
```

mstp enable	Enables MSTP globally within the bridge or for a specified:	su	6.3
[port <PortNameList>]	List of ports.		6.3

Example:

```
> mstp enable port 1
```

mstp set	Sets the following MSTP parameters:	su	6.3
{[forward-delay <NUMBER: 4-30>],	Forward delay is the time taken before a root or designated port starts forwarding after being selected and determined not to satisfy the rapid transition condition. The operational value is set to the value distributed by the root bridge via BPDU and the configured value is not set until this bridge becomes the elected root bridge. The default value is '15'.		6.3
[hello-time <NUMBER: 1-10>],	Hello time is the time between two consecutive periodic BPDUs. The operational value is set to the value distributed by the root bridge via BPDU and the configured value is not set until this bridge becomes the elected root bridge. The minimum value of '1' is not recommended because the periodic BPDU sending takes up the 1 per second transmit hold count allowance. When rapid convergence takes place, only one BPDU is allowed to send within a second for a port delaying the explicit handshake and rapid topology change. The default value is '2'.		6.3

[loopback-blocking <on off>],	Loopback port blocking prevents data loops by detecting their own BPDUs being looped back to them on the same port. The default value is 'off', which is shown as 'disabled' with the mstp show bridge command.	6.3
[max-age <NUMBER: 6-40>],	Maximum age limits the BPDU life span to limit the size of the spanning tree. The default value is '20'.	6.3
[max-hops <NUMBER: 6-40>],	Maximum hops limits the number of hops for BPDUs. The default is '20'.	6.3
[path-cost-def <stp8021d1998 stp8021t2001>],	Path cost default controls the type of internal and external path costs for the bridge. MSTP supports default path costs defined in IEEE802.1D-1998 and IEEE802.1t-2001. The default value is 'stp8021t2001'.	6.3
[tx-hold-count <NUMBER: 1-10>],	Transmit hold count limits the number of BPDUs a bridge can send per second. The default value is '6'.	6.3
[mst-cfg-id-name <String[32]>]	The configuration name is used for calculating the MST Configuration Identifier for the bridge.	6.3
[mst-cfg-id-rev-level <NUMBER: 0-65535>]	The revision level for calculating the MST Configuration Identifier for the bridge. The numeric value is transmitted in MST BPDUs in the Revision Level of the MST Configuration Identifier field. Since this is limited to 2 octets, the range of this value is 0-65535. The default value is '0'.	6.3

Example:

```
> mstp set mst-cfg-id-name "MST Region 1" mst-cfg-id-rev-level 1
```

mstp set cist bridge-priority <NUMBER: 0-15>	The bridge-priority assigned to the CIST for the bridge is used in the priority component of the CIST Bridge Identifier of BPDUs transmitted from this bridge.	su	6.3

Example:

```
> mstp set cist bridge-priority 1
```

mstp set port <PortNameList>	Sets options for the specified ports, including:	su	6.3

[dynamic-ext-path-cost <on off>]	Turns on or off dynamic calculation of the external path cost. When set to 'on', the external port path cost is calculated dynamically based on the port speed. When set to 'off', the external port path cost is the value configured in the 'ext-path-cost' parameter.	6.3
[edge-port <on off>]	Setting the specified port to be consider an edge port allows for rapid port state transition to the forwarding state. For 10/100 ports, the default value for edge-port is 'on'. For other ports, the default is 'off'.	6.3
[migration-check]	Triggers a migration check by the MSTP Port Protocol Migration State Machine. This is a momentary configuration parameter, setting it to 'on' will initiate the migration check and setting it to 'off' will have no effect.	6.3
[ext-path-cost <NUMBER: 1-200000000>]	Sets the external port path cost for the specified port, which takes effect only if 'dynamic-ext-path-cost' is set to 'off'. The default value is '20000'.	6.3
[point-point-mac <auto force-false force-true>]	Sets how to determine the link for the specified port: auto (automatic mechanisms determine the link), force-true (connected to a point-to-point link) or force-false (not connected to a point-to-point link).	6.3
[auto-edge <on off>]	Sets MSTP to automatically identify the edge ports.	6.3
[restricted-role <on off>]	When set to on, this attribute restricts the port from becoming a root port, even if it has the best priority. The default is 'off'.	6.3
[restricted-tcn <on off>]	When set to on, this attribute restricts the port from forwarding topology change notices.	6.3

Example:

```
> mstp set port 2 dynamic-ext-path-cost on
```

mstp set cist-port	Set the CIST port parameters, including:	su	6.3
{[port-priority <NUMBER: 0-15>],	Port priority is the priority component of the CIST Port Identifier field of BPDUs transmitted from the specified port(s).		6.3

[int-path-cost <NUMBER: 1-200000000>],	• Sets the CIST internal root path cost for the specified port(s). Allowable path cost values are 1-200000000. This sets the CIST Internal Root Path Cost field in BPDUs transmitted from the specified port(s). This value will not be used in the BPDU if dynamic internal path cost is enabled for the CIST on the specified port(s). The default is 20000.	6.3
[dynamic-int-path-cost <on off>]]	• Enables or disables dynamic internal port path cost calculations for the CIST for the specified port(s). When enabled, the CIST Internal Root Path Cost field of BPDUs from the specified port(s) will use a value internally calculated based on link rate (and possibly other factors). When disabled, the configured int-path-cost value for the CIST for the specified port(s) will be used.	6.3
{port <PortNameList>}	• Specified port list.	6.3

Example:

```
> mstp set cist-port dynamic-int-path-cost on
```

mstp show	Displays the following by default:	6.3
	• General bridge information. • MST Configuration ID. • CIST information. • CIST Root Priority Vector. • Port information. • Port CIST information.	
	Optionally shows:	
[bridge]	• Detailed bridge information.	6.3
[cist]	• Detailed CIST information.	6.3
[statistics]	• All MSTP port statistics.	6.3

Example:

```
> mstp show
```

mstp show port <PortNameList>	Displays the CIST information for the specified port(s). Optionally, displays:	su/lu	6.3
[statistics]	• Received and transmitted BPDUs for the specified port(s).		6.3
[state-machine]	• State machine information for the specified port(s).		6.3

Example:

```
> mstp show port 2 statistics
```

mstp show mst-cfg-id	Displays the MSTP configuration ID information. Optionally, displays:	su	6.3
[vlan-mapping-table]	VLAN mapping table.		6.3
[xst-mapping-table]	XST mapping table.		6.3

Example:

```
> mstp show mst-cfg-id
```

multicast-services



NOTE: To enable Multicast Services, the Advanced Ethernet feature license must be installed with the `software license install` command.

- <IpMcastAddrRange>=<NUMBER STRING: xxx.xxx.xxx.xxx, 0<=xxx<=255>-<NUMBER STRING: xxx.xxx.xxx.xxx, 0<=xxx<=255>

Command	Description	Access Level	Release Introduced
multicast-services create	Starts multicast services on the specified VLANs.	su	6.1

vlan <VlanList>			6.1

Example:

```
> multicast-services create vlan 778
```

multicast-services delete	Globally disables all multicast features or disables multicast features on the specified VLAN.	su	6.1
[vlan <VlanList>]			6.1

Example:

```
> multicast-services delete vlan 778
```

multicast-services disable	Globally disables all multicast features or disables multicast features on the specified VLAN.	su	6.1
[vlan <VlanList>]			6.1

Example:

```
> multicast-services disable vlan 777
```

multicast-services enable	Globally enables multicast features. This only allows individual features to operate consistent with their own administrative state settings. For example, if multicast is enabled, and IGMP snooping is disabled, IGMP snooping will still be disabled. If the vlan <VlanList> attribute is included, the command enables multicast on the specified VLAN.	su	6.1

[vlan <VlanList>] 6.1

Example:

```
> multicast-services enable vlan 777
```

multicast-services igmp-snooping disable	Disables IGMP snooping globally.	su	6.1

Example:

```
> multicast-services igmp-snooping disable
```

multicast-services igmp-snooping enable	Enables IGMP snooping globally.	su	6.1

Example:

```
> multicast-services igmp-snooping enable
```

multicast-services igmp-snooping reset	Resets multicast IGMP snooping attributes to defaults.	su	6.1

{[default-router-port], • Resets to 0. 6.1

[router-address-range] • Resets to 0.0.0.0-0.0.0.0 6.1

Example:

```
> multicast-services igmp-snooping reset vlan 778 default-router-port
```

multicast-services igmp-snooping set	Sets the IGMP attributes, including:	su	6.1

{[active-linger-timeout <NUMBER: 0-300>], • Active Linger Timeout - Used for inquisitive leaves. If no join message are received before the timer expires, the port is removed from the group. 6.1

[debug <NUMBER: 0-4294967295>] • Debug only. 6.1

[default-router-port <PortName>], • Default Router Port. The port on the device used to communicate with the router. This port sends and receives the IGMP query and join/leave messages. If a router port is not assigned, the value will be 0. Used if the actual router port is not known. 6.1

[leave-mode <fast inquisitive>],	IGMP Leave Mode. Enables inquisitive leave. When enabled, the Active Linger Timeout is used to remove ports from the multicast group membership table. When a leave report is received by the device, the Last Member Query Interval timer is started and a group-specific query will egress the port. The timer is canceled if a membership report is received on the port. The port is removed from the group when the timer expires.	6.1
[last-member-query-interval <NUMBER: 10-100>],	Last Member Query Interval in deciseconds. Max response time inserted into group-specific queries sent in response to leave messages. Also determines the amount of time between group-specific queries. Ignored when inquisitive-leave is disabled.	6.1
[linger-timeout <NUMBER: 10-300>],	Linger Timeout. The time, in seconds, that a filter will remain in the IGMP table after all hosts have left the group. This is done to give sufficient time for the upstream IGMP router to receive and process the leave message. The filter is removed when the Linger Timeout expires.	6.1
[min-response-time <NUMBER: 50-600 >],	Minimum Query Response Time, in deciseconds (1/10 of a second), that hosts have to respond to an IGMP query.	6.1
[server-topology <centralized distributed>]	Server topology.	6.1
[priority <NUMBER: 0-7>],	L2 Packet Priority. 802.1p priority value assigned to IGMP packets for this VLAN. Default priority is 7.	6.1
[query-delay <NUMBER: 1-100 >],	Proxy Query Delay in deciseconds. Devices send query messages to one port at a time. This setting determines the delay between forwarding messages to each port.	6.1
[query-engine <on off>],	IGMP Query Engine. Enables/Disables the IGMP query engine.	6.1
[query-interval <NUMBER: 10-999999 >],	Proxy Query Interval in seconds. Determines the interval, in seconds when the query engine will send IGMP general queries.	6.1

[query-ip-source-addr <IpAddress>],	Proxy Query Source Address. The default value for query-ip-source-addr is 0.0.0.0. This value is used as the source address for all query messages as well as for proxy-reply messages sent to the router. The default value should work in most cases. However, if this address must be changed because of a router on the network, make sure to use the correct address for the router interface you are using, otherwise, the router may discard all proxy-reply messages from the device.	6.1
[query-response-interval <NUMBER: 10-255>],	Proxy Query Response Interval in deciseconds. Determines the rate at which Devices respond to IGMP queries from the router.	6.1
[robustness <NUMBER: 1-2>],	Robustness. Number of IGMP join or IGMP leave messages to send for each multicast group.	6.1
[router-address-range <IpMcastAddrRange>],	Group Address Range reserved for router. Note that addresses specified for the <IpMcastAddrRange> must be between 224.0.0.0 and 239.255.255.255.	6.1
[router-query-interval <NUMBER: 10-999999>]]	Router Query Interval in seconds. Determines the time (in seconds) to wait for the router to send a General Query message.	6.1

Example:

```
> multicast-services igmp-snooping set query-engine on
```

multicast-services server-port add	Adds a port to a server port group.	su	6.1
{vlan <VlanList>}			6.1
{port <PortNameList>}			6.1

Example:

```
> multicast-services server-port add vlan 778 port 10
```

multicast-services server-port remove	Removes a port from a server port group.	su	6.1
{vlan <VlanList>}			6.1
{port <PortNameList>}			6.1

Example:

```
> multicast-services server-port remove vlan 778 port 10
```

multicast-services show brief	Displays a brief summary of multicast configuration and status.	su/lu	6.1

Example:

```
> multicast-services show brief
```

Multicast-Services: Global Enable										
VLAN	Multi	Snoop	UMF	WMF	Router	Chan	IGMP	Router	Linger	Total
				LIAMS	Port	Stream	Groups	Groups	Groups	Member
777	enabl	disab	F	DDDDD	UNKN	10	10	10	0	0
778	enabl	disab	F	DDDDD	UNKN	0	0	0	0	0

multicast-services show configuration	Displays all configuration settings for all VLANs or specified VLANs.	su/lu	6.1

[vlan <VlanList>]	6.1

Example:

```
> multicast-services show configuration vlan 777
```

MULTICAST CONFIGURATION VLAN 777 VLAN#777	
Global Multicast Services	enable
Multicast Services	enable
UMF	flood
WKM Local Control	flood
WKM Adhoc	flood
WKM St-Multicast	flood
WKM SDP-SAP	flood
WKM Internetwork Control	flood
IGMP CONFIGURATION (general)	
IGMP Snooping	disable
IGMP Server Topology	centralized
IGMP Query Engine	off
IGMP Leave Mode	fast
L2 Packet Priority	7
Robustness	1
IGMP CONFIGURATION (proxy query)	
Proxy Query Interval (s)	125
Proxy Query Response Interval (ds)	50
Proxy Query Delay (ds)	10
Proxy Query Source Address	0.0.0.0
Last Member Query Interval (ds)	10
IGMP CONFIGURATION (router)	
Router Query Interval (s)	250
Linger Timeout (s)	120
Active Linger Timeout (s)	30
Minimum Query Response Interval (ds)	50
Group Address Range (start)	0.0.0.0
Group Address Range (end)	0.0.0.0
Default Router Port	0

multicast-services show everything	Displays all multicast configuration and status for all VLANs or specified VLANs.	su/lu	6.1

Example:

```

> multicast-services show everything
+-----+-----+
| MULTICAST CONFIGURATION VLAN 777 VLAN#777 |
+-----+-----+
...
| IGMP CONFIGURATION (general) |
+-----+-----+
...
| IGMP CONFIGURATION (proxy query) |
+-----+-----+
...
| IGMP CONFIGURATION (router) |
+-----+-----+
...
| IGMP Operational Status VLAN 777 VLAN#777 |
+-----+-----+
...
| EXTERNAL IGMP QUERIER (router) |
+-----+-----+
...
| MULTICAST GROUP STATUS |
+-----+-----+
...
| IGMP STATISTICS |
+-----+-----+
...
+-----+-----+

```

multicast-services show group-status	Displays status of all multicast groups for all VLANs. Optionally, displays:	su/lu	6.1
[vlan <VlanList>]	The status for specific VLANs.		6.1
[group-address <IpMcastAddrRange>]	The status for specific group addresses.		6.1

Example:

```
> multicast-services show group-status
```

```
+-----+-----+-----+-----+-----+-----+-----+
|VLAN|IP address   |state|type|source|members|    uptime    |timeout|
+-----+-----+-----+-----+-----+-----+-----+
| 777|225.001.000.001| act |stat|router|   14 | 0d 17h 22m 22s|      |
+-----+-----+-----+-----+-----+-----+-----+
|VLAN|IP address   |state|type|source|members|    uptime    |timeout|
+-----+-----+-----+-----+-----+-----+-----+
| 777|225.001.000.002| act |stat|router|   14 | 0d 17h 22m 22s|      |
+-----+-----+-----+-----+-----+-----+-----+
|VLAN|IP address   |state|type|source|members|    uptime    |timeout|
+-----+-----+-----+-----+-----+-----+-----+
| 777|225.001.000.003| act |stat|router|   14 | 0d 17h 22m 22s|      |
+-----+-----+-----+-----+-----+-----+-----+
|VLAN|IP address   |state|type|source|members|    uptime    |timeout|
+-----+-----+-----+-----+-----+-----+-----+
| 777|225.001.000.004| act |stat|router|   14 | 0d 17h 22m 22s|      |
+-----+-----+-----+-----+-----+-----+-----+
|VLAN|IP address   |state|type|source|members|    uptime    |timeout|
+-----+-----+-----+-----+-----+-----+-----+
| 777|225.001.000.005| act |stat|router|   14 | 0d 17h 22m 22s|      |
+-----+-----+-----+-----+-----+-----+-----+
|VLAN|IP address   |state|type|source|members|    uptime    |timeout|
+-----+-----+-----+-----+-----+-----+-----+
| 777|225.001.000.006| act |stat|router|   14 | 0d 17h 22m 22s|      |
+-----+-----+-----+-----+-----+-----+-----+
|VLAN|IP address   |state|type|source|members|    uptime    |timeout|
+-----+-----+-----+-----+-----+-----+-----+
| 777|225.001.000.007| act |stat|router|   14 | 0d 17h 22m 22s|      |
+-----+-----+-----+-----+-----+-----+-----+
|VLAN|IP address   |state|type|source|members|    uptime    |timeout|
+-----+-----+-----+-----+-----+-----+-----+
| 777|225.001.000.008| act |stat|router|   14 | 0d 17h 22m 22s|      |
+-----+-----+-----+-----+-----+-----+-----+
|VLAN|IP address   |state|type|source|members|    uptime    |timeout|
+-----+-----+-----+-----+-----+-----+-----+
| 777|225.001.000.009| act |stat|router|   14 | 0d 17h 22m 22s|      |
+-----+-----+-----+-----+-----+-----+-----+
|VLAN|IP address   |state|type|source|members|    uptime    |timeout|
+-----+-----+-----+-----+-----+-----+-----+
| 777|225.001.000.010| act |stat|router|   14 | 0d 17h 22m 22s|      |
+-----+-----+-----+-----+-----+-----+-----+
```

multicast-services show groups	Displays multicast groups for all VLANs and ports. Optionally, displays multicast groups for:	su/lu	6.1
[vlan <VlanList>]	Specified VLANs.		6.1
[port <PortNameList>]	Specified ports.		6.1

Example:

```
> multicast-services show groups
```

VLAN	IP address	state	type	source	members	uptime	timeout
777	225.001.000.001	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.002	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.003	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.004	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.005	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.006	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.007	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.008	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.009	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.010	act	stat	router	14	0d 17h 35m 43s	

multicast-services show status	Shows multicast status for all VLANs. Optionally displays status for:	su/lu	6.1
[vlan <VlanList>]	Specified VLANs.		6.1

Example:

```
> multicast-services show groups
```

VLAN	IP address	state	type	source	members	uptime	timeout
777	225.001.000.001	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.002	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.003	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.004	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.005	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.006	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.007	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.008	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.009	act	stat	router	14	0d 17h 35m 43s	
777	225.001.000.010	act	stat	router	14	0d 17h 35m 43s	

multicast-services umf drop	Enables UMF on the specified VLAN(s).	su	6.1
{vlan <VlanList>}			6.1

Example:

```
> multicast-services umf drop vlan 777
```

multicast-services umf flood vlan <VlanList>	Disables UMF on the specified VLAN(s).	su	6.1
{vlan <VlanList>}			6.1

Example:

```
> multicast-services umf flood vlan 777
```

ntp-client

Command	Description	Access Level	Release Introduced
ntp-client add server <IpAddress>	Adds an NTP server by IP address or host name.	su	6.1
Example:			
> ntp-client add server 192.83.249.31			
ntp-client disable [server <IpAddress>]	Disables the NTP client or disables the specified server IP address or host name from being used for date and time polling.	su	6.1
Example:			
> ntp-client disable server 192.83.249.31			
ntp-client enable [server <IpAddress>]	Disables or enables NTP globally or for the specified server IP address or host name.	su	6.1
Example:			
> ntp-client enable server 192.83.249.31			
ntp-client remove server <IpAddress>	Deletes an NTP server by IP address or host name.	su	6.1
Example:			
> ntp-client remove server 192.83.249.31			
ntp-client set	Sets the specified NTP attributes, including:	su	6.1
{[mode '<polling broadcast>'],	Mode.		6.1
[polling-interval <NUMBER: 16,32,64,128,256,512,1024,2048,4096>]]	The polling-interval is the interval (seconds) between NTP and is only valid in polling mode. Any number can be entered for the interval value, but the system will round the number down to the nearest allowed value.		6.3.1
Example:			
> ntp-client set mode polling polling-interval 64			
ntp-client md5-auth add	Adds an NTP MD5 key plain text entry with the following attributes:	su	6.2
{key-id <NUMBER: 1-4294967295>}	Numeric key identifier.		
{md5 <String[31]>}	Alpha-numeric key string.		

Example:

```
> ntp-client md5-auth add key-id 1 md5 myNTPkey
```

ntp-client md5-auth secret	Adds a secret NTP MD5 encrypted key entry with the following attributes:	su	6.2

{key-id <NUMBER: 1-4294967295>}	Numeric key identifier.

{md5 <String[31]>}	Alpha-numeric key string.

Example:

```
> ntp-client md5-auth secret key-id 5 md5 3bf313a5
```

ntp-client md5-auth disable	Disables NTP MD5 authentication.	su	6.2

Example:

```
> ntp-client md5-auth disable
```

ntp-client md5-auth enable	Enables NTP MD5 authentication.	su	6.2

Example:

```
> ntp-client md5-auth enable
```

ntp-client md5-auth import filename <String>	Imports NTP MD5 keys from a file.	su	6.2

Example:

```
> ntp-client md5-auth import filename myKeyFile.key
```

ntp-client md5-auth remove {key-id <NUMBER: 1-4294967295>}	Removes an NTP MD5 key.	su	6.2

Example:

```
> ntp-client md5-auth remove key-id 7
```

ntp-client md5-auth show	Displays the NTP state and MD5 key entries.	su/lu	6.2

Example:

```
> ntp-client md5-auth show
```

```

+----- NTP STATE -----+
| Parameter | Value |
+-----+-----+
| Admin State | Enabled |
| MD5 Auth Admin State | Enabled |
| Mode | Polling |
| Polling Interval (sec) | 16 |
| Config State | user |
| DHCP NTP Option State | Enabled |
+-----+-----+

```

```

+----- NTP MD5 AUTH KEYS -----+
| Key ID | MD5 |
+-----+-----+
| 1 | 1def24c077b5315b |
+-----+-----+

```


ntp-client show	Displays the NTP state and server configurations or the following options:	su/lu	6.1
[oper]	The oper attribute shows operational NTP servers in priority order.		6.1
[state]	The state attribute shows only NTP state information.		6.1
[server <IpAddress>]	Displays NTP information about the specified server IP address or host name.		6.1

Example:

```
> ntp-client show
```

```
+----- NTP CLIENT STATE -----+
| Parameter           | Value           |
+-----+-----+
| Admin State         | Enabled         |
| Mode                | Polling         |
| Polling Interval (sec) | 16              |
| Config State        | user            |
| DHCP NTP Option State | Enabled         |
+-----+-----+
```

```
+----- NTP CLIENT SERVER CONFIGURATION -----+
| IP Address          | HostName        | Config | Admin | Oper | Server |
|                     |                 | State  | State | State | Status  |
+-----+-----+-----+-----+-----+-----+
| 132.236.56.250      |                 | user   | Enabled | Enabled | SysPeer |
| 192.83.249.31       |                 | user   | Enabled | Enabled | Candidate|
+-----+-----+-----+-----+-----+-----+-----+
```

PBT

NOTE: PBT is not supported on the CN 3911 and CN 3920.

Command	Description	Security Level	Release Introduced
pbt remote-bridge create bridge-name <STRING[15]> bridge-mac <MacAddress>	Creates a remote bridge entry to be identified by the specified name and MAC address.	su	6.4

Example:

```
> pbt remote-bridge create bridge-name sw1 bridge-mac 00:02:a1:37:bc:60
```

pbt remote-bridge delete bridge-name <PbtBridge>	Deletes a remote bridge entry.	su	6.4

Example:

```
> pbt remote-bridge delete bridge-name sw1
```

pbt remote-bridge show	Displays a list of all remote bridge entries.	su/lu	6.4

Example:

```
> pbt remote-bridge show
```

pbt remote-bridge show bridge-name <PbtBridge>	Displays information pertaining to the specified remote bridge.	su/lu	6.4

Example:

```
> pbt remote-bridge show bridge-name sw1
```

pbt release bvid <VlanIdList>	Releases a set of reserved BVIDs.	su	6.4

Example:

```
> pbt release bvid 112-115
```

pbt reserve bvid <VlanIdList>	Reserves a set of Vlan IDs to be used for the tunnel BVIDs.	su	6.4

Example:

```
> pbt reserve bvid 112-115
```

pbt set bridge-mac <MacAddress>	Sets the bridge mac address to be used by the device for PBT.	su	6.4

Example:

```
> pbt set bridge-mac 00:02:a1:30:7c:80
```

pbt set reversion-hold-time <NUMBER: 0-4294967295>	Sets the tunnel reversion hold timer value in milliseconds, which is the length of time before traffic is restored from the backup to primary, after the primary tunnel is back up.		6.4

Example:

```
> pbt set reversion-hold-time 4000
```

pbt set service-tag-ethertype <NUMBER: 2049-65535>	Sets the value for the PBT Service EtherType tag. In order for PBT frames to transit on devices other than the LE-311v, set the tag value to '8100'. Also, set the Acceptable frame type mode to 'all' (port set port <PortNameList> {[acceptable-frame-type <all tagged-only>}).	su	6.4

Example:

```
> pbt set service-tag-ethertype 0x88c8
```

pbt set tunnel-reversion <on off>	Turns on or off tunnel reversion, which restores traffic from the backup to the primary, after the primary tunnel is back up. It is recommended that tunnel reversion settings, on or off and reversion delay time, are configured the same on all remote bridges. The default tunnel reversion value is 'off'.	6.4

Example:

```
> pbt set tunnel-reversion on
```

pbt set tunnel-tag-ethertype <NUMBER: 2049-65535>	Sets the value for the PBT Tunnel EtherType tag.	su	6.4

Example:

```
> pbt set tunnel-tag-ethertype 0x88a8
```

pbt show	Displays global PBT information.	su/lu	6.4

Example:

```
> pbt show
```

port

Command	Description	Access Level	Release Introduced
port disable port <PortNameList>	Disables the specified port(s).	su	6.0
Example:			
>port disable port 1			
port enable port <PortNameList>	Enables or disables the specified port(s).	su	6.0
Example:			
>port enable port 1			
port monitor {statistics total-statistics throughput}	Monitors a summary of current, total, or throughput statistics for all ports. Optionally, you can:	su/lu	6.5
[active]	Display active port statistics (non-zero values only).		6.5
[delay <NUMBER: 1-86400>]	Specify a length of time in seconds to display the statistics.		6.5
[count <NUMBER: 0-4294967295>]	Specify the number of times to repeat the display.		6.5

[scale <tera|giga|mega|kilo|none>]]

- Specifies the units (Giga, Mega, Kilo, or None) in which to display the values. For throughput statistics, the default scale is Mega.

6.5

To stop monitoring, press Ctrl+C.

Example:

```
> port monitor statistics active
<Screen clears>
```

```
+-----+-----+-----+-----+-----+-----+
| Port | Byte | Rx | Tx | Pkt | Rx |
+-----+-----+-----+-----+-----+-----+
| 1 | 8326248088 | 0 | 67147162 | 0 |
| 2 | 8326247964 | 0 | 67147161 | 0 |
| 12 | 0 | 28879569152 | 0 | 225621634 |
+-----+-----+-----+-----+-----+-----+
<Ctrl+C>
--break--
```

port monitor port <PortName>
{statistics|total-statistics|throughput}

Monitors a summary of current, total, or throughput statistics for a specific port. Optionally, you can:

su/lu

6.5

[active]

- Display active port statistics (non-zero values only).

6.5

[delay <NUMBER: 1-86400>]

- Specify a length of time in seconds to display the statistics. The default is 5 seconds.

6.5

[count <NUMBER: 0-4294967295>]

- Specify the number of times to repeat the display.

6.5

[scale <tera|giga|mega|kilo|none>]]

- Specifies the units (Giga, Mega, Kilo, or None) in which to display the values. For throughput statistics, the default scale is Mega.

6.5

[type <all|basic|errors|tx|rx>]

- Filters type of statistics: basic (only received and transmitted packets and bytes), tx-only (transmitted only), rx-only (received only), errors or all.

6.5

To stop monitoring, press Ctrl+C.

Example:

```
> port monitor port 1 statistics active delay 10
<Screen clears>
INFO: Waiting 10 seconds for display. Abort with CTRL-c
```

```
+-----+-----+ PORT 1 STATISTICS +-----+
| Statistic          | Value          |
+-----+-----+
| RxBytes            | 1661228286168  |
| RxPkts             | 2089595334     |
| 65To1270ctsPkts    | 1044797670     |
| TxBytes            | 1356516087138  |
| TxPkts             | 1706324179     |
| TxGiantPkts        | 853152795      |
| TxMcastPkts        | 18107          |
+-----+-----+
```

<Ctrl+C>
--break--

port set port <PortNameList>	Sets the attributes for the specified port, including:	su	6.0
{[acceptable-frame-type <all tagged-only>],	• Acceptable frame types mode.		6.0
[advertised-flow-control <asym-tx off sym-asym-rx>],	• Advertised value for flow control.		6.0
[auto-neg <on off>],	• Auto-negotiation.		6.0
[duplex <half full>],	• Duplex mode.		6.0
[description <String[31]>],	• Port description.		6.0
[egress-untag-vlan <Vlan>],	• VLAN for egressing untagged frames.		6.0
[egress-mirror <PortName>],	• Egress port mirroring.		6.0
[fixed-rcos <NUMBER: 0-7>]	• Fixed Resolved CoS value.		6.2
[flow-ctrl <asym-rx asym-tx off sym>],	• Flow control.		6.3
[ingress-mirror <PortName>]	• Ingress port mirroring.		6.0
[ingress-to-egress-qmap]	• Sets the R-CoS queue map to use in mapping internal CoS (R-CoS) at the ingress port to a CoS queue at an egress port.		6.4
[max-frame-size <NUMBER: 1522-9216>],	• Maximum frame size.		6.0
[mirror-port <on off>],	• Mirror port enables/disables all traffic mirrored to this destination port.		6.0
[mode <default rj45 sfp>],	• Connector mode.		6.2
[loopback <on off>],	• Turn port loopback on or off.		6.3.1
[pvid <Vlan>],	• Port vlan ID.		6.0
[resolved-cos-policy <dot1d-tag1-cos fixed-cos l3-dscp-cos>]	• Resolved CoS policy.		6.2

[speed <ten hundred gigabit auto>],	• Speed.	6.0
[untagged-ctrl-vs <VirtualSwitchName>],	• Virtual switch for untagged control frames.	6.3
[untagged-data-vs <VirtualSwitchName>],	• Virtual switch for untagged data frames.	6.3
[untagged-data-vid <VlanId>],	• VLAN ID for untagged data frames.	6.3
[vlan-ingress-filter <on>],	• VLAN Ingress filter assigns frames that do not explicitly match the subscriber VLAN to a VLAN.	6.0
[vs-ingress-filter <on>]]	• Virtual switch Ingress filter.	6.3

Example:

```
>port set port 1 ingress-to-egress-qmap myrcosmap1
```

port show	Displays a summary of port configuration for all ports. Optionally, displays all port:	su/lu	6.0
[capabilities],	• Capabilities.		6.0
[ethernet-config]	• Ethernet configuration.		6.0
[network-config]	• Network configuration.		6.0
[status]	• Link status.		6.0

Example:

```
>port show
```

Port Table			Operational Status					Admin Config			
Port Name	Port Type	Link	Link State Duration	XCVR	STP	Mode	Auto Neg	Link	Mode	Auto Neg	
1	10/100/G	Up	0d 0h 0m 0s		FWD	100/FD	On	Ena	1000/FD	On	
2	10/100/G	Up	0d 0h 0m 0s		FWD	100/FD	On	Ena	1000/FD	On	
3	10/100/G	Up	0d 0h 0m 0s		FWD	100/FD	On	Ena	1000/FD	On	
4	10/100/G	Up	0d 0h 0m 0s		FWD	100/FD	On	Ena	1000/FD	On	
5	10/100/G	Down	0d 0h 0m 0s		FWD	1000/FD	On	Ena	1000/FD	On	
6	10/100/G	Down	0d 0h 0m 0s		FWD	1000/FD	On	Ena	1000/FD	On	
7	10/100/G	Up	0d 0h 0m 0s		FWD	100/FD	On	Ena	1000/FD	On	
8	10/100/G	Down	0d 0h 0m 0s		FWD	1000/FD	On	Ena	1000/FD	On	
9	10/100/G	Up	0d 0h 0m 0s		FWD	100/FD	On	Ena	100/FD	On	
10	10/100/G	Down	0d 0h 0m 0s		FWD	100/FD	On	Ena	100/FD	On	

port show {statistics total-statistics throughput}	Displays a summary of current, total, or throughput statistics for all ports. Optionally, you can:	su/lu	6.0 statistics, 6.5 total-statistics and throughput
[active]	• Display active port statistics (non-zero values only).		6.5
[delay <NUMBER: 1-86400>]	• Specify a length of time in seconds to display the statistics.		6.5

[count <NUMBER: 0-4294967295>]	Specify the number of times to repeat the display.	6.5
[scale <tera giga mega kilo none>]]	Specifies the units (Giga, Mega, Kilo, or None) in which to display the values. For throughput statistics, the default scale is Mega.	6.5

Example:

> port show statistics active

PORT STATISTICS SUMMARY				
Port	Byte		Pkt	
	Tx	Rx	Tx	Rx
1	8326248088	0	67147162	0
2	8326247964	0	67147161	0
12	0	28879569152	0	225621634

port show port <PortName>	Display details or capabilities for the specified port.	su/lu	6.0
[capabilities]	Capabilities.		6.0

Example:

```
>port show port 1
```

PORT INFO		
Field	Admin	Oper
Type	10/100/G	
Description		
Spanning Tree State	Forwarding	
MAC Address	00:02:a1:07:86:e2	
Phy Loopback	Off	
Link State	Enabled	Enabled
State Group Link State		
Mode	rj45	unknown
Speed	1 Gbps	100 Mbps
Duplex	full	full
Flow Control	off	
Auto Negotiation	Enabled	
Flow Control Advertised	off	
PVID	300	300
Untag Ingress Vtag	1	1
Untag Ingress Data Vid	0	0
Fixed Resolved CoS	0	0
Ingress VLAN Filter	Enabled	Enabled
Ingress VS Filter	Off	Off
Acceptable Frame Type	all	all
Egress Untag VLAN	300	300
Max Frame Size	1526	1526
Untagged Data VS		
Untagged Ctrl VS		
Resolved CoS Policy	dot1d-tag1-cos	dot1d-tag1-cos
Service Port Type	Subscriber	Subscriber
Eth VC EtherType	8100	8100
Eth VC EtherType Policy	all	all
Mirror-port	Off	Off
Ingress-mirror		
Egress-mirror		
Ingress to Egress QMap	Default-RCOS	Default-RCOS
XCVR caps mismatch	<NONE>	
VLAN Membership	1, 100, 200	

port show port <PortName> {statistics total-statistics throughput}	Displays a summary of current, total, or throughput statistics for a specific port. Optionally, you can:	su/lu	6.0 statistics, 6.5 total-statistics and throughput
[active]	Display active port statistics (non-zero values only).		6.5
[delay <NUMBER: 1-86400>]	Specify a length of time in seconds to display the statistics.		6.5
[count <NUMBER: 0-4294967295>]	Specify the number of times to repeat the display.		6.5
[scale <tera giga mega kilo none>]]	Specifies the units (Giga, Mega, Kilo, or None) in which to display the values. For throughput statistics, the default scale is Mega.		6.5

[type <all basic errors tx rx>]	Filters type of statistics: basic (only received and transmitted packets and bytes), tx-only (transmitted only), rx-only (received only), errors or all.	6.5

Example:

```
> port show port 1 statistics active
```

```
+----- PORT 1 STATISTICS -----+
| Statistic      | Value          |
+-----+-----+
| TxBytes        | 8383361868     |
| TxPkts         | 67607757       |
| TxBcastPkts    | 67607757       |
+-----+-----+
```

port state-mirror-group add group <PortStateMirrorGroupName[15]>	Adds destination and source ports to a Port State Mirror group.	su	6.2
{[dst-port <PortNameList>],	Destination ports.		6.2
[src-port <PortNameList>]}	Source ports.		6.2

Example:

```
> port state-mirror-group add group PSMG1 src-port 3,4 dst-port 1,2,5,6
```

port state-mirror-group create group <PortStateMirrorGroupName[15]>	Creates a Port State Mirror Group.	su	6.2

Example:

```
> port state-mirror-group create group PSMG1
```

port state-mirror-group delete group <PortStateMirrorGroupName[15]>	Deletes a Port State Mirror Group.	su	6.2

Example:

```
> port state-mirror-group delete group PSMG1
```

port state-mirror-group remove group <PortStateMirrorGroupName[15]> port <PortNameList>	Deletes ports from a Port State Mirror group.	su	6.2

Example:

```
> port state-mirror-group remove group PSMG1 port 1-3
```

port state-mirror-group rename group <PortStateMirrorGroupName[15]> name <String[15]>	Renames a Port State Mirror Group.	su	6.2

Example:

```
> port state-mirror-group rename group PSMG1 name Group1
```

port state-mirror-group set group <PortStateMirrorGroupName[15]>	Sets the attributes for a Port State Mirror Group, including:	su	6.2
name <String[15]>	New name.		6.2

```
type <uni-directional|bi-directional>
```

- Type of group.

6.2

Example:

```
> port state-mirror-group set group PSMG1 type bi-directional
```

```
port state-mirror-group show
```

[group <PortStateMirrorGroupName[15]>]

Displays Port State Mirror Group configurations for all PSMGs or a specified group.

su/lu 6.2

Example:

```
> port state-mirror-group show
```

```
+-----+-----+-----+-----+-----+-----+
| Name | Type | Collective | Member | Counts |
|-----+-----+-----+-----+-----+
| PSMG1 | UniDir | Link up | 1 | 1 |
+-----+-----+-----+-----+-----+

+-----+-----+-----+-----+-----+-----+
| Port State Mirror Group | Port | Type | Member | Operational State |
|-----+-----+-----+-----+-----+-----+
| PSMG1 | 1 | Dst | Link down |
| PSMG1 | 2 | Src | Link up |
+-----+-----+-----+-----+-----+-----+
```

```
port unset port <PortNameList>{
<egress-mirror|ingress-mirror>}
```

Clears the egress mirror or ingress mirror.

su 6.0

Example:

```
>port unset port 1 ingress-mirror
```

```
port xcvr show
```

Displays a summary of transceivers.

su 6.0

Example:

```
> port xcvr show
```

```
+-----+-----+-----+-----+-----+-----+-----+
| Admin | Oper | Vendor Name & Part Number | Ether Medium & | Diag |
| Port | State | State | Connector Type | Data |
+-----+-----+-----+-----+-----+-----+
| 9 | Ena | | WORLDWIDEPACKETS XCVR-100D53 Rev10 | 1000BASE-LX/LC | Yes |
| 10 | Ena | | WORLDWIDEPACKETS XCVR-100D53 Rev10 | 1000BASE-LX/LC | Yes |
+-----+-----+-----+-----+-----+-----+-----+
```

```
port xcvr show port <PhyPortNameList>
```

Displays transceiver information about the specified port including:

su 6.0

```
{[diagnostics],
```

- Diagnostics, if supported by the transceiver.

6.5

```
[state],
```

- Transceiver status.

6.0

[vendor]} • Vendor information. 6.0

Example:

```
> port xcvr show port 10 state
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|   |Admin| Oper|                               |Ether Medium & |Diag|
|Port|State|State| Vendor Name & Part Number         |Connector Type |Data|
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|10  |Ena  |      |WORLDWIDEPACKETS XCVR-100D53 Rev10  |1000BASE-LX/LC |Yes |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

radius

Command	Description	Access Level	Release Introduced
radius add server <IpHost>	Adds a RADIUS server by IP address or host name. Attributes not specified will be set to the default value. Servers are enabled by default.	su	6.3
[priority <NUMBER: 1-8>]	Priority of the RADIUS server in relation to the other RADIS servers.		6.3
[udp-port<NUMBER:1-65535>]	UDP port. Default is 1812.		6.3
[use-for <all user-login>]	Use of the RADIUS server.		6.3

Example:

```
> radius add server 10.10.10.100 priority 1
```

radius disable [server <IpHostRadius>]	Disables RADIUS globally or on the specified server. If RADIUS is disabled, the server uses the configured local password file.	su	6.3

Example:

```
> radius disable
```

radius enable [server <IpHostRadius>]	Enables RADIUS globally or on the specified server. If RADIUS is disabled, the server uses the configured local password file.	su	6.3

Example:

```
> radius enable server 10.10.10.100
```

radius remove server <IpHostRadius>	Removes a server.	su	6.3

Example:

```
> radius remove server 10.10.10.100
```

radius set	Sets the global radius attributes. At least one attribute must be specified.	su	6.3
{[key <String[8-128]>],	The authentication string used to verify that the device is authorized to access the RADIUS server. The key must be between 8 and 128 characters in length and must be the same for all RADIUS servers specified. Allowable key strings include ASCII values 32-126, except for ASCII 34 is not allowed. ASCII 32 (space) characters used at the beginning or end of the key are not allowed and will be discarded. If a space is used in the middle of the string, enclose the string in quotes.		6.3
[retries <NUMBER: 0-3>],	Number of times the client should attempt to contact the RADIUS server before declaring it unreachable.		6.3
[secret <String[128]	Sets the key using a pre-encrypted string.		6.3
[timeout <NUMBER: 1-30>]]	Length of time, in seconds, that the device will wait for a response from the RADIUS server.		6.3
[search-method <priority [NUMBER: 1-8]> cached]]	Specifies to search by either priority or cached (last accessed).		6.3.1
radius set server <IpHost> { [priority <NUMBER:1-8>], [udp-port <NUMBER:1-65535>], [use-for <all dot1x user-login>]}	Updates the host priority, UDP port, or server use.		6.3.1

Example:

```
> radius set key 2manysecrets retries 2 timeout 2
```

radius set server <IpHostRadius>	Sets the RADIUS server attributes, including:	su	6.3
{[priority <NUMBER: 1-8>],	Priority of the RADIUS server in relation to the other RADIS servers.		6.3
[udp-port<NUMBER:1-65535>],	UDP port.		6.3
[use-for <user-login>]	Use of the RADIUS server.		6.3

Example:

```
> radius set server 10.10.10.100 use-for user-login
```

radius show [stats]	Displays the current RADIUS configuration or statistics.	lu/su	6.3

Example:

```
> radius show
+-- RADIUS ATTRIBUTES --+
| Parameter | Value |
+-----+
| Admin State | Enabled |
| Oper State | Enabled |
| Retries | 3 |
| Timeout | 1 |
| Key | ***** |
| Search type | Cached |
+-----+

+----- RADIUS SERVER TABLE -----+
| IP Address | HostName | Pri | UDP | State | App |
| Port |
+-----+
| 10.10.10.100 | | 1 | 1812 | Ena | User-login |
+-----+

> radius show stats
+----- Radius Server Statistics -----+
+-----+
| IP Address : 10.10.10.100 |
| Access Requests : 971 |
| Access Rejects : 0 |
| Access Accepts : 971 |
| Access Challenges : 0 |
| Access Retransmission : 0 |
| Bad Authenticators : 0 |
| Pending Requests : 0 |
| Packets Dropped : 0 |
| Malformed Responses : 0 |
+-----+
```

rmon

Command	Description	Security Level	Release Introduced
rmon alarm add	Sets RMON history attributes, including:	su	6.2
{data-source <String[127]>}	• Interface OID name		6.2
{falling-event-index <NUMBER:1-65535>}	• Falling event index		6.2
{falling-threshold <NUMBER:0-999999999>}	• Falling alarm threshold		6.2
{index <NUMBER:1-65535>}	• Index in the alarm table		6.2
{interval <NUMBER:1-3600>}	• Interval to be used		6.2
[owner <String[127]>]	• Name of the owner		6.2
{rising-event-index <NUMBER:1-65535>}	• Rising event index		6.2

{rising-threshold <NUMBER:0-999999999>}	• Rising alarm threshold	6.2
{sample-type <absolute delta >} {	• Type of sample	6.2
startup-alarm <rising falling both>}	• Startup alarm	6.2

Example:

```
> rmon alarm add data-source 1.3.6.1.2.1.16.1.1.1.5 index 1 interval 30 owner Admin sample-type absolute startup-alarm both falling-event-index 1 fallingthreshold 100 rising-event-index 1 rising-threshold 900
```

rmon alarm remove index <NUMBER:1-65535>	Removes the specified Ethernet statistics entry.	su	6.2

Example:

```
> rmon alarm remove index 1
```

rmon event add	Sets RMON event attributes.	su	6.2
[community <String[127]>]	• Event community name	6.2	
[owner <String[127]>]	• Name of the owner	6.2	
{description <String[127]>}	• Description of the event	6.2	
{index <NUMBER:1-65535>}	• Index in the event table	6.2	
{type <none log snmp-trap log-and-snmptap>}	• Type of event	6.2	

Example:

```
> rmon event add index 1 description Test type log community Network1 owner Admin
```

rmon event remove index <NUMBER:1-65535>	Removes the specified Ethernet statistics entry.	su	6.2

Example:

```
> rmon event remove index 1
```

rmon history add	Sets RMON history attributes.	lu/su	6.2
{data-source <String[127]>}	• Interface OID name	6.2	
{index <NUMBER:1-65535>}	• Index in the history table	6.2	
[interval <NUMBER:1-3600>]	• Interval used for monitoring	6.2	
[num-buckets <NUMBER:1-65535>]	• Number of buckets to use	6.2	
[owner <String[127]>]	• Name of the owner	6.2	
[file-logging <on off>]	• Enables or disables file-logging which makes the history persistent	6.2	

Example:

```
> rmon history add data-source 1.3.6.1.2.1.16.1.1.1.5 index 1 interval 12 num-buckets 78 owner Admin
```

rmon history remove index <NUMBER:1-65535>	Removes the specified Ethernet statistics entry.	su	6.2

Example:

```
> rmon history remove index 1
```

rmon file	Push a file containing historical data to a TFTP server.	su	6.2
{[name<String[16]>]}	File name.		6.2
[interval <NUMBER: 3600...65535>]	Interval for monitoring.		6.2
[server <IP address or host name[64]>]	TFTP server.		6.2
[remote-file-dir <String[127]>]	Remote file directory.		6.2
[state <enable disable>]]	Enables or disables file logging and pushing.		6.2

Example:

```
> rmon show event-table
```

WARNING: This CLI output may take few minutes, depends on the number of entries

```
+-----RMON EVENT STATISTICS-----+
| Index | Description | Event Type | Community | Owner      |
+-----+-----+-----+-----+-----+
| 1     | Test       | log       | Network1  | Admin     |
+-----+-----+-----+-----+-----+
```

rmon show	Displays the specified RMON table, including:	lu/su	6.2
{[alarm-index <NUMBER>]}	Alarm index.		6.2
[alarm-table],	Alarm statistics.		6.2
[event-table],	Event statistics		6.2
[history],	Ethernet history.		6.2
[statistics],	RMON statistics.		6.2
[user-history],	User history.		6.2
[file]]	File.		6.2

Example:

```
> rmon show event-table
```

WARNING: This CLI output may take few minutes, depends on the number of entries

```
+-----RMON EVENT STATISTICS-----+
| Index | Description | Event Type | Community | Owner      |
+-----+-----+-----+-----+-----+
| 1     | Test       | log       | Network1  | Admin     |
+-----+-----+-----+-----+-----+
```

rmon statistics add	Adds an entry for Ethernet statistics specified by:	su	6.2

{data-source <String[127]>}	• Interface OID name	6.2
{index <NUMBER:1-65535>}	• Index in the history table	6.2
[owner <String[127]>]	• Name of the owner	6.2

Example:

```
> rmon statistics add data-source ifindex.10001 index 1
```

rmon statistics remove index <NUMBER:1-65535>	Removes the specified Ethernet statistics entry.	su	6.2

Example:

```
> rmon statistics add data-source ifindex.10001 index 1
```

rmon usr-history add-object	Adds an SNMP object to the user history table. The control-index points to the control record created with the <code>usr-history add-control</code> command.	su	6.2
{sample-type absolute delta}	• Sample type.		6.2
{object <String[127]>}	• OID name.		6.2
{index <NUMBER: 1-1200>}	• Index in the user history table.		6.2
{control-index <NUMBER: 1-1200>}	• Index of control table entry to associate this entry with.		6.2

Example:

```
> rmon usr-history add-object index 1 control-index 1 sample-type absolute object snmpInPkts.0
```

rmon usr-history remove-object	Removes a user history object entry.	su	6.2
{index <NUMBER: 1-1200>}	• Index in the user history table.		6.2
{control-index <NUMBER: 1-1200>}	• Index of the user history control table entry to associate this entry with.		6.2

Example:

```
> rmon usr-history remove-object index 1 control-index 1
```

rmon usr-history add-control	Adds up to 8 information records to control RMON user history. Up to 1200 num-buckets are supported, and they are shared between multiple entries.	su	6.2
[file-logging <on off>]	• Enables or disables file-logging which makes the history persistent		6.2
{index <NUMBER:1-1200>}	• Index in the user history control table		6.2
[interval <NUMBER:1-65535>]	• Interval used for monitoring		6.2
[num-buckets <NUMBER:1-65535>]	• Number of buckets to use		6.2
[owner <String[127]>]	• Name of the owner		6.2

Example:

```
> rmon usr-history add-control index 1
```

rmon usr-history remove-control	Removes a user history control record.	su	6.2
{index <NUMBER:1-1200>}	Index in the user history table		6.2

Example:

```
> rmon usr-history remove-control index 1
```

snmp

NOTE: To allow SNMPv3 packets with an authentication only security level setting (authNoPriv) or an authentication with privacy security level setting (authPriv), the Advanced Security feature license must be installed with the software license install command.

Command	Description	Access Level	Release Introduced
snmp add(DEPRECATED) community <String[64]>	Adds an SNMP community with the following attributes:	su	6.0
ip <IpAddress>	IP address.		6.0
permission <read-only read-write>	Permission.		6.0

Example:

```
>snmp add community MyCommunity ip 1.1.1.1 permission read-only
```

snmp add(DEPRECATED)trap-server <IpAddress> community <CommunityName>	Adds a trap server to a community.	su	6.0

Example:

```
>snmp add trap-server 1.2.3.4 community MyCommunity
```

snmp create user <String[32]>	Creates a user entry and its authentication and privacy protocol attributes, including:	su	6.2
{auth-protocol <noauth md5 sha>}	Authentication protocol.		6.2
[auth-password <String[64]>]	Authentication password is required when the authentication protocol (auth-protocol) is set to 'md5' or 'sha'.		6.2
[priv-protocol <nopriv des>]	Privacy protocol. If the authentication protocol (auth-protocol) is set to 'noauth', then the privacy protocol must be set to 'nopriv'.		6.2

[priv-password <String[64]>]	• Privacy password.	6.2
[auth-secret <String [40]	• Sets the authentication password using a pre-encrypted string.	6.3
[priv-secret <String [40]	• Sets the privacy password using a pre-encrypted string.	6.3

Example:

```
> snmp create user user1 auth-protocol md5 priv-protocol noPriv auth-password mypassword
```

snmp create viewtree <String[32]>	Creates a view tree entry specified by:	su	6.2
{sub-tree <String[64]>}	• The sub-tree is the object identifier (OID) of the MIB.		6.2
{type <include exclude>}	• The type sets whether the specified sub-tree is to be included or excluded from the view. When creating MIB views, it is strongly advised that first the 'excluded' entries are created and then 'included' entries.		6.2

Example:

```
> snmp create viewtree SNMPv3_view sub-tree mgmt type include
```

snmp create access-entry <String[32]>	Creates an access policy for the specified group name with the following attributes:	su	6.2
{sec-model <v1 v2c v3>}	• Security model for access entry.		6.2
{sec-level <noAuth authNoPriv authWithPriv>}	• Security level.		6.2
[read-view <String[64]>]	• Read view name. Left unspecified, the default value is '1.3.6.1' which is every object under internet sub tree.		6.2
[write-view <String[64]>]	• Write view name. The default value is 'null OID', where nothing is included for write access.		6.2
[notify-view <String[64]>]	• Notify view name. The default value is 'null OID', nothing is included for notify access.		6.2

Example:

```
> snmp create access-entry group1 sec-model v1 sec-level noAuth read-view trap notify-view trap
```

snmp create target <String[32]>	Creates a target (trap receiver) entry with the following options:	su	6.2
{addr <IpAddress>}	• Target ip address.		6.2
{param-name <String[32]>}	• Parameter name.		6.2
[tag <String[32]>]	• Transport tag must be set to "TrapTag".		6.2

[udp-port <NUMBER: 1-65535>] • UDP trap port. 6.2

Note: This software version supports SNMPv1 traps. SNMPv2 traps and Inform requests are not supported in this release.

Example:

```
> snmp create target TRAPS addr 10.10.10.10 param-name TRAPS
```

snmp create community-index <String[32]>	Creates mapping between an exiting SNMPv1 community name to SNMPv3 security name (access entry) to convert community based configuration to an SNMPv3 configuration. Options include:	su	6.2
{community <String[64]>}	• Community name.		6.2
{sec-name <String[32]>}	• Security name.		6.2
[transport-tag <String[32]>]	• Transport tag.		6.2

Example:

```
> snmp create community-index comm1 community mycommunity sec-name user1
```

snmp delete user <String[32]>	Deletes the specified user.	su	6.2

Example:

```
> snmp delete user user1
```

snmp delete viewtree<String[32]> {sub-tree <String[64]>}	Deletes the specified viewtree.	su	6.2

Example:

```
> snmp delete viewtree SNMPv3_view
```

snmp delete target <String[32]>	Deletes a target (trap receiver) entry.	su	6.2

Example:

```
> snmp delete target TRAPS
```

snmp delete target-param <String[32]>	Deletes a target parameters entry.	su	6.2

Example:

```
> snmp delete target-param Target1
```

snmp delete access-entry <String[32]>	Deletes access entry with specified group name and attributes, including:	su	6.2
{sec-model <v1 v2c v3>}	• Security model for access entry.		6.2
{sec-level <noAuth authNoPriv authWithPriv>}	• Security level.		6.2

Example:

```
> snmp delete access-entry group1 sec-model v1 sec-level noAuth
```

snmp delete community-index <String[32]>	Deletes the mapping between the specified community name and its corresponding SNMPv3 security group name (access entry).	su	6.2

Example:

```
> snmp delete community-index comm1
```

snmp disable	Disables SNMP agent processes.	su	6.0

Example:

```
>snmp disable
```

snmp enable	Enables SNMP agent processes.	su	6.0

Example:

```
>snmp enable
```

snmp port-traps disable port <PortNameList>	Disables port-based traps for the specified ports.	su	6.0

Example:

```
>snmp port-traps disable port 10
```

snmp port-traps enable port <PortNameList>	Enables port-based traps for the specified ports.	su	6.0

Example:

```
>snmp port-traps enable port 10
```

snmp remove(DEPRECATED) community <CommunityName> ip <IpAddress>	Removes an SNMP community.	su	6.0

Example:

```
>snmp remove community MyCommunity 1.1.1.1
```

snmp remove(DEPRECATED) trap-server <IpAddress> community <CommunityName>	Removes an SNMP trap server from the specified community.	su	6.0

Example:

```
>snmp remove trap-server 1.2.3.4 community MyCommunity
```

snmp security-to-group attach user <String>	Attaches a user to a group with a specified security model. Attributes include:	su	6.2

{sec-model <v1 v2c v3>}	• Security model.	6.2

{group <String[32]>}	• Group to attach to.	6.2

Example:

```
> snmp security-to-group attach user user1 sec-model v1 group group1
```

snmp security-to-group detach user <String> sec-model <v1 v2c v3>	Detaches a user from a group with a specified security model.	6.2

Example:

```
> snmp security-to-group detach user user1 sec-model v1
```

snmp set community(DEPRECATED) <CommunityName> ip <IpAddress> permission <read-only read-write>	Sets the permissions for the specified IP address and community	su	6.0

Example:

```
>snmp set community MyCommunity ip 1.1.1.1 permission read-write.
```

snmp set	Sets SNMP global attributes, including:	su	6.0
{[contact <String[255]>],	• System contact.		6.0
[enhancement-link-up-down-trap <disable enable>]}	• Enables or disables enhanced proprietary link up and down traps.		6.0
[location <String[255]>],	• System location.		6.0
[std-link-up-down-trap <disable enable>]}	• Enables or disables standard link up and down trap.		6.0

Example:

```
> snmp set contact "Customer Support, Ciena"
```

snmp show	Displays global SNMP configuration or the following:	su/lu	6.0
[access-entry]	• Access entries and associated security model, security level, read view, write view, and notify view settings.		6.2
[communities(DEPRECATED)]	• Communities.		6.0
[community-map]	• Community index to community mapping entries.		6.2
[port-traps]	• Port trap states for all ports.		6.0
[trap-server(DEPRECATED)]	• Trap servers.		6.0
[users]	• Users with authorization and privacy protocol settings. Only super users may display users entries.		6.2
[security-to-group]	• User security model and group assignments.		6.2
[target]	• Target (trap receiver) entries.		6.2
[targetParams]	• Target parameter entries.		6.2
[viewtree]	• View tree entries.		6.2

Example:

```
> snmp show
+-----SNMP GLOBAL CONFIGURATION-----+
| Parameter                               | Value                               |
+-----+-----+
| Operational status                      | Enable                             |
| System Contact                          | Customer Support, Ciena            |
| System Location                         | Not Specified                      |
| Standard link-up-down trap              | Enable                             |
| Enhanced link-up-down trap              | Disable                            |
| L2 Sac Trap State                       | On                                  |
| CFM Trap State                          | Enable                             |
| Unknown Security Models                 | 0                                  |
| Invalid Messages                        | 0                                  |
| Unknown PDU Handlers                    | 0                                  |
| UnSupported Security Levels             | 0                                  |
| Not In Time Windows                     | 0                                  |
| Unknown User Names                      | 0                                  |
| Unknown Engine IDs                      | 0                                  |
+-----+-----+
```

software

Command	Description	Access Level	Release Introduced
software install package <name> server <address>	Download and install software into flash memory. Note that this feature is only available on the CN 3940, CN 3960, and CN 5140.	su	6.4.1
[service-disruption <allow deny>]	Allow or deny disruption to service by re-booting.		6.4.1

Example:

```
> software install package saos-06-04-00-0134 server 10.10.10.10 service-disruption allow
```

software license install	Install premium feature license key.	su	6.2
{license-key <key file <filename> server <ip address>}			

Example:

```
> software license install file license.txt server 172.16.172.100
```

software license show	Show properties of the software license.	su	6.2

Example:

```
> software license show
```

Feature Name	Status	License Domain	Admin	Sequence Number	Days Remain
Base-Features	enable		00000	00000000000	00356
Advanced-Security	enable	CN 3911	00002	09999999999	00356
Advanced-Ethernet	enable	CN 3911	00002	09999999999	00356
Advanced-OAM	enable	CN 3911	00002	09999999999	00356
Feature Name	License Key				
Base-Features					
Advanced-Security	X3CBI8SQ0JZAB1				
Advanced-Ethernet	X8CBI8SQ0JZAB4				
Advanced-OAM	XBCBI8SQ0JZAB5				

software license uninstall feature-name <FeatureName>	Uninstall license key for the specified feature name.	su	6.2
software protect	Duplicate all the image files from the running bank to make an identical copy of image files in the standby bank. Note that this feature is only available on the CN 3940, CN 3960, and CN 5140.	su	6.4.1
software report-sequence run	Generates a detailed report indicating the actions required to process the command file.	su	6.0
{command-file <FileName>}			6.0
{server <IpAddress>}			6.0

Example:

```
>software report-sequence run command-file le-lnx.xml server 1.2.3.4
```

software report-sequence upgrade	Generates a detailed report indicating the actions required to perform the desired upgrade specified by:	su	6.0
{package <PackageName>}	Package name string, such as "saos-04-02-00-0083".		6.0
[package-path <PackagePath>]	Full path to the package.		6.0
{server <IpAddress>}	Server IP address.		6.0

Example:

```
>software report-sequence upgrade package saos-06-00-01-0016 server 1.2.3.4
```

software reset	Resets the last command and config files so that an upgrade will be triggered on the next DHCP lease renew.	su	6.0
{[last-config-file]}			6.0
[last-command-file]}			6.0

Example:

```
>software reset last-config-file last-command-file
```

software run	Download command file from TFTP server and run it, specified by:	su	6.0
{command-file <FileName>}	Command file name.		6.0
{server <IpAddress>}	TFTP server IP address.		6.0

Example:

```
>software run command-file le-lnx.xml server 1.2.3.4
```

software show	Displays the software configuration.	su/lu	6.0

Example:

```
>software show
```

+-----+ Software Information Slot #01 +-----+		
Installed Package : saos-06-03-00-0077		
Running Package : saos-06-03-00-0077		
Package Build Info : Fri Sep 19 01:56:07 2008 shdbuilder tango.ciena.com		
Running Kernel : Build 2		
Bootloader Version : 1.2.6		
Running MIB version : 02-03-04-0021		
+-----+		
Last command file: unknown		
Last configuration file: unknown		
+-----+		

software upgrade	Upgrades or downgrades the device to the software package specified	su	6.0
{package <PackageName>}	• Package name string, such as "saos-06-03-00-0083".		6.0
[package-path <PackagePath>]	• Full path to the package.		6.0
{server <IpAddress>}	• Server IP address.		6.0
[service-disruption <allow deny>]	• Allow or deny disruption to service by re-booting.		6.0

Example:

```
>software software upgrade package saos-06-03-00-0016 package-path ciena\packages\saos-06-03-00-0016 server 1.2.3.4 service-disruption allow
NOTE: This operation cannot be interrupted once it has started.
WORKING: downloading file pmf-saos-06-03-00-0016.xml to /ram/pmf-saos-06-03-00-0016.xml
WORKING: downloading file pmf-saos-06-03-00-0016.xml to /ram/pmf-saos-06-03-00-0016.xml
...
```

software validate	Validate the status of the standby image bank and check for its integrity. Note that this feature is only available on the CN 3940, CN 3960, and CN 5140.	su	6.4.1

ssh



NOTE: To enable SSHv2 commands, the Advanced Security feature license must be installed with the software license install command.

Command	Description	Security Level	Release Introduced
ssh-server add {{client <IpAddress>}}	Adds a valid client IP address from which a connection is accepted. By default, all IP addresses are allowed to connect.	su	6.2
Example:			
> ssh-server add client 10.10.10.15			
ssh-server disable	Disables SSH server globally.	su	6.2
Example:			
> ssh-server disable			
ssh-server enable	Enables SSH server globally. The default is enable.	su	6.2
Example:			
> ssh-server enable			
ssh-server key generate	Generates and stores the public/private key pair for the server. The private key pair is encrypted and stored.	su	6.2
Example:			
> ssh-server key generate			
ssh-server set	Sets the SSH server attributes, including:	su	6.2
{[authentication-retries <NUMBER:1-3>]}	The authentication-retries value is the number of times the server will prompt for a user ID and password before declaring the login invalid when the public key file is not found (default 3).		6.2
[listener-port <NUMBER: 22 - 65535>]	The listener-port is the TCP port that listens for SSH or SFTP requests (default 22).		6.2
Example:			
> ssh-server set authentication-retries 2 listener port 10			
ssh-server remove {{client <IpAddress>}}	Removes a client IP address. If all client IP addresses are removed, then any IP address can connect.	su	6.2

Example:

```
> ssh-server remove client 10.10.10.15
```

ssh show	Shows the current SSH configurations.	su/lu	6.2

Example:

```
> ssh show
```

syslog

Command	Description	Access Level	Release Introduced

syslog add collector <IpHostSyslog>	Adds a severity to an existing Syslog collector.	su	6.2

[severity <[emergency], [alert], [critical], [error], [warning], [notice], [info], [debug]>]	Severity values that will be allowed to egress		6.2

Example:

```
> syslog add collector 192.168.10.63 severity debug
```

syslog create collector <IpHost>	Creates a Syslog collector with the following attributes:	su	6.2

[custom-prefix <String[15]>]	Syslog message prefix.		6.2

[facility <NUMBER: 0-23>]	Syslog facility.		6.2

[udp-port <NUMBER: 514-65535>]	UDP port of the Syslog collector (default=514).		6.2

[severity <[emergency], [alert], [critical], [error], [warning], [notice], [info], [debug]>]	Severity values that will be allowed to egress.		6.2

Example:

```
> syslog create collector 192.168.10.63 severity  
emergency,alert,critical,error,warning,notice,info,debug  udp-port 1044
```

syslog delete collector <IpHostSyslog>	Deletes a Syslog collector.	su	6.2

Example:

```
> syslog delete collector 192.168.10.63
```

syslog disable [collector <IpHostSyslog>]	Globally disable Syslog. If the collector option is used, Syslog is only disabled on the specified collector.	su	6.2

Example:

```
> syslog disable collector 192.168.10.63
```

syslog enable [collector <IpHostSyslog>]	Globally enable Syslog. If the collector option is used, Syslog is only enabled on the specified collector.	su	6.2

Example:

```
> syslog enable collector 192.168.10.63
```

syslog remove collector <IpHostSyslog>	Removes one or more Syslog collector severity levels sent to the specified collector.	su	6.2
[severity <[emergency], [alert], [critical], [error], [warning], [notice], [info], [debug]>]			6.2

Example:

```
> syslog remove collector 192.168.10.63 severity debug
```

syslog send	Sends a Syslog message for debugging purposes.	su	6.2
{[event <number>],	For a list of events and the corresponding numbers, run the 'event show' command.		6.2
[msg <String>],	Message string.		6.2
[severity <[emergency], [alert], [critical], [error], [warning], [notice], [info], [debug]>]}	Severity to send.		6.2

Example:

```
> syslog send event 0x30001
```

syslog set collector <IpHostSyslog>	Updates the attributes of an existing Syslog server, including:	su	6.2
[custom-prefix <String[15]>]	custom-prefix - Syslog message prefix.		6.2
[facility <NUMBER: 0-23>]	facility - Syslog facility.		6.2
[udp-port <NUMBER: 514-65535>]	udp-port - udp port of collector (default=514).		6.2

Example:

```
> syslog set collector 192.168.10.63 facility 23
```

syslog show	Displays a summary of Syslog configuration.	lu/su	6.2

Example:

```
> syslog show
```

```
Syslog Admin State: enabled
```

+----- SYSLOG SERVER CONFIGURATION -----+					
IP Address	HostName	Config State	Admin State	Oper State	
192.168.10.128		user	Enabled	Enabled	
192.168.75.45		user	Enabled	Enabled	
192.168.10.63		user	Enabled	Enabled	

syslog show severity-mapping	Displays the complete list of event severities and how they map to Syslog severities.	lu/su	6.2

Example:

```
> syslog show severity-mapping
```

+-- ITU EVENT SEVERITY MAPPING ---+		
Event Severity	Syslog Severity	
cleared	notice	
indeterm	notice	
critical	emergency	
major	alert	
minor	error	
warning	warning	
config	notice	
info	info	
debug	debug	
n/a	critical	

syslog show system-events	Displays the complete list of all possible system events. Note, this list includes events not supported on this platform.	lu/su	6.2

Example:

```
> syslog show system-events
```

+ EVENTS -----+			
Mgr: bcastContainment			
Event Sev	Syslog Sev	Event #	Event
warning	warning	0x10001	Broadcast containment filter %d is droppin
warning	warning	0x10002	Broadcast containment filter %d has stoppe
...			
info	info	0x2B004D	Bridge is new root for the specified MSTI
info	info	0x2B004F	Topology change has occurred, port %d CIST
info	info	0x2B0050	Topology change has occurred, port %d MSTI

syslog show collector <IpHostSyslog>	Displays the configuration information for the specified collector.	lu/su	6.2

Example:

```
> syslog show collector 192.168.10.63
```

COLLECTOR STATE TABLE	
Parameter	Value
Collector Host Name	N/A
Collector IP Address	192.168.10.63
Administrative State	Enabled
Operational State	Enabled
Config State	user
UDP Port	1044
Severity List	emergency alert critical error warning notice info debug
Facility Prefix	3

syslog unset collector <lpHostSyslog> custom-prefix Clears the custom prefix for the specified collector.

su

6.2

Example:

```
> syslog unset collector 192.168.10.63 custom-prefix myPrefix
```

system

Command	Description	Access Level	Release Introduced
system set	Sets the specified system attribute, including:	su	6.0
[[date <yyyy-mm-dd> <yy-mm-dd> <mm-dd>],	Date - If the yy-mm-dd format is used the two digits will be added to a base of 2000. So, 07-12-12 will become Wednesday December 12, 2007.		6.0
[host-name <String>],	Host name.Length is 2-63 characters. No spaces are allowed. At least one character must be alpha (a-z) or a dash (-). An IP address is not allowed. Host name is not case sensitive. Special characters are not allowed: “ % * ? !		6.0
[time <hh:mm:ss> <hh:mm>],	Time.		6.0

[time-offset <NUMBER: -2147483648-2147483648>]]	• Time-offset in seconds from UTC. Positive numbers are east of the UTC; negative numbers are west of the UTC.	6.0
[timestamp <local UTC>]]	• When set to 'local,' any system timestamps will use the configured time-offset. When set to 'UTC,' system timestamps will be based on UTC.	6.5

Example:

```
>system set date 07-12-12
```

system shell set	Configure the global default settings for all shell sessions, including:	su	6.0
{[welcome-banner-file <String[63]>],	• welcome-banner-file - Full path and file name.		6.0
[global-inactivity-timeout <NUMBER: 1-1500>],	• global-inactivity-timeout - If the shell inactivity timer is enabled, this setting provides the length (in minutes) of inactivity before the user is logged out. This setting applies for all Telnet and serial sessions.		6.0
[global-inactivity-timer <on off>],	• global-inactivity-timer - Turns the global inactivity timer on or off.		6.0
[global-more <on off>],	• global-more - Turns on or off global more settings for all sessions.		6.0
[global-more-lines <NUMBER: 0-999>],	• global-more-lines - Configures the number of lines to display before presenting the options to display more lines for all sessions. The default value is zero in which case the system will determine your window size automatically.		6.0
[more <on off>],	• more - Turns on or off the more settings for the current session.		6.0
[more-lines <NUMBER: 0-999>]]	• more-lines - Configures the number of lines to display before presenting the options to display more lines for the current session. The default is zero.		6.0

Example:

```
> system shell set more off
```

system shell show	Displays shell attributes.	su/lu	6.0

Example:

```
> system shell show
+----- Shell Settings -----+
| Parameter                      | Value          |
+-----+-----+
| Global more                    | on             |
| Global more lines              | 0              |
| Global inactivity timer        | off            |
| Global inactivity timeout      | 10 min         |
+-----+-----+
```

system show [date] [host-name] [load-query]	Displays time and load-query by default.	su/lu	6.0
[time] [time-offset] [uptime]	Optionally, displays only the specified system information.		

Example:

```
> system show host-name
```

```
+----- HOST NAME -----+
| Oper | CN 3911 |
| User | CN 3911 |
| DHCP |         |
+-----+
```

system state-dump tftp-server <IpAddress> file-name <FileName>	Dump system state to a file on tftp server	su	6.0

Example:

```
> system state-dump tftp-server 192.168.2.3 file-name StateDump.txt
Writing system info
Writing interface info
Writing chassis info
Writing module info
Writing port info
Writing device ID info
Writing fan info
Writing power info
Writing archive info
Writing alarm info
Writing system config
Writing log files
File StateDump.txt transferred to tftp server 192.168.2.3
```

system unset	Resets the system attributes to default for:	su	6.0
{host-name}	System host name.		6.0

Example:

```
> system unset host-name
```

tacacs



NOTE: To enable TACACS+ commands, the Advanced Security feature license must be installed with the software license install command.

Command	Description	Security Level	Release Introduced
tacacs add server <IP address or host name>	Adds up to 8 servers to the list of TACACS+ servers using either their IP address or DNS host name. If the TACACS server host name has not been resolved, its operational state will be disabled and it will not be used. The TACACS client servers have a priority number of 1through 8. The highest priority server is used first. In the event of a failure, the next server is used until there are no servers left. A failure is defined as one of the following: • The TACACS server operational state is DISABLED • The number of authentication retries has been met • If all servers have been tried, then the authentication is considered to have failed. The user login/authentication attempt is denied.	su	6.3
[priority <NUMBER: 1...8>],	• Sets the priority of the server.		6.3
[tcp-port <NUMBER: 1...65535>]	• Sets the TCP port.		6.3
Example:			
> tacacs add server 10.10.10.100			
tacacs clear [server <IP address or host name>] statistics	Clears TACACS+ statistics globally or per server.	su	6.3
Example:			
> tacacs clear server 10.10.10.100 statistics			
tacacs disable [server <IP address or host name>]	Disables TACACS+ globally or per server.	su	6.3
Example:			
> tacacs disable server 10.10.10.100			

tacacs enable [server <IP address or host name>]	Enables TACACS+ globally or per server.	su	6.3

Example:

```
> tacacs enable server 10.10.10.100
```

tacacs remove server <IP address or host name>	Removes a TACACS+ server from the list of authentication servers.	su	6.3

Example:

```
> tacacs remove server 10.10.10.100
```

tacacs set	Configures TACACS+ attributes.	su	6.3

{[key <string [2...64]>],	Sets the TACACS+ shared key of 2 to 64 characters long. The maximum length of an encrypted string is 128 characters.	6.3

[keyminlen <NUMBER: 2...64]	Sets the minimum length required for entering secret key.	6.3.1

[retires <NUMBER: 0...3>],	Specifies the number of retries that the client performs per server.	6.3

[secret <String [128]	Sets the key using a pre-encrypted string.	6.3

[timeout <NUMBER: 1...30>],	Specifies the timeout period to wait in seconds before initiating a retry.	6.3

[privilegelvlrw <NUMBER: 2...14>],	Specifies the minimum Read-Write privilege level. This is used to map to Super user, and the default value is 2.	6.3

[privilegevlldiag <NUMBER: 3...15>],	Specifies the minimum DIAG privilege level. This is used to map to Diag user, and the default value is 15.	6.3

[search-method <priority [NUMBER: 1-8]> cached]	Specifies to search by either priority or cached (last accessed).	6.3

[server <IP address or host name> [priority <NUMBER: 1...8>][tcp-port <NUMBER: 1...65535>]]]	Adds a server to the list of TACACS+ servers using either the IP address or DNS host name. Optionally, the priority or TCP port of a server.	6.3

Example:

```
> tacacs set key 543432
```

tacacs show [statistics]	Displays TACACS+ configuration. Optionally, displays TACACS+ statistics.	su/lu	6.3

Example:

```
> tacacs show statistics
```

tacacs authentication <disable enable>	Configures TACACS+ authentication. After a user is successfully authenticated, the user privilege level is retrieved from the TACACS+ Server.	su	6.3
	• A user whose TACACS privilege level is greater than or equal to the minimum Read-Write and less than the minimum DIAG is mapped to a Super user. • A user whose TACACS privilege level is greater than or equal to the minimum DIAG is mapped to a DIAG user. • A user whose TACACS privilege level is less than the minimum Read-Write is mapped to a Read-Only user.		
{[add server <IP address or host name> [priority <NUMBER: 1...8>][tcp-port <NUMBER: 1...65535>]],	• Adds up to 8 servers to the list of TACACS+ authentication servers using either their IP address or DNS host name. Optionally, sets the priority or TCP port of a server.		6.3
[clear server <IP address or host name> statistics],	• Clears TACACS+ statistics.		6.3
[disable [server <IP address or host name>]],	• Disables TACACS+ authentication or an authentication server.		6.3
[enable [server <IP address or host name>]],	• Enables TACACS+ authentication or authentication server.		6.3
[remove server <IP address or host name>],	• Removes a server from the TACACS+ authentication server list.		6.3
[set server <IP address or host name> [priority tcp-port]],	• Sets the TACACS+ server priority or TCP port.		6.3
[show [statistics]]	• Displays TACACS+ details and statistics.		6.3

Example:

```
> tacacs authentication enable
```

tacacs authorization <disable enable>	Configures TACACS authorization. TACACS Authorization will not support Attribute-Value types other than "cmd" and "cmd-arg".	su	6.3
{[add server <IP address or host name> [priority <NUMBER: 1...8>][tcp-port <NUMBER: 1...65535>]],	• Adds up to 8 servers to the list of TACACS+ authorization servers using either their IP address or DNS host name. Optionally, sets the priority or TCP port of a server.		6.3
[clear server <IP address or host name> statistics],	• Clears TACACS+ statistics.		6.3

[disable [server <IP address or host name>]],	• Disables TACACS+ authorization or authorization server.	6.3
[enable [server <IP address or host name>]],	• Enables TACACS+ authorization or authorization server.	6.3
[remove server <IP address or host name>],	• Removes a server from the TACACS+ authorization server list.	6.3
[set server <IP address or host name> [priority tcp-port]],	• Sets the TACACS+ server priority or TCP port.	6.3
[show [statistics]]]	• Displays TACACS+ details and statistics.	6.3

Example:

```
> tacacs authorization clear server 10.10.10.200 statistics
```

tacacs accounting <disable enable>	Configures TACACS accounting.	su	6.3
{[add server <IP address or host name> [priority <NUMBER: 1...8>][tcp-port <NUMBER: 1...65535>]],	• Adds up to 8 servers to the list of TACACS+ accounting servers using either their IP address or DNS host name. Optionally, sets the priority or TCP port of a server.		6.3
[clear server <IP address or host name> statistics],	• Clears TACACS+ statistics.		6.3
[disable [server <IP address or host name>]],	• Disables TACACS+ accounting or accounting server.		6.3
[enable [server <IP address or host name>]],	• Enables TACACS+ accounting or accounting server. When accounting is enabled, an Accounting start message is sent. Each server in server list is tried until one responds.		6.3
[remove server <IP address or host name>],	• Removes a server from the TACACS+ accounting server list.		6.3
[set server <IP address or host name> [priority tcp-port]],	• Sets the TACACS+ server priority or TCP port.		6.3
[set session <on off>],	• Turn on or off sending a start and stop message to the accounting server for each login session.		6.3
[set command <on off>],	• Turn on or off sending a start and stop message to the accounting server for each command executed.		6.3
[show [statistics]]]	• Displays TACACS+ details and statistics.		6.3

Example:

```
> tacacs accounting set session on
```

tacacs syslog <disable enable>	Disables or enables sending Syslog messages. When Syslog is enabled, TACACS authorization and authentication messages are sent to configured Syslog collectors.	su	6.3

Example:

```
> tacacs syslog enable
```

telnet-server

A total of 10 users are allowed with no more than 9 limited users at any time.

Command	Description	Security Level	Release Introduced
telnet-server disable	Disable Telnet server.	su	6.3

Example:

```
> telnet-server disable
```

telnet-server enable	Enable Telnet server.	su	6.3

Example:

```
> telnet-server enable
```

telnet-server set	Sets the maximum number of Telnet sessions allowed for users with super, admin, and limited access levels. A total of 10 users are allowed with no more than 9 limited users at any time. Default values are 5 for both types of users.	su	6.3

{[max-limited-users <NUMBER:0-9>], 6.3

[max-super-users <NUMBER:0-10>]} 6.3

Example:

```
> telnet-server set max-limited-users 2 max-super-users 3
```

telnet-server show	Displays the current Telnet server configuration and status.	su/lu	6.3

Example:

```
> telnet-server show
+----TELNET GLOBAL CONFIGURATION--++
| Parameter          | Value          |
+-----+-----+
| Server              | enable         |
| Max Limited User    | 5              |
| Max Super User      | 5              |
| Max System Logins   | 10             |
+-----+-----+

+-----TELNET GLOBAL STATUS-----+
| Attribute           | Value          |
+-----+-----+
| Active Limited Users | 0              |
| Active Super Users   | 1              |
+-----+-----+
```

traffic-profiling



NOTE: To enable traffic-profiling commands, the Advanced Ethernet feature license must be installed with the software license install command.

Command	Description	Security Level	Release Introduced
traffic-profiling enable	Administratively enables the traffic-profiling feature. This settings allows the traffic profiling to operate based on the administrative settings of each port. Optionally:	su	6.2
[port <PortNameList>]	Administratively enables the traffic profiling feature on the specified ports.		6.2

Example:

```
> traffic-profiling enable
```

traffic-profiling disable	Administratively disables the traffic-profiling feature, overriding the per-port administrative settings. Optionally:	su	6.2
[port <PortNameList>]	Administratively disables the traffic profiling feature on the specified ports.		6.2

Example:

```
> traffic-profiling disable
```

traffic-profiling set port <PortName>	Sets the following per-port attributes, including:	su	6.2
{[arp-standard-profile <bypass <Traffic ProfilingStandardName>],	• Profile to use for ARP frames for standard modes.		6.2
[meter-pool <TrafficProfilingMeterPoolName>],	• Sets the traffic profiling meter pool from which to obtain resources.		6.3
[mode <standard-dot1dpri standard-ip-prec standard-dscp standard-vlan standard-vlan-dot1dpri standard-vlan-ipp standard-vlan-dscp],	• Profiling Mode.		6.2
[nonconform-standard-profile <drop <TrafficProfilingStandardName>>]]	• Profile to use for non-conforming frames for standard modes.		6.2

Example:

```
> traffic-profiling set port 1 mode standard-vlan
```

traffic-profiling show	Displays global and per port status of traffic profiling. Optionally, displays:	su/lu	6.2
[meter-pool]	Traffic profiling meter pool details		6.4
[port <PortName>]	Traffic profiling configuration for the specified port name.		6.2
[meter-pool]	Meter pool assignments for all ports.		6.3

Example:

```
> traffic-profiling show port 1
```

```

+----- TRAFFIC PROFILING TABLE -----+
| Port | 1 |
| Profiling Admin State | Disabled |
| Profiling Oper State | Disabled |
| Profiling Mode | standard-dot1dpri |
| Non-Conform Standard Profile | drop |
| ARP Standard Profile | bypass |
+-----+

```

traffic-profiling standard-profile clear statistics	Clear statistics for all standard profiles.	su	6.2

Example:

```
> traffic-profiling standard-profile clear statistics
```

traffic-profiling standard-profile create	Creates a standard profile table with the following attributes:	su	6.2
{port <PortNameList>}	• A port list or individual port.		6.2
[profile <ProfileNumber>]	• Profile number. If a name is specified and Profile ID is not, a Profile ID will be automatically picked for the traffic profile.		6.4

[dot1dpri <NUMBER LIST: 0-7>]	Classifies to the profile based on the 802.1D priority value of matching frames.	6.2
[ip-prec <NUMBER LIST: 0-7>]	Classifies to the profile based on the IP Precedence value of matching frames.	6.2
[dscp <NUMBER LIST: 0-63>]	Classifies to the profile based on the Differentiated Services Code Point (DSCP) value of matching frames.	6.2
[dscp-remark-policy <leave fixed'>]	When enabled, IPv4 frames that classify to the traffic profile will have the DSCP value marked with a fixed value, or leave as is.	6.4
[fixed-dscp <0-63>]	Value to use when remarking an IPv4 frame for a traffic profile with a dscp-remark-policy of fixed.	6.4
{[cir <kbps>],	Committed information rate.	6.2
[pir <kbps>],	Peak information rate.	6.2
[cbs <kbytes>],	Committed burst size.	6.4
[ebs <kbytes>]}	Excess burst size.	6.4
[name <TrafficProfilingStandardName[15]>]	If you do not specify a name, one is automatically created for the profile number (STD#1 through STD#32).	6.2
[vlan <VLAN>]	Classifies to the profile based on the VLAN ID.	6.2

Example:

```
> traffic-profiling standard-profile create port 1 profile 1 cir 3000 pir 3200 dot1dpri 0,1,2
```

traffic-profiling standard-profile delete	Deletes the standard profile specified by:	su	6.2
{port <PortNameList>}	Port name(s).		6.2
{profile <NUMBER: 1-8>}	Profile number.		6.2

Example:

```
> traffic-profiling standard-profile delete port 1 STD#1
```

traffic-profiling standard-profile set	Sets the attributes for the standard profile, including:	su	6.2
{port <PortName>}	The individual port.		6.2
{profile <ProfileNumber>}	Profile number.		6.2
{[dot1dpri <NUMBER LIST: 0-7>]	Classifies to the profile based on the 802.1D priority value of matching frames.		6.2

[ip-prec <NUMBER LIST: 0-7>]	Classifies to the profile based on the IP Precedence value of matching frames.	6.2
[dscp <NUMBER LIST: 0-63>]	Classifies to the profile based on the Differentiated Services Code Point (DSCP) value of matching frames.	6.2
[dscp-remark-policy <leave fixed'>]	DSCP remark policy.	6.4
[fixed-dscp <0-63>]	Fixed DSCP value.	6.4
{[cir <NUMBER>],	Committed information rate.	6.2
[pir <NUMBER>]}	Peak information rate.	6.2
[cbs <kbytes>],	Committed burst size.	6.4
[ebs <kbytes>]}	Excess burst size.	6.4
[name <TrafficProfilingStandardName[15]>]	If you do not specify a name, one is automatically created for the profile number (STD#1 through STD#32).	6.2
[vlan <VLAN>]	Classifies to the profile based on the VLAN ID.	6.2

Example:

```
> traffic-profiling standard-profile set port 1 profile 1 dot1dpri 1
```

traffic-profiling standard-profile show	Displays a list of all standard traffic profiles. Optionally, displays:	su/lu	6.2
[port <PortName>]	Only standard traffic profiles associated with the specified port name.		6.2
[statistics]	Traffic profiling statistics for all ports and profiles, including accepted and dropped traffic in bytes.		6.2

Example:

```
>traffic-profiling standard-profile show port 1
```

STANDARD PROFILE TABLE						CLASSIFIERS	
Port	Profile		BW (Kbps)				
	ID	Name	CIR	PIR			
1	1	STD#1	128	128	IPP	1	
					DSC	1	
1	2	STD#2	0	256			

traffic-profiling standard-profile unset	Removes classification attributes for the specified ports and profiles:	su	6.2
{port <PortNameList>}	List of Port name(s).		6.2
{profile <TrafficProfilingStandardName[15]>}	Profile name.		6.2

[dot1dpri <NUMBER LIST: 0-7>]	• .1D priority value of matching frames.	6.2
[ip-prec <NUMBER LIST: 0-7>]	• IP Precedence value of matching frames.	6.2
[dscp <NUMBER LIST: 0-63>]	• DSCP value of matching frames.	6.2
[vlan]	• VLAN.	6.2

Example:

```
> traffic-profiling standard-profile unset port 1 STD#1 dot1dpri 2
```

traffic-services



NOTE: To enable traffic-services commands, the Advanced Ethernet feature license must be installed with the software license install command.

Command	Description	Security Level	Release Introduced
traffic-services queuing congestion-avoidance-profile create profile <String[15]>	Creates an sRED congestion avoidance profile. The CN 3911, CN 3920, CN 3940, and CN 5140 platforms support sRED profiles.	su	6.4
[green-threshold <NUMBER: 1-100>]	• Lower drop threshold for green traffic in percent from 1-100.		6.4
[green-drop-probability <100pct 6.25pct 3.125pct 1.5625pct 0.78125pct 0.390625pct 0.1953125pct 0.09765625pct>]]	• Drop probability for green traffic. Valid values are: • 100pct - 100 percent • 6.25pct - 6.25 percent or 1/16. • 3.125pct - 3.125 percent or 1/32. • 1.5625pct - 1.5625 percent or 1/64. • 0.78125pct - 0.78125 percent or 1/128. • 0.390625pct - 0.390625 percent or 1/256. • 0.1953125pct - 0.1953125 percent or 1/512. • 0.09765625pct - 0.09765625 percent or 1/1024.		6.4
[yellow-threshold <NUMBER: 1-100>]	• Lower drop threshold for yellow traffic in percent from 1-100.		6.4

```
[yellow-drop-probability
<100pct|6.25pct|3.125pct|1.5625pct|0.7812
5pct|0.390625pct|0.1953125pct|0.09765625
pct>]
```

- Drop probability for yellow traffic. Valid values are:
 - 100pct - 100 percent
 - 6.25pct - 6.25 percent or 1/16.
 - 3.125pct - 3.125 percent or 1/32.
 - 1.5625pct - 1.5625 percent or 1/64.
 - 0.78125pct - 0.78125 percent or 1/128.
 - 0.390625pct - 0.390625 percent or 1/256.
 - 0.1953125pct - 0.1953125 percent or 1/512.
 - 0.09765625pct - 0.09765625 percent or 1/1024.

6.4

Example:

```
> traffic-services queuing congestion-avoidance-profile create profile myprofile1
```

traffic-services queuing congestion-avoidance-profile create profile <String[15]>	Creates an sWRED congestion avoidance profile. The CN 3960 platform supports sWRED profiles.	su	6.4.1
[tcp-green-threshold <NUMBER: 1-100>]	• Start drop threshold for green traffic in percent from 1-100.		6.4.1
[tcp-green-upper-threshold <NUMBER: 1-100>]	• Upper drop threshold for green traffic in percent from 1-100.		6.4.1
[tcp-green-drop-probability <100pct 75pct 50pct 25pct 10pct 9pct 8pct 7pct 6pct 5pct 4pct 3pct 2pct 1pct 0pct>]	• Maximum drop probability for green traffic. Valid values are: • 100pct - 100 percent • 75pct - 75 percent • 50pct - 50 percent • 25pct - 25 percent • 10pct - 10 percent • 9pct - 9 percent • 8pct - 8 percent • 7pct - 7 percent • 6pct - 6 percent • 5pct - 5 percent • 4pct - 4 percent • 3pct - 3 percent • 2pct - 2 percent • 1pct - 1 percent • 0pct - 0 percent		6.4.1
[tcp-yellow-threshold <NUMBER: 1-100>]	• Start drop threshold for yellow traffic in percent from 1-100.		6.4.1
[tcp-yellow-upper-threshold <NUMBER: 1-100>]	• Upper drop threshold for yellow traffic in percent from 1-100.		6.4.1

<pre>[tcp-yellow-drop-probability <100pct 75pct 50pct 25pct 10pct 9pct 8pct 7pct 6pct 5pct 4pct 3pct 2pct 1pct 0pct>]</pre>	• Maximum drop probability for yellow traffic. Valid values are: • 100pct - 100 percent • 75pct - 75 percent • 50pct -50 percent • 25pct -25 percent • 10pct - 10 percent • 9pct - 9 percent • 8pct - 8 percent • 7pct - 7 percent • 6pct - 6 percent • 5pct - 5 percent • 4pct - 4 percent • 3pct - 3 percent • 2pct - 2 percent • 1pct - 1percent • 0pct - 0 percent	6.4.1
<pre>[non-tcp-threshold <NUMBER: 1-100>]</pre>	• Start drop threshold for yellow traffic in percent from 1-100.	6.4.1
<pre>[non-tcp-upper-threshold <NUMBER: 1-100>]</pre>	• Upper drop threshold for yellow traffic in percent from 1-100.	6.4.1
<pre>[non-tcp-drop-probability <100pct 75pct 50pct 25pct 10pct 9pct 8pct 7pct 6pct 5pct 4pct 3pct 2pct 1pct 0pct>]</pre>	• Maximum drop probability for non-TCP traffic. Valid values are: • 100pct - 100 percent • 75pct - 75 percent • 50pct -50 percent • 25pct -25 percent • 10pct - 10 percent • 9pct - 9 percent • 8pct - 8 percent • 7pct - 7 percent • 6pct - 6 percent • 5pct - 5 percent • 4pct - 4 percent • 3pct - 3 percent • 2pct - 2 percent • 1pct - 1percent • 0pct - 0 percent	6.4.1

Example:

```
> traffic-services queuing congestion-avoidance-profile create profile myprofile1
```

<pre>traffic-services queuing congestion-avoidance-profile delete profile <CongestionAvoidanceProfile></pre>	Deletes a congestion avoidance profile.	su	6.4

Example:

```
> traffic-services queuing congestion-avoidance-profile delete myprofile1
```

traffic-services queuing congestion-avoidance-profile rename profile <CongestionAvoidanceProfile> name <String[15]>	Renames a congestion avoidance profile.	su	6.4

Example:

```
> traffic-services queuing congestion-avoidance-profile rename profile myprofile1 name myprofilenew
```

traffic-services queuing congestion-avoidance-profile set profile <CongestionAvoidanceProfile>	Sets an attribute in an sRED congestion avoidance profile. The CN 3911, CN 3920, CN 3940, and CN 5140 platforms support sRED profiles.	su	6.4

[green-threshold <NUMBER: 1-100>]	Lower drop threshold for green traffic in percent from 1-100.		6.4

[green-drop-probability <100pct 6.25pct 3.125pct 1.5625pct 0.78125pct 0.390625pct 0.1953125pct 0.09765625pct>]]	- Drop probability for green traffic. Valid values are: 100pct - 100 percent 6.25pct - 6.25 percent or 1/16. 3.125pct - 3.125 percent or 1/32. 1.5625pct - 1.5625 percent or 1/64. 0.78125pct - 0.78125 percent or 1/128. 0.390625pct - 0.390625 percent or 1/256. 0.1953125pct - 0.1953125 percent or 1/512. 0.09765625pct - 0.09765625 percent or 1/1024.		6.4

[yellow-threshold <NUMBER: 1-100>]	Lower drop threshold for yellow traffic in percent from 1-100.		6.4

[yellow-drop-probability <100pct 6.25pct 3.125pct 1.5625pct 0.78125pct 0.390625pct 0.1953125pct 0.09765625pct>]	- Drop probability for yellow traffic. Valid values are: 100pct - 100 percent 6.25pct - 6.25 percent or 1/16. 3.125pct - 3.125 percent or 1/32. 1.5625pct - 1.5625 percent or 1/64. 0.78125pct - 0.78125 percent or 1/128. 0.390625pct - 0.390625 percent or 1/256. 0.1953125pct - 0.1953125 percent or 1/512. 0.09765625pct - 0.09765625 percent or 1/1024.		6.4

Example:

```
> traffic-services queuing congestion-avoidance-profile set profile myprofile green-threshold
40
```

traffic-services queuing congestion-avoidance-profile set profile <CongestionAvoidanceProfile>	Sets an attribute in an sWRED congestion avoidance profile. The CN 3960 platform supports sWRED profiles.	su	6.4.1
[tcp-green-threshold <NUMBER: 1-100>]	Start drop threshold for green traffic in percent from 1-100.		6.4.1
[tcp-green-upper-threshold <NUMBER: 1-100>]	Upper drop threshold for green traffic in percent from 1-100.		6.4.1
[tcp-green-drop-probability <100pct 75pct 50pct 25pct 10pct 9pct 8pct 7pct 6pct 5pct 4pct 3pct 2pct 1pct 0pct>]	- Maximum drop probability for green traffic. Valid values are: 100pct - 100 percent 75pct - 75 percent 50pct - 50 percent 25pct - 25 percent 10pct - 10 percent 9pct - 9 percent 8pct - 8 percent 7pct - 7 percent 6pct - 6 percent 5pct - 5 percent 4pct - 4 percent 3pct - 3 percent 2pct - 2 percent 1pct - 1 percent 0pct - 0 percent		6.4.1
[tcp-yellow-threshold <NUMBER: 1-100>]	Start drop threshold for yellow traffic in percent from 1-100.		6.4.1
[tcp-yellow-upper-threshold <NUMBER: 1-100>]	Upper drop threshold for yellow traffic in percent from 1-100.		6.4.1

[tcp-yellow-drop-probability <100pct 75pct 50pct 25pct 10pct 9pct 8pct 7pct 6pct 5pct 4pct 3pct 2pct 1pct 0pct>]	• Maximum drop probability for yellow traffic. Valid values are: • 100pct - 100 percent • 75pct - 75 percent • 50pct - 50 percent • 25pct - 25 percent • 10pct - 10 percent • 9pct - 9 percent • 8pct - 8 percent • 7pct - 7 percent • 6pct - 6 percent • 5pct - 5 percent • 4pct - 4 percent • 3pct - 3 percent • 2pct - 2 percent • 1pct - 1 percent • 0pct - 0 percent	6.4.1
[non-tcp-threshold <NUMBER: 1-100>]	• Start drop threshold for yellow traffic in percent from 1-100.	6.4.1
[non-tcp-upper-threshold <NUMBER: 1-100>]	• Upper drop threshold for yellow traffic in percent from 1-100.	6.4.1
[non-tcp-drop-probability <100pct 75pct 50pct 25pct 10pct 9pct 8pct 7pct 6pct 5pct 4pct 3pct 2pct 1pct 0pct>]	• Maximum drop probability for non-TCP traffic. Valid values are: • 100pct - 100 percent • 75pct - 75 percent • 50pct - 50 percent • 25pct - 25 percent • 10pct - 10 percent • 9pct - 9 percent • 8pct - 8 percent • 7pct - 7 percent • 6pct - 6 percent • 5pct - 5 percent • 4pct - 4 percent • 3pct - 3 percent • 2pct - 2 percent • 1pct - 1 percent • 0pct - 0 percent	6.4.1

Example:

```
> traffic-services queuing congestion-avoidance-profile set profile myprofile tcp-green-threshold 40
```

traffic-services queuing congestion-avoidance-profile show	Show congestion avoidance profiles.	su	6.4
[profile <CongestionAvoidanceProfile>]	• Show attributes for a specific congestion avoidance profile.		

Example:

```
> traffic-services queuing congestion-avoidance-profile show
```

----- CONGESTION AVOIDANCE PROFILE DATA -----						
Name			Default-SRED			
Id			1			
Type			SRED			

Green				Yellow		
Threshold		Drop Probability		Threshold	Drop Probability	
75	%	0.09765625pct.(1/1024)		50	%	6.25pct.....(1/16)

Name			custom-default			
Id			2			
Type			SRED			

Green				Yellow		
Threshold		Drop Probability		Threshold	Drop Probability	
75	%	0.09765625pct.(1/1024)		50	%	6.25pct.....(1/16)

Name			green-yellow-1			
Id			3			
Type			SRED			

Green				Yellow		
Threshold		Drop Probability		Threshold	Drop Probability	
100	%	0.09765625pct.(1/1024)		1	%	100pct

traffic-services queuing egress-port-queue-group set queue <NUMBER: 0-7>	Sets the following options for a queue in the queue group. Note that queue 7 is typically reserved for CPU-Sourced traffic and should not be changed.	su	6.4
{[port <PortQueueGroup>],	The port on which the queue group is instantiated.		6.4
[scheduler-weight <NUMBER: 0...1000>],	Scheduler weight of a queue in the queue group relative to other queues in the queue group. Not relevant when the scheduler-type of the queue group is strict-priority.		6.4
[cir <NUMBER: 0...10000000>],	Committed information rate in Kbps.		6.4
[cbs <NUMBER: 0...256>],	Committed burst size in Kbytes.		6.4
[eir <NUMBER: 0...10000000>],	Excess information rate in Kbps.		6.4
[ebs <NUMBER: 0...256>],	Excess burst size in Kbytes.		6.4
[congestion-avoidance-profile <CongestionAvoidanceProfile>]}	Congestion avoidance profile.		6.4

Example:

```
> traffic-services queuing egress-port-queue-group set queue 0 port 9 scheduler-weight 100
```

traffic-services queuing egress-port-queue-group set port <PortQueueGroup>	Sets the scheduler algorithm and shaper rate for the egress port queue group.	su	6.4

[scheduler-algorithm <strict round-robin weighted-deficit-round-robin weighted-round-robin>]	• Scheduler algorithm.		6.4

[shaper-rate]	• Shaper rate in Kbps.		6.4

Example:

```
> traffic-services queuing egress-port-queue-group set port 3 scheduler-algorithm round-robin shaper-rate 1200
```

traffic-services queuing egress-port-queue-group show	Show congestion avoidance profiles.	su	6.4

[queue <NUMBER: 0-7> port <PortQueueGroup>]	• Show attributes for a specific queue and port.		6.4

[port <PortQueueGroup>]	• Show attributes for a specific port.		6.4

Example:

```
> traffic-services queuing egress-port-queue-group show port 9
```

traffic-services queuing egress-port-queue-group unset queue <NUMBER: 0-7> port <PortQueueGroup> congestion-avoidance-profile		su	6.4

Example:

```
> traffic-services queuing egress-port-queue-group unset queue 4 port 12 congestion-avoidance-profile
```

traffic-services queuing queue-map create rcos-map <String[15]>	Creates an R-CoS queue map.	su	6.4

Example:

```
> traffic-services queuing queue-map create rcos-map custom-map-11
```

traffic-services queuing queue-map delete rcos-map <String[15]>	Deletes an R-CoS queue map.	su	6.4

Example:

```
> traffic-services queuing queue-map delete rcos-map custom-map-1
```

traffic-services queuing queue-map rename rcos-map <String[15]> name <String>	Renames an R-CoS queue map.	su	6.4

Example:

```
> traffic-services queuing queue-map rename rcos-map custom-map-11 name custom-map-1new
```


traffic-services queuing queue-map set rcos-map <String[15]>	Sets an attribute in an R-CoS map.	su	6.4
[rcos <#List>]	Specify the R-CoS value associated with the queue.		6.4
[queue <#List>]	Specify the queue.		6.4

Example:

```
> traffic-services queuing queue-map set rcos-map myrcos-map rcos 0 queue 3
```

traffic-services queuing queue-map show	Shows R-CoS queue maps.	su	6.4
[rcos-map <RcosQueueMap>]	Shows attributes for a R-CoS queue map.		6.4

Example:

```
> traffic-services queuing queue-map show custom-map-11
```

twamp



NOTE: To enable TWAMP commands, the Advanced Ethernet feature license must be installed with the software license install command.

Command	Description	Security Level	Release Introduced
twamp client clear statistics	Clears Mini-WIPM statistics for all sessions. Optionally, clears:	su	6.3
[name <SessionName>]	Statistics for the specified session.		6.3
[all]	Statistics for all defined sessions.		6.4
Example:			
> twamp client clear statistics			
twamp client disable	Disables Mini-WIPM.	su	6.3
Example:			
> twamp client disable			
twamp client enable	Enables Mini-WIPM.	su	6.3
Example:			
> twamp client enable			
twamp client session create	Creates a Mini-WIPM session with the following attributes:	su	6.3
name <String [15]>	Unique name for the session.		6.3

host <IpAddress>	• IP address of the target.	6.3
[commport <NUMBER:256-65535>]	• Communications port. By default, the session uses the global active TWAMP port.	6.3
[cos-policy <dscp ip-prec>]	• CoS policy for marking test frames.	6.3
[dscp <NUMBER: 0-63>]	• DSCP value for marking test frames.	6.3
[ip-prec <NUMBER: 0-7>]	• IP precedence value for marking test frames.	6.3
[pkt-size <NUMBER: 64-1500>]	• Packet size.	6.3
[repeat <on off>]	• Specifies whether or not to automatically repeat the test.	6.3
[type <fixed poisson>]	• Packet stream type.	6.3

Example:

```
> twamp client session create name myTest host 192.168.12.345 cos-policy ipprec  
ipprec 7 type fixed
```

twamp client session delete	Deletes a Mini-WIPM session specified by:	su	6.3
{name <SessionName>}	• Unique name for the session.		6.3

Example:

```
> twamp client session delete name myTest
```

twamp client session set	Sets the attributes for the Mini-WIPM session as follows:	su	6.3
{name <SessionName>}	• Unique name for the session.		6.3
{[host <IpAddress>],	• IP address of the target.		6.3
[commport <NUMBER:256-65535>],	• Communications port. By default, the session uses the global active TWAMP port.		6.3
[cos-policy <dscp ip-prec>],	• CoS policy for marking test frames.		6.3
[dscp <NUMBER: 0-63>],	• DSCP value for marking test frames.		6.3
[ip-prec <NUMBER: 0-7>],	• IP precedence value for marking test frames.		6.3
[pkt-size <NUMBER: 64-1500>],	• Packet size.		6.3
[repeat <on off>],	• Specifies whether or not to automatically repeat the test.		6.3
[type <fixed poisson>]}	• Packet stream type.		6.3

Example:

```
> twamp client session create name myTest host 192.168.12.345 cos-policy ipprec  
ipprec 7 type fixed
```

twamp client show	Displays a summary of all created sessions. Optionally, displays:	su	6.3
[statistics	• All statistics.		
[name <SessionName>]	• Limits statistics to a specified session.		6.3
[mode <long short>]	• Sets the mode.		6.3
[period <last 8-hour 24-hour>]]	• Limits to a specific time period.		6.3

Example:

```
> twamp client show
```

twamp client test	Establishes or stops the Mini-WIPM session specified by:	su	6.3
{name <String [15]>}	• Unique name for the session.		6.3
[host <IpAddress>]	• IP address of the target.		6.3
[stop]	• Stops active sessions.		6.3
[all]	• All defined sessions.		6.4

Example:

```
> twamp client test name myTest
```

twamp disable	Disables TWAMP globally. Optionally:	su	6.2
[port <PhyPortNameList>]	• Disables TWAMP for the specified physical port(s). By default, TWAMP is enabled for all physical ports.		6.2

Example:

```
> twamp disable port 5-8
```

twamp enable	Enables TWAMP globally. Optionally:	su	6.2
[port <PhyPortNameList>]	• Enables TWAMP for the specified physical port(s). By default, TWAMP is enabled for all physical ports.		6.2

Example:

```
> twamp enable port 5-8
```

twamp set	Sets the global TWAMP attributes, including:	su	6.2
{[client-dscp <NUMBER: 0-63>],	• Sets the TWAMP client DSCP values in TCP messages used for control session communications. By default, the global DSCP value is 0.		6.3.1

[server-dscp <NUMBER: 0-63>],	Sets the TWAMP server DSCP values in TCP messages used for control session communications. By default, the global DSCP value is 0.	6.3.1
[port <NUMBER: 256-65535>],	Active TWAMP port. Default is 861.	6.2
[timeout <NUMBER>]]	Timeout value for abandoned session recovery.	6.3

Example:

```
> twamp set port 5678
```

twamp show	Displays all TWAMP attributes. Optionally, displays:	su	6.2
[port]	The active TWAMP port only.		6.2

Example:

```
> twamp show
+----- TWAMP State Info -----+
|      Parameter      |      Value      |
+-----+-----+
| Device Admin State  | Disabled        |
+-----+-----+

+-----+-----+-----+
|      Per Port TWAMP State Info      |
+-----+-----+-----+
| Port | Admin | Operational |
+-----+-----+-----+
|  1   | Enabled | Disabled    |
|  2   | Enabled | Disabled    |
|  3   | Enabled | Disabled    |
|  4   | Enabled | Disabled    |
|  5   | Enabled | Disabled    |
|  6   | Enabled | Disabled    |
|  7   | Enabled | Disabled    |
|  8   | Enabled | Disabled    |
|  9   | Enabled | Disabled    |
| 10   | Enabled | Disabled    |
+-----+-----+-----+

+----- Active TWAMP Port -----+
| TCP/UDP Port | 861            |
+-----+-----+

+----- TWAMP Priority -----+
| Priority | echo received |
+-----+-----+
```

twamp unset	Resets the TWAMP attributes	su	6.2
{port}	Active TWAMP port to the default.		6.2
[timeout <NUMBER>]]	Timeout value for abandoned session recovery.		6.3

Example:

```
> twamp unset port
```

twamp light disable	Disables TWAMP Light Responder.	su	6.2

Example:

```
> twamp disable
```

twamp light enable	Enables TWAMP Light Responder.	su	6.2

Example:

```
> twamp light enable
```

twamp server clear session <Session ID: 1-10>	Forces a Mini-WIPM session with the TWAMP Server to shut down.	su	6.3

Example:

```
> twamp server clear session 1
```

twamp server disable	Disables TWAMP Server.	su	6.2

Example:

```
> twamp disable
```

twamp server enable	Enables TWAMP Server.	su	6.2

Example:

```
> twamp light enable
```

user

A user name must have a minimum of 1 character and a maximum of 16 characters. A password may have from 0 to 16 characters.

Command	Description	Access Level	Release Introduced
user auth clear [priority <NUMBER:1-3>]	Clears the authentication provider statistics for all or those with a specified priority.	su	6.3.1
Example:			
<pre>> user auth clear</pre>			
user auth show	Displays the authentication provider statistics, including the priority, method, called, successes, failures, and skipped.	su	6.3.1

Example:

```
> user auth show
----- Authorization Providers -----+
| Method | Called | Success | Failure | Skipped | Scope |
+-----+-----+-----+-----+-----+-----+
| local  |      5 |      4 |      1 |      0 | all  |
+-----+-----+-----+-----+-----+-----+-----+
```

user auth set	Sets the authentication provider attributes:	su	6.3.1
{priority <NUMBER:1-3>}	Authorization priority - The authentication provider with priority 1 is checked first. The authentication provider with priority 2 is checked only if priority 1 is unavailable, and 3 is checked if both 1 and 2 are unavailable.		6.3.1
{method <none local radius tacacs>}	Authorization method. The default is RADIUS only.		6.3.1
{scope <all serial remote> [priority <NUMBER: 1...3>][method <none local radius tacacs>]}	Set the user authentication login priority and type.		6.3.1

Example:

```
> user auth set priority 1 method tacacs scope remote
```

user create user <String[16]>	Creates a user.	su	6.0
{[access-level <limited super>],	Access level to determine the privileges for the user.		6.0
[nopassword],	No password required for the user.		6.0
[password <String[16]>]}	Plain text password.		6.0
[secret <String[34]>]	Sets the password using a pre-encrypted string.		6.3

Example:

```
> user create super1 access-level super password s1033807
```

user delete user <String[16]>	Removes a user.	su	6.0

Example:

```
> user delete super1
```

user set user <String[16]>	Updates the user's attributes, including:	su	6.0
{[access-level <limited super>],	Access level to determine the privileges for the user.		6.0
[nopassword],	No password required for the user.		6.0
[password <String[16]>]}	Plain text password.		6.0

[secret <String[34]>]

- Sets the password using a pre-encrypted string.

6.3

Example:

```
> user set super1 password s38new1
```

user show	Displays all user accounts.	su	6.0

Example:

```
> user show
+-----+ USER ACCOUNT TABLE +-----+
| Username | Privilege | Flags |
+-----+-----+-----+
| MIS      | super    | P     |
| data     | limited  | P     |
| su       | super    | DP    |
| user     | limited  | D     |
+-----+-----+-----+
```

user who	Displays the users who are logged in to the device, including user name, idle time, process ID (PID), and terminal IP address.	su	6.0

Example:

```
> user who
+-----+-----+-----+-----+
| Username | Idle Time | Pid | Terminal |
+-----+-----+-----+-----+
| su       | 0m       | 131204 | /telnet_192.168.3.153:1287 |
| su       | 0m       | 196735 | /telnet_192.168.3.153:1116 |
+-----+-----+-----+-----+
```

user whoami	Display your user name and access level.	su/lu	6.0

Example:

```
> user whoami
username: su access-level: super
```

user kill pid <ProcessID>	Ends the user session for the specified process ID. To find the process ID, use the user who command.	su	6.0

> all-but-me	Ends all user sessions except for the current login.		6.4

Example:

```
> user kill pid 196735
```

virtual-circuit

Commands for configuring and viewing Ethernet Virtual Circuits (VCs).

Command	Description	Security Level	Release Introduced
virtual-circuit clear [vc <VirtualCircuitName[15]>] statistics	Clears virtual circuit statistics for all or the specified virtual circuit.	su	6.2
Example:			
> virtual-circuit clear statistics			
virtual-circuit ethernet create {vc <VirtualCircuitEthernetName[15]>} {vlan <Vlan>}	Creates a static Ethernet virtual circuit for the specified VLAN object. Traffic entering the virtual circuit will be treated with the specified 802.1D priority value.	su	6.2
Example:			
> virtual-circuit ethernet create vc vc1 vlan 1000			
virtual-circuit ethernet delete vc <VirtualCircuitEthernetName[15]>	Deletes the specified Ethernet virtual circuit.	su	6.2
Example:			
> virtual-circuit ethernet delete vc vc1			
virtual-circuit ethernet set {vc <VirtualCircuitEthernetName[15]>} {vlan <Vlan>}	Sets the VLAN for the specified Ethernet virtual circuit.	su	6.2
Example:			
> virtual-circuit ethernet set vc vc1 vlan 2000			
virtual-circuit ethernet set port <PortNameList>	Sets the VLAN Ethernet type and policy for the specified ports.	su	6.2
{[vlan-ethertype <8100 88a8 9100>],			6.2
[vlan-ethertype-policy <all encap-only>]}			6.2

Example:

```
> virtual-circuit ethernet set port vlan-ethertype 9100
```


virtual-circuit ethernet show [vc <VirtualCircuitEthernetName[15]>] [statistics]	Shows the list of Ethernet virtual circuits (VCs), the details of a specified Ethernet VC, statistics for all Ethernet VCs or statistics for a specified Ethernet VC. Note that VC statistics are based on pre-congestion avoidance measurements, and require known DAs for statistics to increment. The CN 3940 and CN 5140 have a statistics limit of 32 VCs, while the CN 3960 statistics can support 128 VCs.	su/lu	6.2

Example:

```
> virtual-circuit ethernet show
+----- ETHERNET VIRTUAL CIRCUIT TABLE -----+
| Name           | VLAN           |
+-----+-----+
| vc1            | 2000           |
+-----+-----+
```

virtual-circuit rename {vc <VirtualCircuitName[15]>} {name <String[15]>}	Renames a virtual circuit.	su	6.2

Example:

```
> virtual-circuit rename vc1 vc2000
```

virtual-circuit show [vc <VirtualCircuitName[15]>] [statistics]	Shows the port ether type virtual circuit info and the Ethernet virtual circuit tables. Optionally, shows all or specified virtual circuit statistics.	su/lu	6.2

Example:

```
> virtual-circuit show
+----- ETHERNET VIRTUAL CIRCUIT TABLE -----+
| Name           | VLAN           |
+-----+-----+
| vc1            | 2000           |
+-----+-----+
```

virtual-switch

Commands for configuring and displaying virtual switch (VS) instances.



CAUTION: When a port is added to a per-port virtual switch instance, the existing VLAN configuration for that port will be removed. A port cannot be a member of a regular VLAN while participating in a VPLS.

Command	Description	Security Level	Release Introduced
virtual-switch add reserved-vlan <VLAN IDList>	Reserves VLANs (at most 127) for use in creating Virtual Switch Instances.(Platform Dependent).	su	6.2
Example:			
> virtual-switch add reserved-vlan 1000			
virtual-switch l2-cft disable vs <VirtualSwitchName>	Disables L2 control frame tunneling for the specified virtual switch.	su	6.3
Example:			
> virtual-switch l2-cft disable			
virtual-switch l2-cft enable vs <VirtualSwitchName>	Enables L2 control frame tunneling for the specified virtual switch.	su	6.3
Example:			
> virtual-switch l2-cft enable			
virtual-switch l2-cft protocol add vs <VirtualSwitchName[15]>]	Adds a control protocol to an L2 control frame tunneling instance for the specified virtual switch with the following parameters:	su	6.3
{ctrl-protocol <802.1x all-bridges-block bridge-block cisco-cdp cisco-dtp cisco-pagp cisco-pvst cisco-stp-uplink-fast cisco-udld cisco-vtp garp-block gmrp gvrp lacp lacp-marker lldp oam rstp vlan-bridge>}	Selects the control protocol to add.		6.3
[disposition <discard forward>]	Sets the disposition. If left unspecified, the disposition is set to the default disposition for the specified control protocol.		6.3
Example:			
> virtual-switch l2-cft protocol add vs cft-vs ctrl-protocol rstp disposition forward			
virtual-switch l2-cft protocol remove vs <VirtualSwitchName[15]>]	Removes a control protocol from an L2 control frame tunneling instance for the specified virtual switch with the following parameter:	su	6.3
{ctrl-protocol <802.1x all-bridges-block bridge-block cisco-cdp cisco-dtp cisco-pagp cisco-pvst cisco-stp-uplink-fast cisco-udld cisco-vtp garp-block gmrp gvrp lacp lacp-marker lldp oam rstp vlan-bridge>}	Selects the control protocol to remove. When you remove a control protocol from a L2 control frame tunneling instance, untagged L2 control frames will be processed according to the default disposition for the control protocol.		6.3

Example:

```
> virtual-switch l2-cft protocol remove vs cft-vs ctrl-protocol rstp
```

virtual-switch l2-cft protocol set vs <VirtualSwitchName[15]>	Sets the disposition of a control protocol to an L2 control frame tunneling instance for the specified virtual switch.	su	6.3
{ctrl-protocol <802.1x all-bridges-block bridge-block cisco-cdp cisco-dtp cisco-pagp cisco-pvst cisco-stp-uplink-fast cisco-udld cisco-vtp garp-block gmrp gvrp lacp lacp-marker lldp oam rstp vlan-bridge>}	Selects the control protocol to modify.		6.3
[disposition <discard forward>]	Sets the disposition.		6.3

Example:

```
> virtual-switch l2-cft protocol set vs cft-vs ctrl-protocol rstp discard
```

virtual-switch l2-cft set vs <VirtualSwitchName[15]>	Sets the L2 control frame tunneling attributes for the specified virtual switch, including:	su	6.3
[priority <NUMBER: 0-7>]	The Fixed .1D priority value to be given to an untagged frame is forwarded (encapsulated) by the L2 control frame tunneling instance. The default Fixed .1D priority value is 6. You can modify it to a value between 0 and 7.		6.3
[tunnel-method <l2pt transparent>]	The tunnel method, transparent or L2PT, controls the classification and processing of untagged L2 control frames. The default mode is L2PT.		6.3

Example:

```
> virtual-switch l2-cft vs cft-vs set priority 3 tunnel-method l2pt
```

virtual-switch l2-cft show [vs <VirtualSwitchName[15]>]	Shows a summary of L2 control frame tunneling instances or details of L2 control tunneling instance for a specified virtual switch.	su/lu	6.2

Example:

```
> virtual-switch l2-cft show vs cft-vs
```

+----- L2 Ctrl Protocol Tunneling - cft-vs -----+	
Parameter	Value
Admin State	Enabled
Tunnel Method	l2pt
Priority	6
Protocol Name	Disposition
rstp	forward
lacp	forward

virtual-switch ethernet add vs <VirtualSwitchName[15]>	Allows attachment circuit to be added. A list of ports can be specified. If only a port is specified and the VS has no other attachment circuits then the VS becomes a Per-port VS with the specified ports. If only a port is specified and the VS is already a Per-port VS then the specified ports are added. If only a port is specified and the VS is a Per-port/per-VLAN VS then an error is returned. If one or more ports are specified and one or more VLANs, then each port will be added to the VS with the specified subscriber VLANs. The <port, VLAN> combination defines the attachment circuit. If only a VLAN is specified an error is returned.	su	6.2
{[port <PortNameList>],	The port name.		6.2
[vlan <VlanList>],	The VLAN.		6.2
[encap-cos-policy <fixed port-inherit vs-inherit>],	Encap COS policy.		6.2
[encap-fixed-dot1dpri <NUMBER: 0-7>]]	The priority setting for fixed COS policy.		6.2

Example:

```
> virtual-switch ethernet add vs vs150 port 5 vlan 2 encap-cos-policy fixed encap-fixed-dot1dpri 1
```

virtual-switch ethernet create vs <VirtualSwitchName[15]>	Creates a virtual switch instance. The virtual circuits can be added to the switch in this cmd or in the set command. The ingress CoS policy values are optional and are only used when there is no virtual circuit attached to the virtual switch.	su	6.2
{[decap-cos-policy <leave>],			6.2
[encap-cos-policy <fixed>],			6.2
[encap-fixed-dot1dpri <NUMBER: 0-7>],			6.2

[subscriber-dot1dpri-policy <leave>],	6.2
[vc <VirtualCircuitName[15]>]]	6.2

Example:

```
> virtual-switch ethernet create vs cft-vs vc cft-vc
```

virtual-switch ethernet delete vs <VirtualSwitchName[15]>	Deletes a virtual switch instance	su	6.2

Example:

```
> virtual-switch ethernet delete vs cft-vs
```

virtual-switch ethernet remove vs <VirtualSwitchName[15]>	Remove subscriber ports from a virtual switch.	su	6.2
{port <PortNameList>}	• By port only.		6.2
[vlan <VlanList>]	• By port and VLAN.		6.2

Example:

```
> virtual-switch ethernet remove vs cft-vs port 1
```

virtual-switch ethernet set port vs <VirtualSwitchName[15]>	Allows an attribute to be set on a virtual switch member.	su	6.4
{[encap-cos-policy <fixed port-inherit vs-inherit>],			6.4
[encap-fixed-dot1dpri <NUMBER: 0-7>],			6.4
[vlan <VlanList>]]	The VLAN. When the member is a per-port member the VLAN key can be omitted, otherwise it is mandatory.		6.4

Example:

```
> virtual-switch ethernet set port vs cft-vs encap-fixed-dot1dpri 6
```

virtual-switch ethernet set vs <VirtualSwitchName[15]>	Allows attributes of the VS to be changed.	su	6.2
{[decap-cos-policy <leave>],			6.2
[encap-cos-policy <fixed>],			6.2
[encap-fixed-dot1dpri <NUMBER: 0-7>],			6.2
[subscriber-dot1dpri-policy <leave>],			6.2
[vc <VirtualCircuitName[15]>]]			6.2

Example:

```
> virtual-switch ethernet set vs cft-vs vc cft-vc
```

virtual-switch ethernet show [vs <VirtualSwitchName[15]>]	Shows the list of Ethernet virtual switches or the details of a specified Ethernet virtual switch. Optionally, shows the statistics for all virtual switches or for the specified virtual switch.	su/lu	6.2

Example:

```
> virtual-switch ethernet show
```

ETHERNET VIRTUAL SWITCH TABLE				
Name	VLAN Active	CPT	Virtual Circuit	Subscriber Count
cft-vs	1000	Dis		0

virtual-switch ethernet unset vs <VirtualSwitchName[15]> vc	Removes the primary virtual circuit for an Ethernet virtual switch.	su	6.2

Example:

```
> virtual-switch ethernet unset vs cft-vs vc cft-vc
```

virtual-switch remove reserved-vlan <VlanIdList>	Remove VLANs from the list of reserved VLANs.	su	6.2

Example:

```
> virtual-switch remove reserved-vlan 1000
```

virtual-switch rename vs <VirtualSwitchName[15]> name <String[15]>	Renames a virtual switch.	su	6.2

Example:

```
> virtual-switch rename vs cft-vs name vs1
```

virtual-switch show [vs <VirtualSwitchName[15]>]	Shows list of reserved VLANs and virtual switches or details of a specified virtual switch.	su/lu	6.2

Example:

```
> virtual-switch show
```

VIRTUAL SWITCH RESERVED VLANS	
VLAN	Virtual Switch [Attached]
1000	(1) cft-vs

ETHERNET VIRTUAL SWITCH TABLE				
Name	VLAN Active	CPT	Virtual Circuit	Subscriber Count
cft-vs	1000	Dis		0

vlan



NOTE: A maximum of 500 VLANs are supported without an Advanced Ethernet (AE) license, and up to 4094 VLANs with an AE license.

Command	Description	Access Level	Release Introduced
vlan add vlan <VlanList> port <PortNameList>	Adds ports to a VLAN with the specified VLAN ID tag.	su	6.0
Example:			
> vlan add vlan 300 port 1,5			
vlan create vlan <VlanIdList> [name <String[31]>]	Creates a VLAN. You can optionally specify a name for the VLAN. If no VLAN name is specified, a default name will be assigned with the form of "VLAN#<VLAN-id>". For example if the VLAN ID is 1000 the VLAN name will be "VLAN1000". Note that VLAN names cannot begin with an integer. For example, 3PUD is not valid, but PUD3 is allowed.	su	6.0
Example:			
> vlan create vlan 300			
vlan delete <VlanList>	Deletes a VLAN, VLAN name, VLAN range or VLAN list. A VLAN can only be deleted if it has no members.	su	6.0
Example:			
> vlan create vlan 300			
vlan remove vlan <VlanList> port <PortNameList>	Removes a port from a VLAN or removes a VLAN ID tag from a port in a VLAN	su	6.0
Example:			
> vlan remove vlan 300 port 1			
vlan rename vlan <VlanList> name <String[31]>	Renames the specified VLAN.	su	6.0
Example:			
> vlan rename vlan 300 MyVlanName			
vlan show [port <PortNameList> vlan <VlanList>]	"VLAN show" displays the VLAN table. Optionally, displays the VLANs to which the specified belongs or displays information for the specified VLAN.	su/lu	6.0

Example:

```
> vlan show
```

+-----+-----+-----+		
VLAN		Ports
ID	VLAN Name	1234567890
+-----+-----+-----+		
127	Mgmt	xxxxxxxxxx
300	VLAN#300	
777	VLAN#777	
+-----+-----+-----+		

```
vlan show [port <PortNameList>|vlan  
<VlanList>] statistics
```

Displays a summary of VLAN statistics.
Optionally, displays statistics for the
specified port(s) or VLAN(s).

su/lu

6.0

Example:

```
> vlan show vlan 127 statistics
```

+----- VLAN 127 STATISTICS -----+		
Counter	Value	
+-----+-----+-----+		
UnicastBytes	0	
NonUnicastBytes	598	
UnicastPkts	0	
NonUnicastPkts	1	
+-----+-----+-----+		

Appendix Service and Support



For technical support, contact Ciena using any of the following methods.

Internet Site

Additional contact information and general product support can be accessed on the Ciena Web site:

www.portal.ciena.com

E-mail Address

To contact Ciena by e-mail, use:

ciena24@ciena.com

Telephone and Fax

To contact Ciena by phone or fax:

North America	800-CIENA24 (1-800-243-6224) OR 1-410-865-4961
Europe, Middle East, and Africa	800-CIENA24-7 (1-800-243-6224-7) OR 44-207-012-5508
Asia and Pacific	800-CIENA24-7 (1-800-243-6224-7) OR 81-3-3248-4743
Phone	+1-509-242-9378
Fax	+1-509-242-9001

Mailing Address

To contact Ciena by mail, address all correspondence to:

Ciena Corporation

1201 Winterson Road

Linthicum, MD 21090

Glossary



The terms defined in this glossary may or may not be found in this manual but are generally found throughout Ciena documentation.

A

Active refers to the Control Module that is operationally controlling the system.

Alarm is classified as either an audible or visible warning notice that is triggered by an event or error condition.

B

BCB (Backbone Core Bridge)

B-DA (Backbone Destination Address) added to PBT frames to identify the PBT tunnel and flood domain interconnects.

BEB (Backbone Edge Bridge)

B-MAC (Backbone MAC Address)

Backup is a redundancy state mode indicating that the Standby Control Module is ready to manage the system in the event that the Active Control Module should failover.

Broadcast Containment prevents services from being disrupted by broadcast storms by creating Broadcast Containment filters and applying them to VLANs or virtual switches.

Broadcast Storm occurs when a large number of broadcast packets are unnecessarily propagated across a network which can degrade performance or even deny service. Broadcast storms are often associated with denial-of-service attacks, network reconvergence, and loops in the network.

B-SA (Backbone Source Address)

B-TAG (Backbone Tag)

B-VID (Backbone VLAN ID)

C

CBS (Committed Burst Rate) is the maximum number of kilobytes that can ingress at the maximum interface speed in order to remain in conformance with the CIR.

CCM (Continuity Check Message) control frames are sent and received across PBT tunnels by CFM to monitor for faults.

CFM (Connectivity Fault Management) monitors the status of services that extend across two or more devices and provides fault notifications.

ChannelStream A ChannelStream is a collection of user-defined multicast groups that are flooded to all ports in a VLAN, bringing these streams far down into the network before they are requested by an IGMP host, thus reducing latency.

CIR (Committed Information Rate) is a designated value that represents the minimum guaranteed bandwidth for network traffic flows that are transmitted and received under normal operating conditions.

C-MAC (Customer MAC Address)

Command File contains a set of instructions on how to deliver the various system software to devices.

Condition refers to an occurrence within the system that exists for a period of time that may be of interest to the user or operator. A condition that persists for an extended period of time may be re-classified as an Event.

CoS (Class of Service) divides services into different levels of priority in order make forwarding decisions when network congestion occurs.

CPE (Customer Premises Equipment)

C-VID (Customer VLAN ID) 801.1Q Customer VLAN tag.

C-VLAN (Customer VLAN)

D

DEI (Drop Eligibility Indicator)

DMAC (Destination MAC Address)

DP (Drop Preference)

DSCP (Differentiated Services Code Point)

E

EBS (Excess Burst Size) is the maximum number of kilobytes that can ingress at the maximum interface

speed in order to remain in conformance with the EIR.

Egress refers to network traffic being sent out of a device or the exit point from a network device.

EIR (Excess Information Rate) is a designated value, in excess of the CIR, that represents an allowance of burstable bandwidth for network traffic flows that are transmitted and received under bursty operating conditions.

EPR (Egress Port Restriction) restricts cross-talk between ports on the same device within a shared VLAN by blocking ARP messages.

Event typically refers to an error condition in the system that has an associated severity. Events can be logged into either the SYSLOG, RAM, or CompactFlash via the event logging system. In addition, some events are converted into SNMP traps.

EIR (Excess Information Rate) represents the average rate in kbps above the CIR that ingress traffic flows are allowed through with an increase in drop precedence.

EVC (Ethernet Virtual Circuit)

F

Fault (or System fault) occurs either when an alarm reaches a critical level or when a component(s) within the system fails.

Fault Detection is defined as the time from a failure causing a loss of service to the system becoming aware of it. Fault detection occurs in individual device managers.

Fault Manager is a device within the system that handles fault monitoring, fault logging, and fault policy management & execution.

Ingress refers to network traffic entering a network device or the point on a device where network traffic enters the device.

I-SID (Instance Service Identifier)

IVL (Independent VLAN Learning)

M

MA (Maintenance Association)

MAID (Maintenance Association Identifier)

MD (Maintenance Domain)

MD Level (Maintenance Domain)

ME (Maintenance Entity)

MEP (Maintenance End Point)

MIP (Maintenance Association Intermediate Point)

MP (Maintenance Point)

MPLS (Multiprotocol Label Switching) is an IETF initiative that sets up a specific path for a given sequence of packets, identified by a label given to

each packet. MPLS allows most packets to be forwarded at layer 2 rather than at layer 3.

MSTP (Multiple Spanning Tree Protocol) is defined by IEEE 802.1Q-2005 where each VLAN has its own Multiple Spanning Tree Instance (MSTI). Each instance has an independent spanning tree topology. MSTP was developed to replace Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) to provide a loop-free topology in bridged networks and achieve fast convergence times.

MTU (Multi-Tenant Unit)

P

PBBN (Provider Backbone Bridge Network)

PBT (Provider Backbone Transport)

PCP (Priority Code Point)

P2P (Point to Point)

PHB (Per-Hop Behavior) is a description of the externally observable forwarding treatment applied at a differentiated services-compliant node to a behavior aggregate.

PHBG (Per-Hop Behavior Group) is a set of one or more PHBs that can only be meaningfully specified and implemented simultaneously, due to a common constraint applying to all PHBs in the set such as a queue servicing or queue management policy.

Primary is a redundancy state mode indicating that the Active Control Module is managing the system.

Provider (or Service Provider) refers to an entity who owns or administrates the network over which services are offered. The provider may or may not offer the services themselves.

Q

QoS (Quality of Service) guarantees minimum and maximum bandwidths for a service as well as its priority relative to other services.

R

RSTP (Rapid Spanning Tree Protocol) is a Layer 2 link management protocol defined in IEEE 802.1W that provides network path redundancy while preventing topology loops. RSTP improves on STP (IEEE 802.1D) by achieving much faster convergence times.

S

SAC (Service Access Control) allows a provider to control packet forwarding based on MAC addresses, either by defining static MAC addresses or by limiting the number of dynamic MAC addresses that are allowed to access the port.

Severity the degree of urgency to which an event is generally classified. Severity typically lists three degrees of urgency; Critical, Major, or Minor.

SFP (Small Form-factor Pluggable)

SI (Service Interface)

is enabled.

SMAC (Source MAC Address)

Spanning Tree Domains is used in a network that employs RSTP, a Spanning Tree Domain limits the reach of RSTP to certain areas of the network.

Standby refers to the secondary Control Module that will assume the role as the Active Control Module in the event of failover.

Sub-port Layer 2 logical interface that subdivides a logical port.

Subscriber VLAN is a VLAN ID that exists in a subscriber's private network that needs to be preserved when traveling in the provider's network.

S-VID (Service VLAN ID) 802.1AD Service VLAN tag.

S-VLAN (Service VLAN)

T

TLS (Transparent LAN Services) allows two or more LANs that are separated geographically to be made to appear as one single LAN.

Tunnel A logical connection that carries virtual circuits.

U

UMF (Unknown Multicast Filtering) filters all multicast streams that are not controlled by IGMP snooping in order to prevent these streams from being flooded to all ports on the device.

V

Virtual Circuit is a logical connection used to carry a service.

Virtual Interface provides the binding between a logical interface and a virtual switch.

Virtual Switch A logical forwarding or flood domain.

VLAN (Virtual Local Area Network) is a logical element used to group resources that have a common set of requirements together, regardless of where they are located physically.

VPLS (Virtual Private LAN Service) is a class of VPN that allows the connection of multiple sites in a single bridged domain over a provider managed MPLS network.

VoIP (Voice over Internet Protocol)

VPN (Virtual Private Network) allows a subscriber to seamlessly connect networks at various locations and make them appear and behave as if they were on the same physical network.

W

WMF (Well-known Multicast Filtering) allows configured router protocols or other special addresses in the multicast range (referred to as well-known multicast groups) to be forwarded when UMF

